

# UTILITY COUNTER- TERRORISM COURSE

CONTINUING EDUCATION  
PROFESSIONAL DEVELOPMENT COURSE





## Printing and Saving Instructions

TLC recommends that you download and save this pdf document and assignment to your computer desktop and open it with Adobe Acrobat DC reader.

Adobe Acrobat DC reader is a free computer software program and you can find it at Adobe Acrobat's website.

You can complete the course by viewing the course on your computer or you can print it out. This course booklet does not have the assignment (the test). Please visit our website and download the assignment (the test).

**Printing Instructions:** Once you have purchased the program, we will give you permission to print this document. If you are going to print this document, it was designed to be printed double-sided or duplexed but can be printed single-sided.

### Internet Link to Assignment...

[http://www.abctlc.com/downloads/PDF/Terrorism ASSIGNMENT.pdf](http://www.abctlc.com/downloads/PDF/Terrorism%20ASSIGNMENT.pdf)

**State Approval Listing Link,** check to see if your State accepts or has pre-approved this course. Not all States are listed. Not all courses are listed. Do not solely trust our list for it may be outdated. It is your sole responsibility to ensure this course is accepted for credit. No refunds.

**Professional Engineers;** Most states will accept our courses for credit but we do not officially list the States or Agencies.

### State Approval Listing URL...

<http://www.abctlc.com/PDF/CEU%20State%20Approvals.pdf>

*You can obtain a printed version from TLC for an additional \$149.95 plus shipping charges.*

All downloads are electronically tracked and monitored for security purposes.



**Some States and many employers require the final exam to be proctored.**

**Do not solely depend on TLC's Approval list for it may be outdated.**

**MOST OF OUR STUDENTS PREFER TO DO THE ASSIGNMENT IN WORD AND E-MAIL OR FAX THE ASSIGNMENT BACK TO US. WE ALSO TEACH THIS COURSE IN A CONVENTIONAL HANDS-ON CLASS. CALL US AND SCHEDULE A CLASS TODAY.**

---

***Responsibility***

*This course contains EPA's federal rule requirements. Please be aware that each state implements drinking water, wastewater, safety and security regulations may be more stringent than EPA's or OSHA's regulations. Check with your state environmental agency for more information. You are solely responsible in ensuring that you abide with your jurisdiction or agency's rules and regulations.*

## Keep this Document

This is a working document. Its purpose is to start the process of security vulnerability assessment and security enhancement.

Security is not an end point, but a goal that can be achieved only through continued efforts to assess and upgrade your system. This is a sensitive document. It should be stored separately in a secure place at your water system.

A duplicate copy should also be retained at a secure off-site location. Access to this document should be limited to key water system personnel and local officials as well as the state drinking water primacy agency and others on a need-to-know basis.

### **SEC. 1433.: 42 USC 300i-2 TERRORIST AND OTHER INTENTIONAL ACTS.**

(a) Vulnerability Assessments. --(1) Each community water system serving a population of greater than 3,300 persons shall conduct an assessment of the vulnerability of its system to a terrorist attack or other intentional acts intended to substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water. The vulnerability assessment shall include, but not be limited to, a review of pipes and constructed conveyances; physical barriers; water collection, pretreatment, treatment, storage and distribution facilities; electronic, computer or other automated systems which are utilized by the public water system; the use, storage, or handling of various chemicals; and the operation and maintenance of such systems. The Administrator, not later than August 1, 2002, after consultation with appropriate departments and agencies of the Federal Government and with State and local governments, shall provide baseline information to community water systems required to conduct vulnerability assessments regarding which kinds of terrorist attacks or other intentional acts are the probable threats to-- `` (A) substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water; or `` (B) otherwise present significant public health concerns.

### **Freedom of Information Act Exception**

Exemption 2's "**circumvention**" protection also should be readily applicable to vulnerability assessments, which are perhaps the quintessential type of record warranting protection on that basis; such records generally assess an agency's vulnerability (or that of another institution) to some form of outside interference or harm by identifying those programs or systems deemed the most sensitive and describing specific security measures that can be used to counteract such vulnerabilities. A prime example of vulnerability assessments warranting protection under "**high 2**" are the computer security plans that all federal agencies are required by law to prepare.

In a decision involving such a document, *Schreibman v. United States Department of Commerce*,<sup>(93)</sup> Exemption 2 coverage was invoked to prevent unauthorized access to information which could result in "alternation [sic], loss, damage or destruction of data contained in the computer system."<sup>(94)</sup> It should be remembered, however, that even such a sensitive document must be reviewed to determine whether any "**reasonably segregable**" portion can be disclosed without harm.





**Various sneaky weapons that a terrorist may use.** Top, is a pen-gun, middle a small 5 shot revolver that can be concealed in a cigarette pack, and a compact .45 semi-automatic that can be carried inside a pocket. The most popular weapon or tool is the cellular telephone and computer. The cell phone is the primary bomb detonation device and the computer is a technological weapon. A thirteen-year-old can hack in to most databases with simple instructions from YouTube. Be ready because trouble is coming. The FBI says, there is a 100 % chance of a large weapon of mass destruction happening in American very soon.

### **Copyright Notice**

1999-2018 Technical Learning College (TLC) No part of this work may be reproduced or distributed in any form or by any means without TLC's prior written approval. Permission has been sought for all images and text where we believe copyright exists and where the copyright holder is traceable and contactable. Other materials including text and artwork are in the public domain or fair use (the state of belonging or being available to the public as a whole, and therefore not subject to copyright.) All material that is not credited or acknowledged or referenced in the rear of this course is the copyright of Technical Learning College. All other unacknowledged references are in the Water/ Wastewater Sampling and Water Chemistry Courses. Most unaccredited photographs have been taken by TLC instructors or TLC students. All written, graphic, photographic or other material is provided for educational information only. We will be pleased to hear from any copyright holder and will make good on your work if any unintentional copyright infringements were made as soon as these issues are brought to the editor's attention. This educational training course and assignment is intended for educational purposes only. Every possible effort was made to ensure that all information provided in this course is accurate. Therefore, Technical Learning College accepts no responsibility or liability whatsoever for the application or misuse of any information included herein.

Requests for acknowledgements or permission to make copies shall be made to the following address: TLC, P.O. Box 3060, Chino Valley, AZ 86323

Information in this document is subject to change without notice. TLC is not liable for errors or omissions appearing in this document.

## **Contributing Editors**

**James L. Six** Received a Bachelor of Science Degree in Civil Engineering from the University of Akron in June of 1976, Registered Professional Engineer in the State of Ohio, Number 45031 (Retired), Class IV Water Supply Operator issued by Ohio EPA, Number WS4-1012914-08, Class II Wastewater Collection System Operator issued by Ohio EPA, Number WC2-1012914-94

**Joseph Camerata** has a BS in Management with honors (magna cum laude). He retired as a Chemist in 2006 having worked in the field of chemical, environmental, and industrial hygiene sampling and analysis for 40 years.

**James Bevan**, Water Quality Inspector S.M.E. Twenty years of experience in the environmental field dealing with all aspects of water regulations on the federal, state, and local levels. Teacher and Proctor in Charge for Backflow Certification Testing at the ASETT Center in Tucson for the past 15 years and possess an Arizona Community College, Special Teaching Certificate in Environmental Studies.

**Dr. Pete Greer** S.M.E., Retired biology instructor, chemistry and biological review.

**Jack White**, Environmental, Health, Safety expert, City of Phoenix. Art Credits.



## Homeland Security Presidential Directive

**Purpose** *This information is subject to change*

The Nation requires a Homeland Security Advisory System to provide a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to Federal, State, and local authorities and to the American people.

Such a system would provide warnings in the form of a set of graduated "Threat Conditions" that would increase as the risk of the threat increases. At each Threat Condition, Federal departments and agencies would implement a corresponding set of "Protective Measures" to further reduce vulnerability or increase response capability during a period of heightened alert.

This system is intended to create a common vocabulary, context, and structure for an ongoing national discussion about the nature of the threats that confront the homeland and the appropriate measures that should be taken in response. It seeks to inform and facilitate decisions appropriate to different levels of government and to private citizens at home and at work.

**Homeland Security Advisory System** has been changed 4/20/2011

### **The National Terrorism Advisory System**

The National Terrorism Advisory System, or NTAS, replaces the color-coded Homeland Security Advisory System (HSAS). This new system will more effectively communicate information about terrorist threats by providing timely, detailed information to the public, government agencies, first responders, airports and other transportation hubs, and the private sector.

It recognizes that Americans all share responsibility for the nation's security, and should always be aware of the heightened risk of terrorist attack in the United States and what they should do.

"The terrorist threat facing our country has evolved significantly over the past ten years, and in today's environment – more than ever – we know that the best security strategy is one that counts on the American public as a key partner in securing our country," said Secretary Napolitano. "The National Terrorism Advisory System, which was developed in close collaboration with our federal, state, local, tribal and private sector partners, will provide the American public with information about credible threats so that they can better protect themselves, their families, and their communities."

Under NTAS, DHS will coordinate with other federal entities to issue detailed alerts to the public when the federal government receives information about a credible terrorist threat.



Every utility should have a security system in place, even a wastewater treatment plant.

Two “Keys” for your security and safety are *hardening* and *surveillance* of your facility. Document everything--times, names, and license plates.

Video and sound surveillance is only as good as your equipment and the operator.

If you use video security, use a digital format which leaves a “watermark” to insure authentication. Digital cameras can see up to 100 miles away and record only when there is “activity”. This type of recording can be placed on a DVD.

Install infrared cameras for areas with no – or low lighting.

Big Brother...



Did you know that video cameras that were easily seen are being replaced by high tech electronic cameras that cannot be seen by the naked eye.

Soon, you will not see video cameras for they will be smaller and easily hidden and most people will assume that they are not being watched. There is also an electronic device similar to a video camera that can see through your clothes to detect weapons.

These devices have been installed at most high security check point and installations.

"Veni, Vidi, Vici" ("I came, I saw, I conquered").  
-- William Shakespeare - **Julius Caesar**

"For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill."  
-- **Sun Tzu**

"Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat."  
-- **Sun Tzu**

"Winning is not everything. It's the only thing."  
-- **Vince Lombardi**



**Terrorist Brief Case:** Bolt-cutters, Pry bar to obtain access to your facility, possibly to obtain other tools to damage your facility. Disposable Cellular telephone communication, possible concealed weapon inside the telephone, defense weapons that can be hidden in a hollowed out felt marker, or even in a disposable coffee cup. Simple prescription pill bottles can be used as several different weapons including an explosive device or a simple "*sound suppressor/ silencer*" on a firearm. *Just* one liter of a biotoxin can contaminate an entire water system of 50,000 people or your entire utilities' domestic water supply.

Some security experts believe that normal Chlorinated water will destroy most bacteria and biotoxins. This is incorrect; because of genetics there are "*Superbugs*" and "*encapsulated bugs*" like coated Aspirin; and de-chlorinating agents, like Sodium Thiosulfate.



# Technical Learning College's Scope and Function

Welcome to the Program,

Technical Learning College (TLC) offers affordable continuing education for today's working professionals who need to maintain licenses or certifications. TLC holds several different governmental agency approvals for granting of continuing education credit.

TLC's delivery method of continuing education can include traditional types of classroom lectures and distance-based courses or independent study. TLC's distance based or independent study courses are offered in a print - based distance educational format. We will beat any other training competitor's price for the same CEU material or classroom training.

Our courses are designed to be flexible and for you do finish the material on your leisure. Students can also receive course materials through the mail. The CEU course or e-manual will contain all your lessons, activities and instruction to obtain the assignments. All of TLC's CEU courses allow students to submit assignments using e-mail or fax, or by postal mail. (See the course description for more information.)

Students have direct contact with their instructor—primarily by e-mail or telephone. TLC's CEU courses may use such technologies as the World Wide Web, e-mail, CD-ROMs, videotapes and hard copies. (See the course description.) Make sure you have access to the necessary equipment before enrolling, i.e., printer, Microsoft Word and/or Adobe Acrobat Reader. Some courses may require proctored closed-book exams depending upon your state or employer requirements.

## **Flexible Learning**

At TLC, there are no scheduled online sessions or passwords you need contend with, nor are you required to participate in learning teams or groups designed for the "typical" younger campus based student. You can work at your own pace, completing assignments in time-frames that work best for you. TLC's method of flexible individualized instruction is designed to provide each student the guidance and support needed for successful course completion.

## **Course Structure**

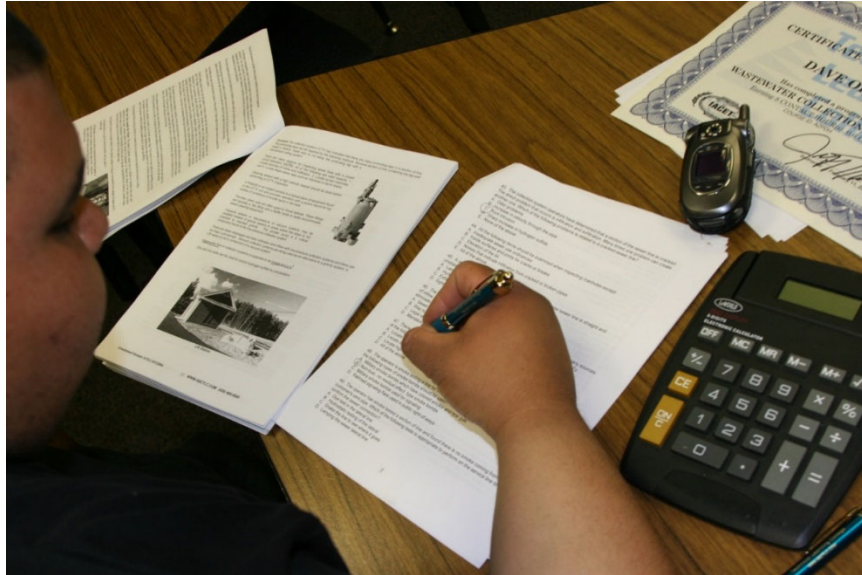
TLC's online courses combine the best of online delivery and traditional university textbooks. You can easily find the course syllabus, course content, assignments, and the post-exam (Assignment). This student friendly course design allows you the most flexibility in choosing when and where you will study.

## **Classroom of One**

TLC offers you the best of both worlds. You learn on your own terms, on your own time, but you are never on your own. Once enrolled, you will be assigned a personal Student Service Representative who works with you on an individualized basis throughout your program of study. Course specific faculty members (S.M.E.) are assigned at the beginning of each course providing the academic support you need to successfully complete each course. Please call or email us for assistance.

### **Satisfaction Guaranteed**

We have many years of experience, dealing with thousands of students. We assure you, our customer satisfaction is second to none. This is one reason we have taught more than 20,000 students.



We welcome you to do the electronic version of the assignment and submit the answer key and registration to us either by fax or e-mail. If you need this assignment graded and a certificate of completion within a 48-hour turn around, prepare to pay an additional rush charge of \$50.

**Contact Numbers**  
**Fax (928) 468-0675**  
**Email [Info@tlch2o.com](mailto:Info@tlch2o.com)**  
**Telephone (866) 557-1746**

# CEU Training Course Description

## Utility Counter-Terrorism CEU Training Course

**Defending against and responding to Catastrophic Threats.** The expertise, technology, and material needed to build the deadliest weapons known to mankind—including chemical, biological, radiological, and nuclear weapons—are spreading inexorably. If our enemies acquire these weapons, they are likely to try to use them.

The consequences of such an attack could be far more devastating than those we suffered on September 11—a chemical, biological, radiological, or nuclear terrorist attack in the United States could cause large numbers of casualties, mass psychological disruption, contamination, significant economic damage, and could overwhelm local medical capabilities.

**Protecting Critical Infrastructure and Key Assets.** Our society and modern way of life are dependent on networks of infrastructure—both physical networks such as our utility and transportation systems and virtual networks such as the Internet. If terrorists attack one or more pieces of our critical infrastructure, they may disrupt entire systems and cause significant damage to the Nation.

We must therefore improve protection of the individual pieces and interconnecting systems that make up our critical infrastructure. Protecting America's critical infrastructure and key assets will not only make us more secure from terrorist attack, but will also reduce our vulnerability to natural disasters, organized crime, and computer hackers.

The basic goal of the **Utility Counter-Terrorism course** is to make sure utility employers and employees know about potential terrorist hazards, how to recognize them and, most importantly, how to protect themselves and correct the hazards.

**Reduce America's vulnerability.** Homeland security involves a systematic, comprehensive, and strategic effort to reduce America's vulnerability to terrorist attack. We must recognize that as a vibrant and prosperous free society, we present an ever-evolving, ever-changing target.

**Homeland security.** This is a concerted national effort to prevent terrorist attacks within the United States; reduce America's vulnerability to terrorism; minimize the damage and have the ability to recover from attacks that do occur.



**Minimize the damage.** The United States will prepare to manage the consequences of any future terrorist attacks that may occur despite our best efforts at prevention.

This course is designed to help minimize the possible incidence or damage from terrorism.

## Where are the Regulations?

Terrorism, Utility Security and Emergency Plans are found in the **Federal Response Plan, Presidential Decision Directive 39, Patriot Act, Homeland Security Presidential Directive** and amendments to the **Safe Drinking Water Act**.

These Acts and Directives require that our utilities and workplaces are prepared for acts of terrorism. It's important that you have some basic understanding of the Act and the benefits and requirements necessary for a safer America.

The federal law or **Patriot Act** requires that all dangers and escapes in your workplace be fully evaluated for possible physical or health hazards. And, it mandates that all information relating to these hazards be available to other agencies in case of a disaster.

### **SEC. 1433.: 42 USC 300i-2**

#### **TERRORIST AND OTHER INTENTIONAL ACTS.**

(a) Vulnerability Assessments. --(1) Each community water system serving a population of greater than 3,300 persons shall conduct an assessment of the vulnerability of its system to a terrorist attack or other intentional acts intended to substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water. The vulnerability assessment shall include, but not be limited to, a review of pipes and constructed conveyances, physical barriers, water collection, pretreatment, treatment, storage and distribution facilities, electronic, computer or other automated systems which are utilized by the public water system, the use, storage, or handling of various chemicals, and the operation and maintenance of such system. The Administrator, not later than August 1, 2002, after consultation with appropriate departments and agencies of the Federal Government and with State and local governments, shall provide baseline information to community water systems required to conduct vulnerability assessments regarding which kinds of terrorist attacks or other intentional acts are the probable threats to--

``(A) substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water; or

``(B) otherwise present significant public health concerns.

This course prepares first responders to take appropriate actions, such as secure the scene, initiate self-protective measures, and notify appropriate agencies of a potential terrorist incident. It gives learners a general understanding and ability to recognize terrorist weapons that are biological, nuclear, incendiary, chemical, or explosive.



### **Goals**

You are one of the first to arrive on the scene of a suspected terrorist incident. As a first responder trained at the awareness level, you are among the first to witness or discover an incident involving criminal activity or terrorism and to initiate an emergency response sequence by notifying the proper authorities. In this role you need the following competencies which you can acquire through training and professional experience:

- An understanding of what terrorism is and the risks associated with such an incident;
- An understanding of the potential outcomes associated with a terrorist incident;
- The ability to recognize the presence of, and identify, criminal activity or terrorism in an emergency;



- An understanding of the role of the first responder as it relates to components of an emergency response plan, including site security and the U.S. Department of Transportation's (DOT) North American Emergency Response Guidebook;
- The ability to realize the need for additional resources, and to make appropriate notifications to an emergency communication center; and
- The ability to self-protect, keeping responder safety as a priority.
- Understand Homeland advisory system and security methods.

## **CURRICULUM OVERVIEW**

This self-study course is designed to provide you with a general introduction to the basic concepts for first-responder awareness at the scene of a potential terrorist incident. To master the basics more thoroughly, it is recommended that you complete this course as well as the TLC's corresponding safety courses, Fire Prevention, Asbestos Awareness, and Hazard Communication

This course includes nine Chapters, a Glossary, a Curriculum Guide, Appendix A: Terrorism Annex to the Federal Response Plan, Appendix B: Presidential Decision Directive 39 (Unclassified), and Appendix C: Related Course List.

**Chapter 1: *Reduce America's vulnerability.*** Homeland security involves a systematic, comprehensive, and strategic effort to reduce America's vulnerability to terrorist attack. We must recognize that as a vibrant and prosperous free society, we present an ever-evolving, ever-changing target.

***Homeland security.*** This is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur.

***Minimize the damage.*** The United States will prepare to manage the consequences of any future terrorist attacks that may occur despite our best efforts at prevention.

### **Chapter 2 *Safety***

- Be familiar with the company's written procedures for respirator use in normal and emergency situations and understand why a respirator is necessary
- Understand the different types of respirators and their purposes
- Know how to make respirators fit correctly and how to use the respirator effectively in emergency situations
- Know the importance of and how to conduct regular inspections, cleaning, and maintenance of respirators
- Understand the limitations and capabilities of respirators
- Know how to recognize medical signs and symptoms that may limit or prevent the effective use of respirators

**Chapter 3: *Terrorism In Perspective defines terrorism,*** presents a historical perspective, and provides an overview of potential threats (biological, nuclear, incendiary, chemical, and explosive).

**Chapter 4: *Incidents and Indicators*** identifies criteria for recognizing suspicious incidents; presents on-scene key indicators, including those for locating terrorist incidents; and lists outward warning signs and detection clues.

**Chapter 5: *Self-Protection*** includes the types of potential harm encountered at the scene of an incident, and means of protection.

**Chapter 6: *Scene Control*** describes initial response and arrival considerations and the appropriate course of action for scene isolation and evacuation.

**Chapter 7: *Notification and Coordination*** provides procedures for activating response resources.

**Chapter 8: *Backflow Awareness*** Review of water distribution related fundamentals. This course will cover the basics of backflow prevention, water quality and hydraulic fundamentals. Backflow Familiarization, Definitions, and Terms.

**Chapter 9: *Cyberterrorism*** Review of the different methods of destroying and protection of your computer files including SCADA and Internet systems.

The Glossary, located at the end of the final Chapter, contains definitions of terms related to first-responder awareness responsibilities and operations.

A Related Course List and a Bibliography are included to help you continue learning after you have completed the course. They consist of a list of references and other recommended courses that may be helpful in learning about emergency response to terrorism.

### **Target Audience**

The primary target audience for this course includes four groups of people, ideally trained to the awareness level in hazardous materials response:

- utility personnel, water, wastewater, gas, electric
- fire personnel;
- emergency medical service responders; and
- hazardous materials responders, first responders.

### **In addition, this course also is designed to benefit**

- law-enforcement personnel;
- emergency communications personnel;
- jurisdictional emergency coordinators;
- emergency management personnel;
- public works management;
- public health workers;
- Armed Forces, Reserves, National Guard; and
- disaster response agencies.



## **How to Complete this CEU Course**

Just a few suggestions to help you gain more from your self-study learning experience. You will benefit most if you do not rush through this course. Do not try to read it cover-to-cover in one sitting.

Throughout the text the authors have inserted questions that encourage you to stop reading, reflect a bit on what you have read, and apply it to your local situation. These questions are called, "**Thinking About My Situation...**" You may not be able to answer all of the questions completely, but the more you reflect on them and try to find answers, the more valuable the learning experience will be. Some of the questions encourage you to go beyond the text and find information in other sources. The questions are designed to apply the Chapter objectives to your local situation.

## **Final Examination for Credit**

Opportunity to pass the final comprehensive examination is limited to three attempts per course enrollment.

**Prerequisites:** None

## **Course Procedures for Registration and Support**

All of Technical Learning College's correspondence courses have complete registration and support services offered. Delivery of services will include, e-mail, web site, telephone, fax and mail support. TLC will attempt immediate and prompt service.

When a student registers for a distance or correspondence course, he/she is assigned a start date and an end date. It is the student's responsibility to note dates for assignments and keep up with the course work.

If a student falls behind, he/she must contact TLC and request an end date extension in order to complete the course. It is the prerogative of TLC to decide whether to grant the request. You may be required to pay \$50.00. All students will be tracked by a unique number assigned to the student.

## **Instructions for Written Assignments**

Utility Counter-Terrorism CEU Training course will be a True/False/Multipliable choice and essay type of an exam. There will also be an exam at the end of each chapter, but these are not graded or need to be submitted. TLC will require that the final exam or assignment is typed and preferably e-mailed to TLC.

You will be tested on the knowledge you have gained from the course. To receive a Technical Learning College Certificate of Completion, you must score 70 percent or higher in order to receive the certificate. Upon successful completion, certificates will be mailed within two to three weeks.

Check with your State agencies to see if the course has been approved for CEU credit

At the end of each Chapter is a final learning activity: "**What I Will Do As Follow-up To This Chapter...**" asking you to apply what you have just learned to your local situation. If used correctly, these final questions could be the springboard to some very worthwhile post-course action steps for you and your department.

After you finish reading the Chapter and answer as many of the reflection questions as possible, you can complete the corresponding learning checks. If you are unable to answer all of the questions, you may want to read the corresponding materials again.

Both training and written materials will inform you about Fire, Utility Counter-Terrorism, First Responder and Evacuation work. In the training session, feel free to ask questions about any information you did not understand. When looking at the written program/exit plan a supervisor should be able to help you with any questions you might have.

### **Feedback Mechanism (examination procedures)**

Each student will receive a feedback form as part of their study packet. You will find this form in the front of the course or lesson.

### **Grading Criteria**

In order to successfully pass this course, you will need to have 70% or better on the final exam.

### **Required Texts**

The Utility Counter-Terrorism CEU training course does not require any other course materials. This course is complete.

### **Recordkeeping and Reporting Practices**

TLC will keep all student records for a minimum of seven years. It is your responsibility to give the completion certificate to the appropriate agencies.

### **ADA Compliance**

TLC will make reasonable accommodations for persons with documented disabilities. Students should notify TLC and their instructors of any special needs.



Course content may vary from this outline to meet the needs of this particular group.

### **Educational Mission of TLC:**

*To provide TLC students with comprehensive and ongoing training in the theory and skills needed for the environmental education field,*

*To provide TLC students with opportunities to apply and understand the theory and skills needed for a successful career,*

*To provide opportunities for TLC students to learn and practice environmental educational skills with members of the community for the purpose of sharing diverse perspectives and experience,*

*To provide a forum in which students can exchange experiences and ideas related to environmental education,*

*To provide a forum for the collection and dissemination of current information related to environmental education, and to maintain an environment that nurtures academic and personal growth.*

# TABLE OF CONTENTS

<b>Chapter 1 Protect our Nation.....</b>	<b>25</b>
Patriot Act.....	33
World Trade Center.....	71
Homegrown Terrorists.....	81
Homeland Security.....	97
Presidential Directives.....	99
SDWA Amendments .....	121
Exercise.....	139
<b>Chapter 2 Safety.....</b>	<b>141</b>
Personal Protective Equipment.....	145
Protective Clothing Applications.....	153
Respiratory Protection.....	161
Respiratory Protection Glossary.....	169
Suspicious Letters Anthrax.....	173
Workplace Violence.....	183
Exercise.....	191
<b>Chapter 3 Terrorism in Perspective.....</b>	<b>193</b>
What is a Threat? .....	195
Biological Incidents.....	201
Terrorist History.....	205
Bio-Chemical .....	207
Bioterrorism.....	213
Nuclear Incidents.....	215
Alpha Particles.....	225
Gamma Rays.....	227
Dirty Bombs.....	229
Incendiary Incidents.....	235
Chlorine Section.....	241
Nerve Agents .....	267
Blood Agents.....	268
Irritating Agents.....	269
Explosive Agents.....	270
Summary.....	275
Glossary .....	277
Exercise.....	283
<b>Chapter 4 Incidents &amp; Indicators.....</b>	<b>287</b>
Crime Scene.....	289
Leave Things Alone.....	291
Outwards Signs.....	293
Bomb Threats.....	295
Suspicious Packages.....	309
Summary.....	313
Exercise.....	315

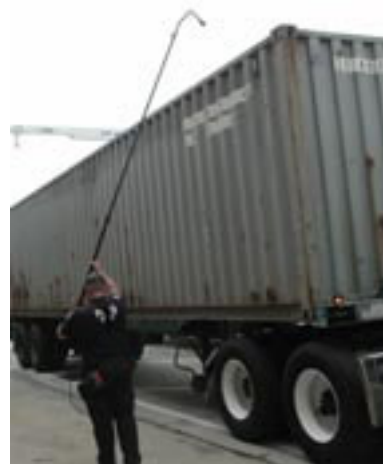
<b>Chapter 5 Self-Protection</b> .....	<b>319</b>
TRACEM.....	321
Chemical .....	323
Time, Distance & Shielding.....	325
Assignment .....	327
<b>Chapter 6 Emergency Planning</b> .....	<b>329</b>
Incident Command Section.....	337
Conducting Size Up.....	353
GEDAPER.....	355
Summary.....	360
Exercise.....	361
<b>Chapter 7 Notification and Coordination</b> .....	<b>363</b>
Federal and State Response.....	365
Presidential Decision.....	366
Exercise.....	361
<b>Chapter 8 Backflow Prevention</b> .....	<b>371</b>
Cross-Connection Terms.....	381
Types of Assemblies.....	389
Fireline.....	397
Exercise.....	403
<b>Chapter 9 Cyberterrorism</b> .....	<b>407</b>
Hackers.....	413
Virus Protection.....	419
SCADA.....	429
Summary.....	447
Exercise.....	450
<b>Bibliography</b> .....	<b>451</b>
<b>SELF-ASSESSMENT GUIDE</b>	
<b>SECURITY VULNERABILITY</b>	
<b>SELF-ASSESSMENT</b> .....	<b>453</b>
<b>ATTACHMENT 1.</b>	
<b>PRIORITIZATION NEEDED ACTIONS</b> .....	<b>471</b>
<b>ATTACHMENT 2.</b>	
<b>EMERGENCY CONTACT LIST</b> .....	<b>473</b>
<b>ATTACHMENT 3.</b>	
<b>THREAT IDENTIFICATION CHECKLIST</b> .....	<b>485</b>
<b>Freedom of Information Act Exemption</b> .....	<b>491</b>
<b>FBI Offices</b> .....	<b>497</b>
<b>Action Plans</b> .....	<b>507</b>

## Utility Counterterrorism Acronyms

**ATSA:** Aviation and Transportation Security Act  
**ATTF:** Anti-Terrorism Task Force  
**CBRN:** Chemical, Biological, Radiological and Nuclear  
**CDC:** Center for Disease Control  
**CIA:** Central Intelligence Agency  
**CIAO:** Critical Infrastructure Assurance Office  
**CTC:** Counter-Terrorism Center  
**DCI:** Director of Central Intelligence  
**DHS:** Department of Homeland Security  
**DoD:** Department of Defense  
**DoE:** Department of Energy  
**EIS:** Epidemic Intelligence Service  
**EPA:** Environmental Protection Agency  
**FAA:** Federal Aviation Administration  
**FBI:** Federal Bureau of Investigation  
**FDA:** Food and Drug Administration  
**FEMA:** Federal Emergency Management Agency  
**FTTTF:** Foreign Terrorist Tracking Task Force  
**HAN:** Health Alert Network  
**HHS:** Health and Human Services  
**HSTF:** Homeland Security Task Force  
**IIPO:** Information Integration Program Office  
**IMS:** Incident Management System  
**INS:** Immigration and Naturalization Service  
**ITDS:** International Trade Data System  
**JTTF:** Joint Terrorism Task Force  
**MRC:** Medical Reserve Corps  
**MLAT:** Mutual Legal Assistance Treaty  
**NCIC:** National Crime Information Center  
**NCS:** National Communication System  
**NDMS:** National Disaster Medical System  
**NEDSS:** National Electronic Disease Surveillance System  
**NIH:** National Institutes of Health  
**NLETS:** National Law Enforcement Telecommunications System  
**NRC:** Nuclear Regulatory Commission  
**NSA:** National Security Agency  
**NSC:** National Security Council  
**NSDI:** National Spatial Data Infrastructure  
**NWP:** Neighborhood Watch Program  
**OHS:** Office of Homeland Security  
**OMB:** Office of Management and Budget  
**TIPS:** Terrorism Information and Preventive Systems  
**TSA:** Transportation Security Administration  
**TSWG:** Technical Support Working Group  
**VIPS:** Volunteers in Police Service  
**WMD:** Weapons of Mass Destruction  
**WTC:** World Trade Center



**Wastewater Headworks  
In the top 10 Vulnerable  
Terrorist Targets, easy to  
destroy and able to cause  
mass disease.**



**Video Camera  
Inspection**



Ever thought about a Terrorist using a Fire Hydrant to distribute a contaminant? It is accidentally done every day by Contractors and easy to conceal as in this photo.



How about the information access a Terrorist can obtain? Drones, Satellite and detailed map information of your facility? They probably know more than you think.



# Chapter 1

## Reasons Why We Need To Protect Ourselves and Our Nation.

**Section Focus:** You will learn the basics of reducing America's vulnerability to terrorist attack. At the end of this section, you the student will be able to understand and describe specific utility security rules, measures and related processes. There is a post quiz at the end of this section to review your comprehension and a final examination in the Assignment for your contact hours.

**Scope/Background:** The United States will prepare to manage the consequences of any future terrorist attacks that may occur despite our best efforts at prevention. Homeland security involves a systematic, comprehensive, and strategic effort to reduce America's vulnerability to terrorist attack. We must recognize that as a vibrant and prosperous free society, we present an ever-evolving, ever-changing target.



**How to make the World's biggest pipe bomb:** Pump a flammable substance into the sewer system and add ignition or add a pesticide and stop the wastewater treatment system entirely.

How are you going to prepare, delay, observe, and prevent these happenings?

We can't stop these attacks. All we can do is minimize the damage and prepare for attacks.

**Terrorism: Terrorist attacks.** Homeland security is focused on terrorism in the United States. The *National Strategy for Homeland Security* characterizes terrorism as any premeditated, unlawful act dangerous to human life or public welfare that is intended to intimidate or coerce civilian populations or governments.

This description captures the core concepts shared by the various definitions of terrorism contained in the U.S. Code, each crafted to achieve a legal standard of specificity and clarity.

This description covers kidnappings; hijackings; shootings; conventional bombings; attacks involving chemical, biological, radiological, or nuclear weapons; cyber-attacks; and any number of other forms of malicious violence.

Terrorists can be U.S. citizens or foreigners, acting in concert with others, on their own, or on behalf of a hostile state.

## The Terrorists

Our enemies seek to remain invisible, lurking in the shadows. We are taking aggressive action to uncover individuals and groups engaged in terrorist activity, but often we will not know who our enemy is by name until after they have attempted to attack us.

Therefore, we must uncover more than just the identities of our enemy. We need to analyze the characteristics shared by terrorists to help us understand where our enemies are weak and where they are strong.

***Terrorists and their tactical advantages.*** Terrorists enjoy certain tactical advantages. They are able to choose the time, place, and method of their attacks. As we reduce our vulnerabilities in one area, they can alter their plans and pursue more exposed targets. They are able to patiently plan their attacks for months and years. Plans are undoubtedly underway today by terrorist cells that we have not yet eliminated.

Terrorists also exploit the advantage of relative anonymity. They hide throughout the world, using the cover of innocent civilians as a shield. Weak states will remain susceptible to terrorist groups seeking safe haven, and may even cooperate with or actively support terrorists.

### Known terrorist groups

Al-Qaeda remains America's most immediate and serious threat despite our success in disrupting its network in Afghanistan and elsewhere. While we have captured or killed hundreds of Al-Qaeda operatives, many remain at large, including leaders working to reconstitute the organization and resume its operations.

Al-Qaeda operatives and cells will continue to plan attacks against high-profile landmarks and critical infrastructure at home and against targets in Europe, the Middle East, Africa, and Southeast Asia. Those attacks may use both conventional and unconventional means in an effort to create as much destruction and kill as many people as possible.

Al-Qaeda is part of a dangerous trend toward sophisticated terrorist networks spread across many countries, linked together by information technology, enabled by far-flung networks of financial and ideological supporters, and operating in a highly decentralized manner. Unlike traditional adversaries, these terrorist networks have no single "**center of gravity**" whose destruction would entail the defeat of the entire organization.

While we have denied Afghanistan as a safe haven for Al-Qaeda, unrest in politically unstable regions will continue to create an environment conducive to terrorism and capable of providing sanctuary to terrorist groups.

### Hezbollah

Until September 11, Hezbollah was responsible for more American deaths than all other terrorist groups combined, including those killed in the 1983 bombing of the U.S. Marine Corps barracks in Lebanon. Hezbollah has never carried out an attack within the United States, but could do so if the situation in the Middle East worsens or the group feels threatened by U.S. actions.

### **Other Terrorist Groups**

Other terrorist groups, from Hamas to the Real Irish Republican Army, have supporters in the United States. To date, most of these groups have largely limited their activities in the United States to fundraising, recruiting, and low-level intelligence, but many are capable of carrying out terrorist acts within the United States. Today we have the Mexican drug cartels and we need to re-examine the terror effect they present to us. There are some that claim the drug cartels and other foreign terrorists groups are combining their efforts.

### **Domestic Organizations**

Terrorist groups also include domestic organizations. The 1995 bombing of the Murrah Federal Building in Oklahoma City highlights the threat of domestic terrorist acts designed to achieve mass casualties. The U.S. government averted seven planned terrorist acts in 1999—two were potentially large-scale, high-casualty attacks being organized by domestic extremist groups.

Both domestic terrorist groups (such as the National Alliance, the Aryan Nation, and the extremist Puerto Rican separatist group Los Macheteros) and special interest extremist groups continue to pose a threat to the peace and stability of our country. The tactics of modern terrorists are unbounded by the traditional rules of warfare.

Terrorists transform objects of daily life into weapons, visiting death and destruction on unsuspecting civilians. Defeating this enemy requires a focused and organized response.



Underneath a water treatment plant backwash filter.  
Rarely is there an Operator in this area.

Is this an area vulnerable to an attack or sabotage?

Could you monitor this area with video cameras?

## Notable Domestic Terrorist Attacks



### **Burning of Washington and the White House (1812)**

The Burning of Washington was a British invasion of Washington, D.C., the capital of the United States, during the War of 1812. On August 24, 1814, after defeating the Americans at the Battle of Bladensburg, a British force led by Major General Robert Ross burned down multiple buildings, including the White House (then called the Presidential Mansion), the Capitol building, as well as other facilities of the U.S. government. The attack was in part a retaliation for the recent American destruction of Port Dover in Upper Canada. The Burning of Washington marks the only time since the American Revolutionary War that a foreign power has captured and occupied the United States capital. It was the only significant foreign attack on Washington, D.C. until the September 11 attacks 187 years later, and remains the most devastating attack in the city's history.

### **The Mountain Meadows Massacre (1857)**

The Mountain Meadows massacre was a series of attacks on the Baker–Fancher emigrant wagon train, at Mountain Meadows in southern Utah. The attacks began on September 7 and culminated on September 11, 1857, resulting in the mass slaughter of the emigrant party by members of the Utah Territorial Militia from the Iron County district, a Mormon group, together with some Paiute Native Americans. Intending to leave no witnesses and thus prevent reprisals, the perpetrators killed all the adults and older children – about 120 men, women, and children in total. Seventeen children, all younger than seven, were spared.

### **Milwaukee Police Department Bombing (1917)**

The Milwaukee Police Department bombing was a November 24, 1917, bomb attack that killed ten people including nine members of local law enforcement. The perpetrators were never caught but are suspected to be an anarchist terrorist cell operating in the United States in the early 20th century. The target was initially an evangelical church in the Third Ward and only killed the police members when the bomb was brought to the police station by a concerned member of the public.

### **Wall Street bombing (1920)**

The Wall Street bombing was a terrorist incident on September 16, 1920, in the Financial District of New York City. A horse-drawn wagon filled with 100 pounds (45 kg) of dynamite was stationed across the street from the headquarters of the J.P. Morgan Inc. bank. The explosion killed 38 and injured 400. Even though no one was found guilty, it is believed that the act was carried out by followers of Luigi Galleani.

### **Burning of Black Wall Street (1921)**

On May 31 and June 1, 1921, a white mob started the Tulsa race riot, attacking residents and businesses of the African-American community of Greenwood in Tulsa, Oklahoma, in what is considered one of the worst incidents of racial violence in United States History. The attack, carried out on the ground and by air, destroyed more than 35 blocks of the district, did \$30 million (2017 dollars) in damages, left 10,000 people homeless and up to 300 dead in a town considered the wealthiest black community in the nation.

### **16th Street Baptist Church Bombing (1963)**

On Sunday, September 15, 1963, members of the United Klans of America set a bomb consisting of a timing device and fifteen sticks of dynamite to explode at a historically-black church in Birmingham, Alabama, that was a local focus of the Civil Rights struggle. The explosion killed four girls between the ages of 11 and 14 and did much other local damage. Three perpetrators were eventually caught years later and sentenced to life imprisonment for their roles. There had been other bombings in Birmingham, then grimly known as "Bombingham" for such attacks.

### **Unabomber Attacks (1978–1995)**

From 1978 to 1995, Harvard University graduate and former mathematics professor Theodore "Ted" Kaczynski – known by the codename "UNABOM" until his identification and arrest by the FBI – carried out a campaign of sending letterbombs to academics and various individuals particularly associated with modern technology. In 1996, his manifesto was published in The New York Times and The Washington Post, under the threat of more attacks. The bomb campaign ended with his capture.

### **Attacks by the Jewish Defense League (1980–1985)**

In a 2004 congressional testimony, John S. Pistole, Executive Assistant Director for Counterterrorism and Counterintelligence for the Federal Bureau of Investigation described the JDL as "a known violent extremist Jewish Organization." FBI statistics show that, from 1980 through 1985, there were 18 terrorist attacks in the U.S. committed by Jews; 15 of those by members of the JDL. Mary Doran, an FBI agent, described the JDL in a 2004 Congressional testimony as "a proscribed terrorist group". Most recently, then-JDL Chairman Irv Rubin was jailed while awaiting trial on charges of conspiracy in planning bomb attacks against the King Fahd Mosque in Culver City, California, and on the office of Arab-American Congressman Darrell Issa. In its report, Terrorism 2000/2001, the FBI referred to the JDL as a "violent extremist Jewish organization" and stated that the FBI was responsible for thwarting at least one of its terrorist acts.

### **Oklahoma City Bombing (1995)**

This truck bomb attack by Timothy McVeigh and Terry Nichols killed 168 people on April 19, 1995 – the deadliest domestic-based terrorist attack in the history of the United States since the era of mass lynchings and race riots. It inspired improvements to United States federal building security.

### **Centennial Olympic Park Bombing (1996)**

The Centennial Olympic Park bombing was a terrorist bombing on July 27, 1996, in Atlanta, Georgia, during the 1996 Summer Olympics, the first of four committed by Eric Robert Rudolph, former explosives expert for the United States Army. Two people died, and 111 were injured.

### **Wisconsin Sikh Temple Shooting (2012)**

On August 5, 2012, Wade Michael Page fatally shot six people (including himself) and wounded four others in a mass shooting at a Sikh temple in Oak Creek, Wisconsin. Page was an American white supremacist and a United States Army veteran from Cudahy, Wisconsin, who was a member of the neo-Nazi skinhead Hammerskin Nation. All of the dead were members of the Sikh faith.

### **Boston Marathon Bombing (2013)**

On April 15, 2013, two homemade bombs detonated 12 seconds and 210 yards apart at 2:49 p.m., near the finish line of the annual Boston Marathon, killing three people and injuring several hundred others, including 16 who lost limbs. Kyrgyz-American brothers Dzhokhar Tsarnaev and Tamerlan Tsarnaev were apprehended and claimed to have been motivated by radical Islamist beliefs.

### **Charleston Church Shooting (2015)**

On June 17, 2015, Dylann Roof, a 21-year-old white supremacist, went into the Emanuel African Methodist Episcopal Church in Charleston, South Carolina, and shot and killed nine people including South Carolina senator Clementa C. Pinckney. Roof was known to be a white supremacist who admired Apartheid South Africa and Rhodesia and owned a website with a manifesto both called The Last Rhodesian in which he outlined his views toward blacks, among other peoples.

### **San Bernardino Shooting (2015)**

On December 2, 2015, 14 people were killed and 24 injured in a mass shooting at the Inland Regional Center in San Bernardino, California, United States. Syed Rizwan Farook and Tashfeen Malik targeted a San Bernardino County Department of Public Health training event and holiday party of about 80 employees in a rented banquet room. Farook was an American-born citizen of Pakistani descent, while his wife was a Pakistani-born legal resident of the U.S. He had attended the event as an employee before the shooting. Both had become radicalized through jihadist material on the internet, and stockpiled supplies in their home.

### **Orlando Nightclub Shooting (2016)**

In the early hours of June 12, 2016, 49 people were killed and 53 were injured in a mass shooting at the Pulse nightclub in Orlando, Florida. The perpetrator, 29-year-old Omar Mateen, was a security guard and person of interest to the FBI in 2013 and 2014. At the time, this event was the deadliest mass shooting in United States history by a single gunman, later eclipsed by the 2017 Las Vegas shooting on October 1, 2017. Additionally, it was the deadliest confirmed terrorist attack on U.S. soil since the 9/11 attacks and the deadliest attack against LGBT people in U.S. history.

### **Congressional Baseball Shooting (2017)**

While the annual Congressional Baseball Game for Charity was going on, James Thomas Hodgkinson opened fire on Republican Congressmen and Congresswomen on the field such as U.S. House Majority Whip Steve Scalise, U.S. Capitol Police Officer Crystal Giner, congressional aide Zack Barth and lobbyist Matt Mika, resulting in 6 getting injured (4 critically) and the perpetrator getting killed. James Thomas Hodgkinson prior to the shooting was a supporter of Democratic presidential candidate Bernie Sanders and had liked various left-wing/liberal and anti-Donald Trump/anti-Republican Facebook pages.

### **Charlottesville Car Attack (2017)**

During the Charlottesville riots/Unite the Right rally on August 11-12, 2017 in Charlottesville, Virginia, by neo-Nazis, neo-fascists, white nationalists, alt-righters, Southern nationalists and Ku Klux Klansmen, Vanguard America (VA) member James Alex Fields drove his car into counter-protesters, killing 1 named Heather Heyer and injuring 28 others.

### **Pittsburgh Synagogue Shooting (2018)**

On October 27, 2018, 11 people died and 6 more were injured at the Tree of Life - Or L'Simcha Congregation in Pittsburgh, Pennsylvania by Robert Bowers a user of Gab. The attack was motivated by anti-Semitism and a belief in the white genocide conspiracy theory.

### **Escondido Mosque Fire and Poway Synagogue Shooting (2019)**

On March 24, 2019, a mosque in Escondido, California, was set on fire; no one was injured and the fire was contained without major damage. The following month, on April 27, 2019, an elderly Jewish woman named Lori Gilbert-Kaye was killed and three others (including Rabbi Yisroel Goldstein) were injured at the Chabad of Poway synagogue in Poway, California. The accused shooter, John T. Earnest, blamed Jews for "white genocide" and other ills in an anti-Semitic and racist open letter on 8chan confessing to the mosque arson and citing inspiration from the Christchurch mosque shooter Brenton Harrison Tarrant and Pittsburgh synagogue shooting perpetrator Robert Bowers.

### **El Paso Walmart Shooting (2019)**

On August 3, 2019, a domestic terrorist attack/mass shooting occurred at a Walmart store in El Paso, Texas, killing 22 people and injuring 24 others. The attack was carried out by Patrick Crusius, who wrote a manifesto titled The Inconvenient Truth and posted it on 8chan where he cited a supposed "Hispanic invasion of Texas" and "simply trying to defend my country from ethnic and cultural replacement brought on by an invasion" as motivations as well as praising the perpetrator of the Christchurch, New Zealand, mosque shootings and read his manifesto The Great Replacement.



## USA Patriot Act

***What must we protect?*** The USA Patriot Act defines critical infrastructure as those “**systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.**”

Our critical infrastructures are particularly important because of the functions or services they provide to our country. Our critical infrastructures are also particularly important because they are complex systems: the effects of a terrorist attack can spread far beyond the direct target, and reverberate long after the immediate damage.

America’s critical infrastructure encompasses a large number of sectors. Our agriculture, food, and water sectors, along with the public health and emergency services sectors, provide the essential goods and services Americans need to survive. Our institutions of government guarantee our national security and freedom, and administer key public functions.

Our defense industrial base provides essential capabilities to help safeguard our population from external threats. Our information and telecommunications sector enables economic productivity and growth, and is particularly important because it connects and helps control many other infrastructure sectors. Our utilities, transportation, banking and finance, chemical industry, and postal and shipping sectors help sustain our economy and touch the lives of Americans every day.

The assets, functions, and systems within each critical infrastructure sector are not equally important. The transportation sector is vital, but not every bridge is critical to the Nation as a whole. Accordingly, the federal government will apply a consistent methodology to focus its effort on the highest priorities, and the federal budget will differentiate resources required for critical infrastructure protection from resources required for other important protection activities.

The federal government will work closely with state and local governments to develop and apply compatible approaches to ensure protection for critical assets, systems, and functions at all levels of society. For example, utilities, local schools, courthouses, and bridges are critical to the communities they serve.

Protecting America’s critical infrastructure and key assets requires more than just resources. The federal government can use a broad range of measures to help enable state, local, and private sector entities to better protect the assets and infrastructures they control.

For example, the government can create venues to share information on infrastructure vulnerabilities and best-practice solutions, or create a more effective means of providing specific and useful threat information to non-federal entities in a timely fashion.





A ticking time bomb, all it needs is a Terrorist to set the fuse. A possible diversion? A possible **“Sucker Punch”**?

Ever thought about the access Trash Collection or Delivery Vehicles have and the potential for Terrorist to use these trucks for a bomb or to sneak into your facility?

The Secret Service will shut down and search Routine Delivery and Sanitation Trucks within a 5 mile area when the President is in the area. They create a wall of steel to protect the President.

How about the security at your facility? Is it an elderly or unskilled person? Is there a real live person? In most cases, it is an unskilled or uneducated person who may have a criminal background. Think about the importance of a background check and reference checks.

What about the access to your facility that a Landscaper has?



## Critical Infrastructure Sectors

- ✓ Agriculture
- ✓ Food
- ✓ Water
- ✓ Public Health
- ✓ Emergency Services
- ✓ Government
- ✓ Defense Industrial Base
- ✓ Information and Telecommunications
- ✓ Energy
- ✓ Transportation
- ✓ Banking and Finance
- ✓ Chemical Industry
- ✓ Postal and Shipping



Nuclear Plant

### Major Initiatives

#### ***Unify America's infrastructure protection effort in the Department of Homeland Security.***

Our country requires a single accountable official to ensure we address vulnerabilities that involve more than one infrastructure sector or require action by more than one agency.

Our country also requires a single accountable official to assess threats and vulnerabilities comprehensively across all infrastructure sectors to ensure we reduce the overall risk to our country, instead of inadvertently shifting risk from one potential set of targets to another.

The Department of Homeland Security will assume responsibility for integrating and coordinating federal infra-structure protection responsibilities.

The Department of Homeland Security would consolidate and focus the activities performed by the Critical Infrastructure Assurance Office (currently part of the Department of Commerce) and the National Infrastructure Protection Center (**FBI**), less those portions that investigate computer crime.

The Department would augment those capabilities with the Federal Computer Incident Response Center (**General Services Administration**), the Computer Security Division of the National Institute of Standards and Technology (**Commerce**), and the National Communications System (**Defense**).

The Department of Homeland Security would also unify the responsibility for coordinating cyber and physical infrastructure protection efforts.

Currently, the federal government divides responsibility for cyber and physical infrastructure, and key cyber security activities are scattered in multiple departments.

While securing cyberspace poses unique challenges and issues, requiring unique tools and solutions, our physical and cyber infrastructures are interconnected.

The devices that control our physical systems, including our electrical distribution system, transportation systems, dams, and other important infrastructure, are increasingly connected to the Internet.

Thus, the consequences of an attack on our cyber infrastructure can cascade across many sectors. Moreover, the number, virulence, and maliciousness of cyber-attacks have increased dramatically in recent years.



### **Hoover Dam**

If your water comes from surface water or impounded water, are you prepared for a water shortage or catastrophic flood from a levee or dam break?

Have you wondered why they built an expensive bridge over the dam?

## Intelligence Report and What to Expect

Juval Aviv was the Israeli Agent upon whom the movie "Munich" was based. He was Golda Meir's bodyguard -- she appointed him to track down and bring to justice the Palestinian terrorists who took the Israeli athletes hostage and killed them during the Munich Olympic Games.

In a lecture in New York City a few weeks ago, he shared information that EVERY American needs to know -- but that our government has not yet shared with us.

He predicted the London subway bombing on the Bill O'Reilly show on Fox News, stating publicly that it would happen within a week. At the time, O'Reilly laughed and mocked him saying that in a week he wanted him back on the show. But, unfortunately, within a week the terrorist attack had occurred.

Juval Aviv gave intelligence (via what he had gathered in Israel and the Middle East) to the Bush Administration about 9/11, a month before it occurred. His report specifically said they would use planes as bombs and target high profile buildings and monuments. Congress has since hired him as a security consultant. Now for his future predictions. He predicts the next terrorist attack on the U.S. will occur very soon.

Forget hijacking airplanes, because he says terrorists will NEVER try and hijack a plane again, as they know the people onboard will never go down quietly again. Aviv believes our airport security is a joke -- that we have been reactionary, rather than proactive, in developing strategies that are truly effective.

### For example:

1) Our airport technology is outdated. We look for metal, and the new explosives are made of plastic.

2) He talked about how some idiot tried to light his shoe on fire. Because of that, now everyone has to take off their shoes. A group of idiots tried to bring aboard liquid explosives. Now we can't bring liquids on board. He says he's waiting for some suicidal maniac to pour liquid explosive on his underwear, at which point, security will have us all traveling naked! Every strategy we have is reactionary.

3) We only focus on security when people are heading to the gates. Aviv says that if a terrorist attack targets airports in the future, they will target busy times on the front end of the airport when/where people are checking in. It would be easy for someone to take two suitcases of explosives, walk up to a busy check-in line, ask a person next to them to watch their bags for a minute while they run to the restroom or get a drink, and then detonate the bags BEFORE security even gets involved. In Israel, security checks bags BEFORE people can even ENTER the airport.

Aviv says the next terrorist attack here in America is imminent and will involve suicide bombers and non-suicide bombers in places where large groups of people congregate. (I. E., Disneyland, Las Vegas casinos, big cities (New York, San Francisco, Chicago, etc.) and that it will also include shopping malls, subways in rush hour, water facilities, train stations, etc., as well as rural America this time (Wyoming, Montana, etc.).

The attack will be characterized by simultaneous detonations around the country (terrorists like big impact), involving at least 5-8 cities, including rural areas.

Aviv says terrorists won't need to use suicide bombers in many of the larger cities, because at places like the MGM Grand in Las Vegas, they can simply valet park a car loaded with explosives and walk away.

Aviv says all of the above is well known in intelligence circles, but that our U. S. Government does not want to "alarm American citizens" with the facts. The world is quickly going to become "a different place", and issues like "global warming" and political correctness will become totally irrelevant.

On an encouraging note, he says that Americans don't have to be concerned about being nuked. Aviv says the terrorists who want to destroy America will not use sophisticated weapons. They like to use suicide as a front-line approach. It's cheap, it's easy, it's effective; and they have an infinite abundance of young militants more than willing to "meet their destiny".

He also says the next level of terrorists, over which America should be most concerned, will not be coming from abroad. But will be, instead, 'homegrown' – having attended and been educated in our own schools and universities right here in the U.S. He says to look for "students" who frequently travel back and forth to the Middle East. These young terrorists will be most dangerous because they will know our language and will fully understand the habits of Americans; but that we Americans won't know/understand a thing about them.

Aviv says that, as a people, Americans are unaware and uneducated about the terrorist threats we will, inevitably, face. America still has only have a handful of Arabic and Farsi speaking people in our intelligence networks, and Aviv says it is critical that we change that fact SOON.

So, what can America do to protect itself? From an intelligence perspective, Aviv says the U.S. needs to stop relying on satellites and technology for intelligence. We need to, instead, follow Israel's, Ireland's and England's hands-on examples of human intelligence, both from an infiltration perspective as well as to trust "aware" citizens to help. We need to engage and educate ourselves as citizens; however, our U. S. government continues to treat us, its citizens, "like babies". Our government thinks we "can't handle the truth" and are concerned that we'll panic if we understand the realities of terrorism. Aviv says this is a deadly mistake.

Aviv recently created/executed a security test for our Congress, by placing an empty briefcase in five well-traveled spots in five major cities. The results? Not one person called 911 or sought a policeman to check it out. In fact, in Chicago, someone tried to steal the briefcase!

In comparison, Aviv says that citizens of Israel are so well "trained" that an unattended bag or package would be reported in seconds by citizen(s) who know to publicly shout, "Unattended Bag!" The area would be quickly & calmly cleared by the citizens themselves. But, unfortunately, America hasn't been yet "hurt enough" by terrorism for their government to fully understand the need to educate its citizens or for the government to understand that it's their citizens who are, inevitably, the best first-line of defense against terrorism.

Aviv also was concerned about the high number of children here in America who were in preschool and kindergarten after 9/11, who were "lost" without parents being able to pick them up, and about our schools that had no plan in place to best care for the students until parents could get there. (In New York City, this was days, in some cases!)

He stresses the importance of having a plan, that's agreed upon within your family, to respond to, in the event of a terrorist emergency. He urges parents to contact their children's schools and demand that the schools, too, develop plans of actions, as they do in Israel.

Does your family know what to do if you can't contact one another by phone?

Where would you gather in an emergency?

He says we should all have a plan that is easy enough for even our youngest children to remember and follow.

Aviv says that the U. S. government has in force a plan that, in the event of another terrorist attack, will immediately cut-off EVERYONE's ability to use cell phones, blackberries, etc... as this is the preferred communication source used by terrorists and is often the way that their bombs are detonated.

How will you communicate with your loved ones in the event you cannot speak?

You need to have a plan.



Consistent water monitoring is required by the State. Many water providers require non-compliance water sampling to ensure the water is safe.

## **Aimed at targeting Dallas home of ex-president Bush FBI charges Saudi man with plotting terrorist attack**

February 24, 2011 The FBI has arrested a 20-year-old Saudi student in Texas suspected of planning a terrorist attack using explosive chemicals. The FBI said his possible targets included the Dallas home of former President George W. Bush.

Khalid Ali-M al-Dawsari, 20, a Saudi national who came to Texas on student visa in 2008, was arrested late Wednesday and faces charges of attempted use of a weapon of mass destruction, according to AFP.

According to the FBI, al-Dawsari wrote himself an email entitled "NICE TARGETS," and then listed two types of targets: hydroelectric dams and nuclear power plants. In another email titled "Tyrant's House," he listed the address of Bush's home. The authorities' affidavit also alleges that al-Dawsari researched using dolls to hide explosives and concealing them in a backpack to target a nightclub.

Prosecutors said al-Dawsari, who was admitted into the United States in 2008 on a student visa, posted extremist messages on a blog, vowing jihad. "You who created mankind... grant me martyrdom for Your sake and make jihad easy for me only in Your path," he wrote.

Earlier this month, a chemical supplier reported his suspicions about al-Dawsari to the FBI, after the man tried to buy large amounts of phenol, which can be used to make explosives. He had tried to have the chemical sent to a freight company, which refused it.

Searches of his apartment uncovered chemicals, beakers and flasks, wiring and a Hazmat suit, among other items, the FBI said. Agents also allegedly discovered a journal which revealed that al-Dawsari came to the United States specifically for terror attacks. One entry describes how al-Dawsari said his scholarship "will help tremendously in providing me with the support I need for Jihad."

"And now, after mastering the English language, learning how to build explosives and continuous planning to target the infidel Americans, it is time for Jihad," he wrote, according to the FBI affidavit.

He was allegedly planning on renting several cars using different identifications, putting bombs in them and fleeing. Al-Dawsari faces life in prison and is expected to make his first court appearance in Texas on Friday.

### **What is Terrorism?**

The unlawful use of force or violence committed by a group or individual against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

-- U.S. Department of Justice



## The Means of Attack

Terrorism is not so much a system of belief, like fascism or communism, as it is a strategy and a tactic— a means of attack. In this war on terrorism, we must defend ourselves against a wide range of means and methods of attack. Our enemies are working to obtain chemical, biological, radiological, and nuclear weapons for the stated purpose of killing vast numbers of Americans.

Terrorists continue to employ conventional means of attack, such as bombs and guns. At the same time, they are gaining expertise in less traditional means, such as cyber-attacks. Lastly, as we saw on September 11, our terrorist enemies are constantly seeking new tactics or unexpected ways to carry out their attacks and magnify their effects.

**Weapons of mass destruction.** The knowledge, technology, and materials needed to build weapons of mass destruction are spreading. These capabilities have never been more accessible and the trends are not in our favor. If our terrorist enemies acquire these weapons and the means to deliver them, they are likely to try to use them, with potential consequences far more devastating than those we suffered on September 11.

Terrorists may conceivably steal or obtain weapons of mass destruction, weapons-usable fissile material, or related technology from states with such capabilities.

Several state sponsors of terrorism already possess or are working to develop weapons of mass destruction, and could provide material or technical support to terrorist groups.

Chemical weapons are extremely lethal and capable of producing tens of thousands of casualties. They are also relatively easy to manufacture, using basic equipment, trained personnel, and precursor materials that often have legitimate dual uses. As the 1995 Tokyo subway attack revealed, even sophisticated nerve agents are within the reach of terrorist groups.

Biological weapons, which release large quantities of living, disease-causing microorganisms, have extraordinary lethal potential. Like chemical weapons, biological weapons are relatively easy to manufacture, requiring straightforward technical skills, basic equipment, and a seed stock of pathogenic microorganisms.

Biological weapons are especially dangerous because we may not know immediately that we have been attacked, allowing an infectious agent time to spread. Moreover, biological agents can serve as a means of attack against humans as well as livestock and crops, inflicting casualties as well as economic damage.

**Radiological weapons**, or “**dirty bombs**,” combine radioactive material with conventional explosives. They can cause widespread disruption and fear, particularly in heavily populated areas. *See Chapter 3 for detailed information.*

Nuclear weapons have enormous destructive potential. Terrorists who seek to develop a nuclear weapon must overcome two formidable challenges. First, acquiring or refining a sufficient quantity of fissile material is very difficult—though not impossible.

## Dirty Bombs

Second, manufacturing a workable weapon requires a very high degree of technical capability—though terrorists could feasibly assemble the simplest type of nuclear device.

To get around these significant though not insurmountable challenges, terrorists could seek to steal or purchase a nuclear weapon. On May 8, 2002, the FBI captured Abdullah Al Muhajir, a U.S. citizen allegedly working with al Qaeda to set off a dirty bomb in an American city. This was unsettling news, to say the least. A dirty bomb is an explosive designed to spread dangerous radioactive material over a wide area. And when people hear "**bomb**" and "**radioactive**" in the same sentence, their minds jump to nuclear war pretty quickly.

It turns out that a dirty bomb's primary destructive power would probably be panic, not radiation damage. It's much closer to the power of an ordinary explosive than it is to the widespread destructive force of a nuclear bomb. But the fear of contamination could be debilitating, in the same way as 2001's anthrax scare terrorized much of the American populace, even though only a few people were

**Conventional means.** While we must prepare for attacks that employ the most destructive weapons, we must also defend against the tactics that terrorists employ most frequently. Terrorists, both domestic and international, continue to use traditional methods of violence and destruction to inflict harm and spread fear. They have used knives, guns, and bombs to kill the innocent.

They have taken hostages and spread propaganda. Given the low expense, ready availability of materials, and relatively high chance for successful execution, terrorists will continue to make use of conventional attacks.

**Cyber-attacks.** Terrorists may seek to cause widespread disruption and damage, including casualties, by attacking our electronic and computer networks, which are linked to other critical infrastructures such as our energy, financial, and securities networks.

Terrorist groups are already exploiting new information technology and the Internet to plan attacks, raise funds, spread propaganda, collect information, and communicate securely. As terrorists further develop their technical capabilities and become more familiar with potential targets, cyber-attacks will become an increasingly significant threat.

**New or unexpected tactics.** Our terrorist enemies are constantly seeking new tactics or unexpected ways to carry out attacks. They are continuously trying to find new areas of vulnerability and apply lessons learned from past operations in order to achieve surprise and maximize the destructive effect of their next attack. Our society presents an almost infinite array of potential targets, allowing for an enormously wide range of potential attack methods.



## Let's Meet the Terrorists

*Some of these people are considered Heroes as well.*



**Edward Joseph "Ed" Snowden** (born June 21, 1983) is an American computer specialist and former CIA employee and NSA contractor who disclosed up to 200,000 classified documents to the press. The cache contains details primary about the United States' NSA mass surveillance program, as well as its counterparts such as the British GCHQ and Israel's ISNU. Currently living in Russia under temporary asylum, Snowden is considered a fugitive by American authorities who have charged him with espionage and theft of government property.

Snowden's release of NSA material was called the most significant leak in US history by Pentagon Papers leaker Daniel Ellsberg. Based on disclosures leaked to *The Guardian* in May 2013, while employed by NSA contractor Booz Allen Hamilton, a series of exposés was published revealing Internet surveillance programs such as the PRISM, XKeyscore, Tempora, STORMBREW and MUSCULAR, as well as the interception of US and European telephone metadata.

Snowden has been a subject of controversy: he has been variously called a hero, a whistleblower, a dissident, a traitor, and a patriot. Response from US officials has been similarly varied; Director of National Intelligence James Clapper condemned Snowden's actions as having done "huge, grave damage" to US intelligence capabilities, while United States Secretary of State John Kerry admitted that the NSA had gone "too far" in some of its surveillance activities and promised that it would be stopped.

In Snowden's own words, his "sole motive" for leaking the documents was "to inform the public as to that which is done in their name and that which is done against them." The disclosures have fueled debates over mass surveillance, government secrecy, and the balance between national security and information privacy. Snowden first made contact with Glenn Greenwald, a journalist working at *The Guardian*, in late 2012. He contacted Greenwald anonymously and said he had "sensitive documents" that he would like to share.

Greenwald found the measures that the source asked him to take to secure their communications, such as encrypting email, too annoying to employ. Snowden then contacted documentary filmmaker Laura Poitras in January 2013.

According to Poitras, Snowden chose to contact her after seeing her report on NSA whistleblower William Binney in *The New York Times*. *The Guardian* reported that what originally attracted Snowden to both Greenwald and Poitras was a Salon article penned by Greenwald detailing how Poitras' controversial films had made her a "target of the government". Greenwald began working with Snowden in either February or in April after Poitras asked Greenwald to meet her in New York City, at which point Snowden began providing documents to them both. Barton Gellman, writing for *The Washington Post*, says his first "direct contact" was on May 16, 2013. According to Gellman, Snowden approached Greenwald after the *Post* declined to guarantee publication of all 41 of the PRISM PowerPoint slides within 72 hours and publish online an encrypted code allowing Snowden the ability to later prove that he was the source.

Snowden communicated using encrypted email, using the codename "Verax". He asked not to be quoted at length for fear of identification by semantic analysis.

According to Gellman, prior to their first meeting in person, Snowden wrote, "I understand that I will be made to suffer for my actions, and that the return of this information to the public marks my end."

Snowden also told Gellman that until the articles were published, the journalists working with him would also be at mortal risk from the United States Intelligence Community "if they think you are the single point of failure that could stop this disclosure and make them the sole owner of this information."

In May 2013, Snowden was permitted temporary leave from his position at the NSA in Hawaii, on the pretext of receiving treatment for his epilepsy. In mid-May Snowden gave an electronic interview to Poitras and Jacob Appelbaum which was published weeks later by *Der Spiegel*. On May 20, 2013, Snowden flew to Hong Kong, where he was staying when the initial articles about the NSA that he had leaked were published. Among other specifics, Snowden divulged the existence and functions of several classified US surveillance programs and their scope, including notably PRISM, NSA call database, and Boundless Informant.

He also revealed details of Tempora, a British black-ops surveillance program run by the NSA's British partner, GCHQ. In July 2013, Greenwald stated that Snowden had additional sensitive information about the NSA that he has chosen not to make public, including "very sensitive, detailed blueprints of how the NSA does what they do". In September 2013, the existence of a classified decryption program codenamed Bullrun was revealed.

By October 2013, Snowden's disclosures had created tensions between the US and some of its close allies after they revealed the US had spied on countries including France, Mexico, Germany, Brazil, Britain, China, and Spain, as well as 35 world leaders.

## Motivations

Snowden's identity was made public by *The Guardian* at his request on June 9, 2013. He explained: "I have no intention of hiding who I am because I know I have done nothing wrong." He added that by revealing his identity he hoped to protect his colleagues from being subjected to a hunt to determine who had been responsible for the leaks. Snowden explained his actions saying: "I don't want to live in a society that does these sort of things [surveillance on its citizens]... I do not want to live in a world where everything I do and say is recorded... My sole motive is to inform the public as to that which is done in their name and that which is done against them."

When Snowden met with representatives of human rights organizations on July 12, he said:

The 4th and 5th Amendments to the Constitution of my country, Article 12 of the Universal Declaration of Human Rights, and numerous statutes and treaties forbid such systems of massive, pervasive surveillance. While the US Constitution marks these programs as illegal, my government argues that secret court rulings, which the world is not permitted to see, somehow legitimize an illegal affair....

I believe in the principle declared at Nuremberg in 1945: "Individuals have international duties which transcend the national obligations of obedience. Therefore individual citizens have the duty to violate domestic laws to prevent crimes against peace and humanity from occurring."

Snowden, in an early June email sent to the *Washington Post*, said that in the past, whistleblowers had been 'destroyed by the experience', and that he wanted to "embolden others to step forward" by demonstrating that "they can win". In October, Snowden spoke out again on his motivations for the leaks in an interview with the *New York Times*, saying that the system for reporting problems does not work. "You have to report wrongdoing to those most responsible for it", Snowden explained, and pointed to the lack of whistleblower protection for government contractors, the use of the 1917 Espionage Act to prosecute leakers, and his belief that had he used internal mechanisms to 'sound the alarm', his revelations "would have been buried forever".

## References

Greenwald, Glenn; MacAskill, Ewen; Poitras, Laura (June 10, 2013). "Edward Snowden: the whistleblower behind the NSA surveillance revelations". *The Guardian* (London).

"Former U.S. officials give NSA whistleblower Snowden award in Russia". *Haaretz*. 10 October 2013.

Mullin, Joe. (June 13, 2013) "NSA leaker Ed Snowden's life on". *Ars Technica*.  
NSA chief says Snowden leaked up to 200,000 secret documents | Reuters

Gellman, Barton; Markon, Jerry (June 9, 2013). "Edward Snowden says motive behind leaks was to expose 'surveillance state'". *The Washington Post*. Retrieved June 10, 2013.

Finn, Peter; Horwitz, Sari (June 21, 2013). "U.S. charges Snowden with espionage". *The Washington Post*. Retrieved June 21, 2013.

"Daniel Ellsberg Calls Edward Snowden A 'Hero,' Says NSA Leak Was Most Important in American History". *Huffington Post*.



## Abu Musab al-Suri



**Mustafa bin Abd al-Qadir Sitt Maryam Nasar** (Arabic: مصطفى بن عبد القادر ست مريم نصار, also known as **Abu Musab al-Suri**) is a suspected al-Qaeda member and writer. He has held Spanish citizenship since the late 1980s following marriage to a Spanish woman.

He is considered by many as 'the most articulate exponent of the modern jihad and its most sophisticated strategies'.

Nasar was reportedly captured in the Pakistani city of Quetta in late October 2005, although exactly where and when is disputed. He was captured by Pakistani security forces and handed over to American custody a month or so later. He was not among the 14 high-profile al-Qaida suspects transferred to the Guantanamo Bay detention camp in late 2006, and it appears that Nasar was renditioned to Syria, where he was a wanted man. He is also wanted in Spain for the 1985 El Descanso bombing, which killed eighteen people, and (as a witness) in connection with the 2004 Madrid train bombings.

Ever since the death of Osama bin Laden, President Obama and his senior lieutenants have been telling war-weary Americans that the end of the nation's longest conflict is within sight. "Core al-Qaida is a shell of its former self," Obama said in a speech in May. "This war, like all wars, must end." That was the triumphal tone of last year's reelection campaign, too.

The truth is much grimmer. Intelligence officials and terrorism experts today believe that the death of bin Laden and the decimation of the Qaida "core" in Pakistan only set the stage for a rebirth of al-Qaida as a global threat. Its tactics have morphed into something more insidious and increasingly dangerous as safe havens multiply in war-torn or failed states—at exactly the moment we are talking about curtailing the National Security Agency's monitoring capability. And the jihadist who many terrorism experts believe is al-Qaida's new strategic mastermind,

Abu Musab al-Suri (a nom de guerre that means "the Syrian"), has a diametrically different approach that emphasizes quantity over quality. The red-haired, blue-eyed former mechanical engineer was born in Aleppo in 1958 as Mustafa Setmariam Nasar; he has lived in France and Spain. Al-Suri is believed to have helped plan the 2004 train bombings in Madrid and the 2005 bombings in London—and has been called the "Clausewitz" of the new al-Qaida.

Whereas bin Laden preached big dramatic acts directed by him and senior Qaida leaders, al-Suri urges the creation of self-generating cells of lone terrorists or small groups in his 1,600-page Internet manifesto. They are to keep up attacks, like multiplying fleas on a dog that finds itself endlessly distracted—and ultimately dysfunctional. (A classic Western book on guerrilla warfare called *The War of the Flea* reportedly influenced al-Suri.) The attacks are to culminate, he hopes, in acts using weapons of mass destruction.

"I think al-Qaida's capabilities for a strike into the United States are more dangerous and more numerous than before 9/11."

Recent terrorist attacks against U.S. targets, from the murderous 2009 spree of Army Maj. Nidal Malik Hasan at Fort Hood to the Boston Marathon bombings last year, suggest that al-Suri's philosophy dominates al-Qaida's newly flattened hierarchy. The late Yemeni-American imam Anwar al-Awlaki, who preached this strategy and induced Hasan's attack, is said to have developed his ideas from al-Suri's. Meanwhile, with new refuges in North Africa, Syria, and Yemen, jihadists have much more territory from which to hatch plots unmolested. Yet the politics at home are changing as the threat abroad is growing.

The revelations dribbled out by fugitive leaker Edward Snowden have outraged members of Congress and world leaders, including those of close allies such as Germany and France. They say they are aghast at American overreach. Writing in *Der Spiegel*, Snowden justified himself this way: "Instead of causing damage, the usefulness of the new public knowledge for society is now clear, because reforms to politics, supervision, and laws are being suggested." Thanks to him, Congress will almost certainly rein in the National Security Agency's data-trolling methods—though it's not yet clear how much.

But the agency's opponents may not realize that the practice they most hope to stop—its seemingly indiscriminate scouring of phone data and emails—is precisely what intelligence officials say they need to detect the kinds of plots al-Suri favors. For the foreseeable future, al-Suri's approach will mean more terrorist attacks against more targets—albeit with a much lower level of organization and competence. "It's harder to track. Future attacks against the homeland will be less sophisticated and less lethal, but there's just going to be more of them," says Michael Hayden, the former NSA director who steered the agency after 9/11 toward deep dives into Internet and telephonic data. Adds Mike Rogers, chairman of the House Intelligence Committee, "I think al-Qaida's capabilities for a strike into the United States are more dangerous and more numerous than before 9/11." For better or worse, the only hope to track them all is an exceptionally deep, organized, and free-ranging intelligence apparatus, experts say.



## Appearances

Nasar has ginger hair, green eyes, and a brown complexion. He was born and grew up in Aleppo in Syria, and attended four years of university studies there at the University of Aleppo's Department of mechanical engineering. In 1980, he joined the Combatant Vanguard organization, a radical offshoot of the Syrian Muslim Brotherhood, which was at the forefront in the Islamic uprising in Syria against Hafez Assad's regime. Nasar was forced to flee Syria at the end of 1980. He then joined the Syrian Muslim Brotherhood organization in exile, receiving training at their bases and safe houses in Iraq and Jordan.

He is reported to have participated in the uprising of Hama in 1982. He emigrated to France and later to Spain in the mid-1980s.

In 1987, Nasar and a small group of Syrian friends left Spain for Peshawar where they met Abdallah Azzam, the godfather of the Arab-Afghan movement. Nasar was enlisted as a military trainer at the camps for Arab volunteer fighters, and he also fought at the frontlines against Soviet Union in Afghanistan and the Communist regime in Kabul after the Soviet withdrawal in 1988.

Nasar met Osama bin Laden in Peshawar and claims to have been a member of his inner circle and working for bin Laden until sometime around 1992, when Nasar returned to Spain. In Peshawar, Nasar became well-known under his pen name Umar Abd al-Hakim after he published a 900 page treatise in May 1991, entitled 'The Islamic jihadi revolution in Syria', also known as 'the Syrian Experience' (*al-tajrubah al-suriyyah*). The treatise was a vehement attack on the Muslim Brotherhood and constituted an important part of the intellectual foundation for al-Qaida and the jihadi current during the 1990s.



From 1985 to 1995 Nasar adopted Spain as his primary place of residence, even though he traveled extensively and spent much time in Afghanistan. In Spain, he married his wife Elena Moreno in 1987 (or 88), who converted to Islam, which allowed him to become a Spanish citizen. They have four children.

Among his associates there were Imad Eddin Yarkas alias Abu Dahdah, head of al-Qaeda's Madrid cell, who was arrested in November 2001, on suspicion of membership in al-Qaida and of involvement in the 11 September 2001 attacks in the United States. He was later acquitted of charges of assisting the 9/11 plotters, but convicted of membership in a terrorist organization. Nasar first moved to London in 1994, and brought his family along in mid-1995. It is possible that he fled Spain because of suspicions he was involved in the 1995 Islamist terror bombings in France. For a time Nasar edited al-Ansar, the most important jihadi magazine at the time, with ties to the Algerian Armed Islamic Group (GIA).

Nasar left the journal in 1996 partly due to disagreements with the new GIA leadership in Algeria and partly as a result of a conflict with its chief editor, Umar Mahmud Uthman Abu Umar, better known as Abu Qatada al-Filastini. The latter is widely regarded as al-Qaeda's principal cleric in Europe.

In 1997, Nasar established a media company called Islamic Conflict Studies Bureau with Mohamed Bahaiah. Through this media office he facilitated two important media events for bin Ladin in Afghanistan, in particular Peter Bergen's famous CNN interview with bin Laden in March 1997.

In the autumn of 1997 Nasar left London for Afghanistan, operating initially as a lecturer and trainer in the Arab-Afghan camps and guesthouses. He settled there with his family in 1998. In 1999 he formed a media and research center in Kabul and in 2000 he was allowed to open his own training camp, the al-Ghuraba Camp, located in Kargha, near Kabul. Nasar's camp was formally part of Taliban's Ministry of defense, and separate from al-Qaida and bin Ladin's organization, whom he had fallen out with in 1998. In a seven-page letter from mid-1998, Nasar launched scathing criticism of bin Ladin for his disdain al-Qaeda has shown towards the Taliban leadership of Afghanistan, including Mullah Omar. He is also highly critical of their strategies, and has denounced al-Qaeda's 1998 attacks on the US embassies in East Africa, and the 11 September attack on New York's Twin Towers, which he argues put a catastrophic end to the jihadi cause.

Due to his prolific writings on strategic and political issues, and his guerrilla warfare experience, Nasar was a popular lecturer and to a certain degree an unofficial adviser for a wide range of jihadi groups in Afghanistan. Organizationally, however, he remained a rather independent figure. While some reports have linked him to Abu Musab al-Zarqawi, who later led al-Qaeda's component of the insurgency in Iraq, his network of contacts was much wider, and included jihadis from Morocco, Algeria, Libya, Egypt, Syria, Lebanon, Iraqi Kurdistan, Saudi Arabia, Yemen, Uzbekistan, and elsewhere. Media reports have also alleged that one of his associates, the Moroccan Amer Azizi, (Uthman al-Andalusi), had met 11 September organizers Mohamed Atta and Ramzi bin al-Shibh in Tarragona, Spain weeks before the attacks, but this seems to be incorrect.

The American occupation of Iraq, he declares, inaugurated a 'historical new period' that almost single-handedly rescued the jihadi movement just when many of its critics thought it was finished. In September 2003, Spanish magistrate Baltasar Garzon indicted 35 members of the Madrid cell for its role in the 11 September attacks, including Nasar. In November 2004, the United States Department of State named Nasar a *Most Wanted Terrorist* and offered a reward of US\$5 million for information about his location.

## References

Michael Hirsh of The Atlantic

Lia, Brynjar *Architect of Global Jihad: The Life of Al Qaeda Strategist Abu Mus'ab Al-Suri* (2008), Columbia University Press ISBN 978-0-231-70030-6

Lacey, Jim, ed. *A Terrorist's Call to Global Jihad: Deciphering Abu Musab al-Suri's Islamic Jihad Manifesto* (2008), Naval Institute Press ISBN 978-1-59114-462-5

## Boston Marathon Bombings – *In our backyard*



During the Boston Marathon on April 15, 2013, two pressure cooker bombs exploded at 2:49 pm EDT (18:49 UTC), killing 3 people and injuring an estimated 264 others. The bombs exploded about 13 seconds and 210 yards (190 m) apart, near the finish line on Boylston Street.

The Federal Bureau of Investigation (FBI) took over the investigation, and on April 18, released photographs and surveillance video of two suspects. The suspects were identified later that day as Dzhokhar and Tamerlan Tsarnaev. Shortly after the FBI released the images, the suspects allegedly killed an MIT police officer, carjacked an SUV, and initiated an exchange of gunfire with the police in Watertown, Massachusetts. During the firefight, an MBTA police officer was injured but survived with severe blood loss. Tamerlan Tsarnaev was run over by his brother Dzhokhar, who was injured but escaped.

An unprecedented manhunt ensued on April 19, with thousands of law enforcement officers searching a 20-block area of Watertown. During the manhunt, authorities asked residents of Watertown and surrounding areas, including Boston, to stay indoors. The public transportation system and most businesses and public institutions were shut down, creating a deserted urban environment of historic size and duration. Around 7 pm, shortly after the "shelter-in-place" advisory was rescinded, a Watertown resident discovered Dzhokhar Tsarnaev hiding in a boat in his back yard. He was arrested and taken to a hospital shortly thereafter.

During an initial interrogation in the hospital, Dzhokhar—who had not been read his *Miranda* rights—said Tamerlan was the mastermind. He said the brothers were motivated by extremist Islamist beliefs and the wars in Iraq and Afghanistan, and that they were self-radicalized and unconnected to any outside terrorist groups. He said they had learned to build explosive devices from an online magazine of the al-Qaeda affiliate in Yemen. He said that he and his brother had decided after the Boston bombings to travel to New York City to bomb Times Square. Dzhokhar was charged on April 22, while still in the hospital, with use of a weapon of mass destruction and malicious destruction of property resulting in death. He has pleaded not guilty to 30 charges

On Patriots' Day, Monday, April 15, 2013, the annual Boston Marathon began without any indications of an imminent attack. Officials swept the area for bombs twice before the explosions; the second sweep occurred one hour before the bombs went off. People were able to come and go freely, and carry bags and items in and out of the area.

At 2:49 pm EDT (18:49 UTC), about two hours after the winner crossed the finish line, but with more than 5,700 runners yet to finish, two bombs detonated on Boylston Street near Copley Square about 210 yards (190 m) apart, just before the finish line. The first exploded outside Marathon Sports at 671–673 Boylston Street at 2:49:43 pm EDT. At the time of the first explosion, the race clock at the finish line showed 04:09:43, reflecting the elapsed time since the Wave 3 start at 10:40 am EDT. The second bomb exploded at 2:49:57 pm EDT, about 13 seconds later and one block farther west at 755 Boylston Street.

The blasts blew out windows on adjacent buildings but did not cause any structural damage. Some runners continued to cross the line until 2:57 pm EDT, 8 minutes after the explosions.

#### **Identification of suspects: Dzhokhar and Tamerlan Tsarnaev**



Tamerlan (front) and Dzhokhar Tsarnaev as seen on security camera footage just prior to the bombing. This and other images released by the FBI taken from other security footage and photos from bystanders would later be considered a "turning point" in the investigation, leading to the subsequent manhunt and capture.

In a news conference held at 5:20 pm on April 18, the FBI released photographs and surveillance videos showing two suspects—each carrying backpacks and walking nonchalantly but purposefully in single file formation—and sought the public's help in identifying them. The FBI released the photos, in part, to limit the damage by those wrongly targeted by incorrect news reports and social media speculations. Authorities later said that releasing the suspect's photos "was a turning point in the investigation, no doubt about it."

Jeff Bauman, a victim who lost both legs, was adjacent to the location of one of the bombs; upon recovering consciousness, he asked for pen and paper and wrote a note to the FBI, "bag, saw the guy, looked right at me". Bauman was later able to provide detailed descriptions to the authorities of a suspect who was seen placing a backpack beside him at the bombing scene two and a half minutes before it exploded, enabling the photo to be identified and circulated quickly. The suspects, initially identified by the FBI as unnamed suspects 1 and 2 (or "black hat" and "white hat", respectively) from photographic and video evidence, had "acted differently" after the explosions; they had stayed to watch the aftermath and walked away "casually", rather than fleeing. Asked for assistance in identifying the suspects, the public provided a deluge of photographs and home movie records to police, which were scrutinized by both authorities and online public social networks.

Despite video footage taken at the scene, the suspects were not identified by authorities before killing a police officer and hijacking a civilian. The actual source of identification was DMV records on the Honda vehicle, which was used in a subsequent kidnapping and then abandoned. The suspects were then identified as two brothers whose family had immigrated to the United States as refugees around 2002: 26-year-old Tamerlan Tsarnaev, born on October 21, 1986, and killed on April 19, 2013, and 19-year-old Dzhokhar Tsarnaev, born on July 22, 1993

### MIT shooting and carjacking



Scenes and approximate times of events of April 18–19

A few hours after the photos were released, the suspects allegedly shot Sean A. Collier of the Massachusetts Institute of Technology Police Department multiple times, killing him for his gun which they could not get out because of the holster's retention system.

Collier, aged 27, was seated in his police car near the Stata Center (Building 32), on the Massachusetts Institute of Technology campus. He was taken to Massachusetts General Hospital in nearby downtown Boston, where he was pronounced dead. Some law enforcement officials have described the killing as an assassination.

The duo then allegedly carjacked a Mercedes-Benz SUV in the Allston-Brighton neighborhood of Boston, Tamerlan taking the owner hostage and telling him that he was responsible for the Boston bombings and for killing a police officer. Dzhokhar followed them in the green Honda, later joining them in the Mercedes-Benz. Later interrogation allegedly revealed that the brothers "decided spontaneously" to go to New York and planned to bomb Times Square.

The suspects forced the hostage to use his ATM cards to obtain \$800 in cash until the daily cash withdrawal limit was reached. They transferred objects to the Mercedes-Benz and one brother followed it in their Honda Civic, for which an all-points bulletin was issued. The car's owner, Danny, a Chinese national, escaped while the suspects stopped at a gas station; he ran across the street to another gas station, asking the clerk to call 911. His cellphone remained in the vehicle, allowing the police to track it.

### **Firefight with police**

Shortly after midnight on April 19, a Watertown police officer identified the brothers in a Honda Civic and the stolen SUV, and a "ferocious" gunfight followed on the 100 block of Laurel Ave, between the brothers and police arriving at the scene. An estimated 200–300 rounds of ammunition were fired and at least one further bomb and several "crude grenades" were thrown.

According to Watertown Police Chief Edward Deveau, the brothers had an "arsenal of guns." Also according to Deveau, the older brother, Tamerlan, ran out of ammunition and was tackled and apprehended by police, while the younger brother Dzhokhar drove the stolen SUV towards police and proceeded to drive over Tamerlan, dragging him a short distance down the street. Dzhokhar Tsarnaev sped off, but about a half-mile away at the corner of Spruce and Lincoln streets he abandoned the car and escaped on foot.

According to two anonymous officials, only one Ruger 9mm pistol was recovered from the scene and one of them said it had a defaced serial number. The *Boston Globe* reported that within a 10-minute span, "police officers fired what may be an unprecedented number of rounds in a single police incident in recent state history ... [spraying] the neighborhood ... [leaving] at least a dozen nearby houses pockmarked with dozens of bullet holes". Tamerlan Tsarnaev was captured and transported to Beth Israel Deaconess Medical Center, where he was pronounced dead on April 19 at 1:35 am The emergency room doctors said that he did not appear to have been run over.

According to the death certificate, Tsarnaev's cause of death was "gunshot wounds of torso and extremities, blunt trauma to head and torso," and "shot by police then run over and dragged by motor vehicle." Tamerlan's younger brother Dzhokhar ran him over with an SUV and dragged him with the vehicle for 20 feet (6.1 m). The death was ruled a homicide.

During the firefight, 33-year-old MBTA Police Officer Richard H. Donahue Jr. was also critically wounded by what may have been friendly fire. He was taken to Mount Auburn Hospital, where he was in critical but stable condition. Fifteen other police officers sustained minor injuries during the firefight.

### **Manhunt and capture of Dzhokhar Tsarnaev**

The FBI released additional photos of the two during the Watertown incident. Early on April 19, Watertown residents received reverse 911 calls asking them to stay indoors. On the morning of April 19, Governor Patrick asked residents of Watertown and adjacent cities and towns (Allston-Brighton, Boston, Belmont, Brookline, Cambridge, Newton, and to "shelter in place". Somerville residents also received a reverse-911 call with orders to shelter in place.

A 20-block area of Watertown was cordoned off and residents were told not to leave their homes or answer the door as officers in tactical gear scoured the area. Helicopters circled the area and SWAT teams in armored vehicles moved through in formation, with officers going door-to-door. On the scene were the FBI, the Bureau of Alcohol, Tobacco, Firearms and Explosives, the Department of Homeland Security, the National Guard, the Boston and Watertown Police departments and the Massachusetts State Police. The show of force was the first major field test of the interagency task forces created in the wake of the September 11 attacks.

The entire public transit network, as well as most Boston taxi service, was suspended, as was Amtrak service to and from Boston. Logan International Airport remained open under heightened security. Universities, schools, many businesses, and other facilities were closed as thousands of law enforcement personnel participated in an unprecedented door-to-door manhunt in Watertown, as well as following up other leads, including at the house the brothers shared in Cambridge. Seven improvised explosive devices were recovered by bomb squads.

The father of the suspected Boston Marathon bombers, speaking from his home in Makhachkala, Dagestan, encouraged his son to: "Give up. Give up. You have a bright future ahead of you. Come home to Russia." He continued, "If they killed him, then all hell would break loose." On television, Dzhokhar's uncle from Montgomery Village, Maryland, pleaded with him to turn himself in.



Post-capture celebrations in Boston's student-heavy Mission Hill neighborhood.

The manhunt ended on the evening of April 19, two hours after the shelter-in-place order had been lifted. Outside the search area, a Watertown resident stepped outside and noticed that the cover on his boat in his back yard was loose. He looked into the boat and saw a body lying in a pool of blood, and he promptly notified police. Authorities surrounded the boat and verified movement through a forward looking infrared thermal imaging device in a State Police helicopter. When the suspect started poking at the tarp of the boat, police began a large volume of gunfire at the boat, stopping only after the Superintendent on the scene called for a cease fire. Celebrations followed law enforcement's capture of Tsarnaev.

According to Boston Police Commissioner Ed Davis, and Watertown Police Chief Deveau, Tsarnaev was shooting from inside the boat at police, "exchanging fire for an hour." After he was captured, Tsarnaev was found not to have any weapons. He was taken into custody at 8:42 pm and transported to Beth Israel Deaconess Medical Center, where he was listed in critical condition with multiple gunshot wounds to the head, neck, legs and hand. Initial reports that the neck wound was from a self-inflicted gunshot from a possible suicide attempt were later contradicted by the revelation that he was unarmed at the time of capture and a description of the neck wound by SWAT team members that the neck wound was a slicing injury, possibly caused by shrapnel from an explosion.

## **Legal proceedings**

### **Interrogation**

United States Senators Kelly Ayotte, Saxby Chambliss, Lindsey Graham, and John McCain, and Representative Peter T. King, suggested that Dzhokhar Tsarnaev, a U.S. citizen, should be tried as an unlawful enemy combatant rather than as a criminal, potentially preventing him from obtaining legal counsel. Other sources, including Alan Dershowitz, a prominent American legal scholar and lawyer, said that doing so would be illegal and would jeopardize the prosecution. The government decided to try Dzhokhar in the federal criminal court system and not as an enemy combatant.

Dzhokhar was questioned for 16 hours by investigators but stopped communicating with them on the night of April 22 after Judge Marianne Bowler read him a *Miranda* warning. Dzhokhar had not previously been given a Miranda warning, as federal law enforcement officials invoked the warning's public safety exception. This raised doubts whether the suspect's statements during this investigation would be admissible as evidence and led to a debate surrounding Miranda rights.

### **Charges and detention**

On April 22, formal criminal charges were brought against Dzhokhar Tsarnaev in the United States District Court for the District of Massachusetts during a bedside hearing while he was hospitalized. He was charged with use of a weapon of mass destruction, and with malicious destruction of property resulting in death. The charges carry potential sentences of life imprisonment or the death penalty. Tsarnaev was judged to be awake, mentally competent, and lucid, and he responded to most questions by nodding. When the judge asked him whether he was able to afford an attorney, he responded "no"; he is represented by the Federal Public Defender's office. On April 26, Dzhokhar Tsarnaev was moved from Beth Israel Deaconess Medical Center to the Federal Medical Center at Fort Devens, about 40 miles (64 km) from Boston. FMC Devens is a federal prison medical facility at a former Army base where he is being held in solitary confinement at a segregated housing unit with 23-hour-per-day lockdown.



On July 10, Dzhokhar Tsarnaev pleaded not guilty to 30 charges in his first public court appearance, including a murder charge for MIT police officer Sean Collier. He was back in court for a status hearing on September 23, and his lawyers requested more time to prepare their defense. On October 2, Tsarnaev's attorneys asked the court to lift the special administrative measures (SAMs) imposed by Attorney General Holder in August, saying the measures have left Tsarnaev unduly isolated from communication with his family and lawyers, and that no evidence suggests he poses a future threat.

### **Motives and backgrounds**

According to FBI interrogators, Dzhokhar and his brother were motivated by extremist Islamic beliefs, and "were not connected to any known terrorist groups"; instead learning to build explosive weapons from an online magazine published by al-Qaeda affiliates in Yemen. It is further alleged that "[Dzhokhar and] his brother considered suicide attacks and striking on the Fourth of July; but ultimately decided to use pressure cooker bombs (capable of remote detonation) and other IEDs." Fox News reported that the brothers "chose the prestigious race as a 'target of opportunity' ... [after] the building of the bombs came together more quickly than expected".

Dzhokhar said he and his brother wanted to defend Islam from the U.S., which conducted the Iraq War and War in Afghanistan, in the view of the brothers, against Muslims. Later a CBS report revealed that a note scrawled by Dzhokhar with a marker on the interior wall of the boat where he was hiding said the bombings were "retribution for U.S. military action in Afghanistan and Iraq", and called the Boston victims 'collateral damage', "in the same way innocent victims have been collateral damage in U.S. wars around the world." According to *The New York Times* the portion of the boat's interior with the note would likely be cut from the hull with permission from the owner and presented in court as evidence.

Despite the seemingly outwardly religious motivation of the Tsarnaev brothers, some political science and public policy scholars suggest that Islam may have only played a secondary role in the attacks. Sympathy towards the political aspirations in the Caucasus region and Tamerlan's inability to become fully integrated into American society appear to be the primary motives in their opinion.

According to *The Los Angeles Times*, a law enforcement official said Dzhokhar "did not seem as bothered about America's role in the Muslim world" as his brother Tamerlan had been. Dzhokhar identified Tamerlan as the "driving force" behind the bombings, and said that his brother had only recently recruited him to help.

Tamerlan Tsarnaev was born in 1986 in the Kalmyk Autonomous Soviet Socialist Republic, North Caucasus. Dzhokhar was born in 1993 in Kyrgyzstan, although some reports say his family claims he was born in Dagestan. The family spent time in Tokmok, Kyrgyzstan, and in Makhachkala, Dagestan. They are half Chechen through their father, Anzor, and half Avar through their mother, Zubeidat. Although they never lived in Chechnya the brothers self-identified as Chechen.



The West New York, NJ, apartment of one of the suspects' sisters was searched by the FBI, the West New York Police Department and the Hudson County Sheriff.

The Tsarnaev family emigrated in 2002 to the United States, where they applied for refugee status, settling in Cambridge, Massachusetts. Tamerlan Tsarnaev attended Bunker Hill Community College but dropped out to become a boxer. His goal was a place on the U.S. Olympic boxing team saying that "unless his native Chechnya becomes independent" he would "rather compete for the United States than for Russia". He was married on July 15, 2010 in the Masjid Al Quran Mosque in Dorchester, to a U.S. citizen, Katherine Russell, who was pregnant with their daughter. He stated that he "didn't understand" Americans and had not a single American friend. He had a history of violence, including an arrest in July 2009 for assaulting his then girlfriend.

The brothers are Muslim, with Tamerlan's aunt stating that he had recently become a devout Muslim. Tamerlan, in the three years before his death, became more devout and religious, and a YouTube channel in his name linked to Salafist and Islamist videos. The FBI was informed by the Russian Federal Security Service (FSB) in 2011 that he was a "follower of radical Islam." In response, the FBI interviewed Tamerlan and his family, and searched databases, but did not find any evidence of "terrorism activity, domestic or foreign." During the 2012 trip to Dagestan, Tamerlan was reportedly a frequent visitor at a mosque on Kotrova Street in Makhachkala, believed by the FSB to be linked with radical Islam. Some experts believe "they were motivated by their faith, apparently an anti-American, radical version of Islam" acquired in the U.S., while others believe the turn to radicalism happened in Dagestan.

At the time of the bombing, Dzhokhar Tsarnaev was a student at the University of Massachusetts Dartmouth, with a major in marine biology. Dzhokhar became a naturalized U.S. citizen on September 11, 2012. Tamerlan's boxing coach reported to NBC that the young brother was greatly affected by his brother and admired him.

Tamerlan Tsarnaev was previously connected, but at the time not a suspect, to the triple homicide in Waltham, Massachusetts on the evening of September 11, 2011. Brendan Mess, Erik Weissman, and Raphael Teken were murdered in Mess' apartment. All had their throats slit from ear to ear, with such great force that they were nearly decapitated. The local district attorney said that it appeared that the killer and the victims knew each other, and that the murders were not random. Tamerlan Tsarnaev had previously described murder victim Brendan Mess as his "best friend." After the bombings and subsequent revelations of Tsarnaev's personal life, the Waltham murders case was reexamined in April 2013 with Tsarnaev as a new suspect. Both ABC and *The New York Times* have reported that there is strong evidence that implicate Tsarnaev for this triple homicide.

Some analysts claim the Tsarnaev brothers' mother, Zubeidat Tsarnaeva, is a radical extremist and supporter of jihad, who influenced her sons' behavior. This prompted the Russian government to warn the U.S. government about the family's behavior, on two occasions. Both Tamerlan and his mother were placed on a terrorism watch list about 18 months before the bombing took place.

According to a *Wall Street Journal* report citing statements by anonymous US officials, Russia withheld information from U.S. intelligence after its initial warning, after which it denied U.S. requests for more information.

#### **Other arrests and detentions**

On April 15, several people who were near the scene of the blast and the surrounding area were taken into custody and questioned about the bombings, including a Saudi man whom police stopped as he was walking away from the explosion, and detained when some of his responses to questions "made them uncomfortable". Law enforcement searched his residence in a Boston suburb. CNN later reported that he was found to have no connection to the attack; an unnamed U.S. official said, "he was just at the wrong place at the wrong time."

On the night of April 18, two men riding in a taxi in the vicinity of the shootout were arrested and released shortly thereafter when police determined they were not involved in the Marathon attacks. Another man was arrested several blocks from the site of the shootout and was forced to strip naked by police who feared he might have concealed explosives. He was released that evening after a brief investigation determined that he was an innocent bystander.

On May 22, the FBI were interviewing Ibragim Todashev, a Chechen from Boston, in Orlando. During the interrogation he was shot and killed by an FBI officer who claimed that Todashev attacked him. *The New York Times* quoted an unnamed law enforcement official as saying that Todashev had confessed to the 2011 Waltham murders and implicated Tsarnaev as well. However, the father of Ibragim Todashev claims that his son is innocent and that federal investigators are biased against Chechens and made up their case against him.

#### **Dias Kadyrbayev, Azamat Tazhayakov and Robel Phillipos**

During the night of April 18–19, police arrested two Kazakhstan natives living in the U.S., Dias Kadyrbayev and Azamat Tazhayakov (19 and 20 years old, respectively) and an unnamed girlfriend of one of the men, at the off-campus housing complex at which Tsarnaev had sometimes stayed in New Bedford, Massachusetts. All three were soon released. The men were Dzhokhar Tsarnaev's roommates.

## Victims

The bombings killed 3 people and injured 264. A number of the injuries were grievous, requiring intensive care, and appeared to be "war-like injuries" of mutilation, shrapnel wounds, and dismemberment. The trauma surgery chief at Boston Medical Center said: "We see patients like this, with mangled extremities, but we don't see 16 of them at the same time, and we don't see patients from blast injuries." An MIT police officer, Sean A. Collier was fatally shot three days after the bombing, and a Transit Police officer was seriously wounded.

## References

Straw, Joseph; Ford, Bev; McShane, Lawrence (April 17, 2013). "Police narrow in on two suspects in Boston Marathon bombings". *The Daily News*. Retrieved May 15, 2013.

Kotz, Deborah (April 24, 2013). "Injury toll from Marathon bombs reduced to 264". *The Boston Globe*. Retrieved April 29, 2013. "Boston public health officials said Tuesday that they have revised downward their estimate of the number of people injured in the Marathon attacks, to 264."

Carter, Chelsea J.; Botelho, Gregory (April 20, 2013). "'Captured!!!' Boston police announce Marathon bombing suspect in custody". CNN. a:"Richard H. Donohue Jr., 33,... was shot and wounded in the incident... Another 15 police officers were treated for minor injuries sustained during the explosions and shootout".

"United States vs. Dzhokhar Tsarnaev, Case 1:13-mj-02106-MBB" (PDF). United States Department of Justice. April 21, 2013. Retrieved April 22, 2013.

Wilson, Scott (April 23, 2013). "Boston bombing suspect cites U.S. wars as motivation, officials say". *The Washington Post*. et al. Retrieved April 23, 2013.

"Boston Suspects Are Seen as Self-Taught and Fueled by Web". *The New York Times*. April 23, 2013.

"What we know about the Boston bombing and its aftermath". CNN. April 19, 2013. Retrieved April 19, 2013.

Estes, Adam Clark; Abad-Santos, Alexander; Sullivan, Matt (April 15, 2013). "Explosions at Boston Marathon Kill 3 — Now, a 'Potential Terrorist Investigation'". *The Atlantic Wire*. Retrieved April 17, 2013.

Fromer, Frederic J. (April 15, 2013). "Justice Department Directing Full Resources To Investigate Boston Marathon Bombings". *Huffington Post*. Retrieved April 22, 2013.

des Lauriers, Richard (April 18, 2013). *Remarks of Special Agent in Charge at Press Conference on Bombing Investigation* (press release). Boston: FBI. Retrieved April 21, 2013.

Tanfani, Joseph; Kelly, Devin; Muskal, Michael (April 19, 2013). "Boston bombing [Update]: Door-to-door manhunt locks down city". *Los Angeles Times* (Boston). Retrieved April 29, 2013.

"As family members called on him to surrender, a 19-year-old college student remained on the run Friday as thousands of police armed with rifles and driving armored vehicles combed the nearly deserted streets of a region on virtual lockdown"

"Boston Lockdown 'Extraordinary' But Prudent, Experts Say". April 22, 2013. Retrieved April 23, 2013.

## 2015 San Bernardino Attack

On December 2, 2015, 14 people were killed and 22 were seriously injured in a terrorist attack at the Inland Regional Center in San Bernardino, California, which consisted of a mass shooting and an attempted bombing. The perpetrators, Syed Rizwan Farook and Tashfeen Malik, a married couple living in the city of Redlands, targeted a San Bernardino County Department of Public Health training event and holiday party, of about 80 employees, in a rented banquet room. Farook was an American-born U.S. citizen of Pakistani descent, who worked as a health department employee. Malik was a Pakistani-born lawful permanent resident of the United States.

After the shooting, the couple fled in a rented sport utility vehicle (SUV). Four hours later, police pursued their vehicle and killed them in a shootout. On December 3, 2015, the Federal Bureau of Investigation (FBI) opened a counter-terrorism investigation. On December 6, 2015, in a prime-time address delivered from the Oval Office, President Barack Obama defined the shooting as an act of terrorism.

According to FBI Director James B. Comey, the FBI's investigation revealed that the perpetrators were "homegrown violent extremists" inspired by foreign terrorist groups. They were not directed by such groups and were not part of any terrorist cell or network. FBI investigators have said that Farook and Malik had become radicalized over several years prior to the attack, consuming "poison on the internet" and expressing a commitment to jihadism and martyrdom in private messages to each other. Farook and Malik had traveled to Saudi Arabia in the years before the attack. The couple had amassed a large stockpile of weapons, ammunition, and bomb-making equipment in their home.

Enrique Marquez Jr., a friend and former neighbor of Farook, was investigated in connection with his purchase of the two rifles used in the attack. Marquez was arrested on December 17, 2015, and charged with three federal criminal counts: conspiracy to provide material support for terrorism, making a false statement in connection with acquisition of firearms, and immigration fraud. Federal prosecutors allege that in 2011, Farook and Marquez conspired to carry out shooting and bombing attacks, which they abandoned at the time.

The attack was the second-deadliest mass shooting in California after the 1984 San Ysidro McDonald's massacre, and the deadliest in the U.S. since the 2012 Sandy Hook Elementary School shooting. It was also the worst terrorist attack to occur in the U.S. since the September 11 attacks.

### Attack

Perpetrators Syed Rizwan Farook and Tashfeen Malik left their six-month-old daughter with Farook's mother at their Redlands home the morning of the attack, saying they were going to a doctor's appointment. Farook, a health inspector for the San Bernardino County Department of Public Health, attended a departmental event at the banquet room of the Inland Regional Center. The event began as a semi-annual all-staff meeting and training event, and was in the process of transitioning into a department holiday party/luncheon when the shooting began. There was a total of 91 invited guests, with 75–80 people stated to have been in attendance.

Coworkers reported that Farook had been quiet and left midway through the event. He posed for photos with other coworkers. At 10:59 am PST, Farook and Malik, armed with semi-automatic pistols and rifles, opened fire on those in attendance.

They wore ski masks and black tactical gear (including load-bearing vests holding magazines and ammunition), but not ballistic or bulletproof vests. The entire shooting took less than four minutes. They fired between 65 and 75 bullets. The perpetrators departed the scene before police arrived. An unidentified source told an NPR journalist that witnesses appeared to recognize Farook by his voice and build. Sources reported that Malik pledged *bay'ah* (allegiance) to the leader of ISIL on a Facebook account associated with her as the attack was underway.

Later reports described the posting as being made on behalf of both shooters. The perpetrators left three explosive devices connected to one another at the Inland Regional Center. The devices were described as pipe bombs constructed with Christmas lights and tied together, combined with a remote controlled car that was switched on. The poorly constructed devices failed to explode. Authorities believe that the pipe bombs were meant to target the emergency personnel responding to the scene. The device was hidden inside a canvas bag, and its build was similar to schematics published in Al Qaeda's *Inspire* magazine.

### **Police Response**

It took four minutes for the first police unit to respond to the shooting following the initial 911 emergency call. At 11:14 am, the San Bernardino Fire Department made a Twitter post about an emergency on the 1300 block of Waterman Avenue, with the police working to clear the scene. Roads in the area were closed to traffic.

Two police officers arrived almost simultaneously; when another officer arrived two minutes later, the three officers entered the building and began to evacuate the survivors. The San Bernardino SWAT team happened to be conducting its monthly training exercise a few miles away from the scene at the time of the attack, which allowed them to quickly arrive at the scene. Ultimately, about 300 officers and agents from city, county, state and federal agencies responded to the active-shooter event, converging on the scene as people were being evacuated.

Police used a battering ram to get into the complex. The FBI and the Los Angeles Police Department Counter-terrorism unit were called in to assist. Police were on the lookout for a black SUV used by the perpetrators to flee the scene.

The explosive devices placed by the perpetrators were later detonated by a bomb squad. The U.S. Department of Homeland Security sent a Pilatus PC-12 surveillance aircraft to the area, which circled the skies above San Bernardino for hours, mainly in the area where the shooting took place and in areas under investigation by police, and departed after the shootout between the perpetrators and police.

### **Shootout**

Law enforcement began the search for the suspects. A witness gave Farook's name to police, who quickly learned that he had rented a black Ford Expedition SUV with Utah license plates four days before the attack. Based on information provided by one of Farook's neighbors, officers went to the perpetrators' Redlands home on North Center Street for surveillance and gave chase when the perpetrators fled the house. At least one fake explosive—a metal pipe stuffed with cloth made to resemble a pipe bomb—was thrown at the police during the pursuit. After the SUV was stopped, the couple exchanged fire with police from inside their vehicle on East San Bernardino Avenue, about 1.7 miles (2.7 km) away from the scene of the mass shooting. It began around 3:00 pm, about four hours after the initial attack at the Inland Regional Center had begun. Police used multiple BearCat armored personnel carriers in confronting the shooters.



The shooters' Ford Expedition SUV, involved in the shootout. Released by the San Bernardino County Sheriff's Department.

The gunfire lasted for around five minutes before both perpetrators were killed. The sheriff's department confirmed that a man and a woman were killed.

One of the shooters died outside the SUV while getting out and trying to cross the street, while the other shooter died inside the vehicle.

Seven police agencies were involved in the final shootout, with 23 officers firing a combined total of approximately 380 rounds. The perpetrators fired 76 rifle rounds. During the shootout, police asked residents to stay indoors.

Initial news reports and witness accounts led to a search for up to three shooters, but police eventually determined that there were only two since only two firearms were used in the attack according to ballistics evidence.

Investigators in armored vehicles at the townhouse of the perpetrators considered ordering an evacuation, but instead ordered the neighborhood to shelter in place and cordoned off the area. From 4:00 pm – 5:30 pm, police asked residents of the area to stay in their homes with doors locked and secure after residents reported a person jumping fences. No one was found; the reports may have been from officers at the scene.

A person detained after running away from the scene of the shootout was thought to be a possible third suspect, but police determined that he was not connected to the shooting; the person was booked on an unrelated outstanding misdemeanor warrant.





## November 2015 Paris Attacks

On the evening of 13 November 2015, a series of coordinated terrorist attacks occurred in Paris and its northern suburb, Saint-Denis. Beginning at 21:20 CET, three suicide bombers struck near the Stade de France in Saint-Denis, followed by suicide bombings and mass shootings at cafés, restaurants and a music venue in central Paris.

The attackers killed 130 people, including 89 at the Bataclan theatre, where they took hostages before engaging in a stand-off with police. Another 368 people were injured, 80–99 seriously. Seven of the attackers also died, while the authorities continued to search for accomplices. The attacks were the deadliest on France since World War II, and the deadliest in the European Union since the Madrid train bombings in 2004. France had been on high alert since the January 2015 attacks on *Charlie Hebdo* offices and a Jewish supermarket in Paris that killed 17 people and wounded 22, including civilians and police officers.

The Islamic State of Iraq and the Levant (ISIL) claimed responsibility for the attacks, saying that it was in retaliation for the French airstrikes on ISIL targets in Syria and Iraq. The President of France, François Hollande, said the attacks were an act of war by ISIL planned in Syria, organized in Belgium, and perpetrated with French complicity.

In response, a three-month state of emergency was declared across the country to help fight terrorism, which involved the banning of public demonstrations, and allowing the police to carry out searches without a warrant, put anyone under house arrest without trial and block websites that encouraged acts of terrorism. On 15 November, France launched the biggest airstrike of Opération Chammal, its contribution to the anti-ISIL bombing campaign, striking ISIL targets in Al-Raqqah. On 18 November, the suspected lead operative of the attacks, Abdelhamid Abaaoud, was killed in a police raid in Saint-Denis, along with at least two other people.

### Attacks

#### Timeline of attacks

13 November:

- **21:20**– First suicide bombing near the Stade de France.
- **21:25** – Shooting at the rue Bichat.
- **21:30**– Second suicide bombing near the Stade de France.
- **21:32** – Shooting at the rue de la Fontaine-au-Roi.
- **21:36** – Shooting at the rue de Charonne.
- **21:40** – Suicide bombing on boulevard Voltaire.
- **21:40** – Three men enter the Bataclan theatre and begin shooting.
- **21:53** – Third suicide bombing near the Stade de France.
- **22:00** – Hostages are taken at the Bataclan.

14 November:

- **00:20** – Security forces enter the Bataclan.
- **00:58** – French police end the siege on the Bataclan.

All times are CET (UTC+1).

Three teams launched six distinct attacks: three suicide bombings in one attack, a fourth suicide bombing in another attack, and shootings at four locations in four separate attacks. Shootings were reported in the vicinity of the rue Alibert, the rue de la Fontaine-au-Roi, the rue de Charonne, the Bataclan theatre, and avenue de la République.

Three explosions occurred near the Stade de France, another on boulevard Voltaire, and two of the Bataclan shooters also detonated their suicide vests as police ended the stand-off. According to the Paris prosecutor, the attackers wore suicide vests that used acetone peroxide as an explosive.

### **Stade de France Explosions**



President François Hollande (pictured in 2013) was at the Stade de France during the attacks

Three explosions occurred near the country's national sports stadium, the Stade de France, in the suburb of Saint-Denis, resulting in four deaths, including the three suicide bombers. The explosions happened at 21:20, 21:30, and 21:53. The first explosion near the stadium was about 20 minutes after the start of an international friendly football match between France and Germany, which President Hollande was attending. The first bomber was prevented from entering the stadium after a security guard patted him down and discovered the suicide vest; a few seconds after being turned away, he detonated the vest, killing himself and a bystander.

Investigators later surmised that the first suicide bomber had planned to detonate his vest within the stadium, triggering the crowd's panicked exit onto the streets where two other bombers were lying in wait. Ten minutes after the first bombing, the second bomber blew himself up near the stadium. Another 23 minutes after that, the third bomber's vest detonated nearby; according to some reports, that location was at a McDonald's restaurant; others state that the bomb detonated some distance away from any discernible target.

Hollande was evacuated from the stadium at half-time, while the German foreign minister, Frank-Walter Steinmeier, remained at the stadium. Hollande met with his interior minister Bernard Cazeneuve to co-ordinate a response to the emergency. Two of the explosions were heard on the live televised broadcast of the match; both football coaches were informed by French officials of a developing crisis, but players and fans were kept unaware of it until the game had finished. Hollande, concerned that the safety of the crowd outside the stadium could not be assured if the match was immediately cancelled, decided that the game should continue without a public announcement.

Following the game, fans were brought onto the pitch to await evacuation as police monitored all the exits around the venue. Security sources said all three explosions were suicide bombings.

The German national football team was advised not to return to their hotel, where there had been a bomb threat earlier in the day, and they spent the night in the stadium on mattresses, along with the French team, who stayed with them in a display of camaraderie.

### **Restaurant shootings and bombing Rues Bichat and Alibert**

The first shootings occurred around 21:25 on the rue Bichat and the rue Alibert, near the Canal Saint-Martin in the 10th arrondissement. Attackers shot at people outside Le Carillon, a café and bar, before crossing the rue Bichat and shooting people inside the restaurant Le Petit Cambodge. According to French police, an eyewitness said one of the gunmen shouted "Allahu Akbar". *Le Monde* reported that 15 people were killed at these locations and 10 were critically injured. The assailants fled in one or two vehicles after the shootings. One vehicle had a Belgian number plate. Doctors and nurses from the nearby Hôpital Saint-Louis were in Le Carillon when the attacks happened and supplied emergency assistance to the wounded.

### **Rue de la Fontaine-au-Roi**

At 21:32, a man with a Kalashnikov rifle fired shots outside Café Bonne Bière, close to the terrace of the Italian restaurant La Casa Nostra, on the rue de la Fontaine-au-Roi where it intersects with the rue du Faubourg-du-Temple south of the rue Bichat. The Paris prosecutor said five people were killed and eight were injured. An eyewitness reported a gunman firing short bursts.

### **Rue de Charonne**

At approximately 21:36, two gunmen fired shots for several minutes at the outdoor terrace of the restaurant La Belle Équipe on the rue de Charonne in the 11th arrondissement where it intersects the rue Faidherbe, before returning to their car and driving away. Nineteen people were killed, and nine were left in critical condition.

### **Boulevard Voltaire bombing**

At about 21:40, on the boulevard Voltaire in the 11th arrondissement, near the place de la Nation, a man sat down in the Comptoir Voltaire café and placed an order before detonating his suicide vest, killing himself and injuring fifteen people, one of them seriously.

### **Bataclan Theatre Massacre**



The Bataclan theatre in 2009

At approximately 21:40, a mass shooting and hostage-taking occurred at the Bataclan theatre on the boulevard Voltaire in the 11th arrondissement. The American band "Eagles of Death Metal" was playing to an audience of around 1,500 people.

About an hour into the concert, a car pulled up outside the venue and three dark-clad men with AKM assault rifles entered the hall. Witnesses heard shouts of "Allahu Akbar" just before the gunmen took up positions on the mezzanine and opened fire on the crowd. Initially, the audience mistook the gunfire for pyrotechnics. The attack lasted 20 minutes, and witnesses also reported seeing the attackers throw hand grenades into the crowd. A radio reporter attending the concert described the attackers as calm and determined, telling CNN they had reloaded three or four times. Survivors escaped via the emergency exit into the street or made their way onto the roof, with some taking refuge in toilets and offices; others lay still on the floor pretending to be dead. The band's members escaped without injury.

Around 22:00, the attackers took 60–100 concertgoers hostage as police gathered outside the venue. They threatened to decapitate a hostage and throw the corpse out of the window every five minutes. A witness who escaped told a journalist that the gunmen had mentioned Syria. One witness in the Bataclan heard a gunman say, "This is because of all the harm done by Hollande to Muslims all over the world." There were further attacks on police and first responders who arrived at the scene.

Starting at 22:15, the Brigade of Research and Intervention (BRI) arrived on the scene, followed by the elite tactical unit, RAID. The assault on the theatre began at 00:20 and lasted three minutes. Police launched the assault because of reports that the attackers had started killing hostages. They initially estimated that 100 people had been killed, but the toll was revised to 89. Two attackers died by detonating their suicide vests. Another was hit by police gunfire and his vest blew up when he fell. Identification and removal of the bodies took 10 hours, a process made difficult because some audience members had left their identity papers in the theatre's cloakroom.

### **Perpetrators**

On 14 November, ISIL claimed responsibility for the attacks. François Hollande said ISIL organized the attacks with help from inside France. Claimed motives were an ideological objection to Paris as a capital of abomination and perversion, retaliation for airstrikes on ISIL in Syria and Iraq, and the foreign policy of Hollande in relation to Muslims worldwide. Shortly after the attacks, ISIL's media organ, the Al-Hayat Media Group, launched a website on the dark web extolling the organization and recommending the encrypted instant messaging service Telegram.

Fabien Clain released an audio recording the day before the attacks in which he personally claimed responsibility for the attacks. Clain is known to intelligence services as a veteran jihadist belonging to ISIL, and of French nationality.

Syrian and Egyptian passports were found near the bodies of two of the perpetrators at two attack sites, but Egyptian authorities said the passport belonged to a victim, Aleed Abdel-Razzak, and not one of the perpetrators. By 16 November, the focus of the French and Belgian investigation turned to Abdelhamid Abaaoud, the radical jihadist they believed was the leader of the plot. Abaaoud, a Belgian of Berber-Moroccan origin, had escaped to Syria after having been suspected in other plots in Belgium and France, including the thwarted 2015 Thalys train attack. Abaaoud had recruited an extensive network of accomplices, including two brothers, Brahim Abdeslam and Salah Abdeslam, to execute terrorist attacks. Abaaoud was killed in the Saint-Denis raid on 18 November.

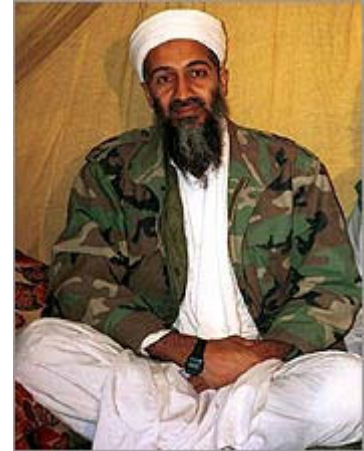
All of the known Paris attackers were EU citizens, who crossed borders without difficulty, albeit registered as terrorism suspects. According to the French prime minister, Manuel Valls, several of the perpetrators had exploited Europe's immigration crisis to enter the continent undetected.

## Al Qaeda

### U.S. Indictment: 'Detonated an Explosive Device'

The following is an excerpt from the indictment returned Wednesday in a Federal District Court in Manhattan against the Saudi exile, Osama bin-Laden:

At all relevant times from, in or about 1989 until the date of the filing of this indictment, an international terrorist group existed which was dedicated to opposing non-Islamic governments with force and violence. This organization grew out of the "mekhtab al khidemat" (the "Services Office") organization which had maintained offices in various parts of the world, including Afghanistan, Pakistan (particularly in Peshawar) and the United States, particularly at the Alkifah Refugee Center in Brooklyn, N.Y.



The group was founded by defendants Osama bin Laden and Muhammad Atef, a.k.a "Abu Hafs al-Masry," together with "Abu Ubaidah al-Banshiri" and others. From in or about 1989 until the present, the group called itself "Al Qaeda" ("the Base").

From 1989 until in or about 1991, the group (hereafter referred to as "Al Qaeda") was headquartered in Afghanistan and Peshawar, Pakistan. In or about 1991, the leadership of Al Qaeda, including its "emir" (or prince) defendant Osama bin Laden, relocated to Sudan. Al Qaeda was headquartered in the Sudan from approximately 1991 until approximately 1996 but still maintained offices in various parts of the world.

In 1996, defendants Osama bin Laden and Muhammad Atef and other members of Al Qaeda relocated to Afghanistan. At all relevant times, Al Qaeda was led by its emir, defendant Osama bin Laden. Members of Al Qaeda pledged an oath of allegiance (called a "bayat") to defendant Osama bin Laden and Al Qaeda.

Al Qaeda opposed the United States for several reasons. First, the United States was regarded as an "infidel" because it was not governed in a manner consistent with the group's extremist interpretation of Islam. Second, the United States was viewed as providing essential support for other "infidel" governments and institutions, particularly the governments of Saudi Arabia and Egypt, the nation of Israel and the United Nations organization, which were regarded as enemies of the group.

Third, Al Qaeda opposed the involvement of the United States armed forces in the [Persian] gulf war in 1991 and in Operation Restore Hope in Somalia in 1992 and 1993, which were viewed by Al Qaeda as pretextual preparations for an American occupation of Islamic countries.

In particular, Al Qaeda opposes the continued presence of American military forces in Saudi Arabia (and elsewhere on the Saudi Arabian peninsula) following the gulf war. Fourth, Al Qaeda opposed the United States Government because of the arrest, conviction and imprisonment of persons belonging to Al Qaeda or its affiliated terrorist groups or with whom it worked, including Sheik Omar Abdel Rahman.

One of the principal goals of Al Qaeda was to drive the United States armed forces out of Saudi Arabia (and elsewhere on the Saudi Arabian peninsula) and Somalia by violence. Members of Al Qaeda issued fatwahs (rulings of Islamic law) indicating that such attacks were both proper and necessary.

Al Qaeda functioned both on its own and through some of the terrorist organizations that operated under its umbrella, including: the Al Jihad group based in Egypt, led by, among others, Dr. Ayman al-Zawahiri, named as a co-conspirator but not as a defendant herein; the Islamic Group (also known as "El Gamaa Islamia" or simply "Gamaa't"), led by Sheik Omar Abdel Rahman and later by Ahmed Refai Taha, a.k.a. "Abu Yasser al-Masri," named as co-conspirators but not as defendants herein; and a number of jihad groups.

Osama bin Laden, the defendant, and Al Qaeda also forged alliances with the National Islamic Front in the Sudan and with representatives of the Government of Iran, and its associated terrorist group Hezbollah, for the purpose of working together against their perceived common enemies in the West, particularly the United States. . . .

On Oct. 3 and 4, 1993, in Mogadishu, Somalia, persons who had been trained by Al Qaeda (and by trainers trained by Al Qaeda) participated in an attack on United States military personnel serving in Somalia as part of Operation Restore Hope, which resulted in the killing of 18 United States Army personnel. . . .

On at least two occasions in the period from, in or about 1992 until in or about 1995, members of Al Qaeda transported weapons and explosives from Khartoum in the Sudan to the coastal city of Port Sudan for transshipment to the Saudi Arabian peninsula. . . .

At various times from at least as early as 1993, Osama bin Laden, the defendant, and others known and unknown, made efforts to obtain the components of nuclear weapons.

At various times from at least as early as 1993, Osama bin Laden, the defendant, and others known and unknown, made efforts to obtain the components of chemical weapons.

**Aug. 7, 1998**

On or about Aug. 7, 1998, in Nairobi, Kenya, and outside the jurisdiction of any particular state or district, Osama bin Laden . . . and others known and unknown . . . together with other members of Al Qaeda . . . detonated an explosive device that damaged and destroyed the United States Embassy in Nairobi, Kenya, and as a result of such conduct directly and proximately caused the deaths of at least 213 persons. . . .

On or about Aug. 7, 1998, in Dar es Salaam, Tanzania, and outside the jurisdiction of any particular state or district, Osama bin Laden . . . and others known and unknown . . . together with other members of Al Qaeda.

## World Trade Center 911

On the morning of September 11 two hijacked Boeing 767 commercial jetliners struck the towers. The airplanes were almost fully fueled, and the intense heat generated by the burning fuel melted the buildings' steel supporting beams.

The south tower stood for about 1 hour after the crash; the north tower for approximately 1 hour and 45 minutes. They then collapsed, floor upon floor, the added weight of each concrete floor causing floors beneath to collapse.

Tenants and visitors left the buildings by stairways, but not everyone was able to escape. Nearly 3,000 people died or were presumed dead as a result of the terrorist attack, including hundreds of firefighters and police who had arrived to help.

The buildings had been designed to withstand a collision from a jet plane, and they had survived a terrorist bomb attack in 1993.

But they could not withstand the heat of the burning fuel. All seven buildings in the complex collapsed during the disaster.



### World Trade Center 9-11-2001

Do you remember where you were on this day?

There are millions of nuts and people that do not believe this event happened and even worse, people that are glad this horrible event happened.

## Pentagon

On September 11, 2001, American Airlines Flight 77 was hijacked and crashed into the west side of the Pentagon in Arlington, Virginia. One hundred eighty-nine people were killed.



Pentagon in Arlington, Virginia

Stress that terrorism may be perpetrated by foreign or domestic individuals or groups. Point out that while the United States has not had as many terrorist incidents as some other countries, we have had several serious attacks, including:

- The bombing of the World Trade Center (1993).
- The bombing of the Murrah Federal Building in Oklahoma City (1995).
- The bombing at the Atlanta Olympic Games (1996).
- Bombings at family planning clinics and gay bars in the Atlanta area (1996 and 1997).
- The destruction of the World Trade Center and a portion of the Pentagon (2001).
- The sending of anthrax through the U.S. Mail (2001).



# FBI TEN MOST WANTED FUGITIVE

MURDER OF U.S. NATIONALS OUTSIDE THE UNITED STATES; CONSPIRACY TO MURDER U.S. NATIONALS OUTSIDE THE UNITED STATES; ATTACK ON A FEDERAL FACILITY RESULTING IN DEATH

## USAMA BIN LADEN *Killed May 1, 2011*



Date of Photograph Unknown

**Aliases:** Osama Bin Muhammad Bin Ladin, Shaykh Usama Bin Ladin, the Prince, the Emir, Abu Abdallah, Mujahid Shaykh, Hajj, the Director

### DESCRIPTION

<b>Date of Birth:</b>	1957	<b>Hair:</b>	Brown
<b>Place of Birth:</b>	Saudi Arabia	<b>Eyes:</b>	Brown
<b>Height:</b>	6' 4" to 6' 6"	<b>Complexion:</b>	Olive
<b>Weight:</b>	Approximately 160 pounds	<b>Sex:</b>	Male
<b>Build:</b>	Thin	<b>Nationality:</b>	Saudi Arabian
<b>Occupation:</b>	Unknown		
<b>Remarks:</b>	Bin Laden is the leader of a terrorist organization known as Al-Qaeda, "The Base". He is left-handed and walks with a cane.		
<b>Scars Marks:</b>	None		

### CAUTION

USAMA BIN LADEN IS WANTED IN CONNECTION WITH THE AUGUST 7, 1998, BOMBINGS OF THE UNITED STATES EMBASSIES IN DAR ES SALAAM, TANZANIA, AND NAIROBI, KENYA. THESE ATTACKS KILLED OVER 200 PEOPLE. IN ADDITION, BIN LADEN IS A SUSPECT IN OTHER TERRORIST ATTACKS THROUGHOUT THE WORLD.

**CONSIDERED ARMED AND EXTREMELY DANGEROUS**

Osama bin Laden, the mastermind of the most devastating attack on American soil in modern times and the most hunted man in the world, was killed in a firefight with United States forces in Pakistan, President Obama announced on Sunday night.

In a dramatic late-night appearance in the East Room of the White House, Mr. Obama declared that “justice has been done” as he disclosed that American military and C.I.A. operatives had finally cornered Bin Laden, the Al Qaeda leader who had eluded them for nearly a decade, in the early hours of Monday local time. American officials said Bin Laden resisted and was shot in the head. He was later buried at sea.

The news touched off an extraordinary outpouring of emotion as crowds gathered outside the White House, in Times Square and at the Ground Zero site, waving American flags, cheering, shouting, laughing and chanting, “U.S.A., U.S.A.!” In New York City, crowds sang “The Star-Spangled Banner.” Throughout downtown Washington, drivers honked horns deep into the night.



“For over two decades, Bin Laden has been Al Qaeda’s leader and symbol,” the president said in a statement televised around the world. “The death of Bin Laden marks the most significant achievement to date in our nation’s effort to defeat Al Qaeda. But his death does not mark the end of our effort. There’s no doubt that Al Qaeda will continue to pursue attacks against us. We must and we will remain vigilant at home and abroad.”

Bin Laden’s demise is a defining moment in the American-led fight against terrorism, a symbolic stroke affirming the relentlessness of the pursuit of those who attacked New York and Washington on Sept. 11, 2001.

What remains to be seen, however, is whether it galvanizes Bin Laden’s followers by turning him into a martyr or serves as a turning of the page in the war in Afghanistan and gives further impetus to Mr. Obama to bring American troops home.

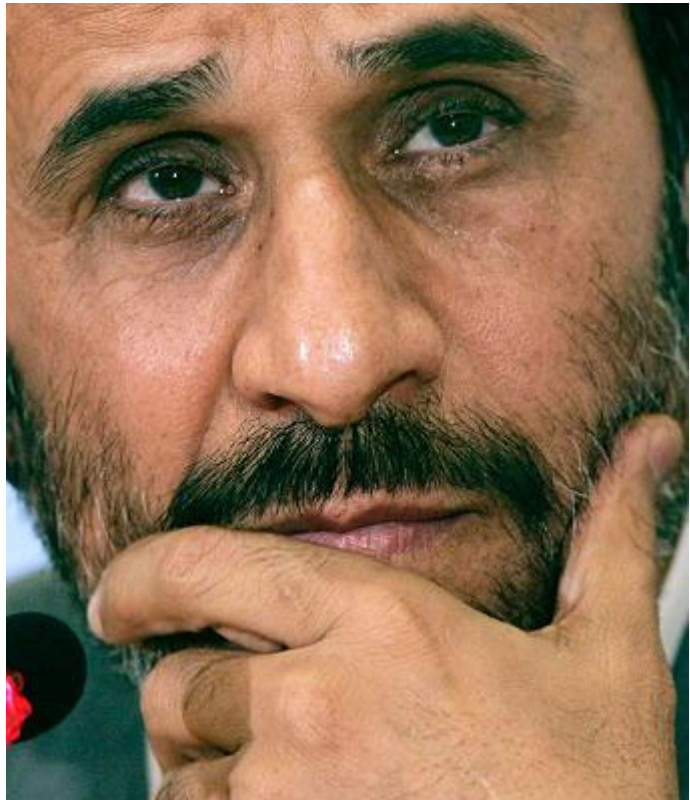
How much his death will affect Al Qaeda itself remains unclear. For years, as they failed to find him, American leaders have said that he was more symbolically important than operationally significant because he was on the run and hindered in any meaningful leadership role. And yet, he remained the most potent face of terrorism around the world and some of those who played down his role in recent years nonetheless celebrated his death.

Given Bin Laden’s status among radicals, the American government braced for possible retaliation. A senior Pentagon official said late Sunday that military bases in the United States and around the world were ordered to a higher state of readiness.

The State Department issued a worldwide travel warning, urging Americans in volatile areas “to limit their travel outside of their homes and hotels and avoid mass gatherings and demonstrations.”

## Mahmoud Ahmadinejad

Mahmoud Ahmadinejad (born 28 October 1956) is the sixth and current President of the Islamic Republic of Iran. He became president on 6 August 2005 after winning the 2005 presidential election by popular vote, the first president of the Islamic Republic not to be a religious cleric in 24 years. Prior to becoming president, Ahmadinejad served as mayor of Tehran, the governor general of Ardabil Province, and served in the Iran–Iraq War as a member of Army of the Guardians of the Islamic Revolution. He is not the most powerful official in Iran; that role belongs to the Supreme Leader of Iran, Ayatollah Ali Khamenei according to Article 113 of Constitution of Iran. Khamenei is the commander-in-chief of the armed forces of Iran and has the final word in all aspects of foreign and domestic policies.



Ahmadinejad is a critic of the George W. Bush Administration and supports strengthened relations with Russia, Venezuela, Syria, and the Persian Gulf states. He has said Iran's nuclear program is for peaceful purposes. He has also refused to end nuclear enrichment despite United Nations Security Council resolutions.

Ahmadinejad argues that the sanctions are "illegal", imposed by "arrogant powers", and that Iran has decided to pursue the monitoring of its nuclear program through "its appropriate legal path", the International Atomic Energy Agency.

He has called for the dissolution of the state of Israel and its government, which he does not regard as legitimate or representative of the population and for free elections in the region. He believes that the Palestinians need a stronger voice in the region's future. One of his most controversial statements was one in which, according to the initial Islamic Republic News Agency translation, he called for Israel to be "wiped off the map," though the interpretation of this quote is disputed. He has also been condemned for describing the Holocaust as a myth, which has led to accusations of anti-semitism; the interpretation of this quote is also disputed. In response to these criticisms, Ahmadinejad said "No, I am not anti-Jew, I respect them very much."

During his presidency, Ahmadinejad launched a gas rationing plan to reduce the country's fuel consumption and cut the interest rate for private and public banking facilities.

**“Nation will rise against nation, and kingdom against kingdom.” - Matthew 24:7**

## Shoe bomb suspect 'did not act alone'



***Hair and prints were reportedly found on Reid's shoes.***

The FBI has discovered forensic evidence that indicates alleged shoe bomber Richard Reid had help making the explosives found in his shoes on board an American-bound flight.

American news reports say hair and palm prints have been found on the shoes, which have been the subject of several tests since Mr. Reid's arrest on 22 December.

Mr. Reid, a Briton converted to Islam, allegedly tried to set fire to explosives in his shoes while on an American Airlines flight from Paris bound for Miami. He denies the charges.

He was overpowered by passengers and sedated by an on-board doctor until the flight was diverted to Boston's Logan Airport, where he was arrested.

American news channel CNN says the FBI has concluded that the presence of such samples means Mr. Reid was aided in assembling the bomb.

### **Powerful explosive**

Mr. Reid is said to have told investigators that he used a recipe from the internet to make a rare explosive known as TATP, or triacetone triperoxide.

He said he bought the ingredients from either a Czech or Slovak man in Amsterdam, one of the many places he traveled through. He also said that he acted alone.



Reid allegedly told investigators he had acted alone

The TATP would have been used to set alight more powerful explosives called PETN, which experts say would have been powerful enough to blow a hole in the side of the plane and cause it to crash. According to the French newspaper Le Parisien, the reported discovery of TATP links Mr. Reid to two Islamic fundamentalist groups linked to Osama Bin Laden's al-Qaeda network. Mr. Reid was formally charged last week in a Boston court with attempted murder and attempted destruction of an airliner.

## Moussaoui



### **Moussaoui: A catalogue of intelligence oversights**

US and UK authorities reportedly missed opportunities to investigate the first man charged with the terror attacks on the United States. Zacarias Moussaoui was arrested in the United States in August after flight instructors grew suspicious because he wanted to learn how to steer a plane - but not how to land or take off.

Questions are now being asked about why his arrest did not lead US investigators to uncover the 11 September hijack plot.

French security sources say they told the Federal Bureau of Investigation (**FBI**) of his suspected links with extremist groups - and that he had spent time in Afghanistan.

### **Immigration charges**

FBI director Robert Mueller said the authorities had decided in August that they lacked legal authority to search Mr. Moussaoui's computer. He was then being held on immigration charges. It was later found to contain information on flight training and crop spraying from planes.

His inquiries about hiring a crop duster plane are now being seen as possible evidence of a plot to spread chemical, biological or radioactive material in an American or western city.

### **French tip-offs 'ignored'**

Security sources in Paris say British police turned down French requests to question him in the 1990s - when he espoused radical Islam as a student in London. The sources said French authorities had alerted UK police after they detected that he had traveled to Afghanistan and Pakistan, the sources said.

The US indictment made public on Tuesday alleges that he spent time in terrorist training camps in Afghanistan. Mr. Moussaoui is alleged to have made the same preparations as the 19 hijackers suspected of carrying out the attacks.

### **Financial links alleged**

He is also said to have received money from the al-Qaeda network led by Osama Bin Laden - the man accused of masterminding the attacks.



Al Qaeda Prisoners that once swore allegiance to Osama Bin Laden and to kill Americans.



Explain that terrorist attacks can occur with or without warning. Because of the nature of terrorist attacks, they can—and are often intended to—result in:

- Mass casualties.
- Loss of critical resources.
- Disruption of vital services.
- Disruption of the economy.
- Individual and mass panic.

## Russia's Resurgence

Since Vladimir Putin became president of Russia, the fortunes of the nation seem to have turned around. Russia's oil production has increased dramatically, almost equaling so far this year that of the world's top oil producer, Saudi Arabia.

Russia is averaging 8.9 million barrels per day. At \$40-100 per barrel, this is infusing wealth very rapidly into Russia's economy. This, in turn, is allowing Putin to pour money into revitalizing Russia's military. Russia recently boasted that she has developed ballistic missile technology that can outwit any defensive system on earth. This is a clear challenge to the United States' planned \$50 billion anti-missile shield.

In Ezekiel 38, it is prophesied that "the chief prince of Meshech," also referred to as Gog and Magog, will lead the invasion of Israel at the Battle of Armageddon. *Webster's Third International Dictionary* defines Meshech as the word for Moscovi or Moscow.

Of course, Moscow is the capital of Russia. We know that the invasion of Israel described in Ezekiel 38-39 is the Battle of Armageddon since the "great supper of our God" is described as occurring in both the Gog-Magog War (Ezekiel39:17-20) and at Armageddon (Revelation 19:17-20).

### Terrorist Goals

- Mass casualties
- Loss of critical resources
- Disruption of vital services
- Disruption of the economy
- Individual and mass panic

### Vladimir Putin

Vladimir Vladimirovich Putin born 7 October 1952 in Leningrad, USSR; now Saint Petersburg, Russia) was the second President of Russia and is the current Prime Minister of Russia as well as chairman of United Russia and Chairman of the Council of Ministers of the Union of Russia and Belarus. He became acting President on 31 December 1999, when president Boris Yeltsin resigned in a surprising move, and then Putin won the 2000 presidential election. In 2004, he was re-elected for a second term lasting until 7 May 2008.

Due to constitutionally mandated term limits, Putin was ineligible to run for a third consecutive Presidential term.



After the victory of his successor, Dmitry Medvedev, in the 2008 presidential elections, he was then nominated by the latter to be Russia's Prime Minister; Putin took the post on 8 May 2008.

Upon graduation Putin was recruited into the KGB. In 1976 he completed the KGB retraining course in Okhta, Leningrad. Then, according to Yuri Felshtinsky and Vladimir Pribylovsky, he served at the Fifth Directorate of the KGB, which combated political dissent in the Soviet Union. According to The Washington Post, he was spying on foreigners in Leningrad. He then received an offer to transfer to foreign intelligence First Chief Directorate of the KGB and was sent for additional yearlong training to the Dzerzhinsky KGB Higher School in Moscow and then in the early eighties—the Red Banner Yuri Andropov KGB Institute in Moscow (now the Academy of Foreign Intelligence).

From 1985 to 1990 the KGB stationed Putin in Dresden, East Germany. Following the collapse of the East German regime, Putin was recalled to the Soviet Union and returned to Leningrad, where in June 1991 he assumed a position with the International Affairs section of Leningrad State University, reporting to Vice-Rector Yuriy Molchanov.

In his new position, Putin maintained surveillance on the student body and kept any eye out for recruits.

It was during his stint at the university that Putin grew reacquainted with Anatoly Sobchak, then mayor of Leningrad. Sobchak served as an Assistant Professor during Putin's university years and was one of Putin's lecturers. Putin formally resigned from the state security services on 20 August 1991, during the KGB-supported abortive putsch against Soviet President Mikhail Gorbachev.



On 16 October 2007 Putin visited Iran to participate in the Second Caspian Summit in Tehran, where he met with Iranian President Mahmoud Ahmadinejad. Other participants were leaders of Azerbaijan, Kazakhstan, and Turkmenistan. This is the first visit of a Soviet or Russian leader to Iran since Joseph Stalin's participation in the Tehran Conference in 1943.

At a press conference after the summit Putin said that "all our (Caspian) states have the right to develop their peaceful nuclear programmes without any restrictions". During the summit it was also agreed that its participants, under no circumstances, would let any third-party state use their territory as a base for aggression or military action against any other participant.



## Homegrown Terrorists Sub-Section

### Timothy McVeigh

Timothy McVeigh seemed just like any other boy while growing up, but at the age of 27, he committed the worst act of terrorism in U.S. history. The answers to why remain as elusive today as they back on April 19, 1995 when 168 people died in the Oklahoma City bombing.



McVeigh was born to an Irish Catholic family in Lockport, New York, and raised in nearby Pendleton, along with two sisters.

He was picked on by bullies at school, and took refuge in a fantasy world in which he retaliated against them; he would later come to regard the U.S. Government as the ultimate bully. He earned his high school diploma from Starpoint Central High School. His parents, Mildred Noreen ("Mickey") Hill and William McVeigh, divorced when he was ten years old. McVeigh was known throughout his life as a loner; his only known affiliations were voter registration with the Republican Party when he lived in New York, and a membership in the National Rifle Association while in the military. Despite the former, he self-identified as a libertarian in a statement that was reported by MSNBC.com and The Washington Post; and in 1996, while in federal prison, he voted for Libertarian candidate Harry Browne in the United States presidential election, 1996. The LP said that he violated the nonaggression principle and thus was not a true libertarian.

His grandfather introduced him to guns, with which he was fascinated. McVeigh told people he wanted to be a gun shop owner, and he sometimes took a gun to school to impress the other boys. McVeigh was also interested in computers, and he hacked into government computer systems on his Commodore 64, under the handle "The Wanderer," which was borrowed from the song by Dion DiMucci. In his senior year, he was named the school's "Most Promising Computer Programmer."

After graduating high school with honors, he became intensely interested in gun rights and the Second Amendment to the United States Constitution, and devoured right-wing, pro-militia magazines such as Soldier of Fortune. He went to work for Burke Armored Car Service. McVeigh was shy, and was said to have only one girlfriend during his high school years. He would later tell journalists that he always said the wrong thing to women he was trying to impress. According to his authorized biography, "his only sustaining relief from his unsatisfied sex drive was his even stronger desire to die."

McVeigh felt the need to personally reconnoiter sites of rumored conspiracies. He visited Area 51 in order to defy government restrictions on picture-taking, and went to Gulfport, Mississippi to determine the veracity of rumors about United Nations operations. These turned out to be false; the Soviet vehicles on the site were being configured for use in U.N.-sponsored humanitarian aid efforts.

Around this time, McVeigh and Nichols also began making bulk purchases of ammonium nitrate fertilizer for resale to survivalists, since rumor had it that the government was preparing to ban it.

According to McVeigh, he had a two-week affair with Marife Nichols; although she denies that it happened. McVeigh told Fortier of his plans to blow up a federal building, but Fortier declined to participate.



Fortier also told his wife about the plans. McVeigh composed two letters to the Bureau of Alcohol, Tobacco and Firearms, the first titled "Constitutional Defenders" and the second "ATF Read."

He denounced government agents as "fascist tyrants" and "storm troopers" and warned, "ATF, all you tyrannical mother fuckers will swing in the wind one day for your treasonous actions against the Constitution of the United States. Remember the Nuremberg War Trials. But...but...but...I only followed orders...Die, you spineless cowardice bastards."

## Theodore John Kaczynski

Accused of being the shadowy Unabomber who bedeviled authorities during an 18-year-long spate of bombings -- acquired a Harvard degree at age 20.

He could have had a dazzling academic career at one of the nation's top mathematics departments.

But he chose another path: that of a recluse who shunned family and friends. Some 18 months after Kaczynski's arrest at his remote, book-filled Montana cabin, the suspect has remained as silent in his prison cell as he had been during his 25-year-long, self-imposed exile.

To the FBI, Kaczynski, 55, was the prize at the end of the nation's longest, most expensive hunt for a serial killer.



Officials point to the mountain of evidence uncovered at the cabin -- including the master copy of the Unabomber manifesto and the typewriter used to create it.

In the eyes of federal investigators, Kaczynski is a cold, calculating, evil man whose contempt for technological advances led him to mastermind the bombings.



Dr. Theodore John Kaczynski (born May 22, 1942), also known as the Unabomber, is an American mathematician and social critic who carried out a campaign of bombings. He was born in Chicago, Illinois, and excelled in academics at a young age. Kaczynski received an undergraduate degree from Harvard University and earned a PhD in mathematics from the University of Michigan.

He became an assistant professor at the University of California, Berkeley at age 25 but resigned two years later. In 1971, he moved to a remote cabin in Lincoln, Montana. From 1978 to 1995, Kaczynski sent 16 bombs to targets including universities and airlines, killing three people and injuring 23.

Kaczynski sent a letter to The New York Times on April 24, 1995 and promised "to desist from terrorism" if The New York Times or The Washington Post published his manifesto. In his *Industrial Society and Its Future* (also called the "Unabomber Manifesto"), he argued that his bombings were extreme but necessary to attract attention to the erosion of human freedom necessitated by modern technologies requiring large-scale organization.

The Unabomber was the target of one of the most expensive investigations in the Federal Bureau of Investigation's (FBI) history. Before Kaczynski's identity was known, the FBI used the handle "UNABOM" ("UNiversity and Airline BOMber") to refer to his case, which resulted in the media calling him the Unabomber. Despite the FBI's efforts, he was not caught as a result of this investigation. Instead, his brother recognized Ted's style of writing and beliefs from the manifesto, and tipped off the FBI. To avoid the death penalty, Kaczynski entered into a plea agreement, under which he pled guilty and was sentenced to life in prison with no possibility of parole.

In 1995, Kaczynski mailed several letters, some to his former victims, outlining his goals and demanding that his 35,000-word paper *Industrial Society and Its Future* (also called the "Unabomber Manifesto") be printed verbatim by a major newspaper or journal; he stated that he would then end his terrorism campaign. There was a great deal of controversy as to whether it should be done.

A further letter threatening to kill more people was sent, and the United States Department of Justice recommended publication out of concern for public safety. The pamphlet was then published by The New York Times and The Washington Post on September 19, 1995, with the hope that someone would recognize the writing style.

Throughout the manuscript, produced on a typewriter without the capacity for italics, Kaczynski capitalizes entire words in order to show emphasis. He always refers to himself as either "we" or "FC" (Freedom Club), though he appears to have acted alone. It has been noted that Kaczynski's writing, while having irregular hyphenations, is virtually free of any spelling or grammatical error, in spite of its production on a manual typewriter without the benefit of a word processor or spell-checker.

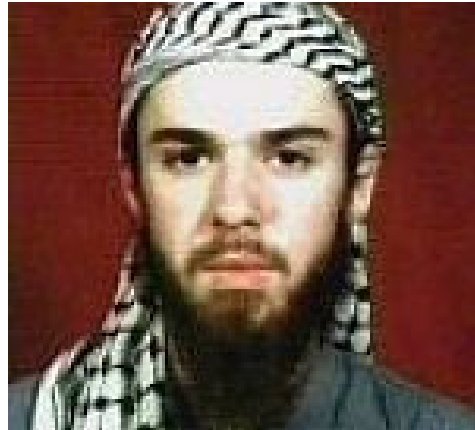
*Industrial Society and Its Future* begins with Kaczynski's assertion that "the Industrial Revolution and its consequences have been a disaster for the human race." The first sections of the text are devoted to psychological analysis of various groups—primarily leftists and scientists—and of the psychological consequences for the individual of life within the "industrial-technological system".

The later sections speculate about the future evolution of this system, argue that it will inevitably lead to the end of human freedom, call for a "revolution against technology", and attempt to indicate how that might be accomplished.

## John Walker Lindh

Spent his formative years in an affluent Northern California community known for its tolerance and open-mindedness. So how did he end up training in al Qaeda camps and fighting on the Taliban front lines in Afghanistan?

**"He's not someone that would, that I would have ever imagined, could pick up a gun at all,"** said his father Frank Lindh, who separated from Marilyn Walker about two years ago. An emotional Walker Lindh addressed a Virginia court at his sentencing hearing October 4, more than 10 months after U.S. military forces detained him in northern Afghanistan.



He apologized for fighting alongside the Taliban, saying, **"had I realized then what I know now ... I would never would have joined them."** The 21-year-old said Osama bin Laden is against Islam and that he "never understood jihad to mean anti-American or terrorism."

**"I understand why so many Americans were angry when I was first discovered in Afghanistan. I realize many still are, but I hope in time that feeling will change,"** he said in a 14-minute statement, according to the Associated Press.

Walker Lindh was sentenced to 20 years in prison as part of an agreement reached in July under which he pled guilty to one count of supplying services to the Taliban and a criminal information charge that he carried a rifle and two hand grenades while fighting against the U.S.-backed Northern Alliance.

As part of the plea deal, the government dropped all other counts in a lengthy criminal indictment, including one of the most serious charges -- conspiracy to kill U.S. nationals. CIA officer Johnny Michael Spann was killed in the Mazar-e Sharif uprising.

**"He was a soldier in the Taliban. He did it for religious reasons. He did it as a Muslim, and history overcame him,"** his attorney, James Brosnahan, said in July. **"John loves America,"** his father said. **"And we love America. God bless America."**

When found in Afghanistan by U.S. military forces in November 2001, Walker Lindh was shoeless, covered in dirt and lying in a hospital bed, where he was recovering from wounds received in the prison battle. Initially, Walker Lindh expressed reluctance to be taped, but with the camera rolling and lights on, he told his story to CNN. Bearded, his face coated in grime, he appeared exhausted as he described his battlefield experiences and his reasons for becoming a Taliban soldier.

**"I was a student in Pakistan, studying Islam,"** Walker-Lindh told CNN in a non-American accent, which he attributed to the fact he been speaking Arabic exclusively for months. **"I came into contact with many people who were connected with the Taliban."** **"I was in [Pakistan's] Northwest Frontier Province. The people there in general have a great love for the Taliban. So I started to read some of the literature of the scholars and my heart became attached to it. I wanted to help them one way or another."**

## Secret Documents

In secret documents summarizing his interrogations by U.S. troops and FBI officials, Walker Lindh said that he studied Arabic and Islam in Yemen starting in July 1998 and, after a brief return home to California, he returned to Yemen.

He went to Pakistan in October 2000 and joined a radical Islamic group, getting military training to fight against Indian forces in Kashmir. After becoming disillusioned with the cause, according to interrogation reports, Walker Lindh asked to join the Taliban.

Because he was not native to Afghanistan and did not speak the local languages, Walker Lindh said he joined the "**Arab group**" -- or al Qaeda, headed by bin Laden.

Aware of al Qaeda's anti-U.S. position, he agreed to attend their camp, the documents said.

Walker Lindh told interrogators that he declined to take part in operations against Israel and the United States, but continued with his training and even met bin Laden.

"At some point during the training, Lindh said he had been offered to swear allegiance to ... al Qaeda," an FBI document said. "***Lindh stated that he declined, however he swore allegiance to Jihad***" -- or holy war against enemies of Islam, as defined by al Qaeda.



## Inspired by 'Malcolm X' movie

Afghanistan was a long way from the Washington, D.C., suburb of Takoma Park, Maryland, where John Walker Lindh spent his earliest years.

His father was a Catholic who worked as a government lawyer, and his mother was a health care aide who became a follower of Buddhism. He was the middle of three children.

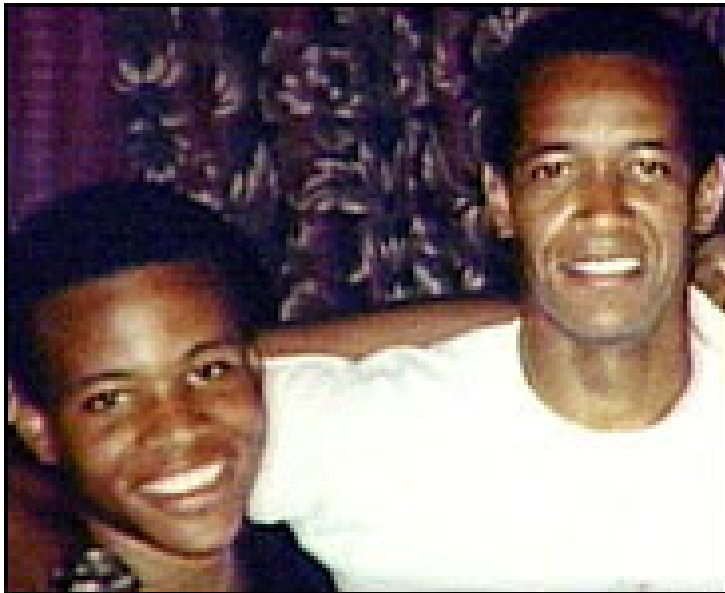
Walker Lindh told interrogators that bin Laden visited the camp several times, usually with one of his sons. Walker Lindh and four others met bin Laden on one occasion, and the al Qaeda leader "***made small talk and thanked them all for taking part in the Jihad***," according to the FBI report.

## Remorse and signs of regret

Shortly before Walker Lindh left for Afghanistan, he sent his parents an e-mail message saying he was heading to a cooler climate. Frank Lindh said he did not know that his son was in Afghanistan until he saw him on CNN.

## John Allen Muhammad and Lee Malvo

Oct. 24, 2002 — A former soldier and a teenager arrested in connection with the sniper hunt were being arraigned Thursday, as sources told NBC News the evidence against them included a rifle of the same caliber as the gun used in the killings and a car modified for easy shooting. Arrested as they slept in the car, the men were identified as John Allen Muhammad, 41, and Lee Malvo, 17. Said one law enforcement source: “***The general sentiment is we got our guys.***”



John Allen Muhammad, 42, right, and John Lee Malvo, 17, who officials described as Mr. Muhammad's stepson, were arrested on firearms charges unrelated to the sniper shootings, officials said.

Malvo was being arraigned as a material witness because he had refused to cooperate with authorities, NBC's Rehema Ellis reported from outside the federal courthouse in Baltimore. Muhammad was to be arraigned on an outstanding weapons warrant unrelated to the sniper case.

Police searched the car and found a Bushmaster rifle, one of the guns officials said is capable of firing a .223-caliber bullet — the type used in the sniper slayings. The rifle will be test-fired to compare the bullets to those recovered from the sniper victims, Williams said. Law enforcement sources told Williams that the car had been modified to make it easy for a person to shoot from the car without being detected. The back seat could be lowered and the trunk opened for a clear shot from the back of the car, the sources said.

The Associated Press reported that a rifle scope and tripod were also found in the car.

Initial reports said Muhammad is Malvo's stepfather, but federal sources later said that was not clear.

### Several Leads

Williams and NBC News' David Bloom cited sources as saying Malvo and Muhammad were tied to the sniper attacks by several leads:

A Tacoma, Wash., home where Muhammad once lived was searched Wednesday, and investigators found bullet fragments as well as a tree stump that had been used for target practice.

A caller to the FBI tip line trying to convince authorities he was the sniper told them to look into a Montgomery, Ala., shooting in September. Montgomery police were notified Sunday, and the city's mayor said Thursday that a fingerprint from Malvo was eventually detected on a magazine about weapons found near that scene.

Malvo's prints reportedly were also found on a piece of paper at one of the sniper crime scenes. A Jamaican bank account provided by the person communicating with police was tied to Malvo, said to have been born in Jamaica.

### How the men were taken

Muhammad and Malvo were taken into custody at 3:19 a.m. ET Thursday after a motorist at a rest stop spotted a car for which police had issued an all-points bulletin just three hours earlier. The alert included a vehicle description and license plate number.

The motorist called police around 1 a.m., and a SWAT team quickly converged on the scene to swoop down on the men.

Police closed off a portion of Interstate 70 near Myersville while they seized Muhammad and Malvo as they slept in a 1990 Chevrolet Caprice. Police said they were taken into custody without incident.

The men were then taken to Montgomery County, where the sniper investigation is based.

***"There's a strong feeling these people are related to the sniper shootings,"*** said Douglas Gansler, the state attorney for Montgomery County. Asked if he believed the sniper was still at large, he said ***"no."***

But two senior federal law enforcement officials told the Associated Press that investigators haven't ruled out the possibility that others gave them some help, in the form of vehicles or other support.

The car is registered to Muhammad in New Jersey — but also lists another man as a co-owner. Nothing more is known about the man at this time.



Bushmaster Rifle, civilian copy of the Military M-16, accurate to 1,000 yards.



## London Bombings July 7 - 21, 2005

The London attacks seem to reinforce previous targeting tactics of simultaneous attacks against civilian population centers and transportation systems. However, it is unclear whether the stations or the trains were the intended targets of the operation. As a result, although the devices used in the attacks exploded near network junctures -- places in the network where various modes of transportation infrastructure intersect -- there is no indication as to whether the proximity to the junctures was coincidental or planned.

Further, while the detonations of the devices were near-simultaneous, the detonation method for the devices has not been conclusively determined at this time in the investigation. Therefore, it is difficult to determine if the sequence of the improvised explosive device (IED) attacks may have been planned in advance and timed for maximum effect on London's transportation system.



### KNOWN TARGETS STRUCK

- Eastbound train between the Liverpool Street and Aldgate Stations – Liverpool Station is the fourth busiest in the London Underground network
- Southbound train approaching the Russell Square Station from King's Cross Station – King's Cross is the third busiest station in the Underground network and a major underground and railway exchange where commuter and long distance lines meet. Based on preliminary analysis, the casualties on the southbound train were higher partly because the bombings occurred in a "deep," limited clearance tunnel. These parts of the tunnel do not have ventilation shafts, escape hatches, or expansive clearance to dissipate the explosion. Several U.S. mass transit systems have similar tunnels.
- Westbound train near the Edgware Road Station – busy station with four underground lines.
- The number 30 bus near Tavistock Square.

### PERPETRATORS

There remain several unresolved questions regarding the motivations and objectives of the attackers, in addition to questions about the connections of these individuals to other Islamic extremists in or outside the U.K. While authorities received no advance warning of the attacks, archived police surveillance video shows four suspected suicide bombers arriving at the Luton Station, north of London, all wearing backpacks.

- Reporting indicates the four were British citizens.
- Investigators believe three of the four individuals boarded different trains departing King's Cross Station.

### ATTACK METHODOLOGY

The three underground explosions happened within 50 seconds of one another at 0850 local London time. The fourth individual boarded a public access double-decker bus serving the Hackney to Marble Arch route; the device exploded at approximately 0947 London time.

Open source and press speculation that the explosive device was designed to generate a secondary explosion targeting emergency response personnel or to inflict greater civilian casualties have not been confirmed.

### **IEDs**

The IEDs used in these attacks have been assessed as small and were carried in the terrorists' backpacks, but the types of explosives and detonators have not been confirmed. Although, the Department of Homeland Security (DHS) and the FBI do not believe the London attack necessarily presumes a similar attack against rail or mass transit targets in the United States, there has been consistent threat reporting for some time, suggesting that terrorists may have an interest in targeting mass transit systems.

### **INDICATORS OF SUICIDE BOMBERS**

The recent suicide bombings in London, as well as previous attacks in Iraq, Saudi Arabia, and other countries, demonstrate that suicide bombings remain a preferred method of attack among extremists. While not all suicide attacks involve bombs carried on an individual's person, the following are possible indicators that an individual is attempting to use his or her body as the delivery method for a bomb. Alone, each indicator can result from legitimate activities; however, multiple indicators may possibly suggest a suicide bomber.

- Wearing inappropriate attire such as loose or bulky clothing inconsistent with current weather conditions;
- Protruding bulges or exposed wires under clothing (possibly through the sleeve);
- Strange chemical odors;
- Sweating, mumbling, or unusually calm and detached behavior;
- Attempts to gain a position near crowds or VIPs;
- Tightened hands (may hold detonation device); or
- Wearing disguises appropriate to target areas to elude detection. Suicide bombers may disguise themselves with military, medic, firefighter, or police uniforms, or may pose as a pregnant woman. It is important to note that there is no clearly defined "profile" for a suicide bomber. Men, women, and older children have all been suicide bombers.

### **SECOND ATTACK JULY 21, 2005**

Explosions struck three London Underground stations and a bus at midday Thursday in a chilling but less deadly replay of the suicide bombings that killed 56 people two weeks ago. Only one person was reported wounded, but the explosions during the lunch hour caused major disruption in the city and were hauntingly similar to the July 7 bombings by four attackers. The London police commissioner confirmed Thursday that four explosions took place in what he described as "serious incidents."

"We've had four explosions — four attempts at explosions," Metropolitan Police

Commissioner Ian Blair said outside police headquarters at Scotland Yard. "At the moment the casualty numbers appear to be very low ... the bombs appear to be smaller" than the July 7 blasts. Meantime, police were searching a London hospital Thursday for a man wearing a blue shirt with wires protruding from a hole in the back, a TV report said. An internal memo at University College Hospital in north London urged staff to watch for the man, described as a black or Asian male, about 6-feet-2, Sky News television reported.



### **Reports of explosions, would-be bomber**

One witness told Sky TV that another subway passenger told him a backpack exploded at the Warren Street station and there were reports of smoke. Sky TV reported that police said no chemical agents were involved in the explosions. Explosions also were reported at the Shepherds Bush and Oval stations. Emergency teams were sent to all three stations after the incidents, which began at 12:38 p.m.

Witnesses said they had seen what could have been a would-be bomber running away after dropping a rucksack on one of the trains. "We all got off on the platform and the guy just ran and started running up the escalator," one witness, who gave her name as Andrea, told the BBC. "Everyone was screaming for someone to stop him. He ran past me...and he ran out of the station. In fact, he left a bag on the train," she said.

### **Bus blast**

Passengers were evacuated off a bus in Hackney, east London, and police cordoned off streets nearby. The bus company said a blast blew out the windows of the bus but a police officer on the scene said there were no signs of damage. A police officer told Reuters: "The bus driver heard a bang at the back of the bus. He thought it was probably a vehicle that had hit him. "He stopped at a nearby bus stop and saw a suspect package at the back of the bus." The fire brigade put on protective clothing before moving towards the bus. Closed-circuit TV cameras on Hackney Road showed the No. 26 bus immobilized at a stop with its indicator lights flashing. The area around the bus had been cordoned off. Prime Minister Tony Blair canceled his afternoon appointments as the developments unfolded.

### **PROTECTIVE MEASURES AGAINST SUICIDE BOMBERS**

Suicide bombings have produced a number of complex challenges for all sectors, principally the emergency services and private sectors. DHS and the FBI recommend the following protective measures for all applicable sectors. The overarching objective for implementing protective measures against a suicide bomber is to thwart potential attacks.

**To employ an effective process, a phased approach is recommended using the following steps:**

- a. Prevention
- b. Detection
- c. Challenge
- d. Response

#### **Prevention Phase:**

- Establish a public relations campaign that reinforces public awareness of a potential threat;
- Maintain a police presence at various locations within a venue, specifically all entrance sites and choke points;
- Review counter-surveillance procedures;
- Identify and pre-designate avenues of evacuation;
- Review crowd control protocols to assist with overall counter-surveillance requirements.

#### **Detection Phase:**

- Conduct random canine searches to avoid taxing valuable resources, stagger search times and patterns as part of counter-surveillance measures;
- Initiate evacuation protocols.

**Challenge Phase:**

- Review and identify measures for challenging a potential suicide bomber;
- Make approaches and negotiations by remote means.

**Response Phase:**

- Be aware of the potential for a secondary bomber or additional explosions;
- Be cognizant of remote initiation of a suicide device, anti-tamper devices, or a timer back-up should the bomber fail to initiate the device.

**SUMMARY**

Police in Pakistan have made what they call an important arrest in the search for the mastermind behind the London bombing attacks. Pakistan, cooperating with British investigators, used a list of telephone numbers to determine who might have had contact with the suspected suicide bombers. London newspapers identify the suspect arrested in Pakistan as Haroon Rashid Aswat. He reportedly visited the British hometowns of all four bombers and selected the targets.

**Haunting similarities**

The incidents paralleled the blasts two weeks ago, which involved explosions at three Underground stations simultaneously — quickly followed by a blast on a bus. Those bombings, during the morning rush hour, also occurred in the center of London, hitting the Underground railway from various directions. Thursday's incidents, however, were more geographically spread out. London Ambulance said it was called to the Oval station at 12:38 p.m. and Warren Street at 12:45 p.m. The July 7 attacks began at 8:51 a.m. "People were panicking. But very fortunately the train was only 15 seconds from the station," witness Ivan McCracken told Sky news. McCracken said another passenger at Warren Street claimed he had seen a backpack explode. The bombs which killed 56 people on board three underground trains and a bus in London on July 7 were carried in backpacks, police said.

**REPORTING NOTICE**

DHS and FBI encourage recipients of this document to report information concerning suspicious or criminal activity potentially related to terrorism to the local FBI Joint Terrorism Task Force (JTTF) – the FBI regional phone numbers can be found online at <http://www.fbi.gov/contact/fo/fo.htm> and the Homeland Security Operations Center (HSOC). The HSOC can be reached via telephone at 202-282-8101 or by email at [HTUHSCenter@dhs.gov](mailto:HTUHSCenter@dhs.gov). For transportation suspicious incidents and threat reporting contact the Transportation Security Operations Center (TSOC) at 703-563-3236/3237 and email [TSCC@tsa.dot.gov](mailto:TSCC@tsa.dot.gov).

## ANTIFA



The logo as it appears on a flag held by an antifa member in Cologne, Germany in 2008



Logo of *Antifaschistische Aktion*, the militant anti-fascist network in 1930s Germany that inspired the antifa movement.

The antifa movement is composed of left-wing, autonomous, militant anti-fascist groups and individuals in the United States. The principal feature of antifa groups is their use of direct action, with conflicts occurring both online and in real life. They engage in varied protest tactics, which include digital activism, property damage, physical violence, and harassment against those whom they identify as fascist, racist, or on the far-right.

Activists involved in the movement tend to be anti-capitalists and subscribe to a range of ideologies, typically on the left. They include anarchists, socialists and communists along with some liberals and social democrats. Their stated focus is on fighting far-right and white supremacist ideologies directly, rather than through electoral means.

## **History**

When Italian dictator Benito Mussolini consolidated power under his National Fascist Party in the mid-1920s, an oppositional anti-fascist movement surfaced both in Italy and countries such as the United States. Many anti-fascist leaders in the United States were syndicalist, anarchist, and socialist émigrés from Italy with experience in labor organizing and militancy. Ideologically, antifa in America sees itself as the successor to anti-Nazi activists of the 1930s; European activist groups that originally organized to oppose World War II-era fascist dictatorships re-emerged in the 1970s and 1980s to oppose white supremacy and skinheads and eventually spread to America. After World War II, but prior to the development of the modern antifa movement, violent confrontations with fascist elements continued sporadically.

Modern antifa politics can be traced to opposition to the infiltration of Britain's punk scene by white power skinheads in the 1970s and 1980s, and the emergence of neo-Nazism in Germany following the fall of the Berlin Wall. In Germany, young leftists, including anarchists and punk fans, renewed the practice of street-level anti-fascism. Columnist Peter Beinart writes that "in the late '80s, left-wing punk fans in the United States began following suit, though they initially called their groups Anti-Racist Action (ARA) on the theory that Americans would be more familiar with fighting racism than they would be with fighting fascism."

Dartmouth College historian Mark Bray, author of *Antifa: The Anti-Fascist Handbook*, credits ARA as the precursor of the modern US antifa groups in the United States and Canada. In the late 1980s and 1990s, ARA activists toured with popular punk rock and skinhead bands in order to prevent Klansmen, neo-Nazis and other assorted white supremacists from recruiting. Their motto was "We go where they go" by which they meant that they would confront far-right activists in concerts and actively remove their materials from public places. In 2002, the ARA disrupted a speech in Pennsylvania by Matthew F. Hale, the head of the white supremacist group World Church of the Creator, resulting in a fight and twenty-five arrests. One of the earliest antifa groups in the U.S. was Rose City Antifa, which was formed in Portland, Oregon in 2007.

Other antifa groups in the U.S. have other genealogies, for example in Minneapolis, Minnesota, where a group called the Baldies was formed in 1987 with the intent to fight neo-Nazi groups directly.

## **Terminology**

The English word antifa is a loanword from German, taken from an abbreviation of the word antifaschistisch ("anti-fascist") and the name of Antifaschistische Aktion. Oxford Dictionaries, which placed "antifa" on its shortlist for word of the year in 2017, said the word "emerged from relative obscurity to become an established part of the English lexicon over the course of 2017". The Anti-Defamation League makes a point that the label "antifa" should be limited to "those who proactively seek physical confrontations with their perceived fascist adversaries," and not be misapplied to include all counter-protesters.



### **Recent ANTIFA Headline**

August 17, 2019 -Violent Antifa protests are breaking out in Portland, Oregon, following the pre-planned “End of Domestic Terrorism” event taking place in the city. City officials have been preparing for the potential of dueling clashes, with the police force at the ready and additional agencies on standby.

According to journalist and editor of Quillette, Andy Ngo, – who warned that Saturday’s events had the potential to be a “powder keg” – things are already taking a violent turn. Man was beaten and maced by Antifa. He wandered off dazed and bloodied and collapsed in a parking lot. No authorities have helped him yet.

Video footage from Saturday’s “End Domestic Terrorism” rally in Portland, Oregon, shows dozens of Antifa members surrounding and attacking a pair of patriot demonstrators – one of which was clad in a Roman gladiator outfit – with unknown liquids as he fends off the violent group away from his young female companion, presumably his daughter.





## Homeland Security Section - Introduction

Our Nation learned a terrible lesson on September 11. American soil is not immune to evil or cold-blooded enemies capable of mass murder and terror. The worst of these enemies—and target number one in our war on terrorism—is the terrorist network Al-Qaeda. Yet the threat to America is not limited to Al-Qaeda or to suicide hijackings of commercial aircraft. The threat is much broader, as we learned on October 4, 2001, when we discovered that a life-threatening biological agent—anthrax—was being distributed through the U.S. mail.

Unless we act to prevent it, a new wave of terrorism, potentially involving the world's most destructive weapons, looms in America's future. It is a challenge as formidable as any ever faced by our Nation. But we are not daunted. We possess the determination and the resources to defeat our enemies and secure our homeland against the threats they pose.

Today's terrorists can strike at any place, at any time, and with virtually any weapon. Securing the American homeland is a challenge of monumental scale and complexity. But the U.S. government has no more important mission.



### Anthrax Letters





A huge high pressure sewer line has ruptured. This looks like a water line break, but it isn't. It is a nightmare and it happens throughout our nation. Most of us will not report this event to the government agencies because we are fearful of the penalties. It seems strange that we are required to report these events but we do not want to lose our jobs or be punished with fines. So instead of reporting, most of us, kind of hide or make-up an excuse not to report the event. Nevertheless, you will be caught one day and you will pay a huge price for not reporting a massive sewage spill. My suggestion is that we as water/wastewater professionals need to have a better relationship with the governing agencies.

This is very difficult to develop, hopefully the governing agencies will open their eyes and become reasonable towards us and receive these reports as professionals and treat us as so.

Are you prepared to deal with a terrorist damaging your system? Well the Government believes that this event could happen. Plans for this type of destruction have been found and currently information suggests that the sewer system is the most likely and most vulnerable target in the U.S. Think of the diseases that would spread within a very short period of time. Plus, this event would impact the entire potable water system.

## Homeland Security Presidential Directive

### Purpose

The Nation requires a Homeland Security Advisory System to provide a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to Federal, State, and local authorities and to the American people.

Such a system would provide warnings in the form of a set of graduated "**Threat Conditions**" that would increase as the risk of the threat increases. At each Threat Condition, Federal departments and agencies would implement a corresponding set of "**Protective Measures**" to further reduce vulnerability or increase response capability during a period of heightened alert.

This system is intended to create a common vocabulary, context, and structure for an ongoing national discussion about the nature of the threats that confront the homeland and the appropriate measures that should be taken in response. It seeks to inform and facilitate decisions appropriate to different levels of government and to private citizens at home and at work.

### Homeland Security Advisory System *Old System out dated 4/20/2011*

The Homeland Security Advisory System shall be binding on the executive branch and suggested, although voluntary, to other levels of government and the private sector. There are five Threat Conditions, each identified by a description and corresponding color. From lowest to highest, the levels and colors are:

**Low = Green;**  
**Guarded = Blue;**  
**Elevated = Yellow;**  
**High = Orange;**  
**Severe = Red.**

The higher the Threat Condition, the greater the risk of a terrorist attack. Risk includes both the probability of an attack occurring and its potential gravity. Threat Conditions shall be assigned by the Attorney General in consultation with the Assistant to the President for Homeland Security.

Except in exigent circumstances, the Attorney General shall seek the views of the appropriate Homeland Security Principals or their subordinates, and other parties as appropriate, on the Threat Condition to be assigned.

Threat Conditions may be assigned for the entire Nation, or they may be set for a particular geographic area or industrial sector. Assigned Threat Conditions shall be reviewed at regular intervals to determine whether adjustments are warranted.

For facilities, personnel, and operations inside the territorial United States, all Federal departments, agencies, and offices other than military facilities shall conform their existing threat advisory systems to this system and henceforth administer their systems consistent with the determination of the Attorney General with regard to the Threat Condition in effect.

Over the last year, you probably have grown tired or used to these warnings.

### **Threat Condition**

The assignment of a Threat Condition shall prompt the implementation of an appropriate set of Protective Measures. Protective Measures are the specific steps an organization shall take to reduce its vulnerability or increase its ability to respond during a period of heightened alert. The authority to craft and implement Protective Measures rests with the Federal departments and agencies. It is recognized that departments and agencies may have several preplanned sets of responses to a particular Threat Condition to facilitate a rapid, appropriate, and tailored response.

Department and agency heads are responsible for developing their own Protective Measures and other antiterrorism or self-protection and continuity plans, and resourcing, rehearsing, documenting, and maintaining these plans. Likewise, they retain the authority to respond, as necessary, to risks, threats, incidents, or events at facilities within the specific jurisdiction of their department or agency, and, as authorized by law, to direct agencies and industries to implement their own Protective Measures.

### **Protective Measures**

They shall continue to be responsible for taking all appropriate proactive steps to reduce the vulnerability of their personnel and facilities to terrorist attack. Federal department and agency heads shall submit an annual written report to the President, through the Assistant to the President for Homeland Security, describing the steps they have taken to develop and implement appropriate Protective Measures for each Threat Condition. Governors, mayors, and the leaders of other organizations are encouraged to conduct a similar review of their organizations' Protective Measures.

The decision whether to publicly announce Threat Conditions shall be made on a case-by-case basis by the Attorney General in consultation with the Assistant to the President for Homeland Security. Every effort shall be made to share as much information regarding the threat as possible, consistent with the safety of the Nation. The Attorney General shall ensure, consistent with the safety of the Nation, that State and local government officials and law enforcement authorities are provided the most relevant and timely information.

The Attorney General shall be responsible for identifying any other information developed in the threat assessment process that would be useful to State and local officials and others and conveying it to them as permitted consistent with the constraints of classification. The Attorney General shall establish a process and a system for conveying relevant information to Federal, State, and local government officials, law enforcement authorities, and the private sector expeditiously.

The Director of Central Intelligence and the Attorney General shall ensure that a continuous and timely flow of integrated threat assessments and reports is provided to the President, the Vice President, Assistant to the President and Chief of Staff, the Assistant to the President for Homeland Security, and the Assistant to the President for National Security Affairs. Whenever possible and practicable, these integrated threat assessments and reports shall be reviewed and commented upon by the wider interagency community.

A decision on which Threat Condition to assign shall integrate a variety of considerations. This integration will rely on qualitative assessment, not quantitative calculation.

# NTAS GUIDE

## National Terrorism Advisory System Public Guide

April 2011

### **The National Terrorism Advisory System**

The National Terrorism Advisory System, or NTAS, replaces the color-coded Homeland Security Advisory System (HSAS). This new system will more effectively communicate information about terrorist threats by providing timely, detailed information to the public, government agencies, first responders, airports and other transportation hubs, and the private sector.

It recognizes that Americans all share responsibility for the nation's security, and should always be aware of the heightened risk of terrorist attack in the United States and what they should do.

"The terrorist threat facing our country has evolved significantly over the past ten years, and in today's environment – more than ever – we know that the best security strategy is one that counts on the American public as a key partner in securing our country," said Secretary Napolitano. "The National Terrorism Advisory System, which was developed in close collaboration with our federal, state, local, tribal and private sector partners, will provide the American public with information about credible threats so that they can better protect themselves, their families, and their communities."

Under NTAS, DHS will coordinate with other federal entities to issue detailed alerts to the public when the federal government receives information about a credible terrorist threat.

NTAS alerts provide a concise summary of the potential threat including geographic region, mode of transportation, or critical infrastructure potentially affected by the threat, actions being taken to ensure public safety, as well as recommended steps that individuals, communities, business and governments can take to help prevent, mitigate or respond to a threat. NTAS Alerts will include a clear statement on the nature of the threat, which will be defined in one of two ways:

"Elevated Threat": Warns of a credible terrorist threat against the United States

“Imminent Threat”: Warns of a credible, specific, and impending terrorist threat against the United States

### **NTAS Alerts**

After reviewing the available information, the Secretary of Homeland Security will decide, in coordination with other Federal entities, whether an NTAS Alert should be issued.

### **Imminent Threat Alert**

Warns of a credible, specific, and impending terrorist threat against the United States.

### **Elevated Threat Alert**

Warns of a credible terrorist threat against the United States.

NTAS Alerts will only be issued when credible information is available.

These alerts will include a clear statement that there is an imminent threat or elevated threat. Using available information, the alerts will provide a concise summary of the potential threat, information about actions being taken to ensure public safety, and recommended steps that individuals, communities, businesses and governments can take to help prevent, mitigate or respond to the threat.

The NTAS Alerts will be based on the nature of the threat: in some cases, alerts will be sent directly to law enforcement or affected areas of the private sector, while in others, alerts will be issued more broadly to the American people through both official and media channels.

### **Sunset Provision**

An individual threat alert is issued for a specific time period and then automatically expires. It may be extended if new information becomes available or the threat evolves.

NTAS Alerts contain a sunset provision indicating a specific date when the alert expires - there will not be a constant NTAS Alert or blanket warning that there is an overarching threat. If threat information changes for an alert, the Secretary of Homeland Security may announce an updated NTAS Alert. All changes, including the announcement that cancels an NTAS Alert, will be distributed the same way as the original alert.

### **The NTAS Alert – How can you help?**

Each alert provides information to the public about the threat, including, if available, the geographic region, mode of transportation, or critical infrastructure potentially affected by the threat; protective actions being taken by authorities, and steps that individuals and communities can take to protect themselves and their families, and help prevent, mitigate or respond to the threat.

## **Terrorism Information**

Terrorism information and intelligence is based on the collection, analysis and reporting of a range of sources and methods. While intelligence may indicate that a threat is credible, specific details may still not be known. As such, Americans should continue to stay informed and vigilant throughout the duration of an NTAS Alert.

Citizens should report suspicious activity to their local law enforcement authorities. The “If You See Something, Say Something” campaign across the United States encourages all citizens to be vigilant for indicators of potential terrorist activity, and to follow NTAS Alerts for information about threats in specific places or for individuals exhibiting certain types of suspicious activity.

Visit [www.dhs.gov/ifyouseesomethingsaysomething](http://www.dhs.gov/ifyouseesomethingsaysomething) to learn more about the campaign.

## **Alert Announcements**

NTAS Alerts will be issued through state, local and tribal partners, the news media and directly to the public via the following channels:

- Via the official DHS NTAS webpage – <http://www.dhs.gov/alerts>
- Via email signup at – <http://www.dhs.gov/alerts>
- Via social media
  - o Facebook – <http://facebook.com/NTASAlerts>
  - o Twitter – <http://www.twitter.com/NTASAlerts>
- Via data feeds, web widgets and graphics o <http://www.dhs.gov/alerts>

The public can also expect to see alerts in places, both public and private, such as transit hubs, airports and government buildings.

## **Frequently Asked Questions**

### **Q – What will happen to the color-coded advisory system?**

A - The new National Terrorism Advisory System replaces the Homeland Security Advisory System that has been in place since 2002. The National Terrorism Advisory System, or NTAS, will include information specific to the particular credible threat, and will not use a color-coded scale.

### **Q – How does the new system work?**

A – When there is credible information about a threat, an NTAS Alert will be shared with the American public. It may include specific information, if available, about the nature of the threat, including the geographic region, mode of transportation, or critical infrastructure potentially affected by the threat, as well as steps that individuals and communities can take to protect themselves and help prevent, mitigate or respond to the threat.

The advisory will clearly indicate whether the threat is Elevated, if we have no specific information about the timing or location, or Imminent, if we believe the threat is impending or very soon.

**Q – As a citizen, how will I find out that an NTAS Alert has been announced?**

A – The Secretary of Homeland Security will announce the alerts publically. Alerts will simultaneously be posted at [DHS.gov/alerts](https://www.dhs.gov/alerts) and released to the news media for distribution. The Department of Homeland Security will also distribute alerts across its social media channels, including the Department’s blog, Twitter stream, Facebook page, and RSS feed.

**Q - What should Americans do when an NTAS Alert is announced?**

A – The NTAS Alert informs the American public about credible terrorism threats, and encourages citizens to report suspicious activity. Where possible and applicable, NTAS Alerts will include steps that individuals and communities can take to protect themselves to help prevent, mitigate or respond to the threat. Individuals should review the information contained in the alert, and based upon the circumstances, take the recommended precautionary or preparedness measures for themselves and their families.

**Q – How should I report suspicious activity?**

A – Citizens should report suspicious activity to their local law enforcement authorities. The “If You See Something, Say Something” campaign across the United States encourages all citizens to be vigilant for indicators of potential terrorist activity, and to follow NTAS Alerts for information about threats in specific places or for individuals exhibiting certain types of suspicious activity.

**Q - I get my news online, so how will I find out about an NTAS Alert?**

A – Americans can go to [DHS.gov/alerts](https://www.dhs.gov/alerts) to see the most recent advisories. Additionally, advisories will be sent out widely through social and mainstream media.

**7. Q - How will NTAS Alerts be cancelled or updated?**

A – The NTAS Alerts carry an expiration date and will be automatically cancelled on that date. If the threat information changes for an alert, the Secretary of Homeland Security may announce an updated NTAS Alert. All changes, including the announcement that cancels an NTAS Alert, will be distributed the same way as the original alert.

**8. Q - Do these alerts apply to Americans in other countries?**

A – NTAS Alerts apply only to threats in the United States and its possessions. The Department of State issues security advisory information for U.S. citizens overseas or traveling in foreign countries.

If You See Something, Say Something Report suspicious activity to local law enforcement or call 911. The National Terrorism Advisory System provides Americans with alert information on homeland security threats. It is distributed by the Department



of Homeland Security. More information is available at: [www.dhs.gov/alerts](http://www.dhs.gov/alerts). To receive mobile updates: [www.twitter.com/NTASAlerts](http://www.twitter.com/NTASAlerts)

### **STAY INFORMED**

- This section notifies the public about where to get more information.
- It encourages citizens to stay informed about updates from local public safety and community leaders.
- It includes a link to the DHS NTAS website <http://www.dhs.gov/alerts> and <http://twitter.com/NTASAlerts>

### **AFFECTED AREAS**

This section includes visual depictions (such as maps or other graphics) showing the affected location(s), sector(s), or other illustrative detail about the threat itself.

### **DURATION**

An individual threat alert is issued for a specific time period and then automatically expires. It may be extended if new information becomes available or the threat evolves.

### **DETAILS**

- This section provides more detail about the threat and what the public and sectors need to know.
- It may include specific information, if available, about the nature and credibility of the threat, including the critical infrastructure sector(s) or location(s) that may be affected.
- It includes as much information as can be released publicly about actions being taken or planned by authorities to ensure public safety, such as increased protective actions and what the public may expect to see.

### **SUMMARY**

The Secretary of Homeland Security informs the public and relevant government and private sector partners about a potential or actual threat with this alert, indicating whether there is an “imminent” or “elevated” threat. If You See Something Say Something used with permission of the NY Metropolitan Transportation Authority.

DATE & TIME ISSUED: XXXX



*Practice, Practice, Practice...*  
Fire Drill, Evacuation Drill, Workplace Violence Drill, Chemical Spill Drill,  
Intrusion Drill, Bomb Drill, Electrical Failure Drill

## Homeland Security - Defined (Older Policy, new policy is still being refined)

In the aftermath of September 11, “**homeland security**” has come to mean many things to many people. It is a new mission and a new term. The federal government defines homeland security as follows:

***Each phrase in the definition has meaning.***

***Concerted national effort.*** The federal government has a critical role to play in homeland security. Yet the nature of American society and the structure of American governance make it impossible to achieve the goal of a secure homeland through federal executive branch action alone.

The Administration’s approach to homeland security is based on the principles of shared responsibility and partnership with the Congress, state and local governments, the private sector, and the American people.

The ***National Strategy for Homeland Security*** belongs and applies to the Nation as a whole, not just to the President’s proposed Department of Homeland Security or the federal government.

***Prevent.*** The first priority of homeland security is to prevent terrorist attacks. The United States aims to deter all potential terrorists from attacking America through our uncompromising commitment to defeating terrorism wherever it appears. We also strive to detect terrorists before they strike, to prevent them and their instruments of terror from entering our country, and to take decisive action to eliminate the threat they pose. These efforts—which will be described in both the ***National Strategy for Homeland Security*** and the ***National Strategy for Combating Terrorism***—take place both at home and abroad. The nature of modern terrorism requires a global approach to prevention.

The ***National Strategy for Homeland Security*** attaches special emphasis to preventing, protecting against, and preparing for catastrophic threats. The greatest risk of mass casualties, massive property loss, and immense social disruption comes from weapons of mass destruction, strategic information warfare, attacks on critical infrastructure, and attacks on the highest leadership of government.

***Terrorist attacks.*** Homeland security is focused on terrorism in the United States. The ***National Strategy for Homeland Security*** characterizes terrorism as any premeditated, unlawful act dangerous to human life or public welfare that is intended to intimidate or coerce civilian populations or governments.

This description captures the core concepts shared by the various definition of terrorism contained in the U.S. Code, each crafted to achieve a legal standard of specificity and clarity.

This description covers kidnappings; hijackings; shootings; conventional bombings; attacks involving chemical, biological, radiological, or nuclear weapons; cyber-attacks; and any number of other forms of malicious violence. Terrorists can be U.S. citizens or foreigners, acting in concert with others, on their own, or on behalf of a hostile state.

**Reduce America's vulnerability.** Homeland security involves a systematic, comprehensive, and strategic effort to reduce America's vulnerability to terrorist attack. We must recognize that as a vibrant and prosperous free society, we present an ever-evolving, ever-changing target.

As we shore up our defenses in one area, the terrorists may exploit vulnerabilities in others. The **National Strategy for Homeland Security**, therefore, outlines a way for the government to work with the private sector to identify and protect our critical infrastructure and key assets, detect terrorist threats, and augment our defenses.

Because we must not permit the threat of terrorism to alter the American way of life, we have to accept some level of terrorist risk as a permanent condition. We must constantly balance the benefits of mitigating this risk against both the economic costs and infringements on individual liberty that this mitigation entails. No mathematical formula can reveal the appropriate balance; it must be determined by politically accountable leaders exercising sound, considered judgment informed by top-notch scientists, medical experts, and engineers.

**Homeland security.** Is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur.

**Minimize the damage.** The United States will prepare to manage the consequences of any future terrorist attacks that may occur despite our best efforts at prevention.

Therefore, homeland security seeks to improve the systems and prepare the individuals that will respond to acts of terror. The **National Strategy for Homeland Security** recognizes that after an attack occurs, our greatest chance to minimize loss of life and property lies with our local first responders—police officers, firefighters, emergency medical providers, public works personnel, and emergency management officials. Many of our efforts to minimize the damage focus on these brave and dedicated public servants.

**Recover.** As an essential component of homeland security, the United States will build and maintain various financial, legal, and social systems to recover from all forms of terrorism.

We must, therefore, be prepared to protect and restore institutions needed to sustain economic growth and confidence, rebuild destroyed property, assist victims and their families, heal psychological wounds, and demonstrate compassion, recognizing that we cannot automatically return to the pre-attack norm.



How easy is it to tap into your water, sewer or gas lines? Very easy...

## Older Homeland Security Presidential Directive

### **Purpose**

The Nation requires a Homeland Security Advisory System to provide a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to Federal, State, and local authorities and to the American people.

Such a system would provide warnings in the form of a set of graduated "**Threat Conditions**" that would increase as the risk of the threat increases. At each Threat Condition, Federal departments and agencies would implement a corresponding set of "**Protective Measures**" to further reduce vulnerability or increase response capability during a period of heightened alert.

This system is intended to create a common vocabulary, context, and structure for an ongoing national discussion about the nature of the threats that confront the homeland and the appropriate measures that should be taken in response. It seeks to inform and facilitate decisions appropriate to different levels of government and to private citizens at home and at work.

### **Homeland Security Advisory System**

The Homeland Security Advisory System shall be binding on the executive branch and suggested, although voluntary, to other levels of government and the private sector. There are five Threat Conditions, each identified by a description and corresponding color. From lowest to highest, the levels and colors are:

**Low = Green;**  
**Guarded = Blue;**  
**Elevated = Yellow;**  
**High = Orange;**  
**Severe = Red.**

The higher the Threat Condition, the greater the risk of a terrorist attack. Risk includes both the probability of an attack occurring and its potential gravity. Threat Conditions shall be assigned by the Attorney General in consultation with the Assistant to the President for Homeland Security.

Except in exigent circumstances, the Attorney General shall seek the views of the appropriate Homeland Security Principals or their subordinates, and other parties as appropriate, on the Threat Condition to be assigned.

Threat Conditions may be assigned for the entire Nation, or they may be set for a particular geographic area or industrial sector. Assigned Threat Conditions shall be reviewed at regular intervals to determine whether adjustments are warranted.

For facilities, personnel, and operations inside the territorial United States, all Federal departments, agencies, and offices other than military facilities shall conform their existing threat advisory systems to this system and henceforth administer their systems consistent with the determination of the Attorney General with regard to the Threat Condition in effect.

Over the last year, you probably have grown tired or used to these warnings.

### **Threat Condition**

The assignment of a Threat Condition shall prompt the implementation of an appropriate set of Protective Measures. Protective Measures are the specific steps an organization shall take to reduce its vulnerability or increase its ability to respond during a period of heightened alert. The authority to craft and implement Protective Measures rests with the Federal departments and agencies. It is recognized that departments and agencies may have several preplanned sets of responses to a particular Threat Condition to facilitate a rapid, appropriate, and tailored response.

Department and agency heads are responsible for developing their own Protective Measures and other antiterrorism or self-protection and continuity plans, and resourcing, rehearsing, documenting, and maintaining these plans. Likewise, they retain the authority to respond, as necessary, to risks, threats, incidents, or events at facilities within the specific jurisdiction of their department or agency, and, as authorized by law, to direct agencies and industries to implement their own Protective Measures.

### **Protective Measures**

They shall continue to be responsible for taking all appropriate proactive steps to reduce the vulnerability of their personnel and facilities to terrorist attack. Federal department and agency heads shall submit an annual written report to the President, through the Assistant to the President for Homeland Security, describing the steps they have taken to develop and implement appropriate Protective Measures for each Threat Condition. Governors, mayors, and the leaders of other organizations are encouraged to conduct a similar review of their organizations= Protective Measures.

The decision whether to publicly announce Threat Conditions shall be made on a case-by-case basis by the Attorney General in consultation with the Assistant to the President for Homeland Security. Every effort shall be made to share as much information regarding the threat as possible, consistent with the safety of the Nation. The Attorney General shall ensure, consistent with the safety of the Nation, that State and local government officials and law enforcement authorities are provided the most relevant and timely information.

The Attorney General shall be responsible for identifying any other information developed in the threat assessment process that would be useful to State and local officials and others and conveying it to them as permitted consistent with the constraints of classification. The Attorney General shall establish a process and a system for conveying relevant information to Federal, State, and local government officials, law enforcement authorities, and the private sector expeditiously.

The Director of Central Intelligence and the Attorney General shall ensure that a continuous and timely flow of integrated threat assessments and reports is provided to the President, the Vice President, Assistant to the President and Chief of Staff, the Assistant to the President for Homeland Security, and the Assistant to the President for National Security Affairs. Whenever possible and practicable, these integrated threat assessments and reports shall be reviewed and commented upon by the wider interagency community.

A decision on which Threat Condition to assign shall integrate a variety of considerations. This integration will rely on qualitative assessment, not quantitative calculation.

## Higher Threat Conditions

Higher Threat Conditions indicate greater risk of a terrorist act, with risk including both probability and gravity. Despite best efforts, there can be no guarantee that, at any given Threat Condition, a terrorist attack will not occur.

An initial and important factor is the quality of the threat information itself. The evaluation of this threat information shall include, but not be limited to, the following factors:

1. To what degree is the threat information credible?
2. To what degree is the threat information corroborated?
3. To what degree is the threat specific and/or imminent?
4. How grave are the potential consequences of the threat?

## Threat Conditions and Associated Protective Measures

The world has changed since September 11, 2001. We remain a Nation at risk to terrorist attacks and will remain at risk for the foreseeable future. At all Threat Conditions, we must remain vigilant, prepared, and ready to deter terrorist attacks. The following Threat Conditions each represent an increasing risk of terrorist attacks. Beneath each Threat Condition are some suggested Protective Measures, recognizing that the heads of Federal departments and agencies are responsible for developing and implementing appropriate agency-specific Protective Measures:

1. **Low Condition (Green).** This condition is declared when there is a low risk of terrorist attacks. Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures they develop and implement:
  1. Refining and exercising, as appropriate, preplanned Protective Measures;
  2. Ensuring personnel receive proper training on the Homeland Security Advisory System and specific preplanned department or agency Protective Measures; and
  3. Institutionalizing a process to assure that all facilities and regulated sectors are regularly assessed for vulnerabilities to terrorist attacks, and all reasonable measures are taken to mitigate these vulnerabilities.
2. **Guarded Condition (Blue).** This condition is declared when there is a general risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Condition, Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement:
  1. Checking communications with designated emergency response or command locations;
  2. Reviewing and updating emergency response procedures; and
  3. Providing the public with any information that would strengthen its ability to act appropriately.
3. **Elevated Condition (Yellow).** An Elevated Condition is declared when there is a significant risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Conditions, Federal departments and agencies should consider the following general measures in addition to the Protective Measures that they will develop and implement:
  1. Increasing surveillance of critical locations;
  2. Coordinating emergency plans as appropriate with nearby jurisdictions;
  3. Assessing whether the precise characteristics of the threat require the further refinement of preplanned Protective Measures; and
  4. Implementing, as appropriate, contingency and emergency response plans.

4. **High Condition (Orange).** A High Condition is declared when there is a high risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Conditions, Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement:
  1. Coordinating necessary security efforts with Federal, State, and local law enforcement agencies or any National Guard or other appropriate armed forces organizations;
  2. Taking additional precautions at public events and possibly considering alternative venues or even cancellation;
  3. Preparing to execute contingency procedures, such as moving to an alternate site or dispersing their workforce; and
  4. Restricting threatened facility access to essential personnel only.
  
5. **Severe Condition (Red).** A Severe Condition reflects a severe risk of terrorist attacks. Under most circumstances, the Protective Measures for a Severe Condition are not intended to be sustained for substantial periods of time. In addition to the Protective Measures in the previous Threat Conditions, Federal departments and agencies also should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement:
  1. Increasing or redirecting personnel to address critical emergency needs;
  2. Assigning emergency response personnel and pre-positioning and mobilizing specially trained teams or resources;
  3. Monitoring, redirecting, or constraining transportation systems; and Closing public and government facilities.



## America- Security Data

### The American Population

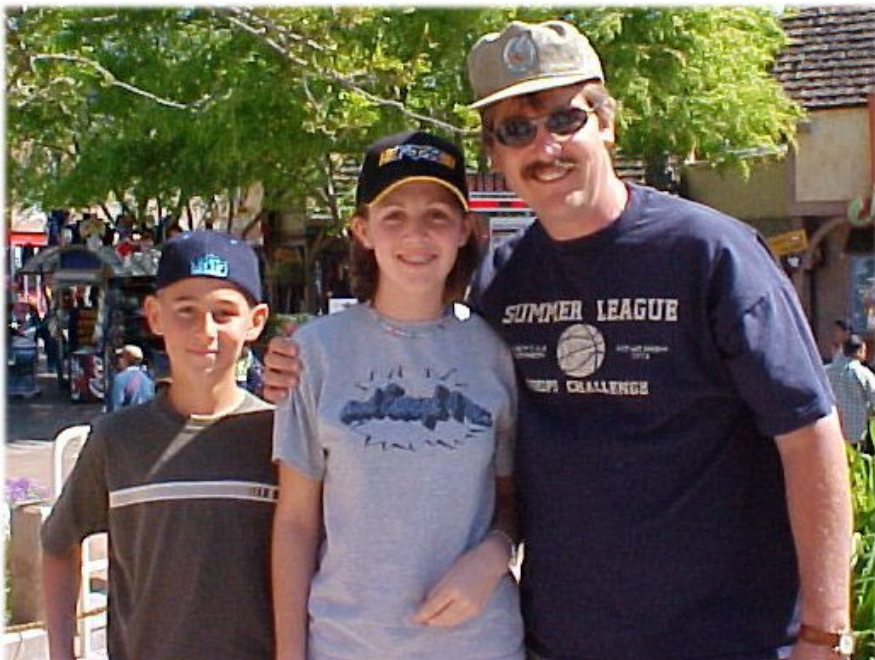
- An estimated 284.8 million people lived in the United States on July 1, 2001  
*Source: U.S. Department of Commerce*
- 54.2% of the Nation's population lives in ten states – three in the Northeast, three in the Midwest, three in the South, and one in the West
- The average population density within the United States is 79.2 people per square mile of land
- The average population density in metropolitan areas is 320.2 people per square mile of land
- Over 225 million Americans live in metropolitan areas
- Nearly 85 million Americans live in metropolitan areas of 5 million people or more
- Each year, the United States admits 500 million people, including 330 million non-citizens, through our borders

*Source: 2000 Census*

- Over 4 million people were processed through security at the last Olympics, over 85,000 at the last Super Bowl, and approximately 20,000 each at the Republican and Democratic National Conventions.

*Source: U.S. Secret Service*

**Culture.** The United States of America is an open, welcoming, pluralistic, diverse society that engages in dialogue rather than the dogmatic enforcement of any one set of values or ideas. Our culture is also characterized by compassion and strong civic engagement.



Home of the Free and the Brave, but for how long? Our Country has enacted too many security rules and laws to prevent unwanted human behavior and it hasn't made a dent in stopping crime, but these laws have dented our personal rights and freedoms.

## Gun Fighting

Never let someone or thing that threatens you get inside arm's length and never say "I got a gun". If you feel you need to use deadly force for heaven's sake let the "first sound they hear is the safety clicking off" and they shouldn't have time to hear anything after that if you are doing your job. 'The average response time of a 911 call is over 3 minutes....the response time of a .44 magnum is 1400 feet per second.'

Clint Smith, Director of Thunder Ranch, is a drill instructor (Thunder Ranch is a firearms training facility in Arizona ). Here are a few of his observation on tactics, firearms, self-defense and life as we know it in the civilized world. "The most important rule in a gunfight is: Always win and cheat if necessary." "Don't forget, incoming fire has the right of way.."

"Make your attacker advance through a wall of bullets. You may get killed with your own gun, but he'll have to beat you to death with it, cause it's going to be empty."

"If you're not shootin', you should be loadin'. If you're not loadin', you should be movin', if you're not movin', someone's gonna cut your head off and put it on a stick." "When you reload in low light encounters, don't put your flashlight in your back pocket.. If you light yourself up, you'll look like an angel or the tooth fairy... and you're gonna be one of 'em pretty soon." "Do something. It may be wrong, but do something."

"Shoot what's available, as long as it's available, until something else becomes available."

"If you carry a gun, people will call you paranoid. That's ridiculous. If you have a gun, what in the hell do you have to be paranoid for." "Don't shoot fast, unless you also shoot good.."

"You can say 'stop' or 'alto' or use any other word you think will work, but I've found that a large bore muzzle pointed at someone's head is pretty much the universal language."

"You have the rest of your life to solve your problems.. How long you live depends on how well you do it." "You cannot save the planet but you may be able to save yourself and your family."

"Thunder Ranch will be here as long as you'll have us or until someone makes us go away, and either way, it will be exciting."

More Excellent Gun Wisdom.....

The purpose of fighting is to win. There is no possible victory in defense..The sword is more important than the shield, and skill is more important than either. The final weapon is the brain. All else is supplemental.

1. Don't pick a fight with an old man. If he is too old to fight, he'll just kill you.
2. If you find yourself in a fair fight, your tactics suck.
3. I carry a gun cause a cop is too heavy.
4. When seconds count, the cops are just minutes away.
5. A reporter did a human-interest piece on the Texas Rangers. The reporter recognized the Colt Model 1911 the Ranger was carrying and asked him 'Why do you carry a 45?' The Ranger responded, 'Because they don't make a 46.'
6. An armed man will kill an unarmed man with monotonous regularity.
7. The old sheriff was attending an awards dinner when a lady commented on his wearing his sidearm. 'Sheriff, I see you have your pistol. Are you expecting trouble?' 'No ma'am. If I were expecting trouble, I would have brought my rifle.'
8. Beware of the woman who only has one gun, because she probably knows how to use it very well.

*'The true soldier fights not because he hates what is in front of him, but because he loves what is behind him.'* G. K. Chesterton

A people that values its privileges above its principles will soon lose both.

## Principles of the *National Strategy for Homeland Security*

Our efforts in the war on terrorism are rooted in the same core American strengths and characteristics that led us to victory in World War II and the Cold War:

- **innovation,**
- **determination, and**
- **commitment to the democratic tenets of freedom and equality.**

With these strengths and characteristics as our guide, eight principles have shaped the design of the *National Strategy for Homeland Security*.

**Require responsibility and accountability.** The *National Strategy for Homeland Security* is focused on producing results. When possible, it designates lead executive branch departments or agencies for federal homeland security initiatives. As the President announced on June 6, 2002, the *Strategy* calls for creating the Department of Homeland Security to clarify lines of responsibility for homeland security in the executive branch.

The new Department would take responsibility for many of the initiatives outlined here. The *Strategy* also makes recommendations to Congress, state and local governments, the private sector, and the American people. **Mobilize our entire society.** The *National Strategy for Homeland Security* recognizes the crucial role of state and local governments, private institutions, and the American people in securing our homeland. Our traditions of federalism and limited government require that organizations outside the federal government take the lead in many of these efforts.

The *Strategy* provides guidance on best practices and organizing principles. It also seeks to empower all key players by streamlining and clarifying federal support processes.

**Manage risk and allocate resources judiciously.** The *National Strategy for Homeland Security* identifies priority programs for our finite homeland security resources. Because the number of potential terrorist acts is nearly infinite, we must make difficult choices about how to allocate resources against those risks that pose the greatest danger to our homeland.

**Seek opportunity out of adversity.** The *National Strategy for Homeland Security* gives special attention to programs that improve security while at the same time advancing other important public purposes or principles. We will build, for example, a national incident management system that is better able to manage not just terrorism but other hazards such as natural disasters and industrial accidents. We will build a medical system that is not simply better able to cope with bioterrorism but with all diseases and all manner of mass-casualty incidents.

### **Objectives of the *National Strategy for Homeland Security***

Homeland security is an exceedingly complex mission. It involves efforts both at home and abroad. It demands a range of government and private sector capabilities. And it calls for coordinated and focused effort from many actors who are not otherwise required to work together and for whom security is not always a primary mission.

This *Strategy* establishes three objectives based on the definition of homeland security:

- **Prevent terrorist attacks within the United States;**
- **Reduce America's vulnerability to terrorism;**
- **Minimize the damage and recover from attacks that do occur.**

## The Objectives

The order of these objectives deliberately sets priorities for America's efforts to secure the homeland management system that will not only stop terrorist penetration but will also facilitate the efficient flow of legitimate commerce and people.

**Foster flexibility.** The *National Strategy for Homeland Security* emphasizes the need for a flexible response to terrorism. The terrorist threat is ever-changing because our terrorist enemies can strategically adapt their offensive tactics to exploit what they perceive to be weaknesses in our defenses.

Therefore, the *Strategy* builds managerial, budgetary, and structural flexibility into the federal government's homeland security structure and suggests similar measures for the rest of the Nation. It allows for the reassessment of priorities and the realignment of resources as the terrorist threat evolves.

**Measure preparedness.** The *National Strategy for Homeland Security* demands accountability from every government body responsible for homeland security initiatives. Every department or agency will create benchmarks and other performance measures by which we can evaluate our progress and allocate future resources.

**Sustain efforts over the long term.** Protecting the homeland from terrorist attack is a permanent mission. Therefore, the *National Strategy for Homeland Security* provides an initial set of initiatives for moving closer to our homeland security objectives. Lead departments and agencies should plan to sustain homeland security initiatives for years and decades, not weeks and months.



How safe are your hazardous chemicals from Terrorists?

## Defending against Catastrophic Threats

The expertise, technology, and material needed to build the most deadly weapons known to mankind—including chemical, biological, radiological, and nuclear weapons—are spreading inexorably. If our enemies acquire these weapons, they are likely to try to use them.

The consequences of such an attack could be far more devastating than those we suffered on September 11—a chemical, biological, radiological, or nuclear terrorist attack in the United States could cause large numbers of casualties, mass psychological disruption, contamination and significant economic damage, and could overwhelm local medical capabilities.

Currently, chemical, biological, radiological, and nuclear detection capabilities are modest and response capabilities are dispersed throughout the country at every level of government. While current arrangements have proven adequate for a variety of natural disasters and even the September 11 attacks, the threat of terrorist attacks using chemical, biological, radiological, and nuclear weapons requires new approaches, a focused strategy, and a new organization.

The ***National Strategy for Homeland Security*** identifies six major initiatives in this area:

- Prevent terrorist use of nuclear weapons through better sensors and procedures;
- Detect chemical and biological materials and attacks;
- Improve chemical sensors and decontamination techniques;
- Develop broad spectrum vaccines, antimicrobials, and antidotes;
- Harness the scientific knowledge and tools to counter terrorism; and
- Implement the Select Agent Program.

***Emergency Preparedness and Response.*** We must prepare to minimize the damage and recover from any future terrorist attacks that may occur despite our best efforts at prevention. An effective response to a major terrorist incident—as well as a natural disaster—depends on being prepared. Therefore, we need a comprehensive national system to bring together and coordinate all necessary response assets quickly and effectively.

We must plan, equip, train, and exercise many different response units to mobilize without warning for any emergency. Many pieces of this national emergency response system are already in place. America's first line of defense in the aftermath of any terrorist attack is its first responder community—police officers, firefighters, emergency medical providers, public works personnel, and emergency management officials. Nearly three million state and local first responders regularly put their lives on the line to save the lives of others and make our country safer.

Yet multiple plans currently govern the federal government's support of first responders during an incident of national significance. These plans and the government's overarching policy for counterterrorism are based on an artificial and unnecessary distinction between "**crisis management**" and "**consequence management**."



The Department of Homeland Security will consolidate federal response plans and build a national system for incident management in cooperation with state and local government. Our federal, state, and local governments would ensure that all response personnel and organizations are properly equipped, trained, and exercised to respond to all terrorist threats and attacks in the United States.

Our emergency preparedness and response efforts would also engage the private sector and the American people.

The ***National Strategy for Homeland Security*** identifies twelve major initiatives in this area:

- Integrate separate federal response plans into a single all-discipline incident management plan;
- Create a national incident management system;
- Improve tactical counterterrorist capabilities;
- Enable seamless communication among all responders;
- Prepare health care providers for catastrophic terrorism;
- Augment America's pharmaceutical and vaccine stockpiles;
- Prepare for chemical, biological, radiological, and nuclear decontamination;
- Plan for military support to civil authorities;
- Build the Citizen Corps;
- Build a national training and evaluation system; and
- Enhance the victim support system.



Using a small detection device to search large packages for nuclear materials.

## Homeland Security Summary

The ***National Strategy for Homeland Security*** establishes, for the first time in our Nation's history, a statement of objectives around which our entire society can mobilize to secure the U.S. homeland from the dangerous and evolving threat of terrorism.

The ***National Security Strategy of the United States*** aims to guarantee the sovereignty and independence of the United States, with our fundamental values and institutions intact. It provides a framework for creating and seizing opportunities that strengthen our security and prosperity.

The ***National Strategy for Homeland Security*** complements the ***National Security Strategy of the United States*** by addressing a very specific and uniquely challenging threat – terrorism in the United States – and by providing a comprehensive framework for organizing the efforts of federal, state, local and private organizations whose primary functions are often unrelated to national security.

The link between national security and homeland security is a subtle but important one. For more than six decades, America has sought to protect its own sovereignty and independence through a strategy of global presence and engagement. In so doing, America has helped many other countries and peoples advance along the path of democracy, open markets, individual liberty, and peace with their neighbors. Yet there are those who oppose America's role in the world, and who are willing to use violence against us and our friends. Our great power leaves these enemies with few conventional options for doing us harm. One such option is to take advantage of our freedom and openness by secretly inserting terrorists into our country to attack our homeland.

Homeland security seeks to deny this avenue of attack to our enemies and thus to provide a secure foundation for America's ongoing global engagement. Thus the ***National Security Strategy of the United States and National Strategy for Homeland Security*** work as mutually supporting documents, providing guidance to the executive branch departments and agencies.

There are also a number of other, more specific strategies maintained by the United States that are subsumed within the twin concepts of national security and homeland security. The ***National Strategy for Combating Terrorism*** will define the U.S. war plan against international terrorism.

The ***National Strategy to Combat Weapons of Mass Destruction*** coordinates America's many efforts to deny terrorists and states the materials, technology, and expertise to make and deliver weapons of mass destruction.

The ***National Strategy to Secure Cyberspace*** will describe our initiatives to secure our information systems against deliberate, malicious disruption.

The ***National Money Laundering Strategy*** aims to undercut the illegal flows of money that support terrorism and international criminal activity.

The ***National Defense Strategy*** sets priorities for our most powerful national security instrument.

## EPA- Security Section

The Environmental Protection Agency, for example, is evaluating the upgrading of air monitoring stations to allow for the detection of certain chemical, biological, or radiological substances. The federal government will also explore systems that can detect whether an individual has been immunized against a threat pathogen or has recently handled threat materials.

The ability to quickly recognize and report biological and chemical attacks will minimize casualties and enable first responders to treat the injured effectively.

Local emergency personnel and health providers must first be able to diagnose symptoms. In addition to existing state laws mandating the reporting of threat diseases by physicians, veterinarians, and public health laboratories, rapid diagnosis of diseases of concern and communication form the cornerstone of a robust response. The Department of Homeland Security will:

***Develop broad spectrum vaccines, antimicrobials and antidotes.*** In many cases, our medical countermeasures cannot address all possible biological agents or may not be suitable for use by the general population.

- Along with the Departments of Health and Human Services and other government and private research entities, pursue new defenses that will increase efficacy while reducing side effects.
- For example, they will explore the utility of attenuated smallpox vaccines and of existing antivirals modified to render those vaccines more effective and safe.
- In collaboration with the private sector, research and work toward development of broad spectrum antivirals to meet the threat of engineered pathogens aimed at both humans and livestock.
- Expand the inventory of diagnostics, vaccines, and other therapies such as antimicrobials and antidotes that can mitigate the consequences of a chemical, biological, radiological, or nuclear attack. Development of safer smallpox vaccines and antiviral drugs will lower the risk of adverse reactions experienced with the traditional vaccine.
- The goal of protecting a diverse population of all ages and health conditions requires a coordinated national effort with a comprehensive research and development strategy and investment plans.



## **TITLE IV--DRINKING WATER SECURITY AND SAFETY**

### **SEC. 401. TERRORIST AND OTHER INTENTIONAL ACTS.**

The Safe Drinking Water Act (title XIV of the Public Health Service Act) is amended by inserting the following new section after section 1432:

SEC. 1433.: 42 USC 300i-2

#### **TERRORIST AND OTHER INTENTIONAL ACTS.**

(a) Vulnerability Assessments.--(1) Each community water system serving a population of greater than 3,300 persons shall conduct an assessment of the vulnerability of its system to a terrorist attack or other intentional acts intended to substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water. The vulnerability assessment shall include, but not be limited to, a review of pipes and constructed conveyances, physical barriers, water collection, pretreatment, treatment, storage and distribution facilities, electronic, computer or other automated systems which are utilized by the public water system, the use, storage, or handling of various chemicals, and the operation and maintenance of such system. The Administrator, not later than August 1, 2002, after consultation with appropriate departments and agencies of the Federal Government and with State and local governments, shall provide baseline information to community water systems required to conduct vulnerability assessments regarding which kinds of terrorist attacks or other intentional acts are the probable threats to--

``(A) substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water; or

``(B) otherwise present significant public health concerns.

(2) <<NOTE: Certification. Deadlines.>> Each community water system referred to in paragraph (1) shall certify to the Administrator that the system has conducted an assessment complying with paragraph (1) and shall submit to the Administrator a written copy of the assessment. Such certification and submission shall be made prior to:

(A) March 31, 2003, in the case of systems serving a population of 100,000 or more.

(B) December 31, 2003, in the case of systems serving a population of 50,000 or more but less than 100,000.

(C) June 30, 2004, in the case of systems serving a population greater than 3,300 but less than 50,000.

(3) Except for information contained in a certification under this subsection identifying the system submitting the certification and the date of the certification, all information provided to the Administrator under this subsection and all information derived therefrom shall be exempt from disclosure under section 552 of title 5 of the United States Code.

(4) No community water system shall be required under State or local law to provide an assessment described in this section to any State, regional, or local governmental entity solely by reason of the requirement set forth in paragraph (2) that the system submits such assessment to the Administrator.

(5) Not later than November 30, 2002, the Administrator, in consultation with appropriate Federal law enforcement and intelligence officials, shall develop such protocols as may be necessary to protect the copies of the assessments required to be submitted under this subsection (and the information contained therein) from unauthorized disclosure. Such protocols shall ensure that--

(A) each copy of such assessment, and all information contained in or derived from the assessment, is kept in a secure location;

(B) only individuals designated by the Administrator may have access to the copies of the assessments; and  
(C) no copy of an assessment, or part of an assessment, or information contained in or derived from an assessment shall be available to anyone other than an individual designated by the Administrator.

At the earliest possible time prior to November 30, 2002, the Administrator shall complete the development of such protocols for the purpose of having them in place prior to receiving any vulnerability assessments from community water systems under this subsection.

(6)(A) Except as provided in subparagraph (B), any individual referred to in paragraph (5)(B) who acquires the assessment submitted under paragraph (2), or any reproduction of such assessment, or any information derived from such assessment, and who knowingly or recklessly reveals such assessment, reproduction, or information other than--

(i) to an individual designated by the Administrator under paragraph (5),

(ii) for purposes of section 1445 or for actions under section 1431, or

(iii) for use in any administrative or judicial proceeding to impose a penalty for failure to comply with this section, shall upon conviction be imprisoned for not more than one year or fined in accordance with the provisions of chapter 227 of title 18, United States Code, applicable to class A misdemeanors, or both, and shall be removed from Federal office or employment.

(B) Notwithstanding subparagraph (A), an individual referred to in paragraph (5)(B) who is an officer or employee of the United States may discuss the contents of a vulnerability assessment submitted under this section with a State or local official.

(7) Nothing in this section authorizes any person to withhold any information from Congress or from any committee or subcommittee of Congress.

(b) Emergency Response Plan.--Each community water system serving a population greater than 3,300 shall prepare or revise, where necessary, an emergency response plan that incorporates the results of vulnerability assessments that have been completed.

Each such community water system shall certify to the Administrator, as soon as reasonably possible after the enactment of this section, but not later than 6 months after the completion of the vulnerability assessment under subsection (a), that the system has completed such plan. The emergency response plan shall include, but not be limited to, plans, procedures, and identification of equipment that can be implemented or utilized in the event of a terrorist or other intentional attack on the public water system. The emergency response plan shall also include actions, procedures, and identification of equipment which can obviate or significantly lessen the impact of terrorist attacks or other intentional actions on the public health and the safety and supply of drinking water provided to communities and individuals. Community water systems shall, to the extent possible, coordinate with existing Local Emergency Planning Committees established under the Emergency Planning and Community Right-to-Know Act (42 U.S.C. 11001 et seq.) when preparing or revising an emergency response plan under this subsection.

(c) Record Maintenance.--Each community water system shall maintain a copy of the emergency response plan completed pursuant to subsection (b) for 5 years after such plan has been certified to the Administrator under this section.

(d) Guidance to Small Public Water Systems.--The Administrator shall provide guidance to community water systems serving a population of less than 3,300 persons on how to conduct vulnerability assessments, prepare emergency response plans, and address threats from terrorist attacks or other intentional actions designed to disrupt the provision of safe drinking water or significantly affect the public health or significantly affect the safety or supply of drinking water provided to communities and individuals.

(e) Funding.--(1) There are authorized to be appropriated to carry out this section not more than \$160,000,000 for the fiscal year 2002 and such sums as may be necessary for the fiscal years 2003 through 2005.

(2) The Administrator, in coordination with State and local governments, may use funds made available under paragraph (1) to provide financial assistance to community water systems for purposes of compliance with the requirements of subsections (a) and (b) and to community water systems for expenses and contracts designed to address basic security enhancements of critical importance and significant threats to public health and the supply of drinking water as determined by a vulnerability assessment conducted under subsection (a). Such basic security enhancements may include, but shall not be limited to the following:

(A) the purchase and installation of equipment for detection of intruders;

(B) the purchase and installation of fencing, gating, lighting, or security cameras;

(C) the tamper-proofing of manhole covers, fire hydrants, and valve boxes;

(D) the rekeying of doors and locks;

(E) improvements to electronic, computer, or other automated systems and remote security systems;

(F) participation in training programs, and the purchase of training manuals and guidance materials, relating to security against terrorist attacks;

(G) improvements in the use, storage, or handling of various chemicals; and

(H) security screening of employees or contractor support services.

Funding under this subsection for basic security enhancements shall not include expenditures for personnel costs, or monitoring, operation, or maintenance of facilities, equipment, or systems.

(3) The Administrator may use not more than \$5,000,000 from the funds made available under paragraph (1) to make grants to community water systems to assist in responding to and alleviating any vulnerability to a terrorist attack or other intentional acts intended to substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water (including sources of water for such systems) which the Administrator determines to present an immediate and urgent security need.

(4) The Administrator may use not more than \$5,000,000 from the funds made available under paragraph (1) to make grants to community water systems serving a population of less than 3,300 persons for activities and projects undertaken in accordance with the guidance provided to such systems under subsection (d).

#### **SEC. 402. OTHER SAFE DRINKING WATER ACT AMENDMENTS.**

The Safe Drinking Water Act (title XIV of the Public Health Service Act) is amended by inserting the following new sections after section 1433 (as added by section 401 of this Act):``SEC. 1434. 42 USC 300i-3

#### **CONTAMINANT PREVENTION, DETECTION AND RESPONSE.**

``(a) In General.--The Administrator, in consultation with the Centers for Disease Control and, after consultation with appropriate departments and agencies of the Federal Government and with State and local governments, shall review (or enter into contracts or cooperative agreements to provide for a review of) current and future methods to prevent, detect and respond to the intentional introduction of chemical, biological or radiological contaminants into community water systems and source water for community water systems, including each of the following:

(1) Methods, means and equipment, including real time monitoring systems, designed to monitor and detect various levels of chemical, biological, and radiological contaminants or

indicators of contaminants and reduce the likelihood that such contaminants can be successfully introduced into public water systems and source water intended to be used for drinking water.

(2) Methods and means to provide sufficient notice to operators of public water systems, and individuals served by such systems, of the introduction of chemical, biological or radiological contaminants and the possible effect of such introduction on public health and the safety and supply of drinking water.

(3) Methods and means for developing educational and awareness programs for community water systems.

(4) Procedures and equipment necessary to prevent the flow of contaminated drinking water to individuals served by public water systems.

(5) Methods, means, and equipment which could negate or mitigate deleterious effects on public health and the safety and supply caused by the introduction of contaminants into water intended to be used for drinking water, including an examination of the effectiveness of various drinking water technologies in removing, inactivating, or neutralizing biological, chemical, and radiological contaminants.

6) Biomedical research into the short-term and long-term impact on public health of various chemical, biological and radiological contaminants that may be introduced into public water systems through terrorist or other intentional acts.

(b) Funding.--For the authorization of appropriations to carry out this section, see section 1435(e).

**SEC. 1435: 42 USC 300i-4.  
SUPPLY DISRUPTION PREVENTION, DETECTION AND RESPONSE.**

(a) Disruption of Supply or Safety.—The Administrator, in coordination with the appropriate departments and agencies of the Federal government, shall review (or enter into contracts or cooperative agreements to provide for a review of) methods and means by which terrorists or other individuals or groups could disrupt the supply of safe drinking water or take other actions against water collection, pretreatment, treatment, storage and distribution facilities which could render such water significantly less safe for human consumption, including each of the following:

(1) Methods and means by which pipes and other constructed conveyances utilized in public water systems could be destroyed or otherwise prevented from providing adequate supplies of drinking water meeting applicable public health standards.

(2) Methods and means by which collection, pretreatment, treatment, storage and distribution facilities utilized or used in connection with public water systems and collection and pretreatment storage facilities used in connection with public water systems could be destroyed or otherwise prevented from providing adequate supplies of drinking water meeting applicable public health standards.

(3) Methods and means by which pipes, constructed conveyances, collection, pretreatment, treatment, storage and distribution systems that are utilized in connection with public water systems could be altered or affected so as to be subject to cross-contamination of drinking water supplies.

(4) Methods and means by which pipes, constructed conveyances, collection, pretreatment, treatment, storage and distribution systems that are utilized in connection with public water systems could be reasonably protected from terrorist attacks or other acts intended to disrupt the supply or affect the safety of drinking water.

(5) Methods and means by which information systems, including process controls and supervisory control and data acquisition and cyber systems at community water systems could be disrupted by terrorists or other groups.

(b) Alternative Sources.--The review under this section shall also include a review of the methods and means by which alternative supplies of drinking water could be provided in the event of the destruction, impairment or contamination of public water systems.

(c) Requirements and Considerations. --In carrying out this section and section 1434--

(1) the Administrator shall ensure that reviews carried out under this section reflect the needs of community water systems of various sizes and various geographic areas of the United States; and

(2) the Administrator may consider the vulnerability of, or potential for forced interruption of service for, a region or service area, including community water systems that provide service to the National Capital area.

(d) Information Sharing.--As soon as practicable after reviews carried out under this section or section 1434 have been evaluated, the Administrator shall disseminate, as appropriate as determined by the Administrator, to community water systems information on the results of the project through the Information Sharing and Analysis Center, or other appropriate means.

(e) Funding.--There are authorized to be appropriated to carry out this section and section 1434 not more than \$15,000,000 for the fiscal year 2002 and such sums as may be necessary for the fiscal years 2003 through 2005."

### **SEC. 403. MISCELLANEOUS AND TECHNICAL AMENDMENTS.**

The Safe Drinking Water Act is amended as follows:

- (1) Section 1414(i)(1) E: 42 USC 300g-3. is amended by inserting ``1433" after ``1417".
- (2) Section 1431: 42 USC 300i. is amended by inserting in the first sentence after ``drinking water" the following: ``, or that there is a threatened or potential terrorist attack (or other intentional act designed to disrupt the provision of safe drinking water or to impact adversely the safety of drinking water supplied to communities and individuals), which".
- (3) Section 1432 <<NOTE: 42 USC 300i-1.>> is amended as follows:
  - (A) By striking ``5 years" in subsection (a) and inserting ``20 years".
  - (B) By striking ``3 years" in subsection (b) and inserting ``10 years".
  - (C) By striking ``\$50,000" in subsection (c) and inserting ``\$1,000,000".
  - (D) By striking ``\$20,000" in subsection (c) and inserting ``\$100,000".
- (4) Section 1442 <<NOTE: 42 USC 300j-1.>> is amended as follows:
  - (A) By striking ``this subparagraph" in subsection (b) and inserting ``this subsection".
  - (B) By amending subsection (d) to read as follows:
    - (d) <<NOTE: There are authorized to be appropriated to carry out subsection (b) not more than \$35,000,000 for the fiscal year 2002 and such sums as may be necessary for each fiscal year thereafter.".

"Those who hammer their guns into plows will plow for those who do not..."- Thomas Jefferson

## **Threat Advisory**

### **U.S. Environmental Protection Agency**

#### **Office of Water**

#### **Water Protection Task Force February 7, 2003**

EPA's Water Protection Task Force is providing the following information to water utilities to assist in their preparations for the newly announced Threat Level Orange:

- Suggested measures under Threat Level Orange
- Joint EPA/CDC Advisory

#### **SUGGESTED MEASURES UNDER THREAT LEVEL ORANGE**

EPA's Water Protection Task Force has compiled a list of suggestions from a number of water utilities to assist in preparations at the various Homeland Security Threat Levels. The suggestions described below pertain to the Threat Level Orange and are organized in the areas of detection, preparedness, prevention, and protection. Water utilities should consider whether the following measures are appropriate for their facilities:

#### **Suggested Measures**

##### **I. Detection:**

- Confirm that county and state health officials will inform water utilities of any potential waterborne illnesses.

##### **II. Preparedness:**

- Post *daily* reminders for staff and contractors of the **THREAT LEVEL ORANGE**; along with a reminder of what events constitute security violations.
- Ensure employees are fully aware of the emergency response communication protocols so that appropriate notifications can be made quickly in the event of an incident. Consider the following list of organizations to be notified:
  - local law enforcement
  - local FBI Field Office
  - National Response Center (800-424-8802)
  - State and local emergency management organizations
  - Governor's office
  - EPA CID Special Agent in Charge (SAC)

- other associated system authorities (wastewater, water)
- local government officials
- state/local health, water, and/or environmental departments
- critical care facilities
- employees
- EMS and fire department as deemed necessary
- Consider when to notify customers and what notification to issue

(Additional information is available in the *Model Emergency Response Guidelines* at [www.epa.gov/safewater/security/](http://www.epa.gov/safewater/security/))

- Evaluate the need for organizing an emergency operations center.

### **III. Prevention:**

- Discontinue tours and prohibit public access to all operational facilities.
- Consider requesting increased law enforcement surveillance, particularly of critical assets and otherwise unprotected areas.

### **IV. Protection:**

- Ensure water treatment/production facility is staffed at all times.
- Consider the need for additional security measures needed for surface water reservoirs.
- Limit mission critical facility access to essential employees and contractors.
- Increase security patrol activity to the maximum level sustainable and ensure tight security in the vicinity of mission critical facilities. Consider varying the schedule of security patrols.
- Prosecute intruders, trespassers, and those detained for tampering to the fullest extent possible under applicable laws.



## Joint EPA/CDC Advisory

DRAFT 5:50pm February 7, 2003

---

### ADVISORY

FOR RELEASE February 7, 2003

Today, the Department of Homeland Security upgraded the Homeland Security Advisory System from yellow level (elevated risk of terrorist attack) to orange level (high risk of terrorist attack).

While there are no data to indicate that water has been specifically targeted, our nation's water infrastructure remains at risk to terrorist attacks, or acts intended to substantially disrupt the ability of a water system to provide a reliable supply of water. Therefore, public health agencies and water utilities are encouraged to continue to work together, keep each other informed of any unusual activities, and confirm the proper operation of notification channels in emergency response plans.

Public health agencies should immediately notify local water utilities and the state's drinking water administrator in the event of an unusual number of cases of gastrointestinal illnesses or other indications of illness that may suggest water contamination by a biological, chemical or radiological agent.

Water utilities should immediately notify public health agencies 24/7 emergency operations number, and the state's drinking water administrator in the event of specific threats received at a water facility, customer complaints in water quality, or if circumstances lead the utility to believe that the water has been or will be contaminated with a biological, chemical or radiological agent.

The Centers for Disease Control and Prevention (**CDC**) and the U.S. Environmental Protection Agency (**EPA**) issue this advisory jointly.

---



# National Infrastructure Protection Center

## HOMELAND SECURITY INFORMATION UPDATE

### Suggested Guidance on Protective Measures

#### Information Bulletin 03-002

February 7, 2003

National Threat Warning System–Homeland Security Information Update–HSAS Threat Level Orange (High); joint guidance from the Department of Homeland Security and the FBI.

As recipients were advised, the Homeland Security Advisory System (HSAS) was raised to High (Orange) from Elevated (Yellow) on 2/7/03. This communication provides critical infrastructure owners/operators suggested guidance for developing protective measures based on this heightened threat condition. This communication also provides potential indicators of threats involving weapons of mass destruction.

#### **PART I: GENERAL PROTECTIVE MEASURES**

In addition to continuing all precautions from the lower threat condition (Yellow), the following general protective measures may be utilized. Recipients are advised to take other appropriate steps, in conjunction with local conditions, policies, and procedures. The list that follows is not intended to be exhaustive, but merely illustrative:

- coordinate necessary security efforts with Armed Forces or law enforcement agencies.
- take additional precautions at public events.
- review contingency plans to work at an alternate site or with a dispersed work force.
- review plans to restrict access to facilities.

#### **PART II: SPECIFIC PROTECTIVE MEASURES FOR INFRASTRUCTURE OWNERS/OPERATORS AT HIGH CONDITION (ORANGE)**

- announce threat condition high (orange) to all employees.
- consider full or partial activation of emergency operations center.
- review policy and plans relating to restricting access to critical facilities and infrastructure.
- conduct periodic inspections of building facilities and HVAC systems for potential indicators/irregularities
- direct people to the Red Cross website for further review of protective measures for families and businesses.
- enhance security at critical facilities.
- institute/increase vehicle, foot and roving security patrols.

- implement random security guard shift changes.
- increase visibility in and around perimeters by increasing lighting and removing or trimming vegetation.
- implement stringent identification procedures to include conducting “hands on” checks of security badges for all personnel, if badges are required.
- remind personnel to properly display badges, if applicable, and enforce visibility.
- rearrange exterior vehicle barriers to alter traffic patterns near facilities.
- arrange for law enforcement vehicles to be parked randomly near entrances and exits.
- approach all illegally parked vehicles in and around facilities, question drivers and direct them to move immediately. If the owner cannot be identified, have vehicle towed by law enforcement.
- if possible, institute a vehicle inspection program to include checking under the undercarriage of vehicles, under the hood, and in the trunk. Provide vehicle inspection training to security personnel.
- instruct citizens to report suspicious activities, packages and people, and report all suspicious activity immediately to local law enforcement.
- x-ray packages, if possible, prior to entry, and inspect handbags, and briefcases, if possible.
- encourage personnel to avoid routines, vary times and routes, and pre-plan with family members and supervisors.
- validate vendor lists for all routine deliveries and repair services.
- restrict vehicle parking close to buildings.
- inspect all deliveries and consider accepting shipments only at offsite locations.
- require identification, sign-in, and escorts for visitors.
- instruct people to be especially watchful for suspicious or unattended packages and articles either delivered or received through the mail.
- send a public information officer to the state joint information center.
- install special locking devices on manhole covers in and around critical infrastructure facilities.
- initiate a system to enhance mail and package screening procedures (both announced and unannounced).
- review current contingency plans and if not already in place, develop and implement procedures for receiving and acting on: threat information, alert notification procedures, terrorist incident response procedures, evacuation procedures, shelter in place procedures, bomb threat procedures, hostage and barricade procedures, chemical, biological, radiological and nuclear (CBRN) procedures, consequence and crisis management procedures, accountability procedures and media procedures.

### **PART III: POTENTIAL INDICATORS OF THREATS INVOLVING WEAPONS OF MASS DESTRUCTION (WMD)**

#### **POTENTIAL INDICATORS OF WMD THREATS OR INCIDENTS:**

- unusual/suspicious packages or containers, especially those found in unlikely or sensitive locations, such as those found near air intake/HVAC systems or enclosed spaces.
- unusual powders or liquids/droplets/mists/clouds, especially found near air intake/HVAC systems or enclosed spaces.
- signs of tampering or break-in to a facility or maintenance/utility area
- reports of suspicious person(s) or activities, especially those involving sensitive locations within or around a building
- dead animals/birds, fish, or insects
- unexplained/unusual odors. Smells may range from fruity/flowery to sharp/pungent, garlic/horseradish-like, bitter almonds, peach kernels, and new mown grass/hay.
- unusual/unscheduled spraying or discovery of spray devices or bottles

The NIPC encourages individuals to report information concerning suspicious activity to their local FBI Joint Terrorism Task Force (JTTF) office, <http://www.fbi.gov/contact/fo/fo.htm>, the NIPC, or to other appropriate authorities. Individuals can reach the NIPC WATCH AND WARNING UNIT at (202) 323-3205, toll free at 1-888-585-9078, or by email to [nipc.watch@fbi.gov](mailto:nipc.watch@fbi.gov).



# What Drinking Water Utilities Can Do Now to Guard Against Terrorist and Security Threats

*Recommendations by the New Mexico Environment Department Drinking Water Bureau  
Modified from Recommendations by the EPA Office of Ground Water and Drinking Water*

## Guarding Against Unplanned Physical Intrusion

- Lock all doors and set alarms at your office, drinking water well houses, treatment plants, and vaults, and make it a rule that doors are locked and alarms are set;
- Limit access to facilities and control access to water supply reservoirs, giving close scrutiny to visitors and contractors;
- Increase security at treatment plants, and post “**Employees Only**” signs in restricted areas;
- Secure hatches, meter boxes, hydrants, manholes and other access points to the water distribution system;
- Increase lighting in parking lots, treatment bays, and other areas with limited staffing;
- Control access to computer networks and control systems, and change the passwords frequently;
- Do not leave keys in equipment or vehicles at any time.
- Disinfection is the most effective means of combating microbiological contaminants. Make sure the system holds a chlorine residual at all times.

## Making Security a Priority For Employees

- Upgrade hiring and employment practices – know your employees;
- Develop a security program with written plans and train employees frequently;
- Ensure all employees are aware of communications protocols with relevant law enforcement, public health, environmental protection, and emergency response organizations;
- Ensure that employees are fully aware of the importance of vigilance and the seriousness of breaches in security, and make note of unaccompanied strangers on site and immediately notify designated security officers or local law enforcement agencies;
- Consider varying the timing of operational procedures if possible in case someone is watching the pattern changes.
- Upon the dismissal of an employee, change any electronic access codes and make sure keys and access cards are returned;

- Provide Customer Service staff with training and checklists on how to handle a threat if it is called in.
- Establish neighborhood watch groups in those residential areas adjacent to water system facilities.

### **Coordinating Actions for Effective Emergency Response.**

- Review existing emergency response plans, and ensure they are current and relevant;
- Develop clear protocols and chains-of-command for reporting and responding to threats along with relevant emergency management, law enforcement, environmental, public health officials, consumers and the media. Practice the emergency protocols regularly;
- Ensure key utility personnel (both on and off duty) have access to crucial telephone numbers and contact information at all times; keep the call list up to date.
- Develop close relationships with local law enforcement agencies, and make sure they know where critical assets are located. Request they add your facilities to their routine rounds;
- Report to county or State health officials any illness among the utility's customers that might be associated with water supplies, and thoroughly investigate any customer complaints;
- Report criminal threats or suspicious behavior toward water utilities immediately to the local sheriff or city police department.
- Meet with local law officials so they can become familiar with plant layout and communications protocol.
- Investing in Security and Infrastructure Improvements.
- Assess the vulnerability of source water protection areas, drinking water treatment plants, distribution networks, and other key infrastructure elements;
- Move as quickly as possible with the most obvious and cost-effective physical improvements, such as tamper-proofing manhole covers, fire hydrants and valve boxes;
- Improve computer system and remote operational security; Seek financing for more expensive and comprehensive system improvements.



## Chapter 1 - Chapter Summary

The expertise, technology, and material needed to build the most deadly weapons known to mankind — including chemical, biological, radiological, and nuclear weapons—are proliferating. If our enemies acquire these weapons, they are likely to try to use them.

The consequences of such an attack could be far more devastating than those we suffered on September 11— a chemical, biological, radiological, or nuclear terrorist attack in the United States could cause large numbers of casualties, mass psychological disruption, and contamination, and could overwhelm local medical capabilities.

Currently, chemical, biological, radiological, and nuclear detection capabilities are modest and response capabilities are dispersed throughout the country at every level of government. Responsibility for chemical, biological, radiological, and nuclear surveillance as well as for initial response efforts often rests with state and local hospitals and public health agencies.

Today, if a natural disaster or terrorist attack causes medical consequences that exceed local and state capabilities, the Department of Health and Human Services would coordinate the deployment of medical personnel, equipment, and pharmaceuticals among the Departments of Agriculture, Defense, Energy, Justice, Transportation, Veterans Affairs, the Environmental Protection Agency, the Federal Emergency Management Agency, General Services Administration, National Communications System, U.S. Postal Service, and the American Red Cross.

While the government's collaborative arrangements have proven adequate for a variety of natural disasters, the threat of terrorist attacks using chemical, biological, radiological, or nuclear weapons with potentially catastrophic consequences demands new approaches, a focused strategy, and a new organization. Our country has already expanded capabilities and improved coordination among federal agencies, but more can be done to prepare and respond.

### Major Initiatives

***Prevent terrorist use of nuclear weapons through better sensors and procedures.*** Our top scientific priority must be preventing terrorist use of nuclear weapons. The Department of Homeland Security will implement a new system of procedures and technologies to detect and prevent the transport of nuclear explosives toward our borders and into the United States.

The Department of Homeland Security will develop and deploy new inspection procedures and detection systems against the entry of such materials at all ports of entry in the United States and at major overseas cargo loading facilities. The Department—in cooperation with the Department of Transportation, state and local governments, and the private sector—will develop additional inspection procedures and detection systems throughout our national transportation structure to detect the movement of nuclear materials within the United States.

It will also initiate and sustain research and development efforts aimed at new and better passive and active detection systems.

***Detect chemical and biological materials and attacks.*** The federal government, with due attention to constraints such as the need for low operating costs, will develop sensitive and highly selective systems that detect the release of biological or chemical agents.



Make it difficult to by-pass security. This type of set-up only allows small service vehicles like golf carts to pass. Think of ways to slow or delay the Terrorist.



## CHAPTER 1 EXERCISE

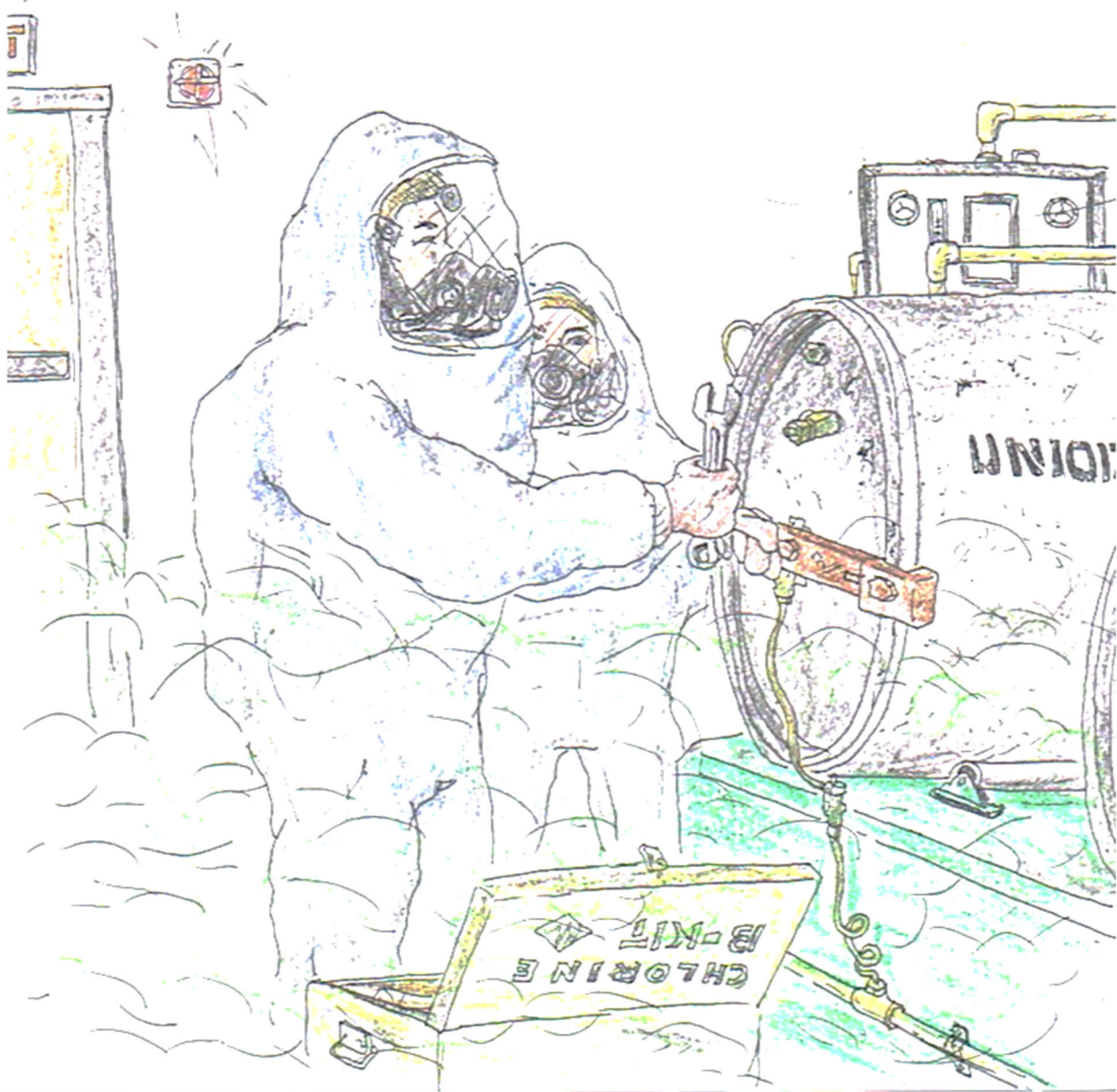
---

This is a chapter review, you can find the final exam on TLC's website under Assignments.

1. Have the events of 911 changed your views of security at your facility? Describe
2. Describe steps to improve your security since the September 11 attacks at your facility.
3. Describe the term "**Threat**".
4. Describe the term "**Vulnerability**".
5. Describe the term "**Terrorism**".
6. Describe the term "**Strategy**".
7. Describe the most vulnerable area at your facility, plant or yard.
8. How would you protect or secure this area? Describe in detail.
9. Describe the general security at your facility.
10. How would you strengthen the general security? Describe.

### ***What I Will Do As Follow-up To This Chapter...***

**Analyze two important areas:** Cost of security measures, and if these security measures limit Customer Service. Most experts claim that security measure upgrades will cost as much or more than the facility is worth.



## Chapter 2: First Responder Safety

**Section Focus:** You will learn the basics of First Responder Safety. At the end of this section, you the student will be able to understand and describe the proper first responder safety procedures. There is a post quiz at the end of this section to review your comprehension and a final examination in the Assignment for your contact hours.

**Scope/Background:** You as a first responder need to work hand-in-hand with members of all first responder disciplines -- law enforcement, fire services, emergency medical services and emergency management officials, as well as innovators and industry -- to develop capabilities that:

- Make first responders safer.
  - Improve communication tool security and effectiveness.
  - Enhance data and information sharing during daily, emergency or joint operations.
- Promote and sustain partnerships with responders and responder organizations across the nation at all levels.
- Help investigate cybercrime and cases involving digital evidence.
  - Secure 911 emergency call systems from cyberattacks.
  - Be familiar with the company's written procedures for respirator use in normal and emergency situations and understand why a respirator is necessary.
  - Understand the different types of respirators and their purposes.
  - Know how to make respirators fit correctly and how to use the respirator effectively in emergency situations.
  - Know the importance of and how to conduct regular inspections, cleaning, and maintenance of respirators.
  - Understand the limitations and capabilities of respirators.
  - Know how to recognize medical signs and symptoms that may limit or prevent the effective use of respirators.



As a first responder, safety is your most important concern. You must protect yourself so that you can protect your fellow responders and the public. If you do not arrive safely at the incident scene, or if you become injured or incapacitated in any way, you will not be able to provide the services required by the initial call for help.

We need to examine some of the pertinent issues of scene control, keeping your safety and survival in mind. The use of personal protective equipment (**PPE**) coupled with positive pressure self-contained breathing apparatus (**SCBA**) will greatly increase your safety. All emergency operations must be organized to be successful. Remember that the initial actions taken by the first responders will affect the final outcome of the incident.

Besides, an organized and well-managed incident creates a safer environment for all involved. One of the best ways to understand the nature of organization is to view it from a systems approach.

A system is a unit of interrelated, dependent parts or functions designed to achieve a common goal.

A good example is the human body. The body's systems--sensory, nervous, muscular, circulatory, reproductive, and skeletal--all play a role in sustaining life. If the systems are not properly interrelated and fail to function as one organism, life is threatened.

Similarly, if the emergency scene is not properly managed, the potential for loss of scene control exists. Not only is scene control lost, there could be other consequences resulting in greater loss of life or injury.

Therefore, the use of an integrated systems approach, such as incident command, is critical to the outcome of the incident.

**If you suspect a chemical, biological, or nuclear incident, this text does not provide you with the necessary training to completely protect yourself.**

**Your principal responsibility in this instance is to call those responders who have the appropriate training and equipment.**



Here is a multi-agency emergency response drill to a simulated Ammonia leak. We evacuated homes in a four block area and videoed taped and analyzed our strengths and weaknesses. The EPA will provide free plume software as part of the Risk Management Program so you can figure the possible damage from a chemical or gas leak. Fire Departments are willing to practice these drills with prior notification, and will even bring in other Fire Departments, the Red Cross and Helicopters to practice.







# Personal Protective Equipment Introduction

## Purpose

Your Employer is required to provide all Employees with required PPE to suit the task and known hazards. This section covers the requirements for Personal Protective Equipment with the exception of PPE used for respiratory protection or PPE required for hazardous material response to spills or releases. Applicable OSHA Standards are 1910 Subpart 1 App B and 1910.120 App B, 132, 133, 136, and 138.

## General Rules

### Design

All personal protective equipment shall be of safe design and construction for the work to be performed.

### Hazard Assessment and Equipment Selection

Hazard analysis procedures shall be used to assess the workplace to determine if hazards are present, or are likely to be present, which necessitate the use of personal protective equipment (PPE).

If such hazards are present, or likely to be present, the following actions will be taken:

- 1) Select, and have each affected Employee use, the proper PPE
- 2) Communicate selection decisions to each affected Employee
- 3) Select PPE that properly fits each affected employee.

### Defective and damaged equipment.

Defective or damaged personal protective equipment shall not be used.

## Training

All Employees who are required to use PPE shall be trained to know at least the following:

- 1) When PPE is necessary;
- 2) What PPE is necessary;
- 3) How to properly don, remove, adjust, and wear PPE;
- 4) The limitations of the PPE
- 5) The proper care, maintenance, useful life and disposal of the PPE.

Each affected Employee shall demonstrate an understanding of the training and the ability to use PPE properly, before being allowed to perform work requiring the use of PPE.

Certification of training for PPE is required by OSHA and shall be accomplished by using the Job Safety Checklist to verify that each affected Employee has received and understood the required PPE training.

## Personal Protective Equipment Selection

### Controlling Hazards

PPE devices alone should not be relied on to provide protection against hazards, but should be used in conjunction with guards, engineering controls, and sound manufacturing practices.

## **PPE Selection Guidelines**

The general procedure for selection of protective equipment is to:

- a) Become familiar with the potential hazards and the type of protective equipment that is available, and what it can do; i.e., splash protection, impact protection, etc.
- b) Compare the hazards associated with the environment (i.e., impact velocities, masses, projectile shape, radiation intensities) with the capabilities of the available protective equipment;
- c) select the protective equipment which ensures a level of protection greater than the minimum required to protect employees from the hazards
- d) fit the user with the protective device and give instructions on care and use of the PPE. It is very important that end users be made aware of all warning labels for and limitations of their PPE.

## **Fitting the Device**

Careful consideration must be given to comfort and fit. PPE that fits poorly will not afford the necessary protection. Continued wearing of the device is more likely if it fits the wearer comfortably. Protective devices are generally available in a variety of sizes. Care should be taken to ensure that the right size is selected.

## **Devices with Adjustable Features**

Adjustments should be made on an individual basis for a comfortable fit that will maintain the protective device in the proper position. Particular care should be taken in fitting devices for eye protection against dust and chemical splash to ensure that the devices are sealed to the face.

In addition, proper fitting of helmets is important to ensure that it will not fall off during work operations. In some cases, a chin strap may be necessary to keep the helmet on an employee's head (chin straps should break at a reasonably low force, however, so as to prevent a strangulation hazard). Where manufacturer's instructions are available, they should be followed carefully.

## **Eye and Face Protection**

Each affected employee shall use appropriate eye or face protection when exposed to eye or face hazards from flying particles, molten metal, liquid chemicals, acids or caustic liquids, chemical gases or vapors, or potentially injurious light radiation.

Each affected employee shall use eye protection that provides side protection when there is a hazard from flying objects. Detachable side protectors are acceptable.

Each affected employee who wears prescription lenses while engaged in operations that involve eye hazards shall wear eye protection that incorporates the prescription in its design, or shall wear eye protection that can be worn over the prescription lenses without disturbing the proper position of the prescription lenses or the protective lenses.

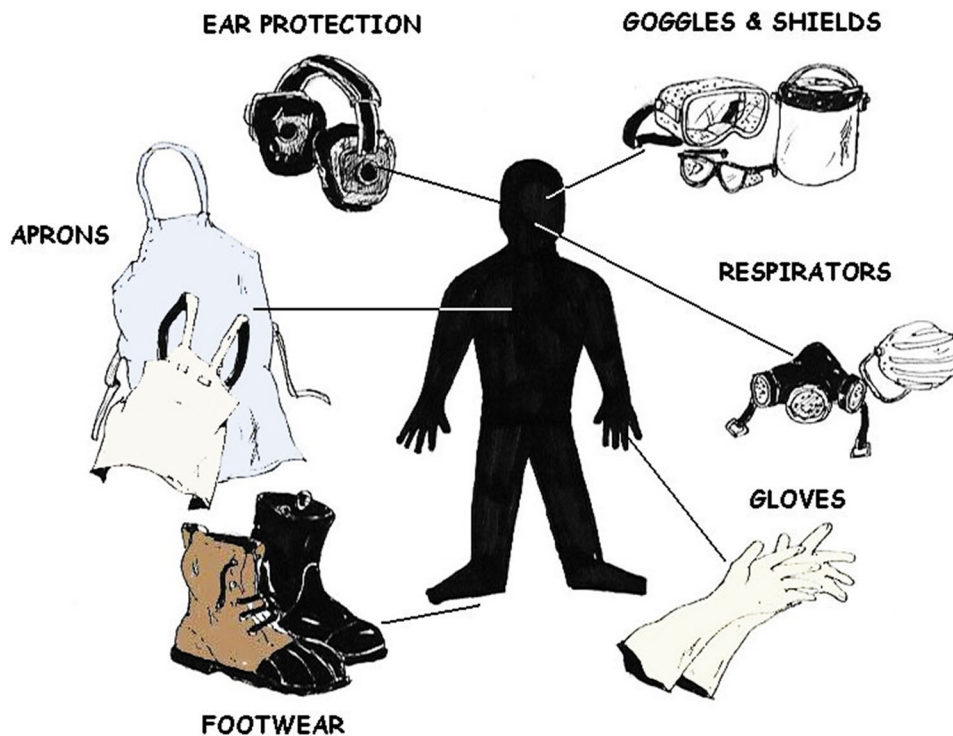
Eye and face PPE shall be distinctly marked to facilitate identification of the manufacturer.

Each affected employee shall use equipment with filter lenses that have a shade number appropriate for the work being performed for protection from injurious light radiation. The following is a listing of appropriate shade numbers for various operations.

## Filter Lenses for Protection Against Radiant Energy

Operations	Electrode Size 1/32 in	Arc Current	Protective Shade
Shielded metal arc welding	Less than 3	Less than 60	7
	3-5	60-160	8
	5-8	160-250	10
	More than 8	250-550	11
Torch brazing			3
Torch soldering			2

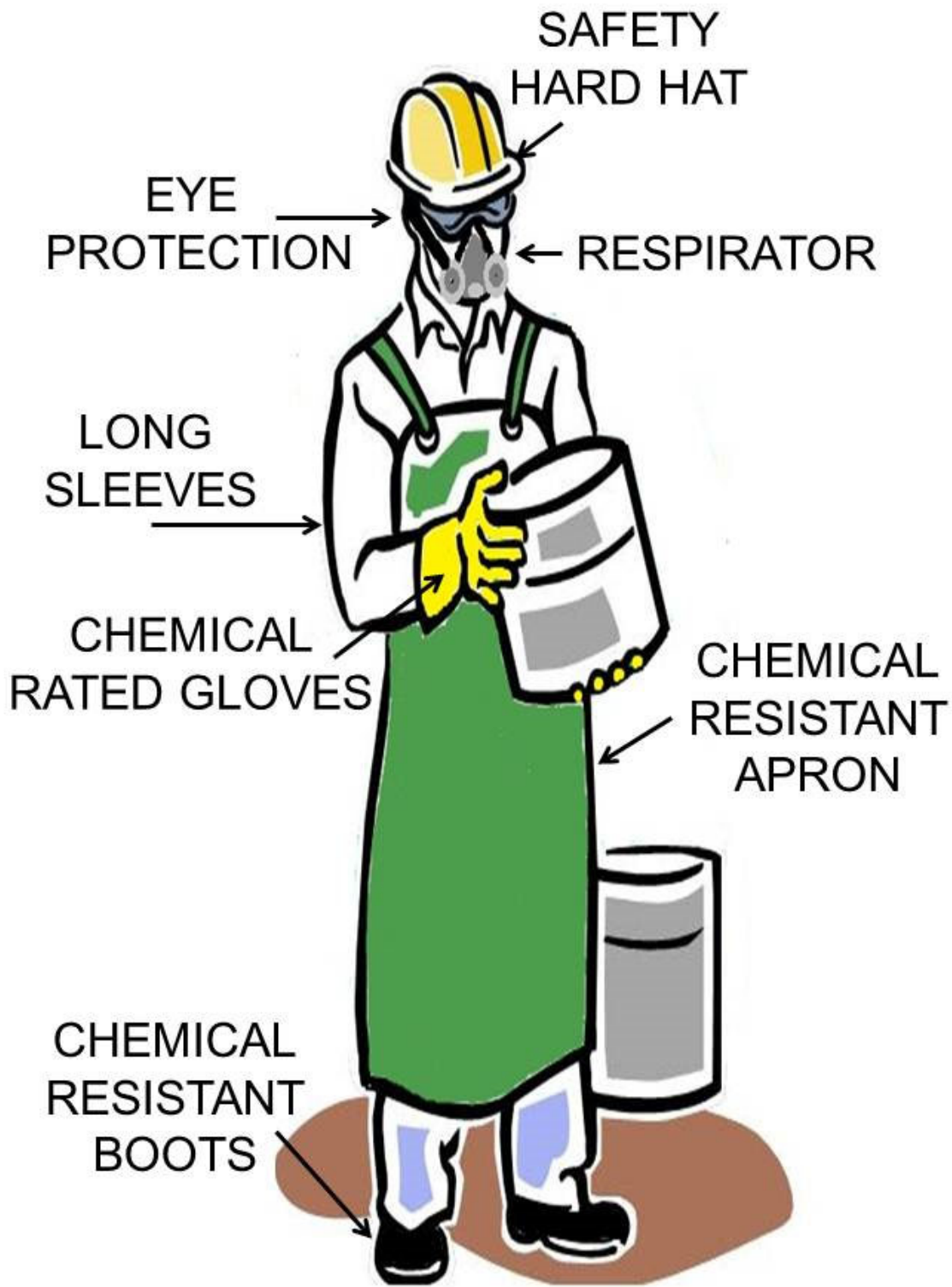
**Note:** as a rule of thumb, start with a shade that is too dark to see the weld zone. Then go to a lighter shade which gives sufficient view of the weld zone without going below the minimum. In oxyfuel gas welding or cutting where the torch produces a high yellow light, it is desirable to use a filter lens that absorbs the yellow or sodium line in the visible light of the (spectrum) operation.



## Selection chart guidelines for eye and face protection

The following chart provides general guidance for the proper selection of eye and face protection to protect against hazards associated with the listed hazard "source" operations.

Source	Hazard	Protection
<b>IMPACT</b> - Chipping, grinding machining, masonry work, woodworking, sawing, drilling, chiseling, powered fastening, riveting, and sanding	Flying fragments, objects, large chips, particles, sand, dirt, etc.	Spectacles with side protection, goggles, face shield  For severe exposure, use face shield
<b>HEAT</b> -Furnace operation and arc welding	Hot sparks	Face shields, spectacles with side. For severe exposure use faceshield.
<b>CHEMICALS</b> -Acid and chemical handling, degreasing, plating	Splash	Goggles, eyecup and cover types. For severe exposure, use face shield.
<b>DUST</b> - Woodworking, buffing, general, buffing, general dusty conditions.	Nuisance dust	Goggles, eye cup and cover type





UNSTABLE EXPLOSIVES



FLAMMABLE



OXIDIZER



COMPRESSED GAS



CORROSIVE



ACUTE TOXICITY



ACUTE TOXICITY  
(skin & eye irritant)



HUMAN HEALTH HAZARD



ACUTE/CHRONIC HAZARDS

**GLOBALLY HARMONIZED SYSTEM CLASSIFICATION LABELS**

## **Selection Guidelines for Head Protection**

All head protection is designed to provide protection from impact and penetration hazards caused by falling objects. Head protection is also available which provides protection from electric shock and burns. When selecting head protection, knowledge of potential electrical hazards is important.

Class A helmets, in addition to impact and penetration resistance, provide electrical protection from low-voltage conductors (they are proof tested to 2,200 volts).

Class B helmets, in addition to impact and penetration resistance; provide electrical protection from high-voltage conductors (they are proof tested to 20,000 volts).

Class C helmets provide impact and penetration resistance (they are usually made of aluminum which conducts electricity), and should not be used around electrical hazards.

Where falling object hazards are present, helmets must be worn. Some examples include: working below other workers who are using tools and materials which could fall; working around or under conveyor belts which are carrying parts or materials; working below machinery or processes which might cause material or objects to fall; and working on exposed energized conductors.

## **Foot Protection**

### **General Requirements**

Each affected employee shall wear protective footwear when working in areas where there is a danger of foot injuries due to falling or rolling objects, or objects piercing the sole, and where employee's feet are exposed to electrical hazards.

### **Selection Guidelines for Foot Protection**

Safety shoes and boots provide both impact and compression protection. Where necessary, safety shoes can be obtained which provide puncture protection.

In some work situations, metatarsal protection should be provided, and in other special situations electrical conductive or insulating safety shoes would be appropriate.

Safety shoes or boots with impact protection would be required for carrying or handling materials such as packages, objects, parts or heavy tools, which could be dropped; and, for other activities where objects might fall onto the feet.

Safety shoes or boots with compression protection would be required for work activities involving skid trucks (manual material handling carts), around bulk rolls (such as paper rolls) and around heavy pipes, all of which could potentially roll over an employee's feet.

Safety shoes or boots with puncture protection would be required where sharp objects such as nails, wire, tacks, screws, large staples, scrap metal etc., could be stepped on by employees causing a foot injury.

## Hand Protection

### General Requirements

Hand protection is required when employees' hands are exposed to hazards such as those from skin absorption of harmful substances; severe cuts or lacerations; severe abrasions; punctures; chemical burns; thermal burns; and harmful temperature extremes.

### Selection guidelines for hand protection

Selection of hand PPE shall be based on an evaluation of the performance characteristics of the hand protection relative to the task(s) to be performed, conditions present, duration of use, and the hazards and potential hazards identified. Gloves are often relied upon to prevent cuts, abrasions, burns, and skin contact with chemicals that are capable of causing local or systemic effects following dermal exposure.

There is no glove that provides protection against all potential hand hazards, and commonly available glove materials provide only limited protection against many chemicals. Therefore, it is important to select the most appropriate glove for a particular application and to determine how long it can be worn, and whether it can be reused. It is also important to know the performance characteristics of gloves relative to the specific hazard anticipated; e.g., chemical hazards, cut hazards, flame hazards, etc.

Before purchasing gloves, request documentation from the manufacturer that the gloves meet the appropriate test standard(s) for the hazard(s) anticipated. Other factors to be considered for glove selection in general include:

(A) As long as the performance characteristics are acceptable, in certain circumstances, it may be more cost effective to regularly change cheaper gloves than to reuse more expensive types.

(B) The work activities of the employee should be studied to determine the degree of dexterity required, the duration, frequency, and degree of exposure of the hazard, and the physical stresses that will be applied.



### Selection of gloves for protection against chemical hazards:

(A) The toxic properties of the chemical(s) must be determined; in particular, the ability of the chemical to cause local effects on the skin and/or to pass through the skin and cause systemic effects.

(B) Generally, any "**chemical resistant**" glove can be used for dry powders;

(C) For mixtures and formulated products (unless specific test data are available), a glove should be selected on the basis of the chemical component with the shortest breakthrough time, since it is possible for solvents to carry active ingredients through polymeric materials.

(D) Employees must be able to remove the gloves in such a manner as to prevent skin contamination.



## Protective Clothing Applications

A. *The purpose of chemical protective clothing and equipment* is to shield or isolate individuals from the chemical, physical, and biological hazards that may be encountered during hazardous materials operations. During chemical operations, it is not always apparent when exposure occurs. Many chemicals pose invisible hazards and offer no warning properties.

B. These guidelines describe the various types of clothing that are appropriate for use in various chemical operations, and provides recommendations in their selection and use. The final paragraph discusses heat stress and other key physiological factors that must be considered in connection with protective clothing use.

C. It is important that protective clothing users realize that no single combination of protective equipment and clothing is capable of protecting you against all hazards. Thus, protective clothing should be used in conjunction with other protective methods. For example, engineering or administrative controls to limit chemical contact with personnel should always be considered as an alternative measure for preventing chemical exposure.

The use of protective clothing can itself create significant wearer hazards, such as heat stress, physical and psychological stress, in addition to impaired vision, mobility, and communication. In general, the greater the level of chemical protective clothing, the greater the associated risks.

For any given situation, equipment and clothing should be selected that provide an adequate level of protection. Overprotection as well as under-protection can be hazardous and should be avoided.

## II. DESCRIPTIONS.

### A. PROTECTIVE CLOTHING APPLICATIONS.

1. Protective clothing must be worn whenever the wearer faces potential hazards arising from chemical exposure. Some examples include:

- **Emergency response;**
- **Chemical manufacturing and process industries;**
- **Hazardous waste site cleanup and disposal;**
- **Asbestos removal and other particulate operations; and**
- **Agricultural application of pesticides.**

2. Within each application, there are several operations which require chemical protective clothing. For example, in emergency response, the following activities dictate chemical protective clothing use:

- ✓ **Site Survey:** The initial investigation of a hazardous materials incident; these situations are usually characterized by a large degree of uncertainty and mandate the highest levels of protection.
- ✓ **Rescue:** Entering a hazardous materials area for the purpose of removing an exposure victim; special considerations must be given to the contamination of the victim and to how the selected protective clothing may affect the ability of the wearer to carry out rescue.

- ✓ **Spill Mitigation:** Entering a hazardous materials area to prevent a potential spill or to reduce the hazards from an existing spill (i.e., applying a chlorine kit on railroad tank car). Protective clothing must accommodate the required tasks without sacrificing adequate protection.
- ✓ **Emergency Monitoring:** Outfitting personnel in protective clothing for the primary purpose of observing a hazardous materials incident without entry into the spill site. This may be applied to monitoring contract activity for spill cleanup.
- ✓ **Decontamination:** Applying decontamination procedures to personnel or equipment leaving the site; in general a lower level of protective clothing is used by personnel involved in decontamination.

**B. THE CLOTHING ENSEMBLE.** The approach in selecting personal protective clothing must encompass an "**ensemble**" of clothing and equipment items which are easily integrated to provide both an appropriate level of protection and still allow one to carry out activities involving chemicals.

In many cases, simple protective clothing by itself may be sufficient to prevent chemical exposure, such as wearing gloves in combination with a splash apron and faceshield (or safety goggles).

**1. The following is a checklist of components that may form the chemical protective ensemble:**

- Protective clothing (suit, coveralls, hoods, gloves, boots);
- Respiratory equipment (SCBA, combination SCBA/SAR, air purifying respirators);
- Cooling system (ice vest, air circulation, water circulation);
- Communications device;
- Head protection;
- Eye protection;
- Ear protection;
- Inner garment; and
- Outer protection (overgloves, overboots, flashcover).

**2. Factors that affect the selection of ensemble components include:**

- ✓ How each item accommodates the integration of other ensemble components. Some ensemble components may be incompatible due to how they are worn (e.g., some SCBA's may not fit within a particular chemical protective suit or allow acceptable mobility when worn).
- ✓ The ease of interfacing ensemble components without sacrificing required performance (e.g. a poorly fitting overglove that greatly reduces wearer dexterity).
- ✓ Limiting the number of equipment items to reduce donning time and complexity (e.g. some communications devices are built into SCBA's which as an unit are NIOSH certified).

### C. LEVEL OF PROTECTION.

1. Table VIII:1-1 lists ensemble components based on the widely used EPA Levels of Protection: Levels A, B, C, and D. These lists can be used as the starting point for ensemble creation; however, each ensemble must be tailored to the specific situation in order to provide the most appropriate level of protection.

For example, if an emergency response activity involves a highly contaminated area or if the potential of contamination is high, it may be advisable to wear a disposable covering, such as Tyvek coveralls or PVC splash suits, over the protective ensemble.

#### TABLE VIII:1-1. EPA LEVELS OF PROTECTION

##### LEVEL A:

Vapor protective suit (meets NFPA 1991)

Pressure-demand, full-face SCBA

Inner chemical-resistant gloves, chemical-resistant safety boots, two-way radio communication

**OPTIONAL:** Cooling system, outer gloves, hard hat

**Protection Provided:** Highest available level of respiratory, skin, and eye protection from solid, liquid and gaseous chemicals.

**Used When:** The chemical(s) have been identified and have high level of hazards to respiratory system, skin and eyes. Substances are present with known or suspected skin toxicity or carcinogenicity. Operations must be conducted in confined or poorly ventilated areas.

**Limitations:** Protective clothing must resist permeation by the chemical or mixtures present. Ensemble items must allow integration without loss of performance.

##### LEVEL B:

Liquid splash-protective suit (meets NFPA 1992)

Pressure-demand, full-facepiece SCBA

Inner chemical-resistant gloves, chemical-resistant safety boots, two-way radio communications  
Hard hat.

**OPTIONAL:** Cooling system, outer gloves

**Protection Provided:** Provides same level of respiratory protection as Level A, but less skin protection. Liquid splash protection, but no protection against chemical vapors or gases.

**Used When:** The chemical(s) have been identified but do not require a high level of skin protection. Initial site surveys are required until higher levels of hazards are identified. The primary hazards associated with site entry are from liquid and not vapor contact.

**Limitations:** Protective clothing items must resist penetration by the chemicals or mixtures present. Ensemble items must allow integration without loss of performance.

##### LEVEL C:

Support Function Protective Garment (meets NFPA 1993)

Full-facepiece, air-purifying, canister-equipped respirator

Chemical resistant gloves and safety boots

Two-way communications system, hard hat

**OPTIONAL:** Faceshield, escape SCBA

**Protection Provided:** The same level of skin protection as Level B, but a lower level of respiratory protection. Liquid splash protection but no protection to chemical vapors or gases.

**Used When:** Contact with site chemical(s) will not affect the skin. Air contaminants have been identified and concentrations measured. A canister is available which can remove the contaminant. The site and its hazards have been completely characterized.

**Limitations:** Protective clothing items must resist penetration by the chemical or mixtures present. Chemical airborne concentration must be less than IDLH levels. The atmosphere must contain at least 19.5% oxygen.

### **Not Acceptable for Chemical Emergency Response**

#### **LEVEL D:**

Coveralls, safety boots/shoes, safety glasses or chemical splash goggles

**OPTIONAL:** Gloves, escape SCBA, face-shield

**Protection Provided:** No respiratory protection, minimal skin protection.

**Used When:** The atmosphere contains no known hazard. Work functions preclude splashes, immersion, potential for inhalation, or direct contact with hazard chemicals.

**Limitations:** This level should not be worn in the Hot Zone. The atmosphere must contain at least 19.5% oxygen.

### **Not Acceptable for Chemical Emergency Response**

#### **D.**

1. The type of equipment used and the overall level of protection should be reevaluated periodically as the amount of information about the chemical situation or process increases, and when workers are required to perform different tasks. Personnel should upgrade or downgrade their level of protection only with concurrence with the site supervisor, safety officer, or plant industrial hygienist.
2. The recommendations in Table VIII:1-1 serve only as guidelines. It is important for you to realize that selecting items by how they are designed or configured alone is not sufficient to ensure adequate protection. In other words, just having the right components to form an ensemble is not enough. The EPA levels of protection do not define what performance the selected clothing or equipment must offer. Many of these considerations are described in the "**limiting criteria**" column of Table VIII: 1-1. Additional factors relevant to the various clothing and equipment items are described in subsequent Paragraphs.

#### **E. ENSEMBLE SELECTION FACTORS.**

1. **Chemical Hazards.** Chemicals present a variety of hazards such as toxicity, corrosiveness, flammability, reactivity, and oxygen deficiency. Depending on the chemicals present, any combination of hazards may exist.
2. **Physical Environment.** Chemical exposure can happen anywhere: in industrial settings, on the highways, or in residential areas. It may occur either indoors or outdoors; the environment may be extremely hot, cold, or moderate; the exposure site may be relatively uncluttered or rugged, presenting a number of physical hazards; chemical handling activities may involve entering confined spaces, heavy lifting, climbing a ladder, or crawling on the ground.

**The choice of ensemble components must account for these conditions.**

3. **Duration of Exposure.** The protective qualities of ensemble components may be limited to certain exposure levels (e.g. material chemical resistance, air supply). The decision for ensemble use time must be made assuming the worst case exposure so that safety margins can be applied to increase the protection available to the worker.
4. **Protective Clothing or Equipment Available.** Hopefully, an array of different clothing or equipment is available to workers to meet all intended applications. Reliance on one particular clothing or equipment item may severely limit a facility's ability to handle a broad range of chemical exposures. In its acquisition of equipment and clothing, the safety department or other responsible authority should attempt to provide a high degree of flexibility while choosing protective clothing and equipment that is easily integrated and provides protection against each conceivable hazard.

**F. CLASSIFICATION OF PROTECTIVE CLOTHING.**

**Personal protective clothing includes the following:**

- ✓ Fully encapsulating suits;
- ✓ Non-encapsulating suits;
- ✓ Gloves, boots, and hoods;
- ✓ Firefighter's protective clothing;
- ✓ Proximity, or approach clothing;
- ✓ Blast or fragmentation suits; and
- ✓ Radiation-protective suits.

1. Firefighter turnout clothing, proximity gear, blast suits, and radiation suits by themselves are not acceptable for providing adequate protection from hazardous chemicals.

2. Table VIII:1-2 describes various types of protection clothing available, details the type of protection they offer, and lists factors to consider in their selection and use.

**TABLE VIII: 1-2. TYPES OF PROTECTIVE CLOTHING FOR FULL BODY PROTECTION**

Description

Type of Protection

Use Considerations

Fully encapsulating suit

- One-piece garment. Boots and gloves may be integral, attached and replaceable, or separate.
- Protects against splashes, dust gases, and vapors.
- Does not allow body heat to escape. May contribute to heat stress in wearer, particularly if worn in conjunction with a closed-circuit SCBA; a cooling garment may be needed. Impairs worker mobility, vision, and communication.

Non-encapsulating suit

- Jacket, hood, pants or bib overalls, and one-piece coveralls.

- Protects against splashes, dust, and other materials but not against gases and vapors. Does not protect parts of head or neck.
- Do not use where gas-tight or pervasive splashing protection is required. May contribute to heat stress in wearer. Tape-seal connections between pant cuffs and boots and between gloves and sleeves.

#### **Aprons, leggings, and sleeve protectors**

- Fully sleeved and gloved apron. Separate coverings for arms and legs. Commonly worn over non-encapsulating suit.
- Provides additional splash protection of chest, forearms, and legs.

Whenever possible, should be used over a non-encapsulating suit to minimize potential heat stress. Useful for sampling, labeling, and analysis operations. Should be used only when there is a low probability of total body contact with contaminants.

#### **Firefighters' protective clothing**

Gloves, helmet, running or bunker coat, running or bunker pants (NFPA No. 1971, 1972, 1973, and boots (1974).

Protects against heat, hot water, and some particles. Does not protect against gases and vapors, or chemical permeation or degradation. NFPA Standard No. 1971 specifies that a garment consists of an outer shell, an inner liner and a vapor barrier with a minimum water penetration of 25 lb/in<sup>2</sup> (1.8 kg/cm<sup>2</sup>) to prevent passage of hot water.

**Decontamination is difficult.** Should not be worn in areas where protection against gases, vapors, chemical splashes or permeation is required.

Proximity garment (approach suit)

- ✓ One- or two-piece over-garment with boot covers, gloves, and hood of aluminized nylon or cotton fabric. Normally worn over other protective clothing, firefighters' bunker gear, or flame-retardant coveralls.
- ✓ Protects against splashes, dust, gases, and vapors.
- ✓ Does not allow body heat to escape. May contribute to heat stress in wearer, particularly if worn in conjunction with a closed-circuit SCBA; a cooling garment may be needed. Impairs worker mobility, vision, and communication.

#### **Blast and fragmentation suit**

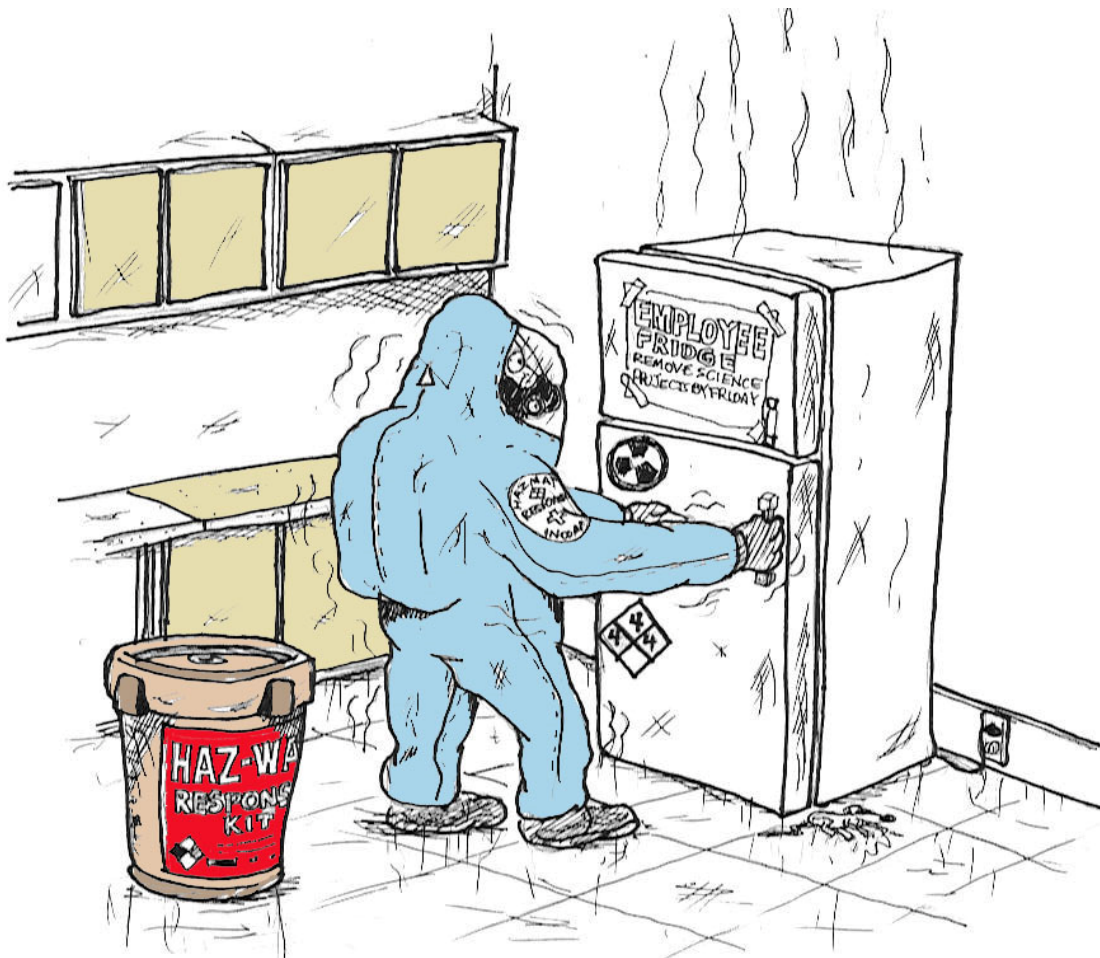
- ✓ Blast and fragmentation vests and clothing, bomb blankets, and bomb carriers.
- ✓ Provides some protection against very small detonations. Bomb blankets and baskets can help redirect a blast.
- ✓ Does not provide for hearing protection.

### Radiation-contamination protective suit

- ✓ Various types of protective clothing designed to prevent contamination of the body by radioactive particles.
- ✓ Protects against alpha and beta particles. Does not protect against gamma radiation.
- ✓ Designed to prevent skin contamination. If radiation is detected on site, consult an experienced radiation expert and evacuate personnel until the radiation hazard has been evaluated.

### Flame/fire retardant coveralls.

- ✓ Normally worn as an undergarment.
- ✓ Provides protection from flash fires.
  - ✓ Adds bulk and may exacerbate heat stress problems and impair mobility



### Are you prepared for an emergency?

How about PPE for your visitors, how about enough materials, food and drinking water for several days.





## Respiratory Protection Sub-Section

### General

In the Respiratory Protection program, hazard assessment and selection of proper respiratory PPE is conducted in the same manner as for other types of PPE. In the control of those occupational diseases caused by breathing air contaminated with harmful dusts, fogs, fumes, mists, gases, smokes, sprays, or vapors, the primary objective shall be to prevent atmospheric contamination.

This shall be accomplished as far as feasible by accepted engineering control measures (for example, enclosure or confinement of the operation, general and local ventilation, and substitution of less toxic materials).

When effective engineering controls are not feasible, or while they are being instituted, appropriate respirators shall be used.

**References: OSHA Standards *Respiratory Protection* (29 CFR 1910.134)**

### Why Respirators Are Needed

Respirators protect against the inhalation of dangerous substances (vapors, fumes, dust, gases). They can also provide a separate air supply in a very hazardous situation.

### ***Some of the health hazards that respirators prevent include***

- *Lung damage*
- *Respiratory diseases*
- *Cancer and other illnesses.*



### Respiratory Protection Responsibilities

The employer is responsible for:

- Providing training in the use and care of respirators
- Ensuring that equipment is adequate, sanitary, and reliable
- Allowing employees to leave area if ill, for breaks, and to obtain parts
- Fit testing
- Providing annual medical evaluation

Providing a powered air-purifying respirator (**PAPR**) if an employee cannot wear a tight-fitting respirator.

### The employee is responsible for:

- Properly using respirators

### Maintaining respirator properly

- Reporting malfunctions
- Reporting medical changes

### Selection of Respiratory Protection

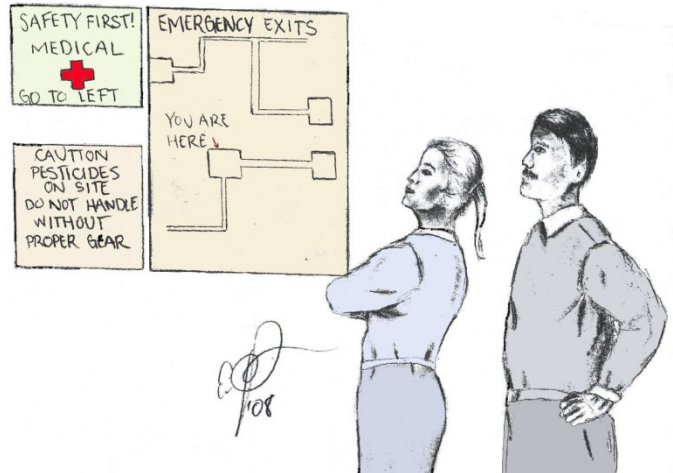
When choosing the correct protection for your work environment, it is important to consider:

- Identification of the substance or substances for which respiratory protection is necessary
- A substance's safety data sheet (**SDS**) (it will state which type of respirator is most effective for the substance)
- Activities of the workers
- Hazards of each substance and its properties
- Maximum levels of air contamination expected
- Probability of oxygen deficiency
- Period of time workers will need to use the respiratory protection devices
- Capabilities and physical limitations of the device used

### Types of Respirators *The following is a description of different types of respirators.*

#### Commonly used Respirators

- **Disposable Dust masks** are worn over the nose and mouth to protect the respiratory system from certain nuisance dusts, mists, etc. They can only provide protection against particular contaminants as specified by the manufacturer (e.g., general dust, fiberglass, etc.). These dust masks cannot be fit tested, and are generally single use. They are not recognized as respiratory protection and may not be worn if a potential for overexposure exists. They are not included in most companies' Respiratory Protection Programs.



- **Half-Face Respirators** with interchangeable filter cartridges can protect the respiratory system from hazardous dusts, fumes, mists, etc. They can only provide protection against certain contaminants up to limited concentrations specified by the manufacturer for the particular cartridge type used (e.g., toluene, acetone).

These generally operate under negative pressure within the respirator, which is created by the wearer breathing through the filter cartridges. As the protection is only gained if there is a proper seal of the respirator face piece, this type requires fit testing prior to respirator assignment and a fit check prior to each use.

- **Full-Face Respirators** operate under the same principle and requirements as the half-face type, however, they offer a better facepiece fit and also protect the wearer's eyes from particularly irritating gases or vapors.

- **Full-face, helmet** or hood-type powered air purifying respirators (**PAPRs**) operate under positive pressure inside the facepiece using a battery operated motor blower assembly to force air through a filter cartridge into the wearer's breathing zone. Use of these respirators is also subject to the manufacturers' guidelines.

#### **Less commonly Used Types Respirators (Air Supplying)**

- **Air-Line Respirators** supply clean air through a small diameter hose from a compressor or compressed air cylinders. The wearer must be attached to the hose at all times, which limits mobility. Use of these respirators is subject to the manufacturers' guidelines.
- **Self-Contained Breathing Apparatus (SCBA)** respirators supply clean air from a compressed air tank carried on the back of the wearer. These types of respirators are highly mobile and are used primarily for emergency response or rescue work, since only a limited amount of air can be supplied by a single tank, generally 20-60 minutes. Units must be thoroughly inspected on a monthly basis and written records must be kept of all inspections, operator training, etc. Use of these respirators is subject to the manufacturer's guidelines

#### **Basic Types of Respirators**

**Air-purifying or filtering respirators.** Such respirators are used when there is enough oxygen (at least 19.5 percent) and contaminants are present below IDLH level. The respirator filters out or chemically "**scrubs**" contaminants, usually with a replaceable filter.

Use color-coded filter cartridges or canisters for different types of contaminants. It's important to select the right filter for the situation.

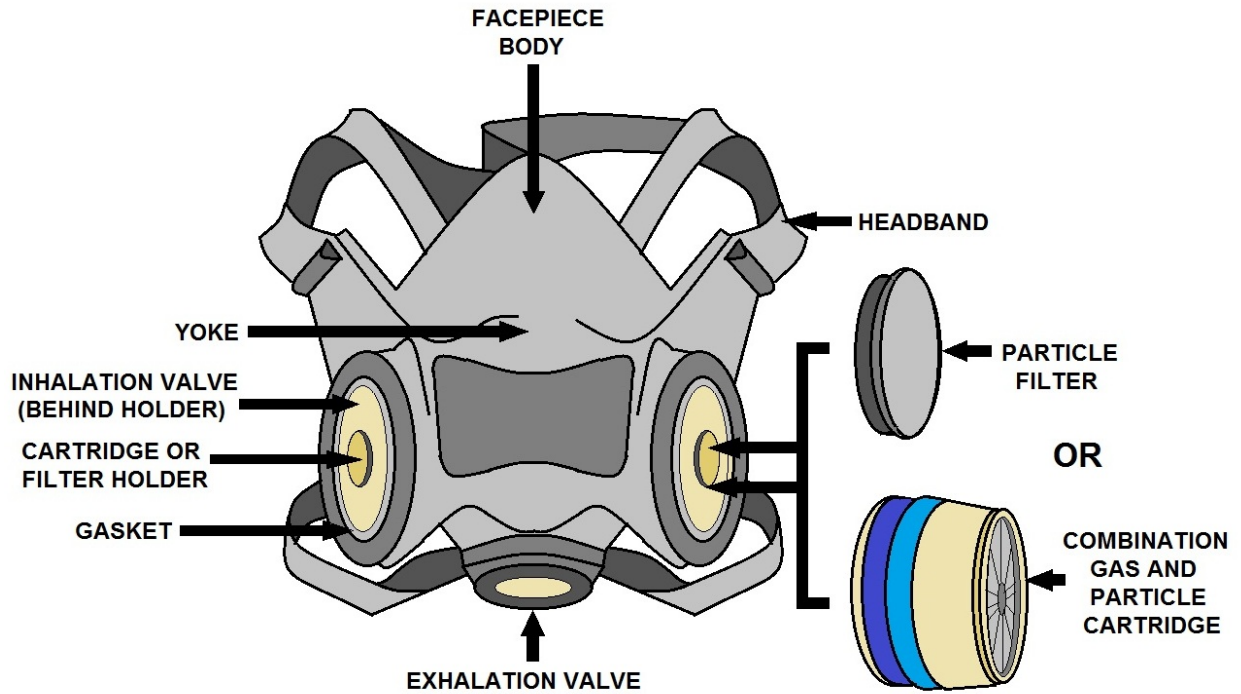
**Air-supplying respirators.** These respirators are required when air-purifying respirators aren't effective.

Air-purifying respirators are not sufficient in the following settings:

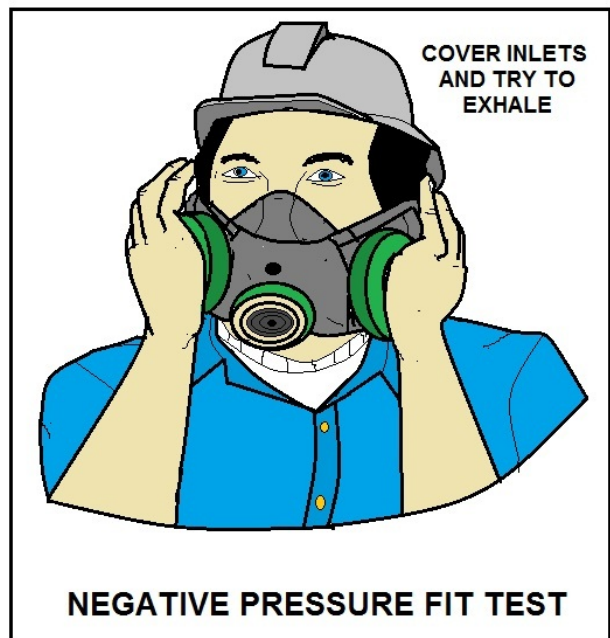
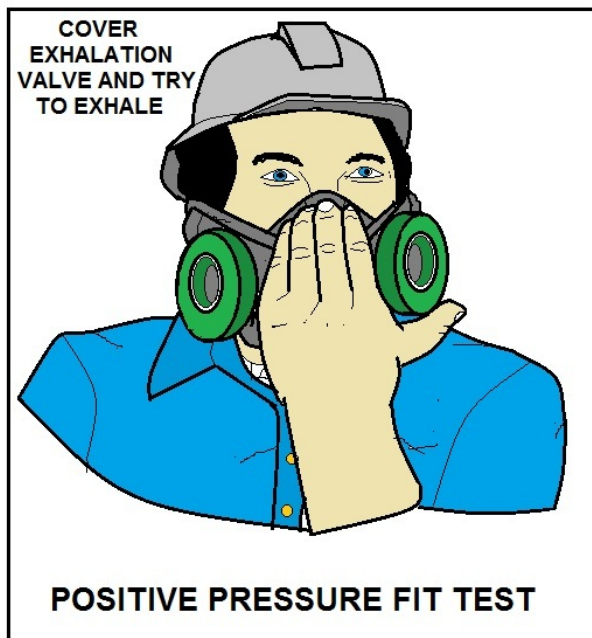
- When there is not enough oxygen
- Confined spaces
- When contaminants cannot be filtered out
- When contaminants are at or above IDLH level.

#### **Different kinds of air-supplying respirators include**

- Those connected by hose to stationary air supply (airline)
- Portable tank self-contained breathing apparatus (**SCBA**).



**BASIC PARTS OF A HALF-FACEPIECE RESPIRATOR**



**POSITIVE AND NEGATIVE PRESSURE FIT CHECKS**

## Gas and Vapor Contaminants

Gas and vapor contaminants can be classified according to their chemical characteristics. True gaseous contaminants are similar to air in that they possess the same ability to diffuse freely within an area or container. Nitrogen, chlorine, carbon monoxide, carbon dioxide and sulfur dioxide are examples.

Vapors are the gaseous state of substances that are liquids or solids at room temperature. They are formed when the solid or liquid evaporates. Gasoline, solvents and paint thinners are examples of liquids that evaporate easily, producing vapors.

***In terms of chemical characteristics, gaseous contaminants may be classified as follows:***

- **Inert Gases** —These include such true gases as helium, argon, neon, etc. Although they do not metabolize in the body, these gases represent a hazard because they can produce an oxygen deficiency by displacement of air.
- **Acidic Gases** —Often highly toxic, acidic gases exist as acids or produce acids by reaction with water. Sulfur dioxide, hydrogen sulfide and hydrogen chloride are examples.
- **Alkaline Gases** —These gases exist as alkalis or produce alkalis by reaction with water. Ammonia and phosgene are two examples.

***In terms of chemical characteristics, vaporous contaminants may be classified as follows:***

- **Organic Compounds** —Contaminants in this category can exist as true gases or vapors produced from organic liquids. Gasoline, solvents and paint thinners are examples.
- **Organometallic Compounds** —These are generally comprised of metals attached to organic groups. Tetraethyllead and organic phosphates are examples.

### **Hazard Assessment**

Proper assessment of the hazard is the first important step to protection. This requires a thorough knowledge of processes, equipment, raw materials, end-products and by-products that can create an exposure hazard.

To determine an atmosphere's oxygen content or concentration levels of particulate and/or gaseous contaminants, air samples must be taken with proper sampling instruments during all conditions of operation. The sampling device and the type and frequency of sampling (spot testing or continuous monitoring) will be dictated by the exposure and operating conditions.

Breathing zone samples are recommended and sampling frequency should be sufficient to assess the average exposure under the variable operating and exposure conditions.

Should contaminant concentrations exceed exposure limits recommended by the American Conference of Governmental Industrial Hygienists (**ACGIH**), OSHA or NIOSH, hazard control procedures must be implemented promptly.

Exposure monitoring plays a critical role in the respirator selection process. The results from such tests will help you determine whether respiratory protection is needed and, if it is, the type of respirator required. Generally, respirator selection is based on three factors:

- The results of your atmospheric monitoring or sampling program;
- The accepted ACGIH, OSHA or NIOSH exposure limits for the substance(s) present;
- The maximum use concentration (of a substance) for which a respirator can be used.

Exposure limits include ACGIH Threshold Limit Values (**TLVs**), OSHA Permissible Exposure Limits (**PELs**), NIOSH Recommended Exposure Levels (**RELs**) and AIHA Workplace Environmental Exposure Levels (**WEELs**). These values are guides for exposure concentrations that healthy individuals can normally tolerate for eight hours a day, five days a week without harmful effects. Unless otherwise noted, exposure limits are eight-hour, time-weighted-average (**TWA**) concentrations.

In general, gas and vapor exposure limits are expressed in ppm by volume (parts of contaminant per million parts of air), while particulate concentrations are expressed as mg/m<sup>3</sup> (milligrams of concentrations per cubic meter of air). For substances that can exist in more than one form (particulate or gaseous), concentrations are expressed in both values.

It is important to note that exposure limits and other exposure standards are constantly changing as more data is gathered about specific chemicals and substances. As such, you must be certain that you are using the most recent data when determining allowable exposure levels for employees.

### **Hazard Control**

Hazard control should start at the process, equipment and plant design levels where contaminants can be effectively controlled at the outset. With operating processes, the problem becomes more difficult. In all cases, however, consideration should be given to the use of effective engineering controls to eliminate and/or reduce exposures to respiratory hazards.

This includes consideration of process encapsulation or isolation, use of less toxic materials in the process and suitable exhaust ventilation, filters and scrubbers to control the effluents.

Because it is sometimes not practical to maintain engineering controls that eliminate all airborne concentrations of contaminants, proper respiratory protective devices should be used whenever such protection is required.

### **Hazard Assessment or Hazard Certification sheet example on the following page.**

Even if you have a written RP Program and complete training records, OSHA will ask for a hazard certification or assessment form on where or why you need RP. For example, if you were required to don SCBA to change a chlorine cylinder once a week, OSHA would request to see how that task was evaluated and certified.



# HAZARD ASSESSMENT SURVEY DATA SHEET

DATE OF EVALUATION:	DATE LAST EVALUATED: N/A
<b>DEPARTMENT:</b>	
DEPARTMENT:	TELEPHONE:
ADDRESS/LOCATION:	NAME OF SECTION SUPERVISOR:
Actions are required by: 29 CFR 1910.1200, 29 CFR 1910.146 and your business or city rules.	NAME OF HAZARD COMMUNICATION PROGRAM MONITOR:
<b>NON-ROUTINE POTENTIAL HAZARDS</b> (Describe the Process) (Who, What, When, Where, How, Why) (Review MSDS)	
<b>EVALUATION</b> (Your Findings/Discrepancies)	
<b>CONTROLS</b> (Existing or Recommended Protective Equipment, Engineering or Administrative Controls)	
<b>Existing:</b>	
<b>Recommended:</b>	
Surveyed By:	Reviewed By:





## Glossary of Respiratory Protection Terms

The following definitions are important terms used in the respiratory protection standard and terms that will assist in the understanding and the application of the NIOSH decision logic.

**Air-Purifying Respirator:** A respirator with an air-purifying filter, cartridge, or canister that removes specific air contaminants by passing ambient air through the air-purifying element. OSHA Definition

**Assigned Protection Factor (APF):** See PROTECTION FACTOR. NIOSH Definition

**Assigned Protection Factor (APF):** [Reserved] OSHA Definition

**Atmosphere-Supplying Respirator:** A respirator that supplies the respirator user with breathing air from a source independent of the ambient atmosphere, and includes supplied-air respirators (SARs) and self-contained breathing apparatus (**SCBA**) units. OSHA Definition

**Breakthrough:** The penetration of challenge material(s) through a gas or a vapor air-purifying element. The quantity or extent of breakthrough during service life testing is often referred to as the percentage of the input concentration. NIOSH Definition

**Canister or Cartridge:** A container with a filter, sorbent, or catalyst, or combination of these items, which removes specific contaminants from the air passed through the container. OSHA Definition

**Demand Respirator:** An atmosphere-supplying respirator that admits breathing air to the facepiece only when a negative pressure is created inside the facepiece by inhalation. OSHA Definition

**Disposable Respirators:** A respirator that is discarded after the end of its recommended period of use, after excessive resistance or physical damage, or when odor breakthrough or other warning indicators render the respirator unsuitable for further use. NIOSH Definition

**Dust:** A solid, mechanically produced particle with a size ranging from submicroscopic to macroscopic. NIOSH Definition

**Emergency Respirator Use Situation:** A situation that requires the use of respirators due to the unplanned generation of a hazardous atmosphere (often of unknown composition) caused by an accident, mechanical failure, or other means and that requires evacuation of personnel or immediate entry for rescue or corrective action. NIOSH Definition

**Emergency Situation:** Any occurrence such as, but not limited to, equipment failure, rupture of containers, or failure of control equipment that may or does result in an uncontrolled significant release of an airborne contaminant. OSHA Definition

**Employee Exposure:** Exposure to a concentration of an airborne contaminant that would occur if the employee were not using respiratory protection. OSHA Definition

**End-Of-Service-Life Indicator (ESLI):** A system that warns the respirator user of the approach of the end of adequate respiratory protection; for example, that the sorbent is approaching saturation or is no longer effective. OSHA Definition

**Escape Gas Mask:** A gas mask that consists of a half-mask facepiece or mouthpiece, a canister, and associated connections, and that is designed for use during escape-only from hazardous atmospheres. NIOSH Definition

**Escape Only Respirator:** Respiratory devices that are designed for use only during escape from hazardous atmospheres. NIOSH Definition

**Escape-Only Respirator:** A respirator intended to be used only for emergency exit. OSHA Definition

**Filter or Air-Purifying Element:** A component used in respirators to remove solid or liquid aerosols from the inspired air. OSHA Definition

**Filtering Facepiece:** A particulate respirator with a filter as an integral part of the facepiece or with the entire facepiece composed of the filtering medium. (See SINGLE-USE DUST or DUST and MIST RESPIRATORS and DISPOSABLE RESPIRATORS.) NIOSH Definition

**Filtering Facepiece (Dust Mask):** A negative pressure particulate respirator with a filter as an integral part of the facepiece or with the entire facepiece composed of the filtering medium. OSHA Definition

**Fit Factor:** A quantitative measure of the fit of a specific respirator facepiece to a particular individual. NIOSH Definition

**Fit Factor:** A quantitative estimate of the fit of a particular respirator to a specific individual, and typically estimates the ratio of the concentration of a substance in ambient air to its concentration inside the respirator when worn. OSHA Definition

**Fit Test:** Means the use of a protocol to qualitatively or quantitatively evaluate the fit of a respirator on an individual. (See also Qualitative fit test QLFT and Quantitative fit test QNFT.) OSHA Definition

**Fume:** A solid condensation particulate, usually of a vaporized metal. NIOSH Definition

**Gas:** An aeriform fluid that is in a gaseous state at standard temperature and pressure. NIOSH Definition

**Helmet:** A rigid respiratory inlet covering that also provides head protection against impact and penetration. OSHA Definition

**High-Efficiency Particulate Air (Hepa) Filter:** A filter that is at least 99.97% efficient in removing monodisperse particles of 0.3 micrometers in diameter. The equivalent NIOSH 42 CFR 84 particulate filters are the N100, R100, and P100 filters. OSHA Definition

**Hood:** Means a respiratory inlet covering that completely covers the head and neck and may also cover portions of the shoulders and torso. OSHA Definition

**Immediately Dangerous to Life or Health (IDLH):** Acute respiratory exposure that poses an immediate threat of loss of life, immediate or delayed irreversible adverse effects on health, or acute eye exposure that would prevent escape from a hazardous atmosphere. **NIOSH Definition**

**Immediately Dangerous to Life or Health (IDLH):** An atmosphere that poses an immediate threat to life, would cause irreversible adverse health effects, or would impair an individual's ability to escape from a dangerous atmosphere. **OSHA Definition**

**Interior Structural Firefighting:** The physical activity of fire suppression, rescue or both, inside of buildings or enclosed structures which are involved in a fire situation beyond the incipient stage. (See 29 CFR 1910.155) OSHA Definition

**Loose-Fitting Facepiece:** A respiratory inlet covering that is designed to form a partial seal with the face. OSHA Definition

**Mist:** A liquid condensation particulate. NIOSH Definition

**Negative Pressure Respirator (Tight Fitting):** A respirator in which the air pressure inside the facepiece is negative during inhalation with respect to the ambient air pressure outside the respirator. OSHA Definition

**Orinasal Respirator:** A respirator that covers the nose and mouth and that generally consists of a quarter- or half-facepiece. NIOSH Definition

**Oxygen Deficient Atmosphere:** An atmosphere with an oxygen content below 19.5% by volume. OSHA Definition

**Physician or Other Licensed Health Care Professional (PLHCP):** Means an individual whose legally permitted scope of practice (i.e., license, registration, or certification) allows him or her to independently provide, or be delegated the responsibility to provide, some or all of the health care services required by paragraph (e) of this section. OSHA Definition

**Planned or Unplanned Entry into an IDLH Environment, an Environment of Unknown Concentration of Hazardous Contaminant, or an Environment of Unknown Composition:**

A situation in which respiratory devices are recommended to provide adequate protection to workers entering an area where the contaminant concentration is above the IDLH or is unknown. NIOSH Definition

**Positive Pressure Respirator:** A respirator in which the pressure inside the respiratory inlet covering exceeds the ambient air pressure outside the respirator. OSHA Definition

**Potential Occupational Carcinogen:** Any substance, or combination or mixture of substances, which causes an increased incidence of benign and/or malignant neoplasms, or a substantial decrease in the latency period between exposure and onset of neoplasms in humans or in one or more experimental mammalian species as the result of any oral, respiratory, or dermal exposure, or any other exposure which results in the induction of tumors at a site other than the site of administration. This definition also includes any substance that is metabolized into one or more potential occupational carcinogens by mammals (29 CFR 1990.103, OSHA Cancer Policy). NIOSH Definition

**Powered Air-Purifying Respirator (PAPR):** An air-purifying respirator that uses a blower to force the ambient air through air-purifying elements to the inlet covering. OSHA Definition

**Pressure Demand Respirator:** A positive pressure atmosphere-supplying respirator that admits breathing air to the facepiece when the positive pressure is reduced inside the facepiece by inhalation. OSHA Definition

**Assigned Protection Factor (APF):** The minimum anticipated protection provided by a properly functioning respirator or class of respirators to a given percentage of properly fitted and trained users.

**Simulated Workplace Protection Factor (SWPF):** A surrogate measure of the workplace protection provided by a respirator.

**Workplace Protection Factor (WPF):** A measure of the protection provided in the workplace by a properly functioning respirator when correctly worn and used.

**Qualitative Fit Test (QLFT):** A pass/fail fit test to assess the adequacy of respirator fit that relies on the individual's response to the test agent. OSHA Definition

**Quantitative Fit Test (QNFT):** Means an assessment of the adequacy of respirator fit by numerically measuring the amount of leakage into the respirator. OSHA Definition

**Recommended Exposure Limit (REL):** An 8- or 10-hour time-weighted average (TWA) or ceiling (C) exposure concentration recommended by NIOSH that is based on an evaluation of the health effects data. NIOSH Definition

**Respiratory Inlet Covering:** The portion of a respirator that forms the protective barrier between the user's respiratory tract and an air-purifying device or breathing air source, or both. It may be a facepiece, a helmet, a hood, a suit, or a mouthpiece respirator with nose clamp. OSHA Definition

**Self-Contained Breathing Apparatus (SCBA):** An atmosphere-supplying respirator for which the breathing air source is designed to be carried by the user. OSHA Definition

**Service Life:** The length of time required for an air-purifying element to reach a specific effluent concentration. Service life is determined by the type of substance being removed, the concentration of the substance, the ambient temperature, the specific element being tested (cartridge or canister), the flow rate resistance, and the selected breakthrough value. The service life for a self-contained breathing apparatus (SCBA) is the period of time, as determined by the NIOSH certification tests, in which adequate breathing gas is supplied. NIOSH Definition

**Service Life:** The period of time that a respirator, filter or sorbent, or other respiratory equipment provides adequate protection to the wearer. OSHA Definition

**Single-Use Dust or Dust and Mist Respirators:** Respirators approved for use against dusts or mists that may cause pneumoconiosis and fibrosis. NIOSH Definition

**Supplied-Air Respirator (SAR) or Airline Respirator:** An atmosphere-supplying respirator for which the source of breathing air is not designed to be carried by the user. OSHA Definition

**This Section:** This respiratory protection standard. OSHA Definition

**Tight-Fitting Facepiece:** A respiratory inlet covering that forms a complete seal with the face. OSHA Definition

**User Seal Check:** An action conducted by the respirator user to determine if the respirator is properly seated to the face. OSHA Definition

**Vapor:** The gaseous state of a substance that is solid or liquid at temperatures and pressures normally encountered. NIOSH Definition



Proper Donning and Doffing is essential to wearing a SCBA and can only be obtained by practice and training. We recommend once a month for all first responders and quarterly for all other staff. Believe it or not, you will have a leak and maybe something worse.

## Suspicious Letter Procedure Example

### Inhalation Anthrax Exposure

In October 2001, four workers died from inhalation of anthrax and an additional 13 developed cutaneous or inhalational disease as a result of intentional terrorist activity. In most cases seen thus far, the disease was linked to unexpected workplace exposures to anthrax spores contained in letters mailed through the United States Postal Service. Fortunately, the number of workplaces contaminated with the spores has also been quite limited. Nevertheless, employers and workers are concerned about possible exposure to *Bacillus anthracis* in the workplace.

### *OSHA to Help Employers Assess Risk*

**WASHINGTON** >--Labor Secretary Elaine L. Chao announced a new model to assist employers and employees in dealing with possible workplace exposures to anthrax in mail handling operations today. The Anthrax Matrix guides employers in assessing risk to their workers, providing appropriate protective equipment and specifying safe work practices for low, medium and high risk levels in the workplace.

"Most employers and employees face little or no risk of exposure to anthrax and need only minimal precautions," Chao said. "But some may have to deal with potential or known exposures, and we want to make sure they have all possible information available to protect Americans at their workplace."

Chao pointed out that there have been only four deaths and 17 confirmed cases of anthrax infection but indicated that the department wants to be proactive in assisting employers and workers concerned about anthrax and other potential terrorist threats.

The Occupational Safety and Health Administration developed the matrix in consultation with the U.S. Postal Service, the Centers for Disease Control (**CDC**), the National Institute for Occupational Safety and Health (**NIOSH**), the Environmental Protection Agency and the FBI. OSHA expects to continually update information on anthrax and other terrorism threats as new guidance becomes available.

"The OSHA information is easy to access and understand," Chao said. "We are providing needed guidance, not creating new requirements. The world has changed since September 11. Threats to our national security now can clearly involve the workplace."

John L. Henshaw, assistant secretary of labor for OSHA said, "***OSHA's role remains the same - assuring the safety and health of America's workers - but the paradigm has shifted. We must shift with it to provide the best possible guidance to help employers and employees address new threats.***"

The Anthrax Matrix, shaped like a pyramid, includes three sections: green for low, yellow for medium and red for high risk of exposure. Each section links to useful information and practical guidance to help determine an appropriate response.

## WORKPLACE RISK PYRAMID

### **RED ZONE:**

Workplaces Where  
Authorities Have Informed  
You That Contamination  
with Anthrax Spores Has  
Been Confirmed or Is  
Strongly Suspected

### **YELLOW ZONE:**

Workplaces Where  
Contamination with Anthrax  
Spores Is Possible

### **GREEN ZONE:**

Workplaces Where  
Contamination with Anthrax  
Spores Is Unlikely



The matrix is available on OSHA's website at [www.osha.gov](http://www.osha.gov).

There is also general information on anthrax and mail handling procedures on the agency's website, links to detailed information from CDC, the U.S. Postal Service, the FBI and other sources of information on biological and chemical hazards and emergency preparedness.

U.S. Labor Department news releases are accessible on the Internet at [www.dol.gov](http://www.dol.gov).

The information in this release will be made available in alternate format upon request (large print, Braille, audio tape or disc) from the COAST office. Please specify which news release when placing your request. Call 202-693-7773 or TTY 202-693-7755.

## Occupational Exposure To Anthrax OSHA Frequently Asked Questions

*NOTE: The following answers do not impose and are not intended to result in the imposition of any new legal obligations or constraints on employers or on the States. The guidance presented here is based on OSHA's understanding of currently available National information, which is being re-evaluated continuously. As additional questions arise and as more information becomes available, this document may change. Therefore, for the most updated version, please visit OSHA's website at <http://www.osha.gov/>.*

---

### **Appropriate Personal Protective Equipment: Respirators And Gloves**

---

#### **1. What types of gloves are recommended as a precaution for anthrax exposure?**

Nitrile or vinyl gloves will protect workers from cutaneous anthrax exposure. Latex gloves offer protection similar to nitrile or vinyl gloves, but can result in sensitization or elicit allergic reactions in a small percentage of people. Since mail handling includes a range of tasks and is conducted in various occupational settings, gloves should be provided in a range of sizes and types to fit a variety of workers and job tasks. Employers whose employees work in situations where a gloved hand presents a hazard (e.g., work close to moving machine parts), can minimize risk by ensuring employee training on work practices, proper machine guarding, and correct fit of workers' gloves.

OSHA's recommendations for assessing workplace risk and determining prudent work practices and personal protective equipment (**PPE**) are addressed in OSHA's Anthrax in the Workplace Risk Reduction Matrix. Please be aware that OSHA's standards for general PPE cover glove selection and use (1910\_0132) as well as hand protection (1910\_0138).

**Note:** The U.S. Postal Service (**USPS**), which continues to work closely with the Centers for Disease Control and Prevention (CDC) regarding the control of anthrax in its facilities (*Morbidity and Mortality Weekly Report* - MMWR - October 26, 2001), has purchased vinyl and nitrile gloves for postal employee protection (USPS News Release Oct 25, 2001).

#### **2. What personal protective equipment would provide effective protection while handling mail if exposure to anthrax spores is a concern? Would this include respirators?**

OSHA's recommendations for assessing workplace risk, prudent work practices, and personal protective equipment (**PPE**) are addressed in the Anthrax in the Workplace Risk Reduction Matrix.

Because the majority of recent cases of confirmed occupational anthrax contamination and infection have been related to mail delivered through the USPS, selecting appropriate personal protective equipment (**PPE**) depends on the amount of mail a worker handles, how he or she handles the mail, and where he or she works. Some factors to consider include: the current patterns of anthrax spore contamination; the nature of the workplace and amount of mail received; whether the facility receives mail directly from a USPS facility that is known to be contaminated with anthrax; and whether the facility uses equipment that might disperse dust or anthrax spores into the air. Employers also should consider factors such as information from law enforcement agencies in assessing employee risk.

For the most part, employers whose workers handle small volumes of mail will not need to do more than to establish handling and screening procedures for mail. These employers may consider providing their employees with vinyl or nitrile gloves. Workers in USPS facilities often handle an extremely high volume of mail and may work around mail sorting equipment that could disperse anthrax spores contained in processed mail. As a result, the workers in these facilities may be at a higher risk of exposure than workers who handle smaller volumes of mail, and higher levels of PPE may be appropriate.

As explained, OSHA does not recommend respirators for the vast majority of workers. If workers request respirators, however, and employers provide filtering facepiece respirators for voluntary use by employees, the employers must make sure that employees are provided with the information contained in Appendix D to OSHA's Standard for Respiratory Protection, 29 CFR 1910.134 ("Information for Employees Using Respirators When Not Required Under the Standard").

To provide effective protection from anthrax spores, the CDC recommends the use of NIOSH-approved respirators that are at least as protective as an N95 respirator. In addition, persons working in areas where oil mist from machinery is present should use respirators equipped with P-type filters (P95 or P100) to prevent the oil mist from degrading the filter.

At worksites where employers require workers to wear respirators, a respiratory-protection program that complies with the provisions of 29 CFR 1910.134 must be implemented. This includes compliance with the standard's requirements for obtaining medical clearance for wearing the respirator and for conducting fit testing before requiring their employees to use respirators. These latter requirements also apply to voluntary use of respirators that are not filtering facepiece respirators.

**3. What precautions should healthcare workers (HCWs) take when treating patients who may be infected and/or contaminated with anthrax (*Bacillus anthracis*)?**

Healthcare workers should use Universal Precautions for all patient care activities. "Universal Precautions" are standard approaches to infection control designed to reduce the risk of transmitting microorganisms from both known and unknown sources of infection. Universal Precautions can include, but are not limited to, appropriate use of gloves, masks, protective clothing, work practices, and housekeeping.

Clinical anthrax illness occurs days or weeks after exposure to the anthrax spores and person-to-person spread of this disease has not been documented. Therefore, after the onset of clinical illness, no precautions specific to anthrax have been recommended. However, if healthcare workers are providing initial care to a patient with suspected recent exposure to anthrax, they should take precautions against the potential for re-aerosolizing any anthrax spores remaining on the exposed individual or clothing. Further direction for appropriate personal protective equipment is available on OSHA's Anthrax in the Workplace Risk Reduction Matrix.



**4. How should contaminated PPE used to handle mail (e.g. gloves) be disposed of? Can it go in regular trash?**

Unless the PPE has been used to handle a suspicious piece of mail, gloves and other personal protective clothing and equipment can be discarded in regular trash once removed. If a worker recognizes and handles a suspicious piece of mail, the worker's protective gear should be treated as potentially contaminated; it should be placed in an appropriately labeled and/or color-coded container that is closable and leak-proof. This container should then be disposed of as infectious/regulated waste.

**5. What are the health and safety precautions for laboratory workers handling anthrax samples?**

The Centers for Disease Control and Prevention (CDC) has published advice for laboratory personnel in the **MMWR** of October 19, 2001. Lab personnel are advised to:

- Use Biological Safety Level 2 facilities and practices (BSL-2 laboratories are suitable for work involving agents of moderate potential hazards) or Biological Safety Level 3 facilities and practices (BSL-3 laboratories are suitable for work involving indigenous or exotic agents that have a potential for respiratory transmission and may cause serious or potentially lethal disease) when working with clinical samples considered potentially infectious;
- Wear protective eyewear (e.g., safety glasses or eye shields) and handle all specimens in a BSL-2 laminar flow hood, use closed-front laboratory coats with cuffed sleeves, and stretch gloves over the cuffed sleeves;
- Avoid any activity that places them at risk for infectious exposure, especially activities that might create aerosols or disperse droplets;
- Decontaminate laboratory benches after each use and dispose of supplies and equipment in proper receptacles;
- Avoid touching mucosal surfaces with hands (gloved or ungloved), and never eat or drink in the laboratory; and
- Remove and reverse gloves before leaving the laboratory, dispose of them in a biohazard container, remove laboratory coat, and wash hands.

More information is available in the CDC Guidelines for State Health Departments (Revised October 14, 2001).

**6. What respirators are recommended for protection against smallpox?**

Unlike anthrax, which is acquired only from direct exposure to anthrax spores, smallpox is a highly contagious disease, often spread from person to person. No general workplace guidance exists regarding respiratory protection for smallpox.

For laboratory work, current recommendations require BSL-4 facilities and practices (laboratories suitable for work with dangerous and exotic agents posing high individual risk of laboratory infections and life-threatening disease) for laboratory personnel. Other recommendations are not available, however the CDC offers additional information regarding the smallpox vaccination on their website.

---

## Emergency Response

---

### 7. What personal protective equipment is recommended for emergency responders in the event of a suspected anthrax threat?

The type of personal protective equipment (**PPE**) needed for effective protection depends on different response situations, what is known or unknown about the situation, and the potential risk. Please be aware that emergency response to an anthrax spore release is covered by the Hazardous Waste Operations and Emergency Response Standard (**HAZWOPER**), so the **PPE** that is selected and used must be consistent with the standard. The standard is performance-oriented and requires the selection and use of PPE to be proportional to the anticipated risk of exposure and appropriate to the nature of the anticipated hazard. Recent releases and contamination have generally been associated with mail sent through the US Postal Service (**USPS**). When mail-handling equipment has already been locked and tagged out, thus providing a reliable assurance that anthrax will not be re-aerosolized due to equipment start-up or operation, workers responding to these types of releases have worn modified Level C protection with a full-face tight-fitting Powered Air Purifying Respirator (**PAPR**). However, activities which may result in spore release, such as removal of a suspect contaminated mail item, or after releases where the agent or method of disbursement is unknown, and/or the release is ongoing will require higher levels of protection.

OSHA's recommendations concerning prudent work practices and PPE for emergency responders are addressed in Anthrax in the Workplace Risk Reduction Matrix.

### 8. For those security personnel who may be asked to secure a room or area because of potential contamination:

**What personal protective equipment should be supplied and worn? What should such personnel do to prevent access to that area or prevent exposed persons from leaving the area?**

If an exposure to anthrax spores is suspected, proper emergency response protocols should be followed. Individuals not specifically trained to handle situations involving anthrax should not be in or near the potentially contaminated area. Emergency responders should secure affected areas.

If security personnel secure the area they are considered emergency responders. Depending on the tasks that they are likely to perform, these individuals may be first responders at either the "**awareness**" or "**operations**" level. See the answers to Questions 1 and 2 for information regarding the use of appropriate personal protective equipment.

Security personnel who will not take any actions other than to cordon off the affected area and/or initiate the emergency response sequence are considered "**first responders at the awareness level.**" Security personnel who are required to close doors, physically isolate the area, or take any other defensive action are considered "first responders at the operations level." Please refer to OSHA Directive CPL 2-2.59A Inspection Procedures for the Hazardous Waste Operations and Emergency Response Standard (April 24, 1998) for information about emergency responders and training levels.

---

**Mail-Related Work Practices**

---

**9. It is standard procedure for the post office employees to use compressed air to clean the mail processing machines (address/zip code reader optics). Is this acceptable? If not, what cleaning method is acceptable?**

The U.S. Postal Service has banned the use of compressed air ("blowout") as a method of machine maintenance because compressed air has a high risk potential for aerosolizing anthrax spores. Other employers should also avoid practices like dry sweeping and blowing off machinery with compressed air; instead employers should use wet-clean, mop, or vacuum methods. When vacuuming mail handling and sorting equipment is chosen, an industrial vacuum that is equipped with a High Efficiency Particulate Air (**HEPA**) filter should be used. Do not use a standard industrial vacuum or a "HEPA" equipped home-style vacuum. Additionally, proper procedures and work practices should be followed during maintenance of machinery in order to protect workers from other potential injuries.

**10. Should mail-handling facilities take air and/or surface samples for traces of anthrax?**

No. Routine sampling is not recommended, unless an employer has a reason to suspect that anthrax contamination has occurred. If there is a suspected exposure or contamination, established emergency response procedures must be followed.

**11. What is the safest way to handle individual letters or packages?**

- Be on the lookout for suspicious envelopes or packages.
- **DO NOT** open suspicious mail.
- Open all mail with a letter opener or other method that minimizes skin contact with the mail and is least likely to disturb contents.
- Open mail with a minimum amount of movement.
- Do not blow into envelopes.
- Do not shake or pour out contents.
- Keep hands away from nose and mouth while working with and opening mail.
- While opening mail, turn off fans, portable heaters, and other equipment that may create air currents.
- Wash hands thoroughly with soap and water after handling mail.
- More information is available in OSHA's *Workplace Response to Anthrax Threat: OSHA Recommendations for Handling Mail*.

**12. What do I do if I come across a suspicious piece of mail?**

- Do **NOT** open the package or letter.
- Do not shake, empty, or otherwise disturb its contents.
- Put the package down and do not handle it further.
- Do not touch or try to clean up the substance.
- Alert others nearby.
- Do not remove ANY items from area.
- Leave the area and gently close the door.
- Wash hands well with soap and water.
- Contact your supervisor, designated responder or other appropriate authority.
- Limit movements within the building to prevent spread of substance.

**13. Is an employer obligated to pay for pre-exposure anthrax tests (i.e. blood, titer, etc.)?**

Employers are not legally required to offer or pay for anthrax exposure tests. Employees may wish to contact the Centers for Disease Control and Prevention (CDC) to obtain information about low-cost or no-cost testing and treatment at (404) 639-3534.

**14. Should I visit my doctor if I have a fever, congestion, or flu-like symptoms?**

If you have not been present in an area where there is a potential for exposure to anthrax spores, the chance of anthrax infection is remote, and antibiotic therapy is usually not indicated. Anthrax is not spread by person-to-person contact. Therefore, there are no recommendations to immunize or treat contacts of persons with clinical anthrax illness, such as household contacts, friends, or coworkers, unless they were also exposed to the same source of infection.

The CDC recommends the anthrax vaccine for employees working in laboratories involved in testing for anthrax, workers who decontaminate sites known to be contaminated with anthrax, and workers who typically work in areas with high naturally occurring concentrations of anthrax (e.g., wool-sorters). Further information can be obtained on-line at the CDC bioterrorism website; or CDC's newly established toll-free CDC Public Response Hotline. For English, call (888) 246-2675; por Español, llame al (888) 246-2857.

**15. Should I get an anthrax vaccination?**

At this time, vaccination against anthrax for the general public to prevent disease is not recommended. Further information can be obtained on-line at the CDC bioterrorism website.

**16. Should I start taking preventive antibiotics?**

The CDC strongly recommends against the use of preventive antibiotics for the general population. Unless there is strong or compelling evidence to suggest that you may have been exposed to anthrax, you should not take preventive antibiotics. However, if you are concerned, you should discuss this with your healthcare provider.

**17. What types of businesses would be expected to prepare for terrorist attacks?**

Terrorist activity is unpredictable, though current anthrax contamination has been primarily isolated to mail handling facilities. For more information regarding potential anthrax exposures in a workplace, refer to OSHA's Anthrax in the Workplace Risk Reduction Matrix.

**18. Since the anthrax hazard is an emergency/unexpected hazard, will OSHA waive the requirements for medical evaluations (medical questionnaire and examinations) for employees required to wear respiratory protection and employees who voluntarily use such protection?**

In worksites where respiratory protection is required to be worn, a respiratory protection program that complies with the provisions of OSHA's Respiratory Protection Standard, 29 CFR 1910.134, must be implemented, including medical examinations as indicated. Medical evaluations are not required for employees who are wearing filtering facepiece respirators on a voluntary basis.

**19. Does 1910.120 (HAZWOPER) apply to initial responders for anthrax releases?**

Yes. The release of anthrax spores into a workplace as an act of terrorism is an emergency situation. Compliance with Hazardous Waste Operations and Emergency Response, 29 CFR 1910.120, is required for emergency response personnel responding to a possible anthrax release. (See response to Question #7, above.)



Mail Room, employees need to be trained on how to handle a suspect package and be provided proper PPE.

## Workplace Violence

### CURRENT STATUS

OSHA does not have a specific standard for workplace violence. However, under the Occupational Safety and Health Act of 1970 (the OSH Act, or the Act), the extent of an employer's obligation to address workplace violence is governed by the General Duty Clause.

***Section 5(a)(1) of the OSH Act, or P.L. 91-596 (the "General Duty Clause") provides that: "Each employer shall furnish to each of his employees employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees." 29 U.S.C. 654(a)(1)***

It is, therefore, OSHA's commitment to encourage employers to develop workplace violence prevention programs. Workplace violence has emerged as an important safety and health issue in today's workplace. Its most extreme form, homicide, is the second leading cause of fatal occupational injury in the United States. Nearly 1,000 workers are murdered, and 1.5 million are assaulted in the workplace each year.

Environmental conditions associated with workplace assaults have been identified and control strategies implemented in a number of work settings. OSHA has developed guidelines and recommendations to reduce worker exposures to this hazard but is not initiating rulemaking at this time.

### HAZARD DESCRIPTIONS

According to the Department of Justice's National Crime Victimization Survey (**NCVS**), assaults and threats of violence against Americans at work number almost 2 million a year. The most common type of workplace violent crime was simple assault with an average of 1.5 million a year. There were 396,000 aggravated assaults, 51,000 rapes and sexual assaults, 84,000 robberies, and 1,000 homicides.

Factors which may increase a worker's risk for workplace assault, as identified by the National Institute for Occupational Safety and Health (**NIOSH**), are:

- Contact with the public
- Exchange of money
- Delivery of passengers, goods, or services
- Having a mobile workplace such as a taxicab or police cruiser
- Working with unstable or volatile persons in health care, social services, or criminal justice settings
- Working alone or in small numbers
- Working late at night or during early morning hours
- Working in high-crime areas
- Guarding valuable property or possessions
- Working in community-based settings

## **Prevention Program Example**

Your Employer should follow guidelines and recommendations which are based on OSHA's Safety and Health Program Management Guidelines and contain the following four basic elements:

1. Management commitment and employee involvement. May include simply clear goals for worker security in smaller sites or a written program for larger organizations.
2. Worksite analysis. Involves identifying high-risk situations through employee surveys, workplace walkthroughs, and reviews of injury/illness data.
3. Hazard prevention and control. Calls for designing engineering and administrative and work practice controls to prevent or limit violent incidents.
4. Training and education. Ensures that employees know about potential security hazards and ways to protect themselves and their co-workers.

## **Training**

Your Employer should be providing Hazard Communication training in which Workplace Violence is addressed for all of our employees. Department Directors should ensure that all employees have been properly trained on the Workplace Violence Program. Documentation of this and other safety training of each employee will be submitted to the Administrative Services Department for placement in the Safety Training Master File.

## **Controls**

Although not exhaustive, OSHA's guidelines and recommendations include policies, procedures, and corrective methods to help prevent and mitigate the effects of workplace violence. Engineering controls remove the hazard from the workplace or create a barrier between the worker and the hazard.

Administrative and work practice controls affect the way jobs or tasks are performed.

### ***Some recommended engineering and administrative controls:***

- Physical barriers such as bullet-resistant enclosures, pass-through windows, or deep service counters
- Alarm systems, panic buttons
- Convex mirrors, elevated vantage points, clear visibility of service and cash register areas
- Bright and effective lighting
- Adequate staffing
- Arrange furniture to prevent entrapment
- Cash-handling controls, use of drop safes
- Height markers on exit doors
- Emergency procedures to use in case of robbery
- Training in identifying hazardous situations and appropriate responses in emergencies
- Video surveillance equipment and closed circuit TV
- Establish liaison with Police Department
- Post-incident response and evaluation

Post-incident response and evaluation are essential to an effective violence prevention program. Your Employer's workplace violence program will provide treatment or counseling for victimized employees and employees who may be traumatized by witnessing a workplace violence incident.



Several types of assistance can be incorporated into the post-incident response including: trauma-crisis counseling; critical incident stress debriefing; or employee assistance programs to assist victims.

Always have security or the local Police ready to arrest an employee or a Trespasser.

Always document all incidents. It is best to have a standardized form for all accidents, events, concerns and incidents. Most utilities have installed video cameras to watch the parking lots, storage areas and equipment.

### **Photograph Below**

Here is a person that had his water turned off for non-payment. He believed that he was being picked on and “threatened the Customer Services Staff.” The Staff was able to push a hidden “Panic Button” and the Security Guards confined this person until Police arrived.

Be prepared for “Nut cases”, 10-16 like this person below and practice your emergency skills on how to handle people that are violent or mentally ill.



## **This gives us something to think about with all our new electronic technology.**

### **GPS**

A couple of weeks ago a friend told me that someone she knew had their car broken into while they were at a football match. Their car was parked on the green which was adjacent to the football stadium and specially allotted to football fans. Things stolen from the car included a garage door remote control, some money and a GPS which had been prominently mounted on the dashboard.

When the victims got home, they found that their house had been ransacked and just about everything worth anything had been stolen.

The thieves had used the GPS to guide them to the house. They then used the garage remote control to open the garage door and gain entry to the house. The thieves knew the owners were at the football game, they knew what time the game was scheduled to finish and so they knew how much time they had to clean out the house. It would appear that they had brought a truck to empty the house of its contents.

### **MOBILE PHONE**

I never thought of this.....

This lady has now changed her habit of how she lists her names on her mobile phone after her handbag was stolen. Her handbag, which contained her cell phone, credit card, wallet... Etc...was stolen.

20 minutes later when she called her hubby, from a pay phone telling him what had happened, hubby says 'I received your text asking about our Pin number and I've replied a little while ago.' When they rushed down to the bank, the bank staff told them all the money was already withdrawn.

The thief had actually used the stolen cell phone to text 'hubby' in the contact list and got hold of the pin number. Within 20 minutes he had withdrawn all the money from their bank account.

### **Moral of the lesson:**

Do not disclose the relationship between you and the people in your contact list.

Avoid using names like Home, Honey, Hubby, Sweetheart, Dad, Mom, etc....

And very importantly, when sensitive info is being asked through texts, CONFIRM by calling back. Also, when you're being text by friends or family to meet them somewhere, be sure to call back to confirm that the message came from them. If you don't reach them, be very careful about going places to meet 'family and friends' who text you.

## Counterfeit or Illegal IDs and Uniforms

The following information is meant to advise law enforcement officials and security guards of the potential security threat presented by the unauthorized use of delivery service, utility company, or police and fire department uniforms, identification (ID), or vehicles to gain access or proximity to facilities not normally accessible to the general public. By using counterfeit or illegally obtained IDs, uniforms, and emergency equipment, unauthorized individuals could impersonate a legitimate service or a law enforcement entity to gain access to restricted areas. This would enable the individuals to conduct surveillance or facilitate an attack against the facility.

Although DHS and the FBI know of no specific plots or threats to gain access to secure facilities using fraudulent delivery, utility, or emergency personnel, recent reporting and past criminal activities suggest these methods could be used. Terrorists may view the use of public safety or service industry uniforms, IDs, and vehicles as a way to decrease scrutiny of their activities as well as increase their level of access to secure areas. This potential threat is even more pronounced during the time of year when commercial package carriers and the U.S. Postal Service experience an increase in shipping and deliveries.

This Information Bulletin is intended to raise awareness of this issue and to provide basic protective measures that should be used by any facility security officer wanting to limit vehicular or personnel access. For specific information and protective measures related to the potential for terrorist use of emergency vehicles to circumvent security procedures, please see Information Bulletin, disseminated on October 14, 2004.

### Details

The use of stolen uniforms, stolen credentials, fabricated badges, and ID cards to gain entry to limited access areas and private residences is not uncommon among criminals. Unsuspecting people have granted access to individuals posing as representatives of utility companies, delivery services, or police or fire officials solely because the individuals wore a uniform.

In October 2004, special agents from the Naval Criminal Investigative Service (NCIS) and the Coast Guard Investigative Service arrested an individual in San Francisco, California, after he attempted to gain access to a U.S. Navy ship by posing as an Army Criminal Investigation Command (CID) agent. Investigation revealed that this case was an attempt to use false identification.



A few days later, a subject allegedly entered a communications business in Virginia and identified himself as a Federal Protective Service Officer from Washington, D.C. The subject briefly showed a badge and requested information on the cost of emergency equipment to be installed on his privately owned vehicle. This case proved to be an attempt to use a valid ID to gain inappropriate facility access.

In the same time period, a legitimate delivery person attempted to gain access to a restricted U.S. Government facility. The employee, who was driving an unmarked rental vehicle, was not in possession of his company ID. Although the security personnel appropriately barred entry to the facility, the incident caused concern for the guards and resulted in unnecessary anxiety and delays while the delivery was investigated. The experience underscored, the need for delivery personnel to carry proper identification and for security guards to verify their legitimacy.

Research indicates that the consolidation of companies within the package delivery industry can create temporary situations where valid deliveries may look suspicious as a company attempts to assimilate an acquisition (i.e., identification and vehicle markings). Independent contractors or rental vehicles may also be used during high volume delivery periods. These periodic deviations from delivery routines require increased vigilance by security personnel.

Individuals may pose as public safety officers to gain access to an otherwise restricted area, to assist in smuggling weapons or contraband into a secure location, or to provide cover for criminal activity. In addition, terrorists may seek to use public safety uniforms or vehicles to conduct surveillance, facilitate an attack on a facility, or deliver a secondary attack targeting legitimate first responders. For example, terrorists in Israel, Iraq, and Saudi Arabia have used ambulances, medic uniforms, and other public safety equipment to facilitate their attacks. As such, it is critical that the identity of all public safety and delivery personnel be verified prior to allowing them access to secure facilities. DHS and the FBI ask both delivery companies and security guards to insist on proper identification.

## **Protective Measures**

### **Facility Security Personnel:**

Enforcing strict access requirements to any sensitive facility or building is a key to deterrence. The following protective measures are suggested:

- Require proper identification for delivery, utility, and other service personnel.
- Question perceived abnormalities in procedures or routines, such as:
  - New delivery or service personnel;
  - Deliveries arriving in a private or rental vehicle;
  - Unscheduled deliveries or appointments;
  - Confirm “emergency” calls or visits.
- Route suspicious vehicles or packages away from the primary point of entry.
  - If possible, have the operator move the suspicious vehicle or package to the far end of a parking lot (away from any nearby buildings) prior to required inspections.
- Encourage all personnel to report suspicious activities immediately and try to obtain as much of the following information as possible:
  - Full name of subject;
  - Nature of suspicious activity;
  - Date of birth;
  - Physical description;
  - Driver’s license;
  - License plate and vehicle description.

- Checklist of indicators for valid deliveries (any deviation may be cause for additional scrutiny):
  - The delivery person is in uniform;
  - The delivery person has a valid company ID;
  - The delivery person should possess an electronic package scanning device or, at a minimum, a delivery record for customer signatures;
  - The delivery vehicle should normally contain other freight for delivery;
  - The delivery vehicle is marked with “a brand name” or is a valid rental.

Note: During peak periods, rental vehicles are used by the major delivery companies.

The following phone numbers and addresses are provided to augment established procedures and ease verification of delivery driver status:

- DHL: 1-800-345-3601
- FedEx: 1-800-Go FedEx (1-800-463-3339)
- UPS: (404) 828-6986 (Corporate Security)
- U.S. Postal Service: (202) 268-7350 (U.S. Postal Inspection Service Command Center Watch Line)

Security plans and procedures should be periodically tested and reviewed by security managers.

#### **Public Safety Agencies:**

- Encourage personnel to safeguard uniforms and IDs, particularly in areas that are accessible to the public (e.g., public gym locker rooms);
- Practice accountability of all public safety vehicles to include tracking vehicles that are in service, in repair status, or sent to salvage;
- Ensure that officers turn off and lock the emergency vehicle's doors when not in the vehicle;
- Immediately put stolen public safety vehicles into a nationwide all-points bulletin;
- Be able to verify to facility security personnel that a police or fire vehicle responding to a facility is an authorized vehicle with authorized personnel.

#### **Conclusion**

Stringent access and security procedures are the key to maintaining the highest level of security while ensuring the safety of personnel and property. Although DHS and the FBI know of no specific threat by means of force or fraudulent entry to a facility, current conditions warrant a thorough review of security policies and procedures. Personnel should continue to closely follow established regulations and local protocols, be alert for suspicious incidents, and when in doubt, apply an abundance of caution. Additionally, immediate and accurate incident reporting is paramount to the safety and security of all private and government facilities.

Information on suspicious activities potentially related to terrorism should be forwarded immediately to the local FBI JTTF and the DHS HSOC as indicated on the first page.

For comments or questions related to the content or dissemination of this Information Bulletin, please contact the DHS/Information Analysis and Infrastructure Protection Directorate's Requirements Division at [DHS.IAIP@DHS.GOV](mailto:DHS.IAIP@DHS.GOV).



## CHAPTER 2 EXERCISE

---

This is a chapter review, you can find the final exam on TLC's website under Assignments.

1. What type of PPE do you have at your facility, plant or yard? Do you have PPE available for non-employees, Customers, Contractors, Maintenance personnel?
2. Describe the procedures to properly keep, store, maintain and use Respirator Protection equipment.
3. Describe the term "**Universal Precautions.**"
4. Write a Hazard Assessment on procedures on receiving a "**suspicious package**" (See Chapter 3 and 4 for assistance).
5. What is Anthrax?
6. Do you believe that your facility is vulnerable to Anthrax or any other airborne virus coming from mail or packages? Describe.
7. How would you correct that vulnerability?
8. Do you have a Workplace Violence Policy? What OSHA Regulation requires a Workplace Violence Policy?
9. What is "**Service Life**"?
10. What is "Immediately Dangerous to Life or Health (**IDLH**)" and does it relates to your position?

***What I Will Do As Follow-up To This Chapter..."***

**Think about...**

**Analyze two important areas:** Safety and Emergency Training.  
Why are these two areas overlooked or not taken seriously?



## Chapter 3: Terrorism in Perspective

---

**Section Focus:** You will learn the basics of conventional terrorism that you may encounter at your utility. At the end of this section, you the student will be able to understand and describe the basic terrorism tactics. There is a post quiz at the end of this section to review your comprehension and a final examination in the Assignment for your contact hours.

**Scope/Background:** Terrorism in Perspective defines terrorism, presents a historical perspective, and provides an overview of potential threats (biological, nuclear, incendiary, chemical, and explosive).



### **Unknown barrel full of mystery chemicals.**

Practice, practice, practice.... It will happen to your facility one day.

### **The Threat is Real**

Terrorists have the knowledge and the capability to strike anywhere in the world. We have seen that, when properly motivated, they will do whatever they have to do in order to achieve their goals. Recent examples of terrorist attacks include the World Trade Center bombing, February 1993; the Tokyo Subway nerve agent attack, March 1995; and the Oklahoma City bombing, April 1995.

There have been smaller bombing incidents, not necessarily classed as terrorist events, at the 1996 Olympics, at family planning clinics, and, recently, at social clubs. The list most likely will continue to grow.

All communities--especially those in free societies--are vulnerable to incidents involving terrorism. Nearly all of these communities contain some high-visibility target. These targets usually are situated along routes with high transportation and access potential.

Many may have manufacturing and testing facilities. Other examples of locations that may become targets for criminal or terrorist activity include:

- Utilities-water, power, sewer
- public assembly;
- public buildings;
- mass transit systems;
- places with high economic impact;
- telecommunications facilities; and
- places with historical or symbolic significance.

### **Wreak Havoc**

Despite our security consciousness, if terrorists intend to wreak havoc it will be difficult to stop them.

An act of terrorism can occur anywhere, at any minute, when you would least expect it. No jurisdiction-urban, suburban, or rural-is totally immune.

### **What Is Terrorism?**

---

The Federal Bureau of Investigation (FBI) defines terrorism as "***the unlawful use of force against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in the furtherance of political or social objectives.***"

**This definition includes three elements:**

1. Terrorist activities are illegal and involve the use of force.
2. The actions intend to intimidate or coerce.
3. The actions are committed in support of political or social objectives.

In one sense, it makes no difference to a first responder whether the incident is a terrorist act or not. You still will respond and be among the first on the scene. Naturally, the size and the kind of terrorist action are key factors.

But the important point to note is that an act of terrorism is essentially different from normal emergencies. You will have to deal with a new set of circumstances far different from the structural fire, the auto wreck, even the hazardous materials incident.

## What Is a Threat?

---

*One way to look at it is to see threat as consisting of two elements:*

**Motive and ability.** In one sense, determining the threat is a law enforcement function. On a more practical level, emergency responders need to realize that any individual or group that has both the motive and the ability can perpetrate an act of terrorism. There are many groups that possess both the motive and the ability; the law enforcement community monitors these groups constantly to assess the level of threat.

The criminal component is the most important element separating a terrorist organization and its actions from a legitimate organization. However, any organization, legitimate or not, can resort to terrorist means to achieve its political or social agenda. We also need to remember that a terrorist can act alone.

What makes the terrorist event so dangerous is that it is intended to cause damage, to inflict harm, and, in some cases, to kill. The fire that starts in someone's home as a result of careless smoking was probably not set with the intention to damage, hurt, or kill. There are exceptions, of course, as in the case of arson, but normally most of the incidents you will respond to are not criminal in nature. Terrorists will go to great lengths to make sure the event has the intended impact, even if it means destroying a whole building and killing all of its occupants.

Recent bombing incidents have shown that there can be a sequence of events carefully timed to inflict further harm on those whose job it is to respond to assist others. This shows the depth to which terrorists can descend to achieve their ends.

Some additional hazards will include

- Computer or Internet or SCADA viruses or hacker attacks.
- Drones attacks to your power supply system. A simple chain dropped on a transformer.
- Armed resistance –ANATIFA
- USE OF WEAPONS – EMPLOYEE OR PUBLIC
- BOOBY TRAPS– EMPLOYEE OR PUBLIC
- Secondary events

Experts generally agree that there are five categories of terrorist incidents. We need to take a brief look at the five: **biological, nuclear, incendiary, chemical, and explosive**. We will cover computer hackers in a later chapter

The acronym **B-NICE** is a simple way to remember the five. **B-NICE**

As we discuss these incidents, it is important to remember the four routes of entry: inhalation, absorption, ingestion, and injection. As with other incidents, responders should exercise good judgment in using personal protective equipment (**PPE**) and training provided to them. See **Chapter 2**.

The use of protective clothing, including positive-pressure, self-contained breathing apparatus, will enhance your chances of safe and successful response, especially in situations where you may face secondary contamination.



### **Protective Clothing or Equipment Available**

Hopefully, an array of different clothing or equipment is available to workers to meet all intended applications. Reliance on one particular clothing or equipment item may severely limit a facility's ability to handle a broad range of chemical exposures. In its acquisition of equipment and clothing, the safety department or other responsible authority should attempt to provide a high degree of flexibility while choosing protective clothing and equipment that is easily integrated and provides protection against each conceivable hazard.

## **Emergency Response Vehicles as Weapons**

Terrorist planners consider emergency response vehicles to be an ideal mechanism for impersonation of security personnel or other first responders to augment the planning or execution of terrorist incidents. The use of specialty vehicles has occurred widely overseas by al-Qaida, as well as other groups, and has proven effective in penetrating layered security barriers, screening, and other protective measures implemented for counterterrorism purposes.

Since 9/11, al-Qaida has successfully employed impersonation to provide the advantage needed to stage a successful attack against either soft or hard (protected) targets. The group employed impersonation in the November 2003 attack in Riyadh, Saudi Arabia through use of both a police vehicle and fake uniforms to successfully enter a secure compound and detonate an explosive carried in another vehicle. In June 2004, al-Qaida staged a fake roadblock, again impersonating Saudi security personnel through use of a police vehicle, to successfully abduct and subsequently murder an American citizen.

Recent reports that al-Qaida has stolen up to 15 police vehicles in Riyadh—with possible help from insiders within the Saudi security forces—further support the group's increased use of impersonation. Terrorist organizations have impersonated emergency response personnel in other countries, such as Israel, through successful use of fake ambulances. Additionally, there have been recent suspicious incidents in New Jersey that heighten concern over the potential terrorist acquisition of ambulances. Three closely spaced incidents, occurring within a one-week time period, involved a line of abnormal questioning by nervous men regarding ambulance operation, servicing depots, and operator licensing requirements. The Westchester County, NY Department of Emergency Services subsequently issued an alert based on these incidents on August 12, 2004.

### **The Feasibility of Impersonation in the United States**

The disparate number of law enforcement and other emergency response organizations within the United States coupled with jurisdictional overlap at the county, state, and federal level makes impersonation, particularly of first responders, a viable threat. Law enforcement vehicles are stolen fairly frequently across the United States, though such incidents have thus far been limited to non-terrorist criminal acts. However, recent information indicates that terrorist planners may be looking at acquiring specialty vehicles in the United States for purposes of evading heightened security measures.

#### **SUGGESTED PROTECTIVE MEASURES**

Facility security personnel:

- Be familiar with local first responder uniforms and vehicles—including those outside your immediate locale.
- Establish procedures to notify perimeter/gate security of the impending arrival of emergency vehicles.
- Verify vehicle access permission to include emergency responder vehicles. Verify the vehicle was requested by the facility and was sent by an appropriate agency before allowing the emergency vehicle to enter the facility.
- Institute a robust vehicle inspection program to include checking under the undercarriage of vehicles, under the hood, and in the trunk of all vehicles attempting to enter the site.

- In addition to Jersey barriers and manned checkpoints, ensure appropriate use of ditching and berms to prevent vehicles from driving through perimeter fencing.
- Establish multiple, layered entry points at high risk facilities. Move initial security check points as far as practical from key assets and large personnel concentrations.
- Install remotely controlled barriers to a remote secure site with closed circuit TV and phones to monitor initial access points. This would help counter an attack in which terrorists kill guards and open the barrier device themselves.
- Facilities deemed to be high risk may consider establishing off-site delivery facilities where all vehicles bring outside cargo for screening.
- Critical infrastructure and key resource (CI/KR) security forces, in conjunction with law enforcement, fire protection, emergency medical agencies, and utility services, should establish indicators for identifying legitimate uses of official vehicles.
- Verification of vehicle and operator legitimacy should be incorporated into all traffic control plans and actions by all CI/KR and emergency agency parties.
- CI/KR managers should institute policies prohibiting unexpected large vehicles from entering the facility.
- Practice accountability of all emergency vehicles to include tracking vehicles that are in service, in repair status, or sent to salvage.
- Be able to verify to facility security personnel that an emergency vehicle responding to a facility is an authorized vehicle with authorized personnel/operators.
- Provide Buffer Zone security at all threat levels.
- Be prepared to deploy explosive detection devices and explosive detection canine teams at specific threat levels.
- Practice key accountability – use keys (made from the manufacturer or aftermarket) that cannot be duplicated without written permission from the agency; or use keys with an electronic chip installed. Do not label keys with the vehicle number on the key chain—using the VIN number instead would require much more effort to determine which vehicle matches each set of keys.
- Store emergency response vehicles in a secure compound that would require the operator to utilize some sort of access control system, like a pass code or an identification number if a guard is not available for lot security. An electronic inventory should be kept of emergency vehicles that are not in use. Consider implementing an operator log to record a vehicle as “in use” before it exits the parking compound. Also consider requiring private ambulance services to provide a secure location to park their emergency vehicles.
- Install Vehicle Tracking GPS/kill switches, such as ‘On Star’, in vehicles that would enable the vehicle to be turned off from a remote location, making the vehicle inoperative if it were reported stolen.
- Kill switches/engine immobilizers/transmission locks concealed within the vehicle could prevent the vehicle from being started or from being put into gear after it is started.
- Ensure that officers turn off and lock the emergency vehicle’s doors when not in the vehicle.
- Installation of vehicle tracking devices and coded entry and operation systems should be considered by all fleet operators.

- Uniforms, vehicle access, operating devices and codes, and other “legitimizing” equipment of vehicle operators and vehicle fleets should be treated as high-value, accountable items by all fleet operators.
- Parking, storage, garaging, maintenance, and other resting places for vehicles should have sufficient security measures to preclude theft, tampering, surreptitious loading and affixing, and other illegitimate acts targeting vehicles and their respective legitimate operators.
- All vehicle anomalies, procedural violations, and other suspicious activities should be reported to the appropriate authorities as soon as they are discovered.

**Law enforcement agencies:**

- Conduct awareness training at all levels of Law Enforcement concerning individual actions dealing with securing emergency vehicles.
- Immediately put stolen emergency vehicles into a nationwide all-points bulletin.

**DHS:**

- Ensure all personnel are provided timely Indications and Warning updates regarding present and emerging threats.
- Ensure all personnel are aware of any changes to the HSAS security levels.

**Recipients are encouraged to review the following joint DHS/FBI information bulletins on related threats:**

- “Potential for Terrorist Use of Rental Vehicles: Indicators for the Car, Truck and Limousine Rental Community,” dated August 5, 2004.
- “Potential Threat to Homeland Using Heavy Transport Vehicles,” dated July 30, 2004.

Information on suspicious activities potentially related to terrorism should be forwarded immediately to the local FBI JTTF and the DHS HSOC as indicated on the first page.

For comments or questions related to the content or dissemination of this Information Bulletin, please contact the DHS/Information

Analysis and Infrastructure Protection Directorate’s Requirements Division at [DHS.IAIP@DHS.GOV](mailto:DHS.IAIP@DHS.GOV).





It would be very easy to hide inside the grass and vegetation around this facility. How will you minimize this type of danger? Remember two keys to proper security. **Detection and deterrence.**



## Biological Incidents

Several biological agents can be adapted and used as terrorist weapons. These include anthrax (sometimes found in sheep), tularemia (or rabbit fever), cholera, encephalitis, the plague (sometimes found in prairie dog colonies), and botulism (found in improperly canned food).

Biological agents pose very serious threats given their fairly accessible nature, and the potential for their rapid spread. The potential for devastating casualties is high in a biological incident. These agents are disseminated in the following ways: by the use of aerosols (spray devices), oral (contaminating food or water supplies), dermal (direct skin contact with the substance) exposure, or injection.

There are four common types of biological agents: bacteria, viruses, rickettsia, and toxins.

### Bacteria and Rickettsia

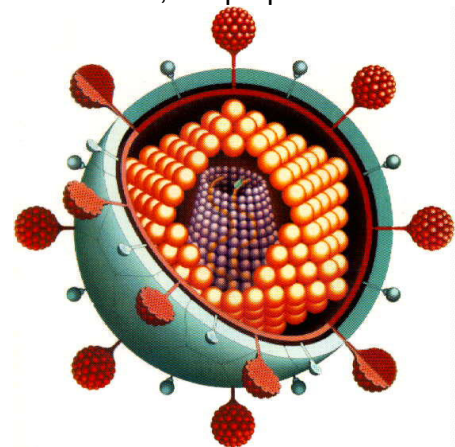
Bacteria are single-celled organisms that multiply by cell division and can cause disease in humans, plants, or animals. Although true cells, rickettsia are smaller than bacteria and live inside individual host cells. Examples of bacteria include anthrax (*Bacillus anthracis*), cholera (*Vibrio cholerae*), plague (*Yersinia pestis*), and tularemia (*Francisella tularensis*); an example of rickettsia is Q fever (*Coxiella burnetii*).



You may be familiar with the disease anthrax, associated with cattle, sheep, and horses serving as hosts. Handling of contaminated hair, wool, hides, flesh, or other animal substances can lead to contracting cutaneous (dermal) anthrax. However, the purposeful dissemination of spores in aerosol, such as for terroristic purposes, is another way people could contract it and is a more dangerous form of the disease.

### Virus

Viruses are the simplest type of microorganisms. They lack a system for their own metabolism and therefore depend upon living cells to multiply. This means that a virus will not live long outside of a host.



Types of viruses that could serve as biological agents include smallpox, Venezuelan equine encephalitis, and the viral hemorrhagic fevers such as the Ebola and Marburg viruses, and Lassa fever.

### Toxins

Toxins are toxic substances of natural origin produced by an animal, plant, or microbe. They differ from chemical agents in that they are not manmade and typically they are much more complex materials.



Toxins, in several cases, are easily extracted for use as a terrorist weapon, and, by weight, usually are more toxic than many chemical agents.

The four common toxins thought of as potential biological agents are botulism (botulinum), SEB (staphylococcal enterotoxin B), ricin, and mycotoxins.

Ricin is a toxin derived from the castor bean plant, available worldwide. There have been several documented cases involving ricin throughout the U.S., particularly in rural areas.



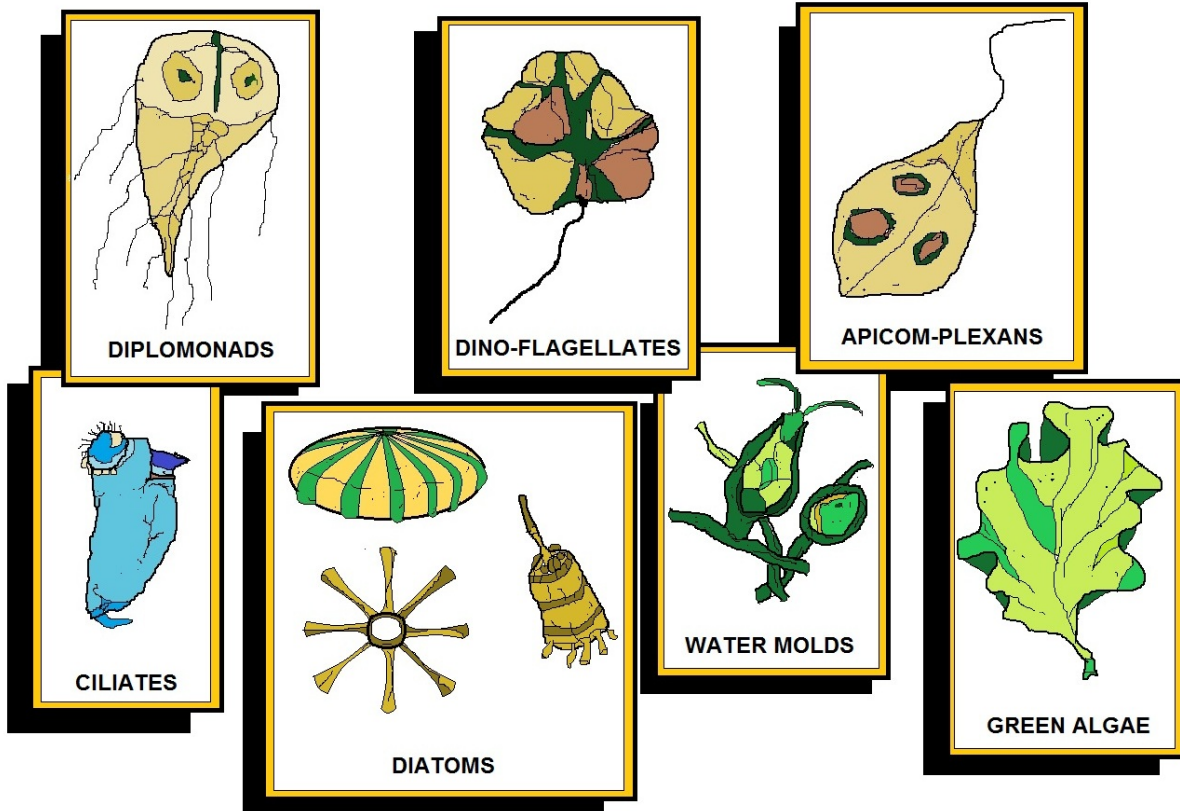
Castor Bean Plant

### Routes of Exposure

The primary routes of exposure for biological agents are inhalation and ingestion. Skin absorption and injection also are potential routes of entry, but are less likely.



Inspect every suspicious delivery vehicle and be suspect of un-labeled chemicals or as this truck does not display a placard but seems to have hazardous materials on board. We surveyed 25 facilities and none of these inspected delivery trucks.



# KINGDOM PROTISTA

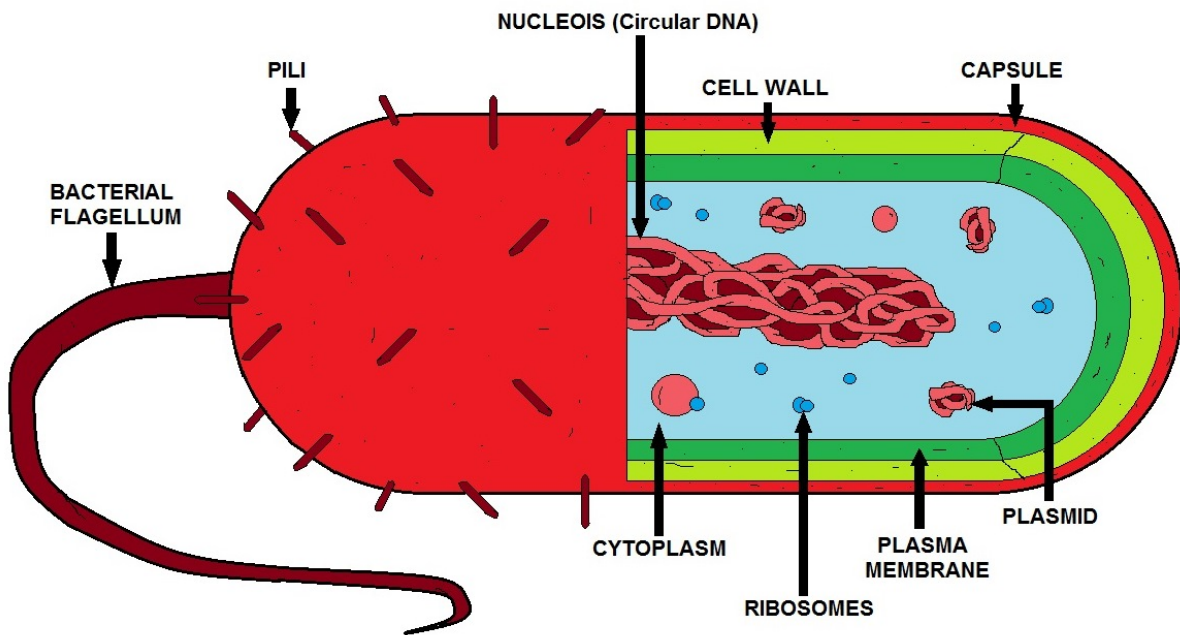
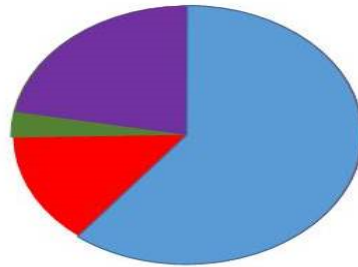


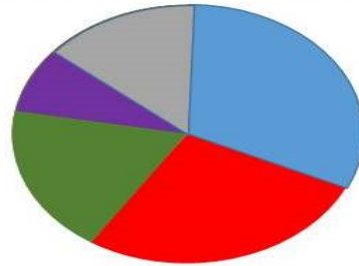
DIAGRAM OF VIBRIO CHOLERA BACTERIA

**A. SOURCE OF NOROVIRUS**

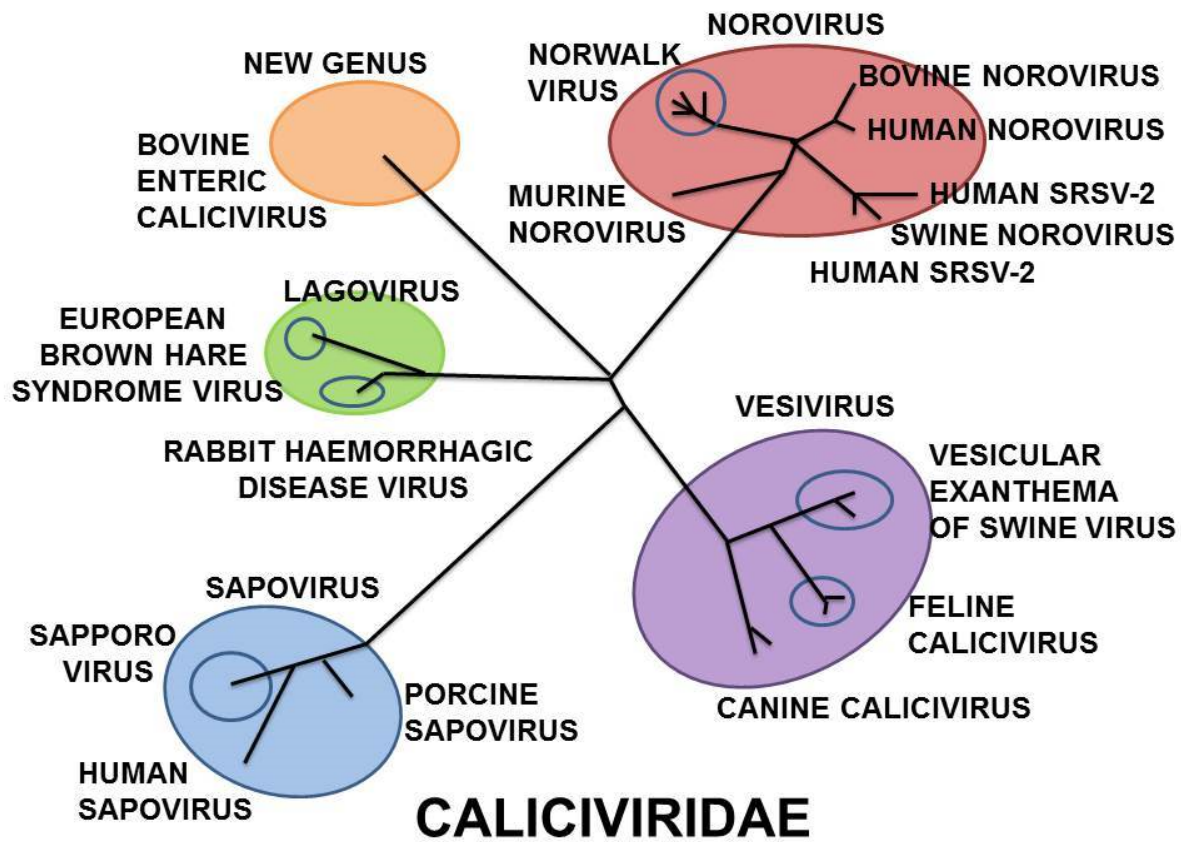


- FOODBORNE
- PERSON-TO-PERSON
- WATERBORNE
- UNKNOWN

**B. SETTING FOR OUTBREAK**



- RESTAURANTS
- NURSING HOMES
- SCHOOLS
- VACATION SETTINGS
- UNKNOWN



## Terrorist Master Nerve Gas Attacks

In 1995 a Nerve Gas attack on a subway in Tokyo rewrote the terrorist handbook forever. The religious cult had manufactured the fatal sarin gas in-house.

Uprooted weapon scientists from Iraq, Russia and South Africa are hunting for new jobs and spreading germ secrets.

Radical states with reputations for supporting terror such as Iran and Libya have arsenals of germ and chemical weapons and have passed on know-how and technology to terrorist groups.

Terrorists, including Osama Bin Laden, are increasingly interested in pestilential germs. Some boast openly of being able to kill foes with deadly plagues.

Beleaguered Iraq is reported to be showing great interest in transferring its bio-chemical weapons expertise to terrorist groups

### **QUOTE-UNQUOTE**

***"Germ terrorism... is the single most dangerous threat to our national security in the foreseeable future."***

R. James Woolsey, Director of Central Intelligence 1993-95

***"Eventually this is going to hurt us; there is no question in my mind."***

M. Blitzer, Ex FBI Directing section on Domestic Terrorism

***"Jihad has at last discovered how to win the holy war - lethal germs."***

Nasser Asad Al-Tamimi, Islamic Radical

***"If I have indeed acquired these weapons, then I thank God for enabling me to do so. And if I seek to acquire these weapons, I am carrying out a duty. It would be a sin for Muslims not to try to possess the weapons that would prevent the infidels from inflicting harm on Muslims."***

Osama Bin Laden, Terrorist suspected of bombing the World Trade Center and Embassies in Africa

***"The sleeping giant was awoken in Japan, now the rest of the world will have to learn the lesson."***

Mohammed X, Arabia Forums

Remember there are extremists that memorize and worship these sayings and think about ways to destroy your facility.

## Newspaper Article from London

### December 2002

The Manchester raid occurred a week after Scotland Yard disclosed that it had discovered a laboratory in London that was allegedly used to produce the deadly poison Ricin.

Five men and one woman were arrested in a series of raids on properties in the north and west of the capital.

Four Algerian men appeared in court on terrorism charges on Monday and were remanded in custody. They were jointly charged under Section 57 of the Terrorism Act and the Chemical Weapons Act. A fifth man arrested with the group appeared separately to face two charges under the Forgery and Counterfeiting Act 1981.

Ricin, a naturally occurring toxin that is produced from castor oil beans, is one of the world's deadliest substances. It has no known antidote and is considered by experts to be ideal for political assassinations, possibly in the form of an aerosol.

Plans by al-Qaeda to produce Ricin were found by *The Times* in the Afghan capital Kabul in November 2001 and Iraq is also known to have included Ricin in its biological weapons programme.



Easy to make a toxic substance and our free society makes it easy to distribute. It is just a matter of time and this will happen.

## Bio-Chemical Terror

The threat of bio-chemical terror has initiated a revolution in security thinking.

Until new portable sensor technology is available (in about 2005), security forces have very little control - beyond intelligence sources - of the transfer of lethal materials. Only small quantities are required for great effect.

These can be contained in plastic or glass and thus pass freely through metal-detectors or x-ray devices. Their proximity in appearance to pharmaceuticals, perfumeries, and cosmetics is such that a primitive labeling would not give security personnel cause for suspicion.

Many of these agents can be designed in aerosol form and can be silently distributed through unguarded air-condition systems.

### Biological Agents of Destruction

In its crude form, anthrax can be manufactured in-house using widely-available biological skills and materials. An extremely infectious disease found in livestock, inhalation causes flu-like symptoms for a number of days, followed by a brief respite while the disease lies dormant, then the onset of respiratory failure, shock and death.

Vaccinations are presently being upgraded in the US to include the full range of anthrax types. American special units and general emergency personnel are to receive vaccinations in addition to soldiers.

Certain antibiotics together with antidote are to some degree effective in treating, although how far is still highly uncertain (tests for strains have been done only on animals).

Effectiveness for the very old and very young (the vulnerable heart of the civilian frontier) is extremely doubtful. Moreover, treatment should begin immediately- creating problems in the event of an undeclared attack (**90 percent fatality**).

Like many other biological killers, anthrax spores can be contained in plastic aerosol form.

Most of America's enemies have anthrax stockpiles. Terrorist groups in the Middle East and their supporters have shown a keen interest in the virus that has claimed the spotlight of the American media.

Other Biological agents cultivated for terrorist use include: Botulism, plague, Ricin and Aflatoxin. Where Americans have reason to fear a large scale (mass casualty) attack - a single crop sprayer over a major city could kill 3 million.

Biological weapons can be used in many different ways, in a variety of scenarios. For example, Ricin is a deadly toxin that could be used for assassinations; insects could be used to spread deadly diseases; food or water supplies could be contaminated (4). Undoubtedly, however, rapid, large-scale anti- personnel use of biological agents requires their dissemination through the air and inhalation into the lungs.

When used effectively in this way biological weapons have an area coverage which makes them equivalent to nuclear weapons as weapons of mass destruction. There are many estimates in the open literature that confirm this conclusion.

For example, the Office of Technology Assessment of the United States Congress has calculated that a mere 100 kg of anthrax spores, spread as a line source and allowed to drift on the wind on a clear, calm night over Washington DC, could kill between 1 and 3 million people (5). The difference between nuclear and biological weapons of mass destruction, as the Iraqi example clearly demonstrates, is that it is much easier and cheaper to produce a biological weapons arsenal.

The ease with which such agents can be produced means that they could also be available to rogue states or even sub-state terrorist groups. It is known that the Japanese sect which used Sarin nerve gas against commuters on the Tokyo underground was also interested in the use of anthrax.

Anthrax is one of a group of so-called '*classical*' biological warfare agents. It was weaponized in the US offensive biological weapons program which ran from 1942 to 1969. Anthrax is an obvious agent of choice because it forms a spore which is resistant to environmental damage.

Also, as the Joint CB Technical Data Source Book pointed out (6): "***...The mortality rate for respiratory anthrax is essentially 100 per cent. Since early diagnosis of inhalation anthrax is unlikely, treatment with antibiotics is ineffective...***"

Nevertheless, there was doubt about the utility of biological weapons during the Cold War period when biological weapons were often seen as unpredictable and uncontrollable.

Yet a senior UK official specifically rejected this view in an article in the Journal of the Royal United Services Institute in 1992. He argued that by 1969 (7): "***...The utility of BW had been demonstrated by all means, short of use in war, and the established feasibility could clearly not become disestablished with time...***" Moreover, the threat from biological weapons has continued to develop since 1969.

Infectious diseases caused by microbial agents - bubonic plague, cholera, influenza, leprosy, measles, smallpox, tuberculosis, typhoid fever, typhus, yellow fever etc. - have long created misery for human populations in both peace and war. And sporadic attempts have been made in the past to deliberately use disease as a weapon of war: the British, for example, gave Native American Indians blankets contaminated with smallpox.

Yet, it was only towards the end of the last century that scientific understanding of these diseases and their agents began to develop. Inevitably, perhaps, this precise new knowledge was applied in warfare, an example being the attempts by both sides in the First World War to infect vital stocks of horses with the disease glanders.

The large-scale Japanese, British, and American offensive biological weapons programs then followed in the 1930s, '40s, '50s, and '60s. Knowledge of bacteria developed faster than that of viruses and it seems probable that the Soviet/Russian program, which was only officially terminated in the 1990s, would have benefited from the growing knowledge of viral agents and diseases.



Only in the early 1970s did genetic engineering--the effective transfer of functional genes across species--become possible, and the growth of modern biotechnology began. Genetic engineering, as is well recognized, allows the easier production of militarily significant quantities of toxins. Essentially, it has become possible to produce strategic weapons, using very limited physical and financial resources, with a relatively small number of trained personnel. It also allows the possibility of enhancing the characteristics of biological warfare agents in order to improve their environmental stability, their infectivity and their resistance to antibiotics. Humans have long been involved in modifying other species by deliberate, selective breeding--for example, to produce the vast range of modern dog varieties.

But the difference between this traditional activity and modern capabilities, like making a human gene function in a bacterium, can hardly be overstated. These dangers are clearly set out in the background scientific papers produced for the Fourth Review Conference of the Biological Weapons Convention in 1996 (8). It was also recognized at the Review Conference that the Human Genome Project, which will deliver a complete account of the structure of our genetic material by the early years of the next century, could pose new dangers. A number of analysts have argued that knowledge of the human genome at this level, combined with the obvious diversity of human groups, and the current advances in gene therapy, could perhaps allow the development of '*ethnic*' biological weapons targeted at specific groups.

There is, additionally, an obvious danger that our growing knowledge of bioregulatory peptides will allow the development of a new range of anti-personnel agents.

Such misuse of biological knowledge could happen if the international community is unable to enforce the disarmament norm embodied in the Biological Weapons Convention.

Also, our overconfidence (as a species) that we have beaten microbial pathogens has been severely dented. The phenomenon of drug-resistant tuberculosis has epitomized the threat that could affect any of us even in the developed world. Microbial pathogens can evolve very quickly to evade the defenses we erect.

Alongside this renewed threat from '*old*' diseases, there are new threats from diseases with frightening characteristics, such as Ebola, as the human population expands and moves in large numbers into different ecosystems.

The analysis of the threats we face today is much more complex than a decade ago, and potential errors that could lead to worst-case analyses abound, but as two naval analysts recently pointed out (10): "***Functional distortion in intelligence analysis amounts to de-emphasis of security threats that may be acknowledged and real, but which existing forces can do little about, or that cannot be countered without significant investment in capabilities that differ from those in hand...***"

Ignoring the very real dangers in the evolving threat from biological agents would appear to fit into this precise category of distortion, and the consequences of that mistake could be extremely dangerous.

Yet, if the problem is recognized and properly prioritized, a great deal can be done to reinforce the norm of international behavior embodied in the Biological and Toxin Weapons Convention.

At a scientific level, for example, our ability to detect and identify agents and toxins has increased considerably in recent years. Alongside rapid increases in specific knowledge about individual disease agents, broader generalizations about the mechanisms of pathogenicity are becoming possible. This should increasingly allow a more generic approach to be taken in dealing with emerging threats.

An interesting example of what might become possible is the Unconventional Pathogen Countermeasures Program in the Defense Sciences Office of the US Defense Advanced Research Projects Agency (**DARPA**). This program is seeking novel and unconventional methods of providing protection against pathogens used adversarially.

**Table 1. Critical biological agent categories for public health preparedness**

Biological agent(s)	Disease
<b>Category A</b>	
<i>Variola major</i>	Smallpox
<i>Bacillus anthracis</i>	Anthrax
<i>Yersinia pestis</i>	Plague
<i>Clostridium botulinum</i> (botulinum toxins)	Botulism
<i>Francisella tularensis</i>	Tularemia
Filoviruses and Arenaviruses (e.g., <i>Ebola virus</i> , <i>Lassa virus</i> )	Viral hemorrhagic fevers
<b>Category B</b>	
<i>Coxiella burnetii</i>	Q fever
<i>Brucella spp.</i>	Brucellosis
<i>Burkholderia mallei</i>	Glanders
<i>Burkholderia pseudomallei</i>	Melioidosis
Alphaviruses (VEE, EEE, WEE <sup>a</sup> )	Encephalitis
<i>Rickettsia prowazekii</i>	Typhus fever
Toxins (e.g., Ricin, Staphylococcal enterotoxin B)	Toxic syndromes
<i>Chlamydia psittaci</i>	Psittacosis
Food safety threats (e.g., <i>Salmonella spp.</i> , <i>Escherichia coli</i> O157:H7)	
Water safety threats (e.g., <i>Vibrio cholerae</i> , <i>Cryptosporidium parvum</i> )	
<b>Category C</b>	
Emerging threat agents (e.g., <i>Nipah virus</i> , hantavirus)	

<sup>a</sup>Venezuelan equine (VEE), eastern equine (EEE), and western equine encephalomyelitis (WEE) viruses

**Table 2. Criteria and weighting<sup>a</sup> used to evaluate potential biological threat agents**

Disease	Public health impact		Dissemination potential		Public perception	Special preparation	Category
	Disease	Death	P-D <sup>b</sup>	P - P <sup>c</sup>			
Smallpox	+	++	+	+++	+++	+++	A
Anthrax	++	+++	+++	0	+++	+++	A
Plague <sup>d</sup>	++	+++	++	++	++	+++	A
Botulism	++	+++	++	0	++	+++	A
Tularemia	++	++	++	0	+	+++	A
VHF <sup>e</sup>	++	+++	+	+	+++	++	A
VE <sup>f</sup>	++	+	+	0	++	++	B
Q Fever	+	+	++	0	+	++	B
Brucellosis	+	+	++	0	+	++	B
Glanders	++	+++	++	0	0	++	B
Melioidosis	+	+	++	0	0	++	B
Psittacosis	+	+	++	0	0	+	B
Ricin toxin	++	++	++	0	0	++	B
Typhus	+	+	++	0	0	+	B
Cholera <sup>g</sup>	+	+	++	+/-	+++	+	B
Shigellosis <sup>g</sup>	+	+	++	+	+	+	B

<sup>a</sup>Agents were ranked from highest threat (+++) to lowest (0).

<sup>b</sup>Potential for production and dissemination in quantities that would affect a large population, based on availability, BSL requirements, most effective route of infection, and environmental stability.

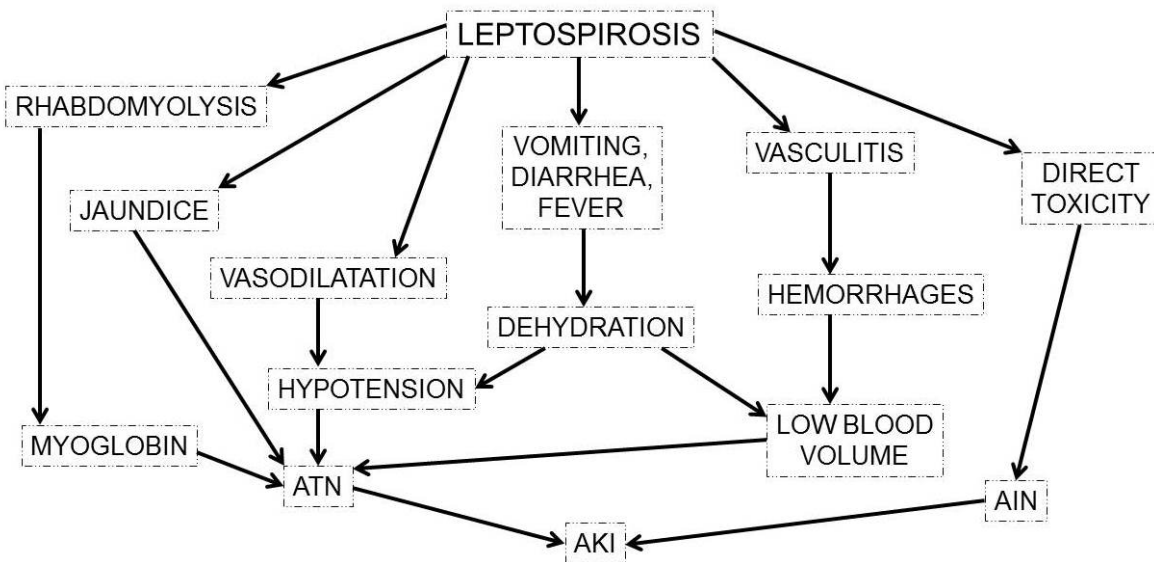
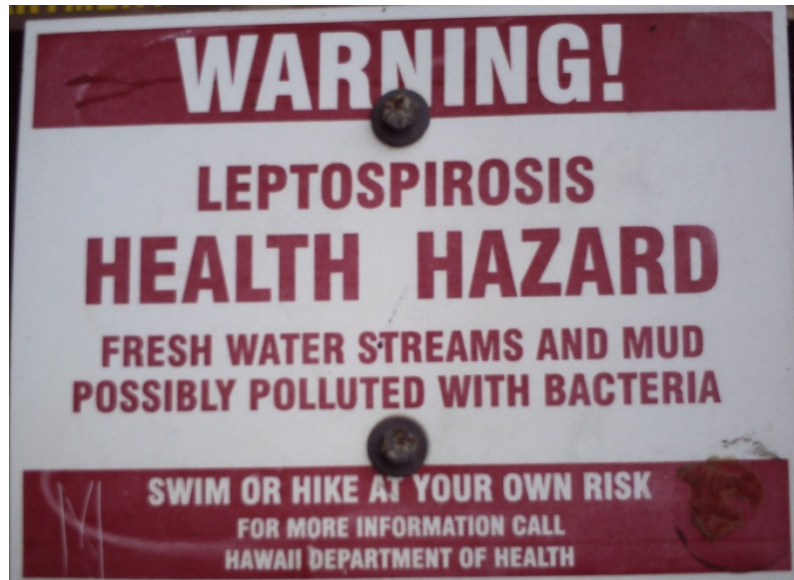
<sup>c</sup>Person-to-person transmissibility.

<sup>d</sup>Pneumonic plague.

<sup>e</sup>Viral hemorrhagic fevers due to Filoviruses (*Ebola*, *Marburg*) or Arenaviruses (e.g., *Lassa*, *Machupo*).

<sup>f</sup>Viral encephalitis.

<sup>g</sup>Examples of food- and waterborne diseases.



### PHYSIOPATHOLOGY OF AKI IN LEPTOSPIROSIS

The bugs are easily available, all a terrorist need is to simply collect and cultivate. We found a kit to do this activity online for \$19.95.

## Bioterrorism

Although use of conventional weapons such as explosives or firearms is still considered the most likely means by which terrorists could harm civilians, multiple recent reports cite an increasing risk and probability for the use of biological or chemical weapons.

Indeed, the use of biological and chemical agents as small- and large-scale weapons has been actively explored by many nations and terrorist groups.

Although small-scale bioterrorism events may actually be more likely in light of the lesser degrees of complexity to be overcome, public health agencies must prepare for the still-possible large-scale incident that would undoubtedly lead to catastrophic public health consequences. The selection and prioritization of the potential biological terrorism agents described in this report were not based on the likelihood of their use, but on the probability that their use would result in an overwhelming adverse impact on public health.

Most evaluations of potential risk agents for biological warfare or terrorism have historically been based on military concerns and criteria for troop protection. However, several characteristics of civilian populations differ from those of military populations, including a wider range of age groups and health conditions, so that lists of military biological threats cannot simply be adopted for civilian use. These differences and others may greatly increase the consequences of a biological attack on a civilian population.

Civilians may also be more vulnerable to food- or waterborne terrorism, as was seen in the intentional *Salmonella* contamination of salad bars in The Dalles, Oregon, in 1984. Although food and water systems in the United States are among the safest in the world, the occurrence of nationwide outbreaks due to unintentional food or water contamination demonstrates the ongoing need for vigilance in protecting food and water supplies. Overall, many other factors must be considered in defining and focusing multiagency efforts to protect civilian populations against bioterrorism.

Category A agents are being given the highest priority for preparedness.

For Category B, public health preparedness efforts will focus on identified deficiencies, such as improving awareness and enhancing surveillance or laboratory diagnostic capabilities. Category C agents will be further assessed for their potential to threaten large populations as additional information becomes available on the epidemiology and pathogenicity of these agents. In addition, special epidemiologic and laboratory surge capacity will be maintained to assist in the investigation of naturally occurring outbreaks due to Category C "**emerging**" agents. Linkages established with established programs for food safety, emerging infectious diseases, and unexplained illnesses will augment the overall bioterrorism preparedness efforts for many Category B and C agents.

The above categories of agents should not be considered definitive. The prioritization of biological agents for preparedness efforts should continue. Agents in each category may change as new information is obtained or new assessment methods are established. Disease elimination and eradication efforts may result in new agents being added to the list as populations lose their natural or vaccine-induced immunity to these agents.

Conversely, the priority status of certain agents may be reduced as the identified public health and medical deficiencies related to these agents are addressed (e.g., once adequate stores of smallpox vaccine and improved diagnostic capabilities are established, its rating within the special preparedness needs category would be reduced, as would its overall rating within the risk-matrix evaluation process).

To meet the ever-changing response and preparedness challenges presented by bioterrorism, a standardized and reproducible evaluation process similar to the one outlined above will continue to be used to evaluate and prioritize currently identified biological critical agents, as well as new agents that may emerge as threats to civilian populations or national security.

## References

1. Leitenberg, M. (1996) Biological Weapons Arms Control. Contemporary Security Policy, 17, (1), 1-79.
2. Select Committee on Intelligence (1996) Current and Projected National Security Threats to the United States and its Interests Abroad. US Senate, 104th Congress, Second Session. Written Answers 10th May, S. Hrg 104-510
3. United Nations (1995) Report of the Secretary General on the status of the implementation of the Special Commission's plan for the ongoing monitoring and verification of Iraq's compliance with relevant parts of section C of Security Council resolution 687 (1991). S/1995/864, 11 October. United Nations, New York.
4. US Army Medical Research Institute of Infectious Diseases (1994) Biological Weapons Proliferation: Technical Report. DNA-MIPR-90-715. Defense Nuclear Agency, Alexandria, VA.
5. Office of Technology Assessment (1993) Proliferation of Weapons of Mass Destruction: Assessing the Risks. OTA-ISC-559. Congress of the United States, Washington, DC
6. Desert Test Center (1973) Joint CB Technical Data Source Book, Volume VII, Bacterial Diseases, Part II: Anthrax. DTC 73-27. Fort Douglas, Utah.
7. Carter, G. B. (1992) Biological warfare and biological defense in the United Kingdom 1940-1979. Royal United Services Institute Journal, December, 67-74.
8. United Nations (1996) Background paper on new scientific and technological developments relevant to the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction. BWC/CONF.IV/4. United Nations, Geneva.
9. Dando, M. R. (1997) 'Discriminating' bio-weapons could target ethnic groups. International Defense Review (Special Issue: Chemical and Biological Warfare), 30 (3), 77-78.
10. Hirschfeld, T. and Carus, W. S. (1997) We need to understand. Proceeding of the US Naval Institute, February, 65-68.
11. Dando, M. R. (1996) New developments in biotechnology and their impact on biological warfare. In O. Thranert (ed.), Enhancing the Biological Weapons Convention, J.H.W. Dietz Verlag, Bonn.  
\*\*\*\*\*
12. Danzig, R. (1996) Biological Warfare: A Nation at Risk - A Time to Act. Strategic Forum, 58, 1-4.
13. DARPA is the central research and development organization for the US Department of Defense. It manages and directs basic and applied research and development projects where risks of failure are high but success could provide dramatic advances. The agency, for example, created ARPNET the antecedent of the Internet. The Unconventional Pathogens Countermeasures Program is run by Dr Shaun Jones and Dr Steven Morse. This paper was originally written at the invitation of that program for their internet information site under the title "**The Threat from Biological Agents**".

## Nuclear Incidents

There are two fundamentally different threats in the area of nuclear terrorism. One is the use, threatened use, or threatened detonation of a nuclear bomb. The other is the detonation, or threatened detonation, of a conventional explosive incorporating nuclear materials (radiological dispersal devices or **RDD**). It is unlikely that any terrorist organization could acquire or build a nuclear device, or acquire and use a fully functional nuclear weapon.

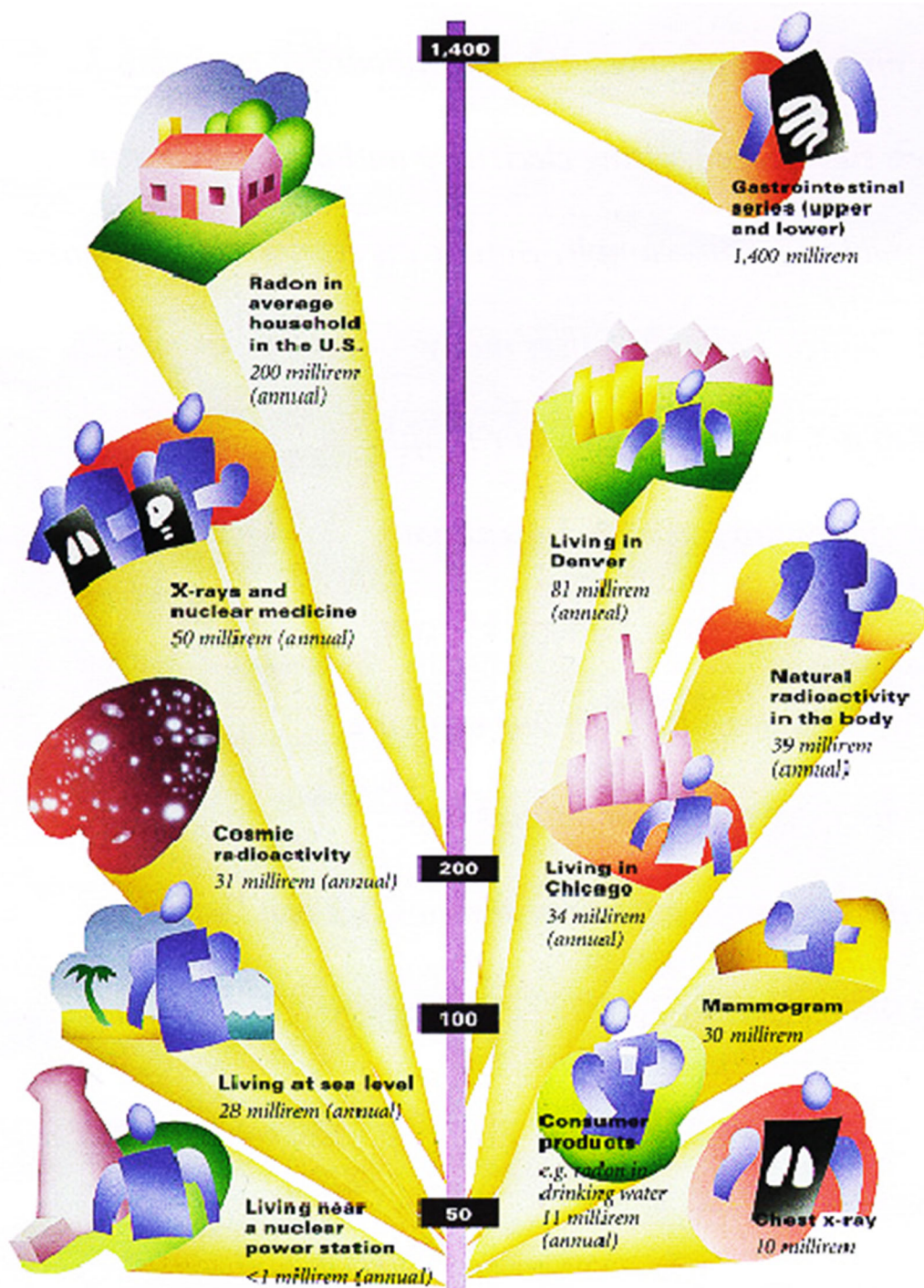
The number of nations with nuclear capability is small, and each places a high priority on the control of its nuclear weapons. Even if a nation supporting terrorism could develop a nuclear capability, experts believe it would be implausible for that nation to turn a completed weapon over to a group that might use it against them. The theft of a completed nuclear weapon also is unlikely. All nuclear nations have placed their nuclear arsenals under the highest security. All Western and former Soviet nuclear weapons are protected with a Permissible Action Link (**PAL**) system that renders the weapon harmless until the proper code is entered.

The greatest potential terrorist threat for a nuclear weapon would be to use such a device as a form of extortion. The U.S. government has plans to meet such a threatened use. Presently, there is no known instance of any nongovernmental group close to obtaining or producing a nuclear weapon.

The purpose of an attack where nuclear materials are incorporated into a conventional explosive (**RDD**) would be to spread radioactive materials around the bomb site. This would disrupt normal, day-to-day activities, and would raise the level of concern among first responders regarding long-term health issues. It would prove to be difficult to perform complete environmental decontamination.

Another possible scenario involving nuclear materials would be the detonation of a large device, such as a truck bomb (large vehicle with high quantities of explosives), in the vicinity of a nuclear power plant or a radiological cargo in transport. Such an attack could have widespread effects. The frequency of shipments of radiological materials is increasing throughout the world.

There are three main types of nuclear radiation emitted from radioactive materials: **alpha, beta, and gamma radiation.**





## Radiation Introduction

Radiation is energy in the form of waves and particles. It is a natural phenomenon that has existed since the beginning of time and is found everywhere.

Exposure to radiation is measured in millirems. The average person receives approximately 360 millirem per year from all sources of natural and man-made radiation. We are exposed to naturally occurring background radiation every day of our lives from such things as the earth, cosmic rays, radon gas, naturally radioactive foods such as bananas, buildings made of naturally radioactive materials such as granite, and even each other, as our bodies are naturally radioactive. The greatest single source of background exposure (an average of 200 millirem per year) comes from radon gas.

We are also exposed to man-made radiation from such things as dental x-rays, medical procedures, and televisions. Certain activities increase our exposure to radiation such as smoking (cigarette smoke contains radioactive particles) or airline travel (radiation exposure is higher at higher elevations).

### Schematic: **RADIATION: RISKS AND REALITIES**

United States Environmental Protection Agency

#### **TYPICAL BACKGROUND RADIATION LEVELS**

Location Dose

U.S. National Average 300 millirem/year

Connecticut 284 millirem/year

Colorado (Denver) 364 millirem/year

France (near Radon Springs) 1,600 millirem/year

India (parts of) 1, 140 millirem/year

Brazil (parts of) 17,500 millirem/year

Note: An individual's exposure to radiation dose is measured in "rem."

Most radiation dose is so small that it is measured in millirem (1/1,000 or .001 rem).

#### **SOURCES OF RADIATION**

(1 rem = 1,000 millirem)

Annual Radiation Dose (millirem/year)

##### **I. Natural Radiation Sources**

- A. Cosmic (from outer space)
  - Connecticut and Massachusetts 28
  - Colorado 125
- B. Terrestrial (from the earth's surface)
  - Connecticut and Massachusetts 16
  - Colorado 63
- C. Food Consumed and the Human Body Itself 40
- D. Inhaled Indoor (Radon) 200

##### **SUBTOTAL OF A, B, C, D**

- Connecticut and Massachusetts 284
- Colorado (Denver) 428

##### **II. Technologically Enhanced Exposures to Natural Sources**

- A. Radioactivity in Building Materials 7
  - (varies from wood frame to brick to stone)

- B. Air Travel (round trip cross-country) 5
- C. Natural Gas (Radon-222)
  - Cooking (lung) 5
  - Heating (lung) 22
- D. Smoking (30 cigarettes/day)
- Certain areas of the lung Up to 16,000

### **III. Man-made Sources**

- A. Medical Diagnosis (per capita) 53
- B. Consumer Products (TV) 1
- C. Nuclear Power Station (within 50 miles) 0.1
  - (at site boundary) 1 to 3

The average resident of Connecticut and Massachusetts receives a total of about 360 millirem/year from natural and other common sources of radiation.

References: National Council on Radiation Protection and Measurements Report No. 92 (12/87), Report No. 93 (9/87), Report No. 94 (12/87), Report No. 95 (12/87).

## HEALTH EFFECTS OF RADIATION EXPOSURE

### *Whole Body Radiation Dose Effects'*

1,000,000 Millirem - Death occurs with 30 days of exposure in 100 percent of the cases.

500,000 Millirem - Clinical recovery if exposure rate is not more than 10,000 - 50,000 millirem/day.

450,000 Millirem - 50 percent die within 30 days of exposure (without medical care)

200,000 Millirem - 1 percent die within 30 days (without medical care), 5 percent suffer nausea.

25,000 Millirem - EPA Protective Action Guide for Emergency Workers, possible clinical effects.

4,500 Millirem - NU's administrative guideline for maximum annual dose to workers.

3,000 Millirem - NRC's calendar quarter exposure limit for workers.

500 Millirem - NRC regulation level for an individual in the general public from all man-made sources (except medical)

300 Millirem - Average annual natural background level in United States.

25 Millirem - EPA's annual limit for dose to individuals in the public who live within two miles of a nuclear plant

<1 Millirem - Average annual dose to individuals in the public who live within two miles of a nuclear plant

(1) Unless otherwise noted, total dose occurs within a few hours to one day.

(2) 1,000 mrem = 1 rem

### Activities Which Result in a Dose of 0.1 mrem

#### Type of Exposure

2.4 hours at the elevation of Denver.

15 minutes at 30,000 feet of commercial subsonic jet travel.

4.5 months at a location 20 feet higher in elevation.

4.4 hours in a tightly insulated energy-efficient house.

1 year @ 8 hours per night sleeping with another person.

#### Source of Radiation

Cosmic/terrestrial

Cosmic rays

Cosmic rays

Radon gas

Natural Potassium-40

Radiation in the building materials

#### What is Radioactivity?

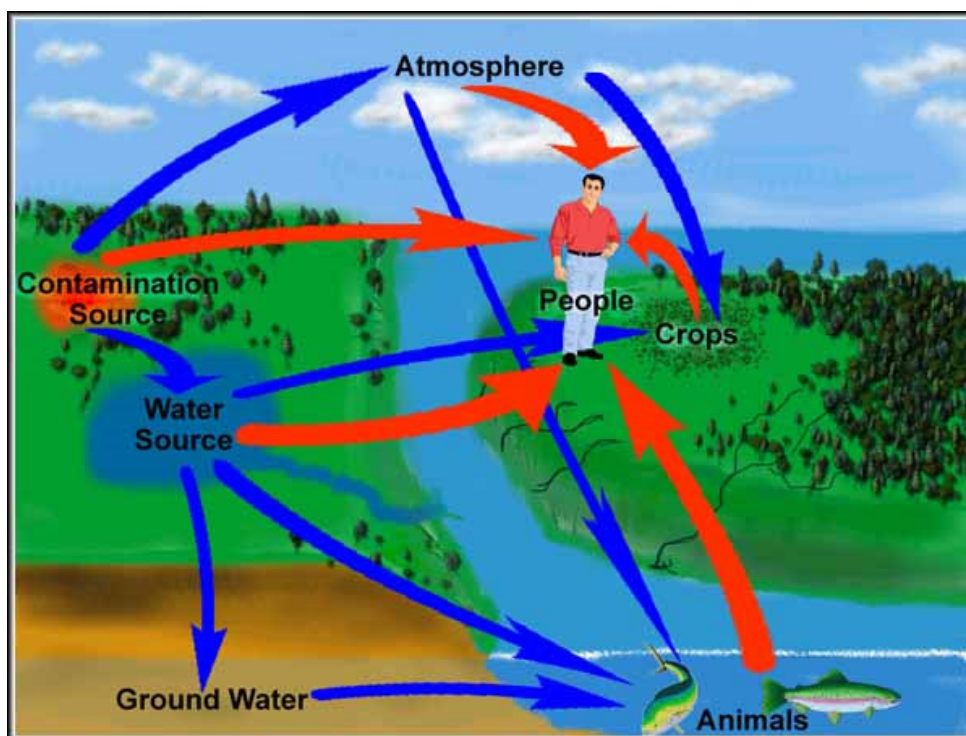
Radioactivity occurs when unstable nuclei of atoms decay and emit particles. These particles may have high energy and can have bad effects on living tissue. There are many types of radiation.

## How does Nuclear Waste get to You?

The planet's water cycle is the main way radiation is spread in the environment. When radioactive waste mixes with water, it is ferried through this water cycle. Radionuclides in water are absorbed by surrounding vegetation and ingested by local marine and animal life. Radiation can also be in the air and can be deposited on people, plants, animals, and soil.

People can inhale or ingest radionuclides in air, drinking water, or food. Depending on the half-life of the radiation, it could stay in a person for much longer than a lifetime.

The half-life is the amount of time it takes for a radioactive material to decay to one half of its original amount. Some materials have half-lives of more than 1,000 years!



Paths of Radiation to the Body.

### What can we do about nuclear waste?

According to a report from the U.S. National Academy of Sciences, it will take 3 million years for radioactive waste stored in the United States as of 1983 to decay to background levels. So, presently, the only solution is to store the waste in a place so that the environment won't be contaminated. The problem with storing nuclear waste is both political as well as technological. In terms of politics, no one wants it stored near them. So there's much dispute as to where radioactive waste should be stored. In addition, storing so much waste is a major technological challenge. According to a report issued by the British Parliament, ***"In considering arrangements for dealing safely with such wastes, man is faced with time scales that transcend his experience."***

**Radioactive wastes come in many different forms including the following:**

- protective clothing of people in contact with radioactive materials
- the remains of lab animals used in experiments with radionuclides
- cooling water, used fuel rods, and old tools and parts from nuclear power plants
- mill tailings from uranium-enrichment factories
- old medical radiation equipment from hospitals and clinics
- used smoke detectors which contain radioactive americium-241 sensors

## **Types of Nuclear Waste**

### **High-level waste**

Nuclear waste is divided into several categories. High-level waste consists mostly of spent nuclear reactor fuel from both commercial power plants and military facilities, as well as reprocessed materials which can emit large amounts of radiation for hundreds of thousands of years. Commercial nuclear power plants in the U.S. alone produce 3,000 tons of high-level waste each year.

The amount of spent fuel removed annually from the approximately 100 reactors in the U.S. would fill a football field to a depth of one foot. When spent fuel is removed from a reactor core, it still emits millions of rems of radiation.

In the absence of high-level waste repositories, nuclear power plants generally store their spent fuel rods in lead-lined concrete pools of water. These pools somewhat contain the spread of gamma radiation by keeping the rods relatively cool.

They also help prevent fission. The average commercial power plant puts 60 used assemblies into temporary storage each year and will probably continue to do so until the year 2000, when responsibility for spent fuel will be transferred to the Department of Energy. Space is running out at many plants, though.

The plants have another option--storing their spent fuel at other plants still under construction. It is theoretically possible to reduce the amount of storage space that spent fuel rods require by removing them from their assemblies, bundling them tightly, and then packing them into heavily shielded dry storage, but repacking these highly radioactive rods may present too much of a challenge.

For long-term storage of high-level waste, a waterproof, geologically stable repository and leak-proof waste container is required. Packaging has to be tailored to the volume of the waste, the actual radioactive isotopes of elements it contains, how radioactive it is, its isotopes' half-lives, and how much heat it still generates. One technique for packaging high-level wastes involves melting them with glass and pouring the molten material into impermeable containers.

The containers could be buried in soil or in a rock pile and surrounded by fill material and a barrier wall. From the 1940s through the 1960s, barrels of radioactive waste were frequently dumped in oceans. This ended in 1970 when the EPA (Energy Protection Agency) determined that at least one-fourth of these barrels were leaking.

### **Self-Burial**

A new, possibly safer proposal under consideration for long-term ocean storage includes offshore drilling and a procedure known as self-burial. In offshore drilling, holes would be drilled into the seabed and filled with barrels of waste. In self-burial, specially shaped barrels would be dumped and left to sink to the ocean floor.

Geologic disposal is currently the most popular solution for waste disposal. During the 1980s, the U.S. government invested more than \$2 billion into geologic disposal. In this form of disposal, mined tunnels with deep holes for waste canisters would be built using conventional mining techniques. Monitoring and waste retrieval would be relatively easy. In 1987, a site was chosen for the first permanent high-level commercial nuclear waste storage repository in the United States--Yucca Mountain, 100 miles northwest of Las Vegas, Nevada. Expected to cost up to \$15 billion, this repository is scheduled to go into operation by the year 2010.

Over the years, a number of other ideas for high-level waste disposal have been proposed and, at least temporarily, abandoned. One was disposal in space, in which sealed containers of radioactive material would be sent up into distant orbits. This would be an expensive and risky operation, as problems on the launch pad or in space could expose the earth and atmosphere to an enormous amount of radiation. Another suggestion was burying waste under the Antarctic ice sheets.

However, this would risk irradiating that area and the surrounding sea. A much safer idea, which would render disposal unnecessary, is to bombard radioactive waste with subatomic particles to transform it into less harmful isotopes. Unfortunately, this attractive proposal awaits still unrealized technology.

### **Mill Tailings**

Mill tailings, left over when ore is refined and processed is the largest by volume of any form of radioactive waste. Only 1% of uranium ore contains uranium--the rest is left on-site as a sand-like residue. These tailings are generally left outdoors in huge piles, where they blow around, releasing radioactive materials into the surrounding air and water.

By 1989, some 140 million tons of mill tailings had accumulated in the United States alone, with 10 to 15 million tons added each year. Although their radiation is generally less concentrated than other types of waste, some of the isotopes in these tailings are long-lived and can be hazardous for many thousands of years.

Until their radioactive risk was known, mill tailings were sometimes used as foundation and building materials, especially in western states. When their risk was discovered, these materials in the buildings had to be monitored.

These monitored sites are generally safer, although some groundwater contamination still occurs at them. It has been recommended that tailings be stored underground in clay pits, far from population centers.

## Low-Level Waste

Low-level wastes are usually defined in terms of what they are not. They are not spent fuel, milling tailings, reprocessed materials, or transuranic materials. Low-level waste includes the remainder of radioactive wastes and materials generated in power plants (such as contaminated reactor water), plus those wastes created in medical laboratories, hospitals, and industry. Wastes in this category usually, although not always, release smaller amounts of radiation for a shorter amount of time.

"**Low level**" does not mean "**not dangerous**," though. Although its radioactivity is usually less concentrated than that of high-level waste, low-level waste can be dangerous for up to tens of thousands of years.

Most low-level wastes come from reactors. These wastes can be divided up into two categories:

- Fuel wastes are fission products that leak out of fuel rods and into cooling water.
- Nonfuel wastes result when stray neutrons bombard anything in the core other than fuel--such as the reactor vessel itself--and cause them to become radioactive.

The remainder of low-level wastes comes from industry and institutional sources, including pharmaceutical plants, universities, and medical facilities. Instead of going to low-level waste dumps, these wastes are often kept on-site for the short time it takes for them to decay to safe levels. Then they are deposited into sanitary landfills. However, it is likely that liquid wastes are literally poured down the drain, whether or not they are still radioactive.

Low-level waste landfills were first built in the 1960s. In near-surface land burial, containers of waste fill a trench and are covered and surrounded by compacted earth. There are currently a few burial grounds in the U.S. to which most commercial low-level waste materials emitting detectable amounts of radiation are sent.

A few other landfills are currently inactive due to severe waste-containment problems and radioactive leakage. Waste containers in near-surface landfills are prone to corrosion, particularly in moist climates.

### Landfills

Landfills provide a false sense of comfort because they are "**out of sight, out of mind**." More worthwhile alternatives include above-ground landfills and storing waste at existing nuclear plant sites.

There are a number of unresolved issues regarding disposal of low-level wastes. The current institution control period (the amount of time a waste site must remain under guard after it has been filled and closed) is only 100 years.

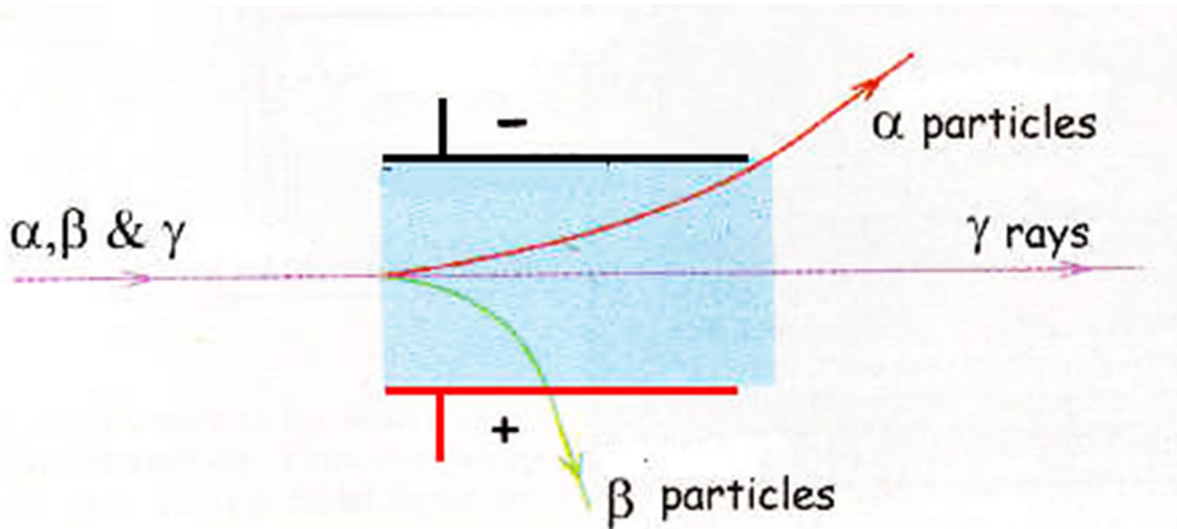
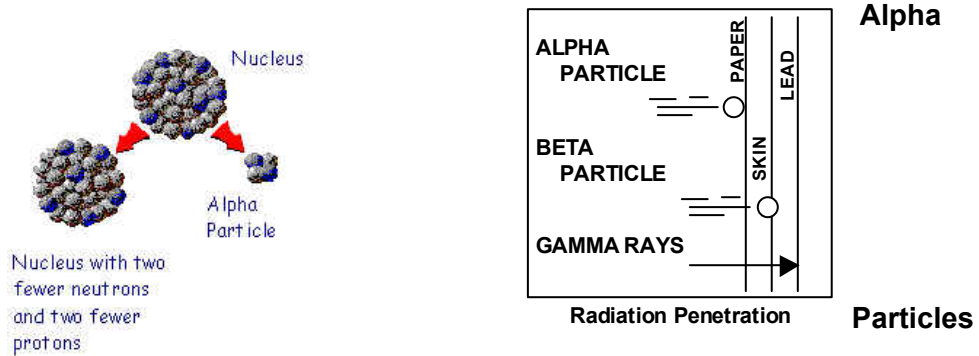
Yet the hazards presented by some low-level wastes can continue for thousands of years. What keeps future generations from uncovering and being contaminated by these substances?





## Alpha Particles

Alpha particles are the heaviest and most highly charged of the nuclear particles. However, alpha particles cannot travel more than a few inches in air and are completely stopped by an ordinary sheet of paper. The outermost layer of dead skin that covers the body can stop even the most energetic alpha particle. However, if ingested through eating, drinking, or breathing contaminated materials, they can become an internal hazard.



Experiments where alpha particles were collided with various atoms showed that they were the same mass and charge as a Helium nucleus.

From this we know that an Alpha particle consists of two neutrons and two protons and so carries a charge of +2.

If a nucleus, made up from lots of protons and neutrons, ejects an Alpha particle, what is left behind?

If the nucleus has changed as a result of ejecting an Alpha, has the source material changed into a different element?

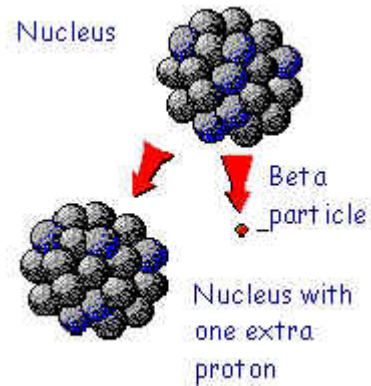
### Alpha Summary

Alpha particles consist of two neutrons and two protons (helium atoms with two electrons removed). The daughter nucleus therefore has an atomic (serial) number two lower and a mass number four lower than the parent nucleus.

### Penetrating power

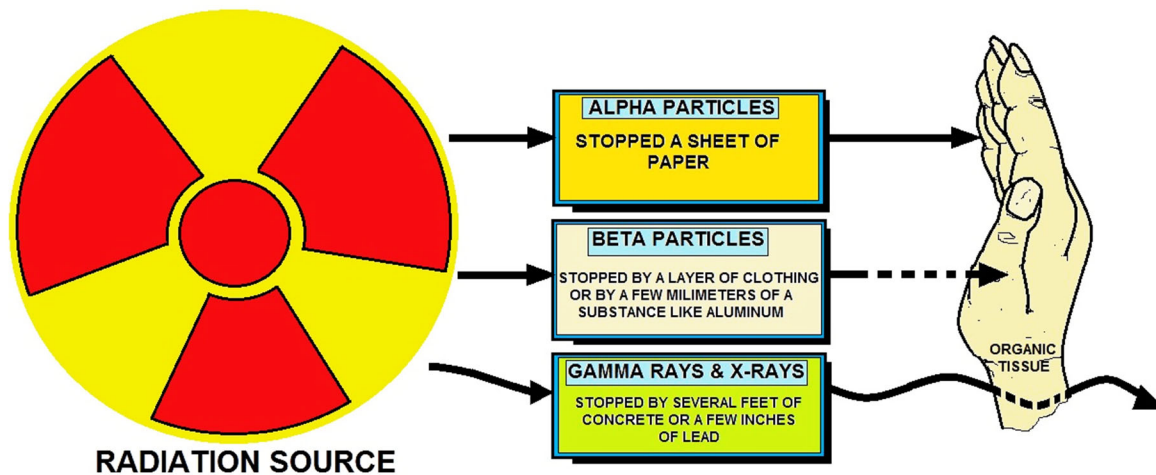
Alpha particles have a range in air of up to about 40 - 100mm

Alpha particles can be stopped with a thin layer of paper



### Radiological Characteristics

Radiological characteristics are the result of water coming in contact with radioactive materials. This could be associated with atomic energy.



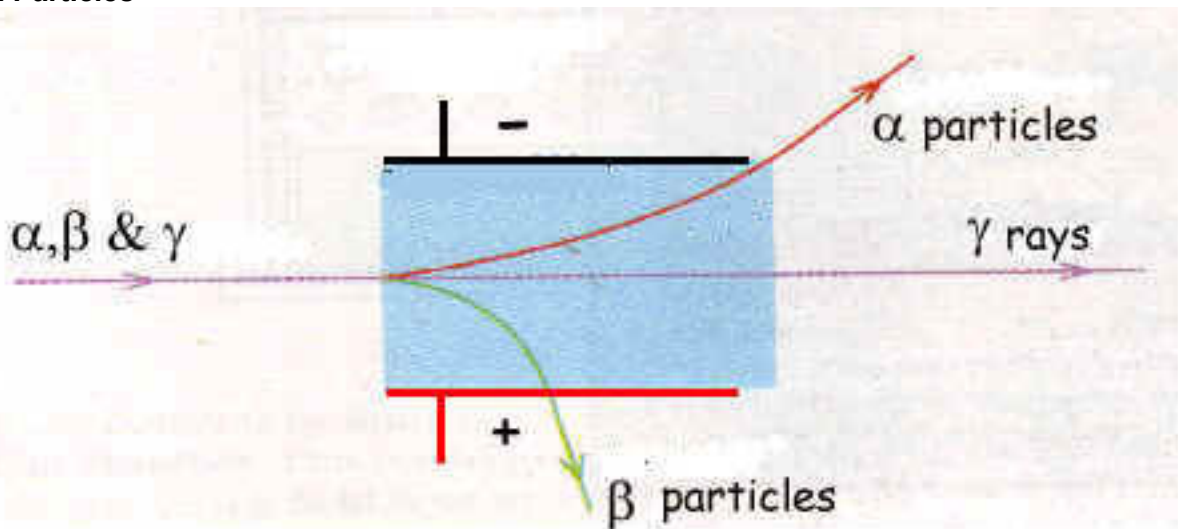
**PENETRATING POWER OF ALPHA / BETA PARTICLES AND GAMMA RAYS AND X-RAYS**

## Beta Particles

Beta particles are smaller and travel much faster than alpha particles. Typical beta particles can travel several millimeters through tissue, but they generally do not penetrate far enough to reach the vital inner organs. Exposure to beta particles from outside the body is normally thought of as a slight hazard.

However, if the skin is exposed to large amounts of beta radiation for long periods of time, skin burns may result. If removed from the skin shortly after exposure, beta-emitting materials will not cause serious burns. Like alpha particles, beta particles are considered to be an internal hazard if taken into the body by eating, drinking, or breathing contaminated materials. Beta-emitting contamination also can enter the body through unprotected open wounds.

### Beta Particles



### Beta Particles

Experiments show that Beta particles are the same as electrons but come from within the nucleus and not from the electron cloud. The emission of a beta particle results from a neutron changing into a positively charged proton. The daughter nucleus therefore has an atomic (serial) number one higher than the parent nucleus.

### Penetrating power

Beta particles have a range in air of up to about 1000mm  
Beta particles can be stopped with a few mm of aluminum.

### Gamma Rays

Gamma rays are a type of electromagnetic radiation transmitted through space in the form of waves. Gamma rays are pure energy and therefore are the most penetrating type of radiation. They can travel great distances and can penetrate most materials. This creates a problem for humans, because gamma rays can attack all tissues and organs.

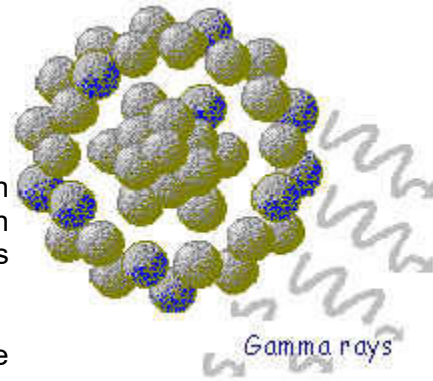
Gamma radiation has very distinctive, short-term symptoms. Acute radiation sickness occurs when an individual is exposed to a large amount of radiation within a short period of time.

Symptoms of acute radiation sickness include skin irritation, nausea, vomiting, high fever, hair loss, and dermal burns.

Gamma emission usually occurs in association with alpha and beta emission.

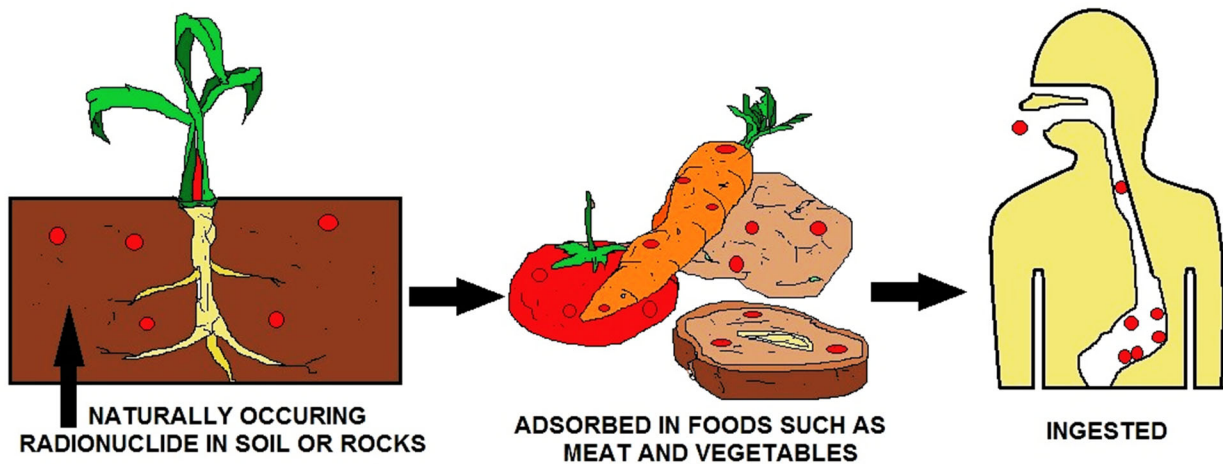
Gamma rays possess no charge or mass; thus emission of gamma rays by a nucleus does not result in a change in chemical properties of the nucleus but merely in the loss of a certain amount of radiant energy.

The emission of gamma rays is a compensation by the atomic nucleus for the unstable state that follows alpha and beta processes in the nucleus.



### Radiological Characteristics

Radiological characteristics are the result of water coming in contact with radioactive materials. This could be associated with atomic energy.



### RADIONUCLIDES

## What is a Dirty Bomb?

Conceptually, a dirty bomb (or **radiological dispersion bomb**) is a very simple device. It's a conventional explosive, such as TNT (**trinitrotoluene**), packaged with radioactive material. It's a lot cruder and cheaper than a nuclear bomb, and it's also a lot less effective. But it does have the combination of explosive destruction and radiation damage.

High explosives inflict damage with rapidly expanding, very hot gas. The basic idea of a dirty bomb is to use the gas expansion as a means of propelling radioactive material over a wide area rather than as a destructive force in its own right. When the explosive goes off, the radioactive material spreads in a sort of dust cloud, carried by the wind that reaches a wider area than the explosion itself.

The long-term destructive force of the bomb would be **ionizing radiation** from the radioactive material. Ionizing radiation, which includes alpha particles, beta particles, gamma rays and X-rays, is radiation that has enough energy to knock an **orbital electron** off of an atom.

Losing an electron throws off the balance between the atom's positively charged protons and negatively charged electrons, giving the atom a net electrical charge (the atom becomes an **ion**). The free electron may collide with other atoms to create more ions. If this happens in a person's body, the ion can cause a lot of serious problems, because an ion's electrical charge may lead to unnatural chemical reactions inside cells. Among other things, the charge can break DNA chains.

A cell with a broken strand of DNA will either die or the DNA will develop a mutation. If a lot of cells die, the body can develop various diseases. If the DNA mutates, a cell may become cancerous, and this cancer may spread. Ionization radiation may also cause cells to malfunction, resulting in a wide variety of symptoms collectively referred to as radiation sickness. Radiation sickness can be deadly, but people can survive it, particularly if they receive a bone marrow transplant.

In a dirty bomb, the ionizing radiation would come from **radioactive isotopes** (also called radioisotopes). Radioactive isotopes are simply atoms that **decay** over time. In other words, the arrangement of protons, neutrons and electrons that make up the atom gradually changes, forming different atoms.

This **radioactive decay** releases a lot of energy in the form of ionizing radiation. We're exposed to small doses of ionizing radiation all the time -- it comes from outer space, it comes from natural radioactive isotopes, it comes from X-ray machines. This radiation can and does cause cancer, but the risk is relatively low because you only encounter it in very small doses.

A dirty bomb would boost the radiation level above normal levels, increasing the risk of cancer and radiation sickness to some degree. Most likely, the bomb wouldn't kill many people right away, but it could possibly kill people years down the road.

## Designs of Nuclear Bombs

*To build an atomic bomb, you need:*

- A source of fissionable or fusionable fuel
- A triggering device
- A way to allow the majority of fuel to fission or fuse before the explosion occurs (otherwise the bomb will fizzle out)



The first nuclear bombs were fission devices, and the later fusion bombs required a fission-bomb trigger. We will discuss the designs of the following devices:

- Fission bombs (in general)
- Gun-triggered fission bomb (**Little Boy**), which was detonated over Hiroshima, Japan, in 1945
- Implosion-triggered fission bomb (**Fat Man**), which was detonated over Nagasaki, Japan, in 1945
- Fusion bombs (in general)
- Teller-Ulam design of a hydrogen fusion bomb, which was test-detonated on Elugelap Island in 1952

### Fission Bombs

A fission bomb uses an element like uranium-235 to create a nuclear explosion. You will need to understand the basic process behind radioactive decay and fission. Uranium-235 has an extra property that makes it useful for both nuclear-power production and nuclear-bomb production -- U-235 is one of the few materials that can undergo induced fission. If a free neutron runs into a U-235 nucleus, the nucleus will absorb the neutron without hesitation, become unstable and split immediately. As soon as the nucleus captures the neutron, it splits into two lighter atoms and throws off two or three new neutrons (the number of ejected neutrons depends on how the U-235 atom happens to split). The two new atoms then emit gamma radiation as they settle into their new states. There are three things about this induced fission process that makes it interesting:

- ✓ The probability of a U-235 atom capturing a neutron as it passes by is fairly high. In a bomb that is working properly, more than one neutron ejected from each fission causes another fission to occur. This condition is known as supercriticality.
- ✓ The process of capturing the neutron and splitting happens very quickly, on the order of picoseconds ( $1 \times 10^{-12}$  seconds).
- ✓ An incredible amount of energy is released, in the form of heat and gamma radiation, when an atom splits. The energy released by a single fission is due to the fact that the fission products and the neutrons, together, weigh less than the original U-235 atom.

## Equation $e = m c^2$

The difference in weight is converted to energy at a rate governed by the equation  $e = m c^2$ . A pound of highly enriched uranium as used in a nuclear bomb is equal to something on the order of a million gallons of gasoline. When you consider that a pound of uranium is smaller than a baseball and a million gallons of gasoline would fill a cube that is 50 feet per side (50 feet is as tall as a five-story building), you can get an idea of the amount of energy available in just a little bit of U-235.

In order for these properties of U-235 to work, a sample of uranium must be enriched. Weapons-grade uranium is composed of at least 90-percent U-235.

In a fission bomb, the fuel must be kept in separate subcritical masses, which will not support fission, to prevent premature detonation. Critical mass is the minimum mass of fissionable material required to sustain a nuclear fission reaction. This separation brings about several problems in the design of a fission bomb that must be solved:

- The two or more subcritical masses must be brought together to form a supercritical mass, which will provide more than enough neutrons to sustain a fission reaction, at the time of detonation.
- Free neutrons must be introduced into the supercritical mass to start the fission.
- As much of the material as possible must be fissioned before the bomb explodes to prevent fizzle.

To bring the subcritical masses together into a supercritical mass, two techniques are used:

- Gun-triggered
- Implosion

Neutrons are introduced by making a neutron generator. This generator is a small pellet of polonium and beryllium, separated by foil within the fissionable fuel core. In this generator:

1. The foil is broken when the subcritical masses come together and polonium spontaneously emits alpha particles.
2. These alpha particles then collide with beryllium-9 to produce beryllium-8 and free neutrons.
3. The neutrons then initiate fission.

Finally, the fission reaction is confined within a dense material called a tamper, which is usually made of uranium-238. The tamper gets heated and expanded by the fission core. This expansion of the tamper exerts pressure back on the fission core and slows the core's expansion. The tamper also reflects neutrons back into the fission core, increasing the efficiency of the fission reaction.

Later in this course, countermeasures for these hazards will be discussed.

## **‘Dirty bomb’: Mystery Russian ‘superweapon’ kills five**

August 13,2019

### **News Article**

An explosion in Russia has been played down by officials — but now they’ve been forced to admit people have died and many more are at risk.

When an experimental missile exploded at a secret Russian base, things were immediately odd. Children from the nearby city of Severodvinsk were sent home from school. Its 185,000 residents were told to stay indoors. Doses of iodine were distributed. All shipping was barred from the area for at least 30 days.

What could cause such a reaction?

How could a relatively small explosion cause such confusion?

Russia’s nuclear energy agency Rosatom eventually stepped forward: It explained that a missile testing an “isotope power source for a liquid-fuelled rocket engine” had misfired.

Little else is officially known but military analysts have been speculating. Was it some sort of “dirty bomb”, with a radioactive warhead?

Could it have been a failed launch from a nuclear-powered submarine?

Suspicion has also fallen on one of President Vladimir Putin’s vaunted new “superweapons”. A new Rosatom statement offers some detail on the event: “The rocket tests were carried out on the offshore platform ... After the tests were completed, the rocket fuel ignited, followed by detonation. After the explosion, several employees were thrown into the sea.”

### **STORMY PETREL**

The idea of using a nuclear-reactor powered ramjet isn’t new

It appears to have been thought up by Nazi rocket scientists during the dying days of World War II. With the fall of Berlin, these experts were divided up between the United States and the Soviet Union.

Both nations embarked upon experimental nuclear-powered missile projects in the 1950s. It was quickly recognised the radiation-spewing technology was far too perilous to be practical.

But a boisterous President Putin revealed what he called the 9M730 Burevestnik (Petrel) early last year as one of six new “superweapons”. NATO calls it the SSC-X-9 “Skyfall”.



## Japan's Nuclear Nightmare

Japan's Fukushima Daiichi nuclear power plant experienced full meltdowns at three reactors in the wake of an earthquake and tsunami in March 2011, the country's Nuclear Emergency Response Headquarters said in May 2011. The nuclear group's new evaluation, released Monday, goes further than previous statements in describing the extent of the damage caused by an earthquake and tsunami on March 11.

Reactors 1, 2 and 3 experienced a full meltdown, it said. The plant's owner, Tokyo Electric Power Co., admitted last month that nuclear fuel rods in reactors 2 and 3 probably melted during the first week of the nuclear crisis. It had already said fuel rods at the heart of reactor No. 1 melted almost completely in the first 16 hours after the disaster struck. The remnants of that core are now sitting in the bottom of the reactor pressure vessel at the heart of the unit and that vessel is now believed to be leaking.

The Japanese government has more than doubled the estimate for the amount of radiation released by the Fukushima nuclear plant crippled by the March 11 earthquake and tsunami. The Nuclear and Industrial Safety Agency (NISA), a government nuclear watchdog, also said at a briefing in Tokyo today that it believed reactor cores at some of the units at the complex melted much more quickly than the plant operator had previously suggested.

Using fresh evidence on the severity of the nuclear disaster, NISA now estimates the total amount of radiation released into the atmosphere in the first week of the crisis was 770,000 terabecquerels. The agency previously estimated that about 370,000 terabecquerels of radioactive material were released during the period.

The latest radiation figure was still only about 10 per cent of the radiation released from the 1986 Chernobyl disaster, the safety agency said. The group of around 300 technicians, soldiers and firemen who work in shifts of 50, have been exposed repeatedly to dangerously high radioactive levels as they attempt to avert a nuclear disaster. The mother of one of the men has admitted that the groups have discussed their situation and have accepted that death is a strong possibility.

"My son and his colleagues have discussed it at length and they have committed themselves to die if necessary in the long-term."

Nicolas Sarkozy, the French president, said the world needed international safety standards on nuclear power by the end of the year as fears surrounding the extent of radiation leaks in Japan continued to grow. Mr. Sarkozy, on the first trip by a foreign leader to Japan since the devastating earthquake and tsunami on March 11, said he would call a meeting of the G20's nuclear power watchdogs to discuss safety regulations. "We must address this anomaly that there are no international safety norms for nuclear matters ... We need international safety standards before the end of the year."

The International Atomic Energy Agency said radioactivity safety limits had been exceeded as far as 25 miles away and urged the government to re-examine its exclusion zone in which residents are banned. Spot tests conducted by the watchdog at Iitate village, 25 miles northwest of Fukushima, showed readings twice as high as levels at which the agency recommends evacuation.

But Naoto Kan, the prime minister, said there were no plans to extend the zone from the current 12 miles, affecting 70,000 residents. There is a further "stay indoors" policy for a further 130,000 people who live up to 19 miles away.

Meanwhile, Japan asked trading partners at the World Trade Organization not to "overact" by unnecessarily restricting the import of food produce. A growing number of international food companies are shunning Japanese products amid fears of contamination, despite government assurances of safety. Nearly three weeks have passed since the disaster, which left 27,000 killed or missing, a quarter of a million homeless and critical damage to the Fukushima Daiichi nuclear plant.

Forecast as the world's costliest natural disaster, the government is estimated to require over 125 billion in emergency budgets to cover costs for disaster relief and the biggest reconstruction project since the end of the second world war.

Criticism of Tokyo Electric Power, operator of the nuclear plant, has continued to mount following stiff government reprimands for earlier miscalculations of radiation figures. Designed to deal with only small-scale accidents, there were reportedly no details on drafting firefighters from Tokyo, the use of military resources or the borrowing of US equipment – all of which have been part of the company's crisis response.

## Incendiary Incidents

An incendiary device is any mechanical, electrical, or chemical device used intentionally to initiate combustion and start a fire. A delay mechanism consists of chemical, electrical, or mechanical elements. These elements may be used singly or in combinations. Incendiary materials are materials that burn with a hot flame for a designated period of time. Their purpose is to set fire to other materials or structures.

Incendiary devices may be simple or elaborate and come in all shapes and sizes. The type of device is limited only by the terrorist's imagination and ingenuity.

An incendiary device can be a simple match applied to a piece of paper, or a matchbook-and-cigarette arrangement, or a complicated self-igniting chemical device. Normally, an incendiary device is a material or mixture of materials designed to produce enough heat and flame to cause combustible material to burn once it reaches its ignition temperature.



Each device consists of three basic components: **an igniter or fuse, a container or body, and an incendiary material or filler.** The container can be glass, metal, plastic, or paper, depending on its desired use.

A device containing chemical materials usually will be in a metal or other nonbreakable container. An incendiary device that uses a liquid accelerator usually will be in a breakable container, e.g., glass.

Generally, crime scene investigators find three types of incendiary devices: **electrical, mechanical, or chemical.** These may be used singularly or in combinations.

Only specially trained personnel should handle incendiary devices discovered prior to ignition. Handling of such devices by inexperienced individuals can result in ignition and possible injury or death. In addition, proper handling is critical for crime scene preservation.

### Characteristics of Fire

Below are some simple facts that explain the particular characteristics of fire.

#### Fire is FAST!

There is little time!

In less than 30 seconds a small flame can get completely out of control and turn into a major fire. It only takes minutes for thick black smoke to fill a house. In minutes, a house can be engulfed in flames. Most fires occur in the home when people are asleep. If you wake up to a fire, you won't have time to grab valuables because fire spreads too quickly and the smoke is too thick. There is only time to escape.

#### Fire is HOT!

Heat is more threatening than flames.

A fire's heat alone can kill. Room temperatures in a fire can be 100 degrees at floor level and rise to 600 degrees at eye level. Inhaling this super-hot air will scorch your lungs. This heat can melt clothes to your skin. In five minutes a room can get so hot that everything in it ignites at once: this is called flashover.

### **Fire is DARK!**

Fire isn't bright, it's pitch black.

Fire starts bright, but quickly produces black smoke and complete darkness. If you wake up to a fire you may be blinded, disoriented and unable to find your way around the home you've lived in for years.

### **Fire is DEADLY!**

Smoke and toxic gases kill more people than flames do.

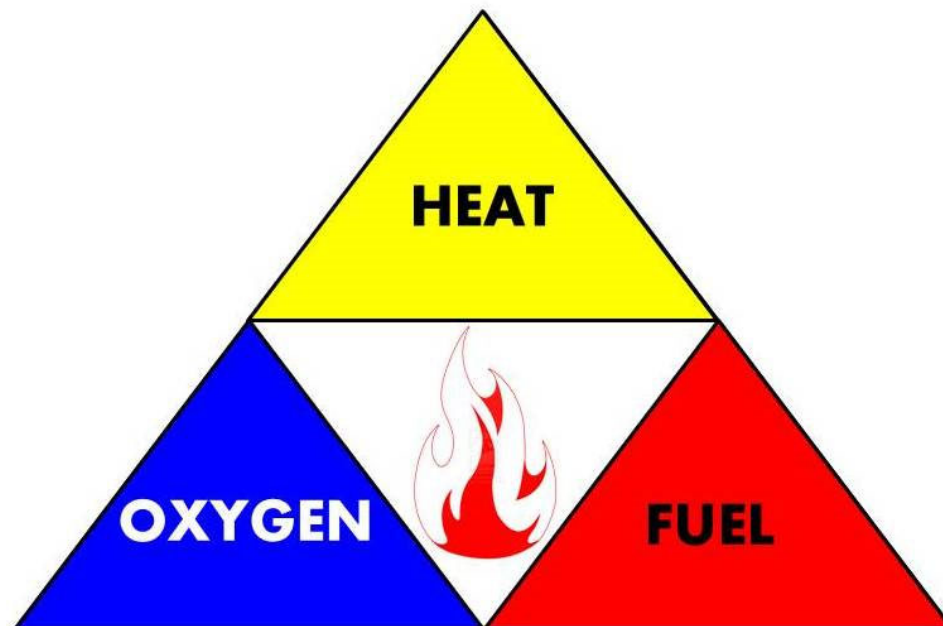
Fire uses up the oxygen you need and produces smoke and poisonous gases that kill. Breathing even small amounts of smoke and toxic gases can make you drowsy, disoriented and short of breath. The odorless, colorless fumes can lull you into a deep sleep before the flames reach your door. You may not wake up in time to escape.

### **The Fire Triangle**

In order to understand how fire extinguishers work, you first need to know a little bit about fire.

Four things must be present at the same time in order to produce fire:

- Enough oxygen to sustain combustion,
- Enough heat to raise the material to its ignition temperature,
- Some sort of fuel or combustible material, and
- The chemical, exothermic reaction that is fire.



**FIRE TRIANGLE**

Oxygen, heat, and fuel are frequently referred to as the "**fire triangle**." Add in the fourth element, the chemical reaction, and you actually have a fire "**tetrahedron**." The important thing to remember is: take any of these four things away, and you will not have a fire or the fire will be extinguished.

Essentially, fire extinguishers put out fire by taking away one or more elements of the fire triangle/tetrahedron.

## **Fire Safety**

Fire safety, at its most basic, is based upon the principle of keeping fuel sources and ignition sources separate.

The percentage of combustible gas in the air is important, too. For example, a manhole filled with fresh air is gradually filled by a leak of combustible gas such as methane or natural gas, mixing with the fresh air. As the ratio of gas to air changes, the sample passes through three ranges: lean, explosive and rich.

In the lean range there isn't enough gas in the air to burn. On the other hand, the rich range has too much gas and not enough air. However, the explosive range has just the right combination of gas and air to form an explosive mixture.

Care must be taken, however, when a mixture is too rich, because dilution with fresh air could bring the mixture into the flammable or explosive range. An analogy is the automobile that won't start on a cold morning (a lean atmosphere because the liquid gasoline has not vaporized sufficiently), but can be flooded with too much gasoline (a rich atmosphere with too much vaporization). Eventually, when the right mixture of gas and air finally exists (explosive), the car starts.

### **The Fire Tetrahedron**

Modern day thinking now accepts there is a fourth element required to sustain combustion. It is Chemical Reaction and must be present with all the other elements at the same time in order to produce fire. The four elements are:-

- Enough oxygen to sustain combustion,
- Enough heat to raise the material to its ignition temperature,
- Some sort of fuel or combustible material, and
- The chemical, exothermic reaction that is fire.

Once you have three sides of the fire triangle you promote a fourth element, a chemical reaction, consequently you have a fire "**tetrahedron**." The important thing to remember is, take any of these four things away, and you will not have a fire or the fire will be extinguished.

To extinguish a fire by the fourth element you need to interfere with the chemical reaction. One way is to mop up the free radicals in the chemical reaction using certain chemicals.

BCF and other Halon extinguishers will achieve this. It also creates an inert gas barrier; however, this type of extinguisher is being phased out. In the future other extinguishing agents may be found using this principle.

Not all fires are the same, and they are classified according to the type of fuel that is burning. If you use the wrong type of fire extinguisher on the wrong class of fire, you can, in fact, make matters worse. It is therefore very important to understand the four different fire classifications.

**Class A** - Wood, paper, cloth, trash, plastics. Solid combustible materials that are not metals.

**Class B** - Flammable liquids: gasoline, oil, grease, acetone. Any non-metal in a liquid state, on fire. This classification also includes flammable gases.

**Class C** - Electrical: energized electrical equipment. As long as it's "**plugged in**," it would be considered a class C fire.

**Class D** - Metals: potassium, sodium, aluminum, magnesium  
Unless you work in a laboratory or in an industry that uses these materials, it is unlikely you'll have to deal with a Class D fire. It takes special extinguishing agents (Metal-X, foam) to fight such a fire.



Practice extinguishing small fires on an annual basis.

## Chemical Incidents

### *Chemical agents fall into five classes:*

- **Nerve agents**, which disrupt nerve impulse transmissions.
- **Blister agents**, also called vesicants, which cause severe burns to eyes, skin, and tissues of the respiratory tract.
- **Blood agents**, which interfere with the ability of blood to transport oxygen.
- **Choking agents**, which severely stress respiratory system tissues.
- **Irritating agents**, which cause respiratory distress and tearing designed to incapacitate. They also can cause intense pain to the skin, especially in moist areas of the body. They are often called Riot Control Agents.

### Nerve Agents

Nerve agents are similar in nature to organophosphate pesticides, but with a higher degree of toxicity. All are toxic at small concentrations (a small drop could be fatal). The agents include sarin (**GB**) used by terrorists against Japanese civilians and by the Iraqis against Iran; Soman (**GD**); tabun (**GA**); and V agent (**VX**). These materials are liquids that typically are sprayed as an aerosol for dissemination. In the case of GA, GB, and GD, the first letter "**G**" refers to the country (**Germany**) that developed the agent, and the second letter indicates the order of development. In the case of VX, the "**V**" stands for "**venom**" while the "**X**" represents one of the chemicals in the specific compound.

The victims' symptoms will be an early outward warning sign of the use of nerve agents. There are various generic symptoms similar to organophosphate poisoning. The victims will salivate, lacrymate, urinate, and defecate without much control.



### *Other symptoms may include*



- **eyes:** pinpointed pupils, dimmed and blurred vision, pain aggravated by sunlight;
- **skin:** excessive sweating and fine **muscle tremors**;
- **muscles:** involuntary twitching and contractions;
- **respiratory system:** runny nose and nasal congestion, chest pressure and congestion, coughing and difficulty in breathing;
- **digestive system:** excessive salivation, abdominal pain, nausea and vomiting, involuntary defecation and urination; and
- **nervous system:** giddiness, anxiety, difficulty in thinking and sleeping (nightmares).



Practice and time your response to incidents, below is a temporary shelter.





## Chlorine Section



### 1-Ton Chlorine Containers

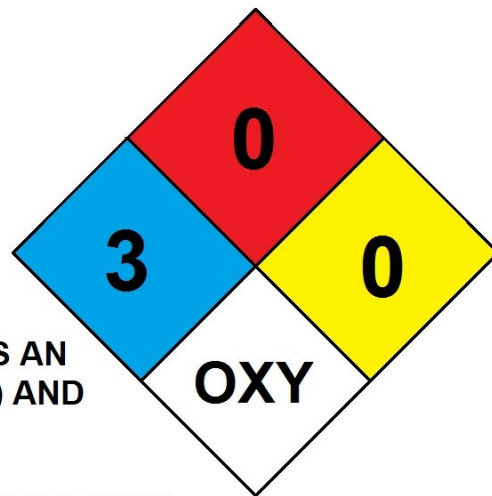
The top line or valve is for extracting the gas, and the bottom line is for extracting the Cl<sub>2</sub> liquid. Never place water on a leaking metal cylinder. The water will help create acid which will make the leak larger.





150-Pound Chlorine Cylinder

- ◆ CHLORINE IS EXTREMELY IRRITATING AND CAN BURN THE EYES AND SKIN
- ◆ IF INHALED, CHLORINE CAUSES RESPIRATORY DISTRESS, AND POSSIBLY BE FATAL
- ◆ LIQUID CHLORINE RELEASE FORMS AN IMMEDIATE CLOUD (FLASH VAPOR) AND COOLS TO  $-29^{\circ}\text{F}$
- ◆ EXPOSURE TO CHLORINE LIQUID CAN CAUSE SEVERE FROSTBITE, AS WELL AS CHEMICAL BURNS.



## THE HEALTH EFFECTS OF CHLORINE EXPOSURE

## Chlorine Exposure Limits and Related Information

This information is necessary to pass your pre-test.

### \* OSHA PEL 1 PPM - IDLH 10 PPM and Fatal Exposure Limit 1,000 PPM

The current Occupational Safety and Health Administration (**OSHA**) permissible exposure limit (**PEL**) for chlorine is 1 ppm (3 milligrams per cubic meter ( $\text{mg}/\text{m}^3$ )) as a ceiling limit. A worker's exposure to chlorine shall at no time exceed this ceiling level. \* **IDLH 10 PPM**

Physical and chemical properties of chlorine: A yellowish green, nonflammable and liquefied gas with an unpleasant and irritating smell. Can be readily compressed into a clear, amber-colored liquid, a noncombustible gas, and a strong oxidizer. Solid chlorine is about 1.5 times heavier than water and gaseous chlorine is about 2.5 times heavier than air. Atomic number of chlorine is 17. Cl is the elemental symbol and  $\text{Cl}_2$  is the chemical formula.

Monochloramine, dichloramine, and trichloramine are also known as Combined Available Chlorine.  $\text{Cl}_2 + \text{NH}_4$ .

$\text{HOCl}$  and  $\text{OCl}^-$ ; The **OCL-** is the hypochlorite ion and both of these species are known as free available chlorine. These are the two main chemical species formed by chlorine in water and they are known collectively as hypochlorous acid and the hypochlorite ion. When chlorine gas is added to water, it rapidly hydrolyzes. The chemical equation that best describes this reaction is  $\text{Cl}_2 + \text{H}_2\text{O} \rightarrow \text{H}^+ + \text{Cl}^- + \text{HOCl}$ . Hypochlorous acid is the most germicidal of the chlorine compounds with the possible exception of chlorine dioxide.

Yoke-type connectors should be used on a chlorine cylinder's valve, assuming that the threads on the valve may be worn.

The connection from a chlorine cylinder to a chlorinator should be replaced by using a new, approved gasket on the connector. Always follow your manufacturer's instructions.

On 1 ton Chlorine gas containers, the chlorine pressure reducing valve should be located downstream of the evaporator when using an evaporator. This is the liquid chlorine supply line and it is going to be made into Chlorine gas.

In water treatment, chlorine is added to the effluent before the contact chamber (before the clear well) for complete mixing. One reason for not adding it directly to the chamber is that the chamber has very little mixing due to low velocities.

Here are several safety precautions when using chlorine gas. In addition to protective clothing and goggles, chlorine gas should be used only in a well-ventilated area so that any leaking gas cannot concentrate. Emergency procedures in the case of a large uncontrolled chlorine leak are as follows: Notify local emergency response team, warn and evacuate people in adjacent areas, and be sure that no one enters the leak area without adequate self-contained breathing equipment.

Here are several symptoms of chlorine exposure. Burning of eyes, nose, and mouth, coughing, sneezing, choking, nausea and vomiting, headaches and dizziness, fatal pulmonary edema, pneumonia, and skin blisters. A little  $\text{Cl}_2$  will corrode the teeth and then progress to throat cancer.



ABC Repair Kit



Rail Car Tanker

## Chlorine Timeline

### 1879

This marked the first time that chlorine was applied as a disinfectant. William Soper of England treated the feces of typhoid patients before disposal into the sewer. He used chlorinated lime, which was a common form of chlorine used initially. (White, 1972)

### 1893

This date was the first time that chlorine was applied as a disinfectant on a plant scale basis. This application was made at Hamburg, Germany. (White, 1972)

### 1903

This marked the first time chlorine gas was used as a disinfectant in drinking water. This took place in Middlekerke, Belgium. Prior to this date, chlorine was applied through the use of hydrated lime, chloride of lime, or bleaching powder. The use of chlorine gas was designed by Maurice Duyk, a chemist for the Belgian Ministry of Public Works. (Pontius, 1990)

### 1908

The first full scale chlorine installation at a drinking water plant in the United States was initiated in this year. This installation took place at the Bubbly Creek Filter Plant in Chicago. This plant served the Chicago Stockyards and was designed by George A. Johnson. The raw water contained a large amount of sewage which was causing sicknesses in the livestock. Johnson implemented chlorine through chloride of lime, and the bacterial content of the water dropped drastically. (Pontius, 1990)

### 1910

C. R. Darnall became the first to use compressed chlorine gas from steel cylinders, which is an approach still commonly used today. His installation was in Youngstown, Ohio. His implementation used a pressure-reducing mechanism, a metering device, and an absorption chamber. It was moderately successful, but his setup was only used once.

### 1912

John Kienle, chief engineer of the Wilmington, Delaware water department, invented another way to apply chlorine to drinking water. He developed a way to push compressed chlorine from cylinders into an absorption tower in which water was flowing opposite the flow of the chlorine. Because the gas flow was opposite the water flow, the chlorine was able to disinfect the water. (Pontius, 1990)

### 1913

An Ornstein chlorinator was installed at Kienle's Wilmington, Delaware water treatment plant. This marked the first time a commercial chlorination system was installed at a municipal water treatment plant. The chlorinator used the same basic premise that Kienle's previous installation did, but the Ornstein chlorinator used both a high and low pressure gauge to more accurately control the amount of chlorine added to the system. (Pontius, 1990)

**1914**

On October 14, 1914, the Department of the Treasury enacted the first set of standards that required the use of disinfection for drinking water. These standards called for a maximum level of bacterial concentration of 2 coliforms per 100 milliliters. Because chlorination was the main disinfectant at the time, these standards dramatically increased the number of treatment plants using chlorine. (White, 1972)

**1919**

Two important discoveries were made during this year. Wolman and Enslow discovered the concept of chlorine demand which states that the amount of chlorine needed to disinfect the water is related to the concentration of the waste and the amount of time the chlorine has to contact the water. The other important discovery of 1919 was by Alexander Houston. He discovered that chlorine can also eliminate taste and odor problems in water. (Pontius, 1990)

**1925**

New drinking water standards were enacted that reduced the maximum permissible limit of coliforms from 2 to 1 coliform per 100 milliliters. This increased the amount and frequency of chlorination again. (White, 1972)

**1939**

The theory of the chlorine breakpoint was discovered in this year. Chlorine breakpoint theory is discussed in the following section. (White, 1972)

**1960**

A new implementation practice was discovered in this year. The compound loop principle of chlorinator control was implemented, which is the most recent major discovery in chlorine application. (White, 1972)

**1972**

A report entitled "Industrial Pollution of the Lower Mississippi River in Louisiana" was published containing the first evidence of disinfection byproducts in drinking water resulting from organic pollution in source water. (Pontius, 1990)

As is evident by the dates in the timeline, most of the innovation in chlorination occurred over 70 years ago. Very few innovations or discoveries have been made recently. Most of the current research is being performed in other areas of disinfection. These areas include ozone, chlorine dioxide, and UV radiation. Chlorine is still the most widely used disinfectant in the United States, but other areas of the world are beginning to use other methods of disinfection with increasing frequency. Since chlorine is still widely used, a thorough understanding of how it disinfects and is implemented is important to those interested in water treatment.

## Chlorine Supplement Pre-Quiz

1. How should the connection from a chlorine cylinder to a chlorinator be replaced?
2. How many turns should a chlorine gas cylinder be initially opened?
3. If the temperature of a full chlorine cylinder is increased by 50°F or 30°C, what is the most likely result?
4. What is meant by the specific gravity of a liquid?
5. Which metals are the only metals that are **TOTALLY** inert to moist chlorine gas?
6. What will be discharged when opening the top valve on a one-ton chlorine cylinder?
7. What are the approved methods for storing a chlorine cylinder?
8. What are normal conditions for a gas chlorination start-up?
9. Name a safety precaution when using chlorine gas?
10. What compounds are formed in water when chlorine gas is introduced?
11. Why should roller bearings not be used to rotate a one-ton chlorine cylinder?
12. What are the physical and chemical properties of chlorine?
13. What are the necessary emergency procedures in the case of a large uncontrolled chlorine leak?
14. Name several symptoms of chlorine exposure.
15. 5 lbs. of a 70% concentration sodium hypochlorite solution is added to a tank containing 650 gallons of water. What is the chlorine dosage?

16. As soon as  $\text{Cl}_2$  gas enters the throat area, a victim will sense a sudden stricture in this area - nature's way of signaling to prevent passage of the gas to the lungs. At this point, the victim must attempt to do two things. Name them.

17. Positive pressure SCBAs and full face piece SARs can be used in oxygen deficient atmospheres containing less than what percentage of oxygen in the atmosphere?

18. Death is possible from asphyxia, shock, reflex spasm in the larynx, or massive pulmonary edema. Populations at special risk from chlorine exposure are individuals with pulmonary disease, breathing problems, bronchitis, or chronic lung conditions.

A. TRUE

B. FALSE

19. Chlorine gas reacts with water producing a strongly oxidizing solution causing damage to the moist tissue lining the respiratory tract when the tissue is exposed to chlorine. The respiratory tract is rapidly irritated by exposure to 10-20 ppm of chlorine gas in air, causing acute discomfort that warns of the presence of the toxicant.

A. TRUE

B. FALSE

20. Even brief exposure to 1,000 ppm of  $\text{Cl}_2$  can be fatal.

A. TRUE

B. FALSE

21. What are the two main chemical species formed by chlorine in water and what name are they known collectively as?

22. When chlorine gas is added to water, it rapidly hydrolyzes according to the reaction:

23. Which chemical reaction equation represents the dissociation of hypochlorous acid?

24. This species of chlorine is the most germicidal of all chlorine compounds with the possible exception of chlorine dioxide.



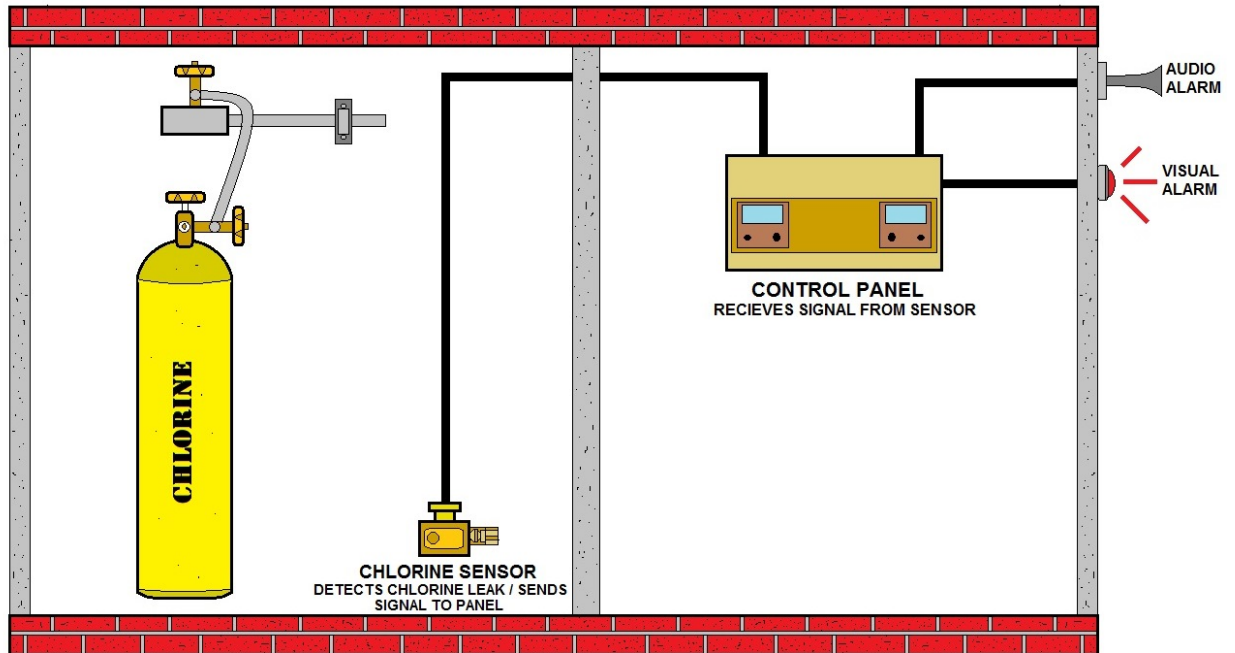
Here are both half ton container and 150 pound chlorine gas cylinders.  
Answers in rear section before the final assignment.



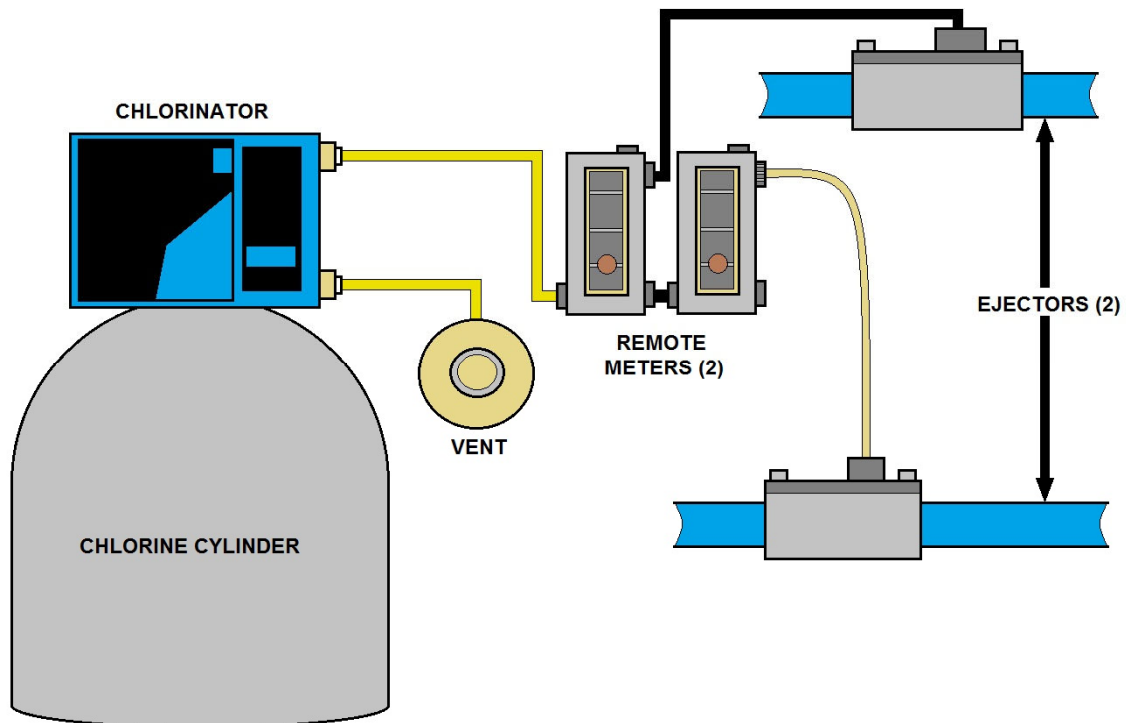


Chlorine evaporators next to a rail tank chlorine cylinder. Bottom photograph, SCBA should always be stored on the outside of the chlorine storage room.





**CHLORINE STORAGE ROOM**



## Chlorine Introduction

**Name:** Chlorine  
**Symbol:** Cl  
**Atomic Number:** 17  
**Atomic Mass:** 35.4527 amu  
**Melting Point:** -100.98 °C (172.17 K, -149.764 °F)  
**Boiling Point:** -34.6 °C (238.55 K, -30.279997 °F)  
**Number of Protons/Electrons:** 17  
**Number of Neutrons:** 18  
**Classification:** Halogen  
**Crystal Structure:** Orthorhombic  
**Density @ 293 K:** 3.214 g/cm<sup>3</sup>  
**Color:** Green  
**Uses:** Water purification, bleaches  
**Obtained From:** Salt  
**Date of Discovery:** 1774  
**Discoverer:** Carl Wilhelm Scheele  
**Name Origin:** From the Greek word *khlôros* (green)



### Chlorine Gas Information Identifiers

1. CAS No.: 7782-50-5
2. RTECS No.: FO2100000
3. DOT UN: 1017 20
4. DOT label: Poison gas

### Safety Data

**NIOSH IDHL:** 25 ppm  
**NIOSH Ceiling:** 0.5ppm/15 minutes  
**PEL/TWA:** 1 ppm  
**TLV/TWA:** 1 ppm  
**TLV/STEL:** 3 ppm  
**TLV/IDLH:** 25 ppm



Chlorinators

### Physical Data

1. Molecular weight: 70.9
2. Boiling point (at 760 mm Hg): -34.6 degrees C (-30.28 degrees F)
3. Specific gravity (liquid): 1.41 at 20 degrees C (68 degrees F) and a pressure of 6.86 atm
4. Vapor density: 2.5
5. Melting point: -101 degrees C (-149.8 degrees F)
6. Vapor pressure at 20 degrees C (68 degrees F): 4,800 mm Hg
7. Solubility: Slightly soluble in water; soluble in alkalis, alcohols, and chlorides.
8. Evaporation rate: Data not available.

### **Chlorine's Appearance and Odor**

Chlorine is a greenish-yellow gas with a characteristic pungent odor. It condenses to an amber liquid at approximately -34 degrees C (-29.2 degrees F) or at high pressures. Odor thresholds ranging from 0.08 to part per million (ppm) parts of air have been reported. Prolonged exposures may result in olfactory fatigue.

### **Reactivity**

1. **Conditions Contributing to Instability:** Cylinders of chlorine may burst when exposed to elevated temperatures. Chlorine in solution forms a corrosive material.
2. **Incompatibilities:** Flammable gases and vapors form explosive mixtures with chlorine. Contact between chlorine and many combustible substances (such as gasoline and petroleum products, hydrocarbons, turpentine, alcohols, acetylene, hydrogen, ammonia, and sulfur), reducing agents, and finely divided metals may cause fires and explosions. Contact between chlorine and arsenic, bismuth, boron, calcium, activated carbon, carbon disulfide, glycerol, hydrazine, iodine, methane, oxomonosilane, potassium, propylene, and silicon should be avoided. Chlorine reacts with hydrogen sulfide and water to form hydrochloric acid, and it reacts with carbon monoxide and sulfur dioxide to form phosgene and sulfuryl chloride. Chlorine is also incompatible with moisture, steam, and water.
3. **Hazardous Decomposition Products:** None reported.
4. **Special Precautions:** Chlorine will attack some forms of plastics, rubber, and coatings.

### **Flammability**

#### ***Chlorine is a non-combustible gas.***

The National Fire Protection Association has assigned a flammability rating of 0 (no fire hazard) to chlorine; however, most combustible materials will burn in chlorine.

1. **Flash point:** Not applicable.
2. **Autoignition temperature:** Not applicable.
3. **Flammable limits in air:** Not applicable.
4. **Extinguishant:** For small fires use water only; do not use dry chemical or carbon dioxide. Contain and let large fires involving chlorine burn. If fire must be fought, use water spray or fog.

### **Fires involving chlorine should be fought upwind from the maximum distance possible.**

Keep unnecessary people away; isolate the hazard area and deny entry. For a massive fire in a cargo area, use unmanned hose holders or monitor nozzles; if this is impossible, withdraw from the area and let the fire burn. Emergency personnel should stay out of low areas and ventilate closed spaces before entering.

Containers of chlorine may explode in the heat of the fire and should be moved from the fire area if it is possible to do so safely. If this is not possible, cool fire exposed containers from the sides with water until well after the fire is out.

Stay away from the ends of containers. Firefighters should wear a full set of protective clothing and self-contained breathing apparatus when fighting fires involving chlorine.

## Chlorine Exposure Limits

### \* OSHA PEL

The current **OSHA** permissible exposure limit (**PEL**) for chlorine is 1 ppm (3 milligrams per cubic meter ( $\text{mg}/\text{m}^3$ )) as a ceiling limit. A worker's exposure to chlorine shall at no time exceed this ceiling level [29 CFR 1910.1000, Table Z-1].

### \* NIOSH REL

The National Institute for Occupational Safety and Health (**NIOSH**) has established a recommended exposure limit (**REL**) for chlorine of 0.5 ppm ( $\text{mg}/\text{m}^3$ ) as a TWA for up to a 10-hour workday and a 40-hour workweek and a short-term exposure limit (**STEL**) of 1 ppm ( $\text{mg}/\text{m}^3$ ) [NIOSH 1992].

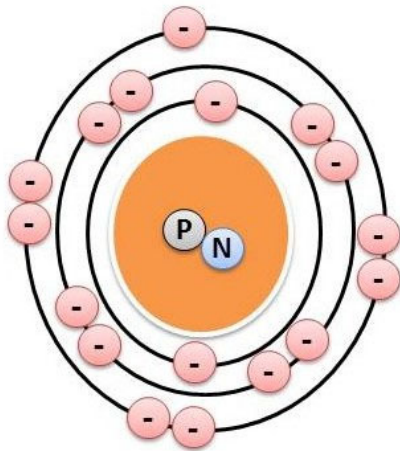
### \* ACGIH TLV





The American Conference of Governmental Industrial Hygienists (**ACGIH**) has assigned chlorine a threshold limit value (**TLV**) of 0.5 ppm ( $\text{mg}/\text{m}^3$ ) as a TWA for a normal 8-hour workday and a 40-hour workweek and a **STEL** of 1 ppm ( $\text{mg}/\text{m}^3$ ) for periods not to exceed 15 minutes. Exposures at the STEL concentration should not be repeated more than four times a day and should be separated by intervals of at least 60 minutes [ACGIH 1994, p. 15].

### \* Rationale for Limits

The NIOSH limits are based on the risk of severe eye, mucous membrane and skin irritation [NIOSH 1992]. The ACGIH limits are based on the risk of eye and mucous membrane irritation [ACGIH 1991, p. 254].

## Chlorine's Atomic Structure



-  ELECTRONS = 17
-  PROTONS = 17
-  NEUTRONS = 18
-  NUCLEUS

### Isotopes

Isotope	Half Life
Cl-35	Stable
Cl-36	301000.0 years

Cl-37	Stable
Cl-38	37.2 minutes



Top photograph, this blue device prevents the liquid from being pulled and freezing the lines. Bottom photograph, the application of an ammonia mist to detect a chlorine gas leak.



## Chlorine Basics

Chlorine is one of 90 natural elements, the basic building blocks of our planet. To be useful, an element must be relatively abundant or have extremely desirable properties. Chlorine has both characteristics. As a result -- over the course of many decades of careful research and development -- scientists have learned to use chlorine and the products of chlorine chemistry to make drinking water safe, destroy life-threatening germs, produce life-saving drugs and medical equipment, shield police and fire fighters in the line of duty, and ensure a plentiful food supply.

In 1774, in his small experimental laboratory, Swedish pharmacist Carl Wilhem Scheele released a few drops of hydrochloric acid onto a piece of manganese dioxide. Within seconds, a greenish-yellow gas arose. Although he had no idea at the time, he had just discovered chlorine.

The fact that the greenish-yellow gas was actually an element was only recognized several decades later by English chemist Sir Humphrey Davy. Until that time, people were convinced that the gas was a compound of oxygen. Davy gave the element its name on the basis of the Greek word *khloros*, for greenish-yellow. In 1810 he suggested the name "*chloric gas*" or "*chlorine*."

One of the most effective and economical germ-killers, chlorine also destroys and deactivates a wide range of dangerous germs in homes, hospitals, swimming pools, hotels, restaurants, and other public places. Chlorine's powerful disinfectant qualities come from its ability to bond with and destroy the outer surfaces of bacteria and viruses. First used as a germicide to prevent the spread of "child bed fever" in the maternity wards of Vienna General Hospital in Austria in 1846, chlorine has been one of society's most potent weapons against a wide array of life-threatening infections, viruses, and bacteria for 150 years.

**When the first men to set foot on the moon returned to earth (Apollo 11 mission: 24.7.69) a hypochlorite solution was chosen as one of the disinfectants for destroying any possible moon germs.**

### What Happens to Chlorine When it Enters the Environment?

- When released to air, chlorine will react with water to form hypochlorous acid and hydrochloric acid, which are removed from the atmosphere by rainfall.
- Chlorine is slightly soluble in water. It reacts with water to form hypochlorous acid and hydrochloric acid. The hypochlorous acid breaks down rapidly. The hydrochloric acid also breaks down; its breakdown products will lower the pH of the water (makes it more acidic).
- Since chlorine is a gas it is rarely found in soil. If released to soil, chlorine will react with moisture forming hypochlorous acid and hydrochloric acid. These compounds can react with other substances found in soil.
- Chlorine does not accumulate in the food chain.

## Disinfectant Qualities

Restaurants and meat and poultry processing plants rely on chlorine bleach and other chlorine-based products to kill harmful levels of bacteria such as *Salmonella* and *E. coli* on food preparation surfaces and during food processing. Chlorine is so important in poultry processing that the US Department of Agriculture requires an almost constant chlorine rinse for much of the cutting equipment. In fact, no proven economical alternative to chlorine disinfection exists for use in meat and poultry processing facilities.

## Properties

Because it is highly reactive, chlorine is usually found in nature bound with other elements like sodium, potassium, and magnesium. When chlorine is isolated as a free element, chlorine is a greenish yellow gas, which is 2.5 times heavier than air. It turns to a liquid state at  $-34^{\circ}\text{C}$  ( $-29^{\circ}\text{F}$ ), and it becomes a yellowish crystalline solid at  $-103^{\circ}\text{C}$  ( $-153^{\circ}\text{F}$ ). Chemists began experimenting with chlorine and chlorine compounds in the 18th century. They learned that chlorine has an extraordinary ability to extend a chemical bridge between various elements and compounds that would not otherwise react with each other. Chlorine has been especially useful in studying and synthesizing organic compounds -- compounds that have at least one atom of the element carbon in their molecular structure. All living organisms, including humans, are composed of organic compounds.

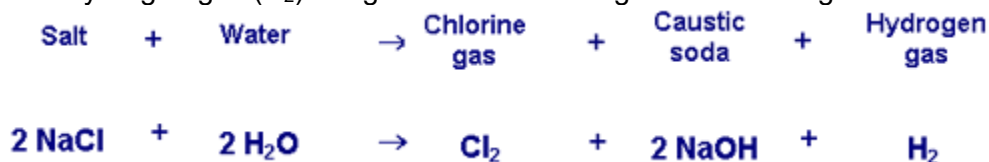
Chlorine is one of the most abundant chemical elements on Earth. It is ubiquitous in soils, minerals, plants and animals. Seawater is a huge reservoir of dissolved chlorine weathered from the continents and transported to the oceans by Earth's rivers.

Chlorine is also one of the most useful chemical elements. Each chemical element has its own set of unique properties and chlorine is known as a very reactive element--so reactive, in fact, that it is usually found combined with other elements in the form of compounds. More than 3,500 naturally occurring chlorinated organic (associated with living organisms) compounds alone have been identified.

Chlorine's chemical properties have been harnessed innovatively for good use. For example, this element plays a huge role in public health. Chlorine-based disinfectants are capable of removing a wide variety of disease-causing germs from drinking water and wastewater as well as from hospital and food production surfaces. Additionally, chlorine plays an important role in the manufacture of thousands of products we depend upon every day, including such diverse items as cars, computers, pharmaceuticals and military flak jackets. As the ninth largest chemical produced in the U.S. by volume, chlorine is truly a "workhorse chemical."

## Released From the Salt of the Earth

Chlorine is produced industrially from the compound sodium chloride, one of the many salts found in geologic deposits formed from the slow evaporation of ancient seawater. When electricity is applied to a brine solution of sodium chloride, chlorine gas ( $\text{Cl}_2$ ), caustic soda ( $\text{NaOH}$ ) and hydrogen gas ( $\text{H}_2$ ) are generated according to the following reaction:





## Co-Products

As the reaction demonstrates, chlorine gas cannot be produced without producing caustic soda, so chlorine and caustic soda are known as "co-products," and their economics are inextricably linked. Caustic soda, also called "alkali," is used to produce a wide range of organic and inorganic chemicals and soaps. In addition, the pulp and paper, alumina and textiles industries use caustic soda in their manufacturing processes. Thus, the "chlor-alkali" industry obtains two very useful chemicals by applying electrical energy to sea salt.



## Definitions

### Chlorine Gas Feed Room

A chlorine gas feed room, for the purposes of this document, is a room that contains the chlorinator(s) and active cylinder(s) used to apply chlorine gas at a water or wastewater facility.

### Chlorine Gas Storage Room

A chlorine gas storage room, for the purposes of this document, is a room other than a chlorine gas feed room, in which full, partial, or empty chlorine gas cylinders or ton containers are stored at a water or wastewater facility.

### Gas Chlorinator

A gas chlorinator is a device used to meter and control the application rate of chlorine gas into a liquid. There is the danger of the gas escaping at a water or wastewater treatment facility. The gas chlorinator should be isolated from a water or wastewater treatment plant.

### Chlorine Cabinet

A chlorine cabinet is a pre-assembled or factory built unit that contains the equipment used to apply chlorine gas at a water or wastewater treatment facility. It is isolated from a water or wastewater treatment plant.

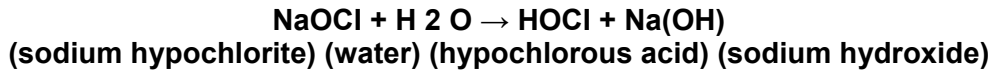
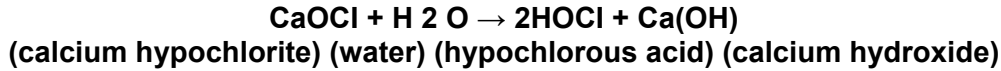
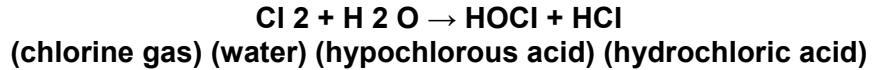


Top photograph, a view of the top of a 150 gas cylinder. Bottom, always work in pairs when working around Chlorine. Here the hoist is being used to move the container.



## Chemistry of Chlorination

Chlorine can be added as sodium hypochlorite, calcium hypochlorite or chlorine gas. When any of these is added to water, chemical reactions occur as these equations show:



All three forms of chlorine produce hypochlorous acid (HOCl) when added to water. Hypochlorous acid is a weak acid but a strong disinfecting agent. The amount of hypochlorous acid depends on the pH and temperature of the water. Under normal water conditions, hypochlorous acid will also chemically react and break down into a hypochlorite ion



The hypochlorite ion is a much weaker disinfecting agent than hypochlorous acid, about 100 times less effective.

Let's now look at how pH and temperature affect the ratio of hypochlorous acid to hypochlorite ions. As the temperature is decreased, the ratio of hypochlorous acid increases. Temperature plays a small part in the acid ratio. Although the ratio of hypochlorous acid is greater at lower temperatures, pathogenic organisms are actually harder to kill. All other things being equal, higher water temperatures and a lower pH are more conducive to chlorine disinfection.

### Types of Residual

If water were pure, the measured amount of chlorine in the water should be the same as the amount added. But water is not 100% pure. There are always other substances (interfering agents) such as iron, manganese, turbidity, etc., which will combine chemically with the chlorine.

This is called the **chlorine demand**. Naturally, once chlorine molecules are combined with these interfering agents, they are not capable of disinfection. It is free chlorine that is much more effective as a disinfecting agent.

So let's look now at how free, total and combined chlorine are related. When a chlorine residual test is taken, either a total or a free chlorine residual can be read.

**Total residual is all chlorine that is available for disinfection.**

**Total chlorine residual = free + combined chlorine residual.**

Free chlorine residual is a much stronger disinfecting agent. Therefore, most water regulating agencies will require that your daily chlorine residual readings be of free chlorine residual.

**Break-point chlorination** is where the chlorine demand has been satisfied, and any additional chlorine will be considered **free chlorine**.

### **Residual Concentration/Contact Time (CT) Requirements**

Disinfection to eliminate fecal and coliform bacteria may not be sufficient to adequately reduce pathogens such as Giardia or viruses to desired levels. Use of the "**CT**" disinfection concept is recommended to demonstrate satisfactory treatment, since monitoring for very low levels of pathogens in treated water is analytically very difficult.

The CT concept, as developed by the United States Environmental Protection Agency (Federal Register, 40 CFR, Parts 141 and 142, June 29, 1989), uses the combination of disinfectant residual concentration (mg/L) and the effective disinfection contact time (in minutes) to measure effective pathogen reduction. The residual is measured at the end of the process, and the contact time used is the T10 of the process unit (time for 10% of the water to pass).

$$\text{CT} = \text{Concentration (mg/L)} \times \text{Time (minutes)}$$

The effective reduction in pathogens can be calculated by reference to standard tables of required CTs.

### **Required Giardia/Virus Reduction**

All surface water treatment systems shall ensure a minimum reduction in pathogen levels: 3-log reduction in Giardia; and 4-log reduction in viruses.

These requirements are based on unpolluted raw water sources with Giardia levels of = 1 cyst/100 L, and a finished water goal of 1 cyst/100,000 L (equivalent to 1 in 10,000 risk of infection per person per year). Higher raw water contamination levels may require greater removals as shown on Table 4.1.

**TABLE 4.1**

**Level of Giardia Reduction**  
**Raw Water Giardia Levels\***  
**Recommended Giardia Log**  
**Reduction**

< 1 cyst/100 L 3-log

1 cyst/100 L - 10 cysts/100 L 3-log - 4-log

10 cysts/100 L - 100 cysts/100 L 4-log - 5-log

> 100 cysts/100 L > 5-log

\*Use geometric means of data to determine raw water Giardia levels for compliance.

### **Required CT Value**

Required CT values are dependent on pH, residual concentration, temperature, and the disinfectant used. The tables attached to Appendices A and B shall be used to determine the required CT.

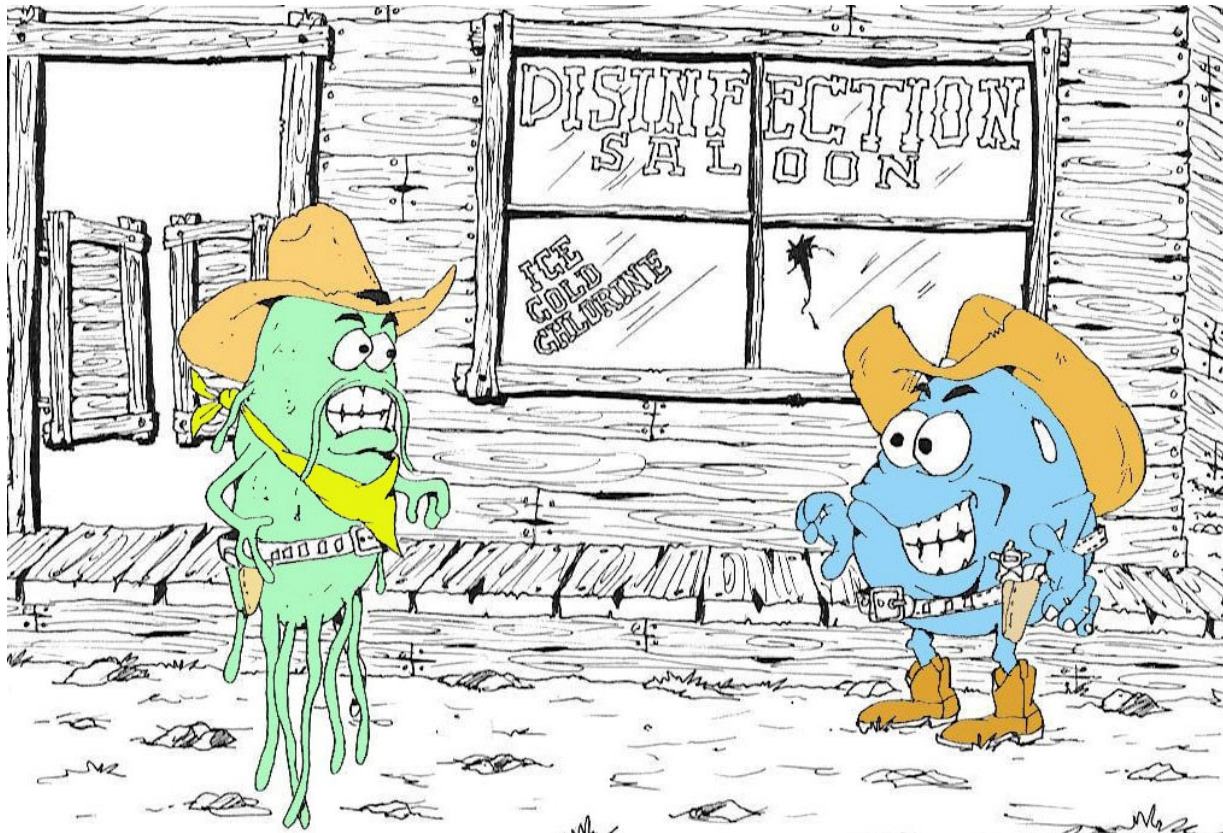
### Calculation and Reporting of CT Data

Disinfection CT values shall be calculated daily, using either the maximum hourly flow and the disinfectant residual at the same time, or by using the lowest CT value if it is calculated more frequently. Actual CT values are then compared to required CT values.

Results shall be reported as a reduction Ratio, along with the appropriate pH, temperature, and disinfectant residual. The reduction Ratio must be greater than 1.0 to be acceptable.

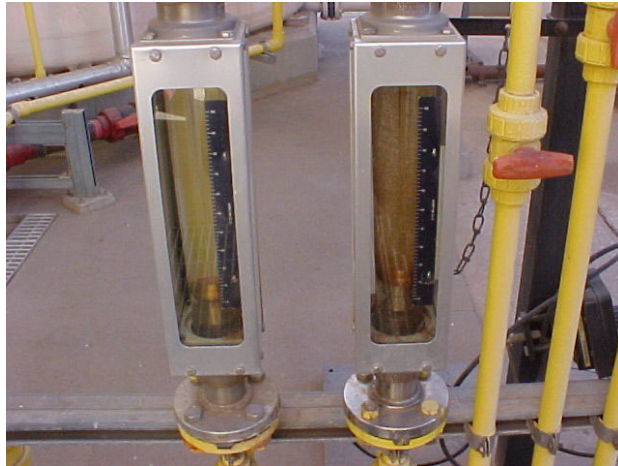
Users may also calculate and record actual log reductions.

**Reduction Ratio = CT actual divide by CT required.**



## Chlorinator Components

- A. Ejector
- B. Check Valve Assembly
- C. Rate Valve
- D. Diaphragm Assembly
- E. Interconnection Manifold
- F. Rotometer Tube and Float
- G. Pressure Gauge
- H. Gas Supply



Chlorine measurement devices or Rotometers.



**Chlorine Safety Information:** There is a fusible plug on every chlorine tank. This metal plug will melt at 158 to 165° F. This is to prevent a build-up of excessive pressure and the possibility of cylinder rupture due to fire or high temperatures.

		MICROBIOLOGICAL SAFETY	CHEMICAL SAFETY	CUSTOMER AESTHETICS	EASE OF MONITORING	ABILITY TO TREAT DIFFICULT WATER	COST OF OPERATING	CAPITAL COSTS	STATE OF COMMERCIAL DEVELOPMENT	SCALE-UP	WASTE PRODUCTION AND ENERGY USE	RELIABILITY
GROUNDWATER	CHLORINE	-	-	-	+	+	+	+	+	+	+	-
	UF ONLY	-	+	+	-	+	●	●	-	-	●	-
	UV ONLY	+	+	+	●	+	+	●	+	+	●	●
	Alternate + Residual (1)	+	●	●	+	+	●	-	+	+	+	+
SURFACE WATER	CHLORINE ONLY	-	-	-	+	-	+	+	+	+	+	+
	Conventional pre-treat + CHLORINE	+	-	-	+	-	●	●	+	+	●	-
	UF ONLY	-	-	●	-	-	●	●	-	-	●	-
	Conventional pre-treat +UF	●	+	+	-	+	-	-	-	-	-	-
	Coventional pre-treat + OZONE + UV	-	●	-	-	+	-	-	-	-	-	-
	MF + UV	●	+	-	●	-	+	●	-	-	●	+
	Conventional pre-treat + UV	●	+	+	●	-	+	●	+	+	●	●
	Conventional pre-treat + OZONE + UV	+	●	+	+	+	-	-	+	+	●	+
	Alternative + Residual (2)	+	●	●	+	+	-	-	+	+	+	+

Conventional pre-treat = Coagulation / Sedimentation  
 UF - Ultrafiltration MF - Microfiltration  
 + = Better than average  
 - = Worse than average  
 ● = Average

(1) UF + Chlorine residual or Conv + UV + Chlorine residual  
 (2) Conv pre-treat + UF + Chlorine residual or MF + UV + Chlorine residual or Conv pre-treat + UV + Residual

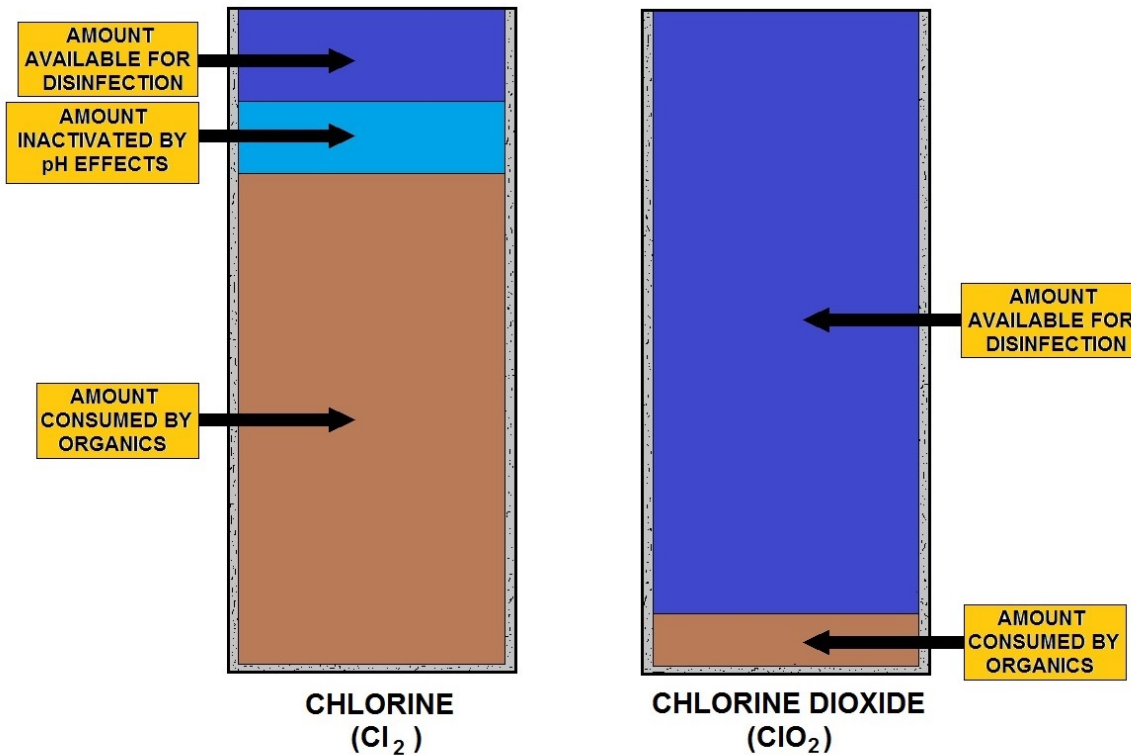
### ASSESSMENT TO DETERMINE EFFECTIVE DISINFECTION METHODS

	CHLORINE AS A DISINFECTANT	ULTRAVIOLET GERMICIDAL IRRADIATION (UV) AS A DISINFECTANT
DISINFECTION BYPRODUCTS (DBPs)	X	No
CHEMICAL RESIDUE	X	No
NON-CORROSIVE	X	No
COMMUNITY SAFETY RISKS	X	No
EFFECTIVE AGAINST CRYPTOSPORIDIUM AND GIARDIA	X	Yes
WELL-SUITED FOR CHANGING REGULATIONS	X	Yes

### CHLORINE vs. UV FOR DISINFECTION

DISINFECTION OF WATER	
DISINFECTANT	WHAT DISINFECTANT IS USED FOR
OZONE (O <sub>3</sub> )	USED IN DESTROYING BACTERIA, ODORS AND VIRUSES (Scrambles DNA in Viruses to prevent reproduction)
CHLORINE (Cl <sub>2</sub> )	USED TO KILL DISEASE-CAUSING PATHOGENS SUCH AS BACTERIA, VIRUSES AND PROTOZOANS
POTASSIUM PERMANGANATE (KMnO <sub>4</sub> )	USED TO REMOVE IRON AND HYDROGEN SULFIDE, AND ALSO USED IN TREATMENT PLANTS TO CONTROL ZEBRA MUSSEL FORMATIONS
COPPER SULFATE (CuSO <sub>4</sub> )	USED CONTROL PLANT AND ALGAE GROWTH
CALCIUM HYPOCHLORITE (Ca(ClO) <sub>2</sub> )	DESTROYS DISEASE-CAUSING ORGANISMS INCLUDING BACTERIA, YEAST, FUNGUS, SPORES AND VIRUSES
CALCIUM HYDROXIDE (Lime) (CaO)	USED FOR pH CONTROL IN WATER TREATMENT TO PREVENT CORROSION OF PIPING

### TYPES OF DISINFECTION FOR WATER TREATMENT



THE DIFFERENCE IN USING CHLORINE AND CHLORINE DIOXIDE AS A DISINFECTANT



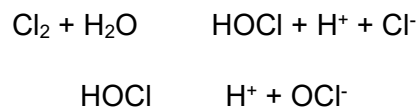
## Chlorine Review

**Chlorine Demand:** The minimum amount of chlorine needed to react in a water purification system; used as a monitoring measurement by system operators.

**Chlorine Residual:** The concentration of chlorine in the water after the chlorine demand has been satisfied. The concentration is normally expressed in terms of total chlorine residual, which includes both the free and combined or chemically bound chlorine residuals.

**Combined Chlorine Residual:** The amount of chlorine used up in a water purification system; used as a monitoring measurement by system operators. Combined chlorine is defined as the residual chlorine existing in water in chemical combination with ammonia or organic amines which can be found in natural or polluted waters. Ammonia is sometimes deliberately added to chlorinated public water supplies to provide inorganic chloramines.

**Free Chlorine:** Free chlorine is defined as the concentration of residual chlorine in water present as dissolved gas ( $\text{Cl}_2$ ), hypochlorous acid ( $\text{HOCl}$ ), and/or hypochlorite ion ( $\text{OCl}^-$ ). The three forms of free chlorine exist together in equilibrium.



Their relative proportions are determined by the pH value and temperature. Regardless of whether pre-chlorination is practiced or not, a free chlorine residual of at least 10 mg/L should be maintained in the clear well or distribution reservoir immediately downstream from the point of post-chlorination and .2 mg/L in the distribution system to guard against backflow.

**Total Chlorine Residual:** The total of free residual and combined residual chlorine in a water purification system; used as a monitoring measurement by system operators. Total chlorine is the sum of free and combined chlorine. When chlorinating most potable water supplies, total chlorine is essentially equal to free chlorine since the concentration of ammonia or organic nitrogen compounds (needed to form combined chlorine) will be very low. When chloramines are present in the municipal water supply, then total chlorine will be higher than free chlorine.

**Pre-chlorination:** The addition of chlorine at the plant headworks or prior to other water treatment or groundwater production processes and mainly used for disinfection and control of tastes, odors, and aquatic growths.

**Post-chlorination:** The addition of chlorine after a process or adding chlorine downstream to meet a demand in the system.

**Breakpoint chlorination:** Breakpoint chlorination means adding  $\text{Cl}_2$  to the water until the  $\text{Cl}_2$  demand is satisfied. Until all the microorganisms are killed.

**What is the process of chlorination called as a treatment process and how does it differ from sterilization?**

**Chlorination:** A method of water disinfection where gaseous, liquid, or dissolved chlorine is added to a water supply system. Water which has been treated with chlorine is effective in preventing the spread of disease. The chlorination of public drinking supplies was originally met with resistance, as people were concerned about the health effects of the practice. The use of chlorine has greatly reduced the prevalence of waterborne disease as it is effective against almost all bacteria and viruses, as well as amoeba. Sterilization kills everything.

**What are the physical properties of chlorine, what hazards does it present, what advantages does it have over most other disinfectants, and how does it react with bacteria?**

Physical and chemical properties of chlorine: A yellowish green, nonflammable and liquefied gas with an unpleasant and irritating smell. Can be readily compressed into a clear, amber-colored liquid, a noncombustible gas, and a strong oxidizer. Solid chlorine is about 1.5 times heavier than water and gaseous chlorine is about 2.5 times heavier than air. Atomic number of chlorine is 17. Cl is the elemental symbol and Cl<sub>2</sub> is the chemical formula.

Chlorine reacts with bacteria as if it was very corrosive and burns the skin or covering killing the bacteria.

**What is the purpose of a fusible plug, at what temperature does it melt, and where is it located on 150-lb. and 1-ton cylinders?**

Fusible plug is a safety device that melts. If the temperature of a full Cl<sub>2</sub> cylinder is increased by 50° F or 30° C, a rupture may occur. It will melt at 158 to 165 degrees F. It is found on the side of a 1 ton container and on top of the 150 pound cylinder and is located in the valve below the valve seat.

**What is the correct procedure to follow in changing a chlorine cylinder and what item should always be replaced with a new one in doing so?**

Hook up the chlorinator to the container or cylinder with the chlorine valve turned off. Use the gas side not the liquid if using a 1 ton container. Remove the cylinder valve outlet cap and check the valve face or damage. Clean with wire brush if necessary. If the valve face is smooth, clean proceed with hooking up the cylinder. Check the inlet face of the chlorinator and clean if necessary. Place a new lead gasket on the chlorinator inlet, place the chlorinator on the cylinder valve, install the yoke clamp and slowly tighten the yoke clamp until the two faces are against the lead gasket. Tighten the yoke, compressing the gasket one half to three quarters turn, do not over tighten. Replace the lead gasket with every change out.

**How, when and where should chlorine residuals be taken and what information do they provide?** The sample must be taken within the distribution system of your PWS. If you take it before the distribution system you will not get an accurate reading. The sample must be taken at the same tap that you take the Bac-t sample.

Approved method for storing a 150 - 200-pound chlorine cylinder: Secure each cylinder in an upright position, attach the protective bonnet over the valve and firmly secure each cylinder. Never store near heat. Always store the empty in an upright, secure position with proper signage.

## Nerve Agent Section

Nerve agents resemble water or light oil in pure form and possess no odor. The most efficient distribution is as an aerosol. Small explosions and equipment to generate mists (spray devices) may be present. Nerve agents kill insect life, birds, and other animals as well as humans. Many dead animals at the scene of an incident may be another outward warning sign or detection clue.



Mustard gas and phosgene were used in World War 1

## Blister Agents

Blister agents are also referred to as mustard agents due to their characteristic smell. They are similar in nature to other corrosive materials first responders encounter. They readily penetrate layers of clothing and are quickly absorbed into the skin. Mustard (**H, HD**), and lewisite (**L**) are common blister agents. All are very toxic, although much less so than nerve agents. A few drops on the skin can cause severe injury, and three grams absorbed through the skin can be fatal. Clinical symptoms may not appear for hours or days. The symptoms of blister agents include:

- **eyes:** reddening, congestion, tearing, burning, and a "**gritty**" feeling; in severe cases, swelling of the eyelids, severe pain, and spasm of the eyelids;
- **skin:** within 1 to 12 hours, initial mild itching followed by redness, tenderness, and burning pain, followed by burns and fluid-filled blisters. The effects are enhanced in the warm, moist areas of the groin and armpits;
- **respiratory system:** within 2 to 12 hours, burning sensation in the nose and throat, hoarseness, profusely running nose, severe cough, and shortness of breath; and
- **digestive system:** within two to three hours, abdominal pain, nausea, blood-stained vomiting, and bloody diarrhea.



**Blister agents** are heavy, oily liquids, dispersed by aerosol or vaporization, so small explosions or spray equipment may be present. In a pure state they are nearly colorless and odorless, but slight impurities give them a dark color and an odor suggesting mustard, garlic, or onions.

Outward signs of blister agents include complaints of eye and respiratory irritation along with reports of a garlic-like odor. Similar symptoms will occur among many individuals exposed.

## Blood Agents

Blood agents interfere with the ability of the blood to transport oxygen, and result in asphyxiation. Common blood agents include hydrogen cyanide (**AC**) and cyanogen chloride (**CK**). Cyanide and cyanide compounds are common industrial chemicals with which emergency responders sometimes deal. CK can cause tearing of the eyes and irritate the lungs. All blood agents are toxic at high concentrations and lead to rapid death. Affected persons require removal to fresh air and respiratory therapy. Clinical symptoms of patients affected by blood agents include:



- **respiratory distress;**
- **vomiting and diarrhea; and**
- **vertigo and headaches.**

Under pressure, blood agents are liquids. In pure form, they are gases. Precursor chemicals are typically cyanide salts and acids. All have the aroma of bitter almonds or peach blossoms. They are common industrial chemicals and are readily available.

## Choking Agents

Choking agents stress the respiratory tract. Severe distress causes edema (fluid in the lungs), which can result in asphyxiation resembling drowning. Chlorine and phosgene, common industrial chemicals, are choking agents. Clinical symptoms include severe eye irritation and respiratory distress (coughing and choking). Most people recognize the odor of chlorine. Phosgene has the odor of newly cut hay. As both are gases, they must be stored and transported in bottles or cylinders. Most of these chemical agents are easy to produce.



A small chlorine cylinder is super deadly to employees and the public. These cylinders are way too easy to steal, too easy to purchase. Anyone with a sixth grade education can set-up these up as a terror weapons.

## Irritating Agents

Irritating agents, also known as riot control agents or tear gas, are designed to incapacitate. Generally, they are nonlethal; however, they can result in asphyxiation under certain circumstances. Common irritating agents include chloropicrin, MACE (**CN**), tear gas (**CS**), capsicum/pepper spray, and dibenzoxazepine (**CR**). Clinical symptoms include:

- eyes and throat: burning or irritation; tearing of the eyes;
- respiratory system: respiratory distress, coughing, choking, and difficulty breathing; and
- digestive system: high concentrations may lead to nausea and vomiting.

These agents can cause pain, sometimes severe, on the skin, especially in moist areas. Most exposed persons report the odor of pepper or of tear gas. Outward warning signs include the odor of these agents and the presence of dispensing devices. Many are available over the counter.

The primary routes of exposure for chemical agents are inhalation, ingestion, and skin absorption/contact. Injection is a potential source of entry, but is less likely. With the exception of blister agents, inhalation is the primary route of exposure for chemical agents. However, skin absorption/contact with irritant nerve agents and blister agents is also a highly possible route of exposure.



Drill and prepare for these chemical agents. Trust me, it is coming in either an accident or intentional chemical release event! Don't wait on the Fire Department to deal with your chemical problems; you need to be ready to deal with a Chlorine or chemical release.

## Explosive Incidents



The last category of potential terrorist incidents we need to examine briefly is the explosive incident.

**Explosive incidents.** The U.S. Department of Transportation (DOT) defines an explosive as a substance fitting into one of these two categories:

- any substance or article, including a device, designed to function by explosion (e.g., an extremely rapid release of gas and heat); or
- any substance or article, including a device, which, by chemical reaction within itself, can function in a similar manner even if not designed to function by explosion, unless the substance or article is otherwise classified.

It is estimated that 70 percent of all terrorist attacks worldwide involve explosives. It is apparent that bombs are the current weapon of choice amongst terrorist groups. The FBI reports that of 3,163 bombing incidents in the U.S. in 1994, 77 percent were due to explosives. In these situations 78 percent of all bombs detonated or ignited. Another 22 percent failed to function as designed; only 4 percent were preceded by a warning or threat.

### **The FBI also noted three other interesting facts:**

- When public safety agencies know of the presence of a device, they have only a 20 percent chance of finding it.
- Hundreds more "hoax" bomb incidents are reported each year.
- Residential properties are the most common targets for bombers.

The conclusion is that improvised explosive and incendiary devices are designed and assembled to explode and cause fires. Explosions rapidly release gas and heat, affecting both structures and people. Bombings are the types of terrorist attacks most likely to be encountered.

Bombs nearly always work as designed. An important point to remember is that explosions can cause fires, and fires can cause explosions. First responders should always be aware of the potential for secondary devices.

The five types of incidents previously discussed are similar, in some respects, to routine emergencies. Responders still can protect themselves using sound judgment and the basic equipment they are trained to use.

## Chemical Dispersal Devices

Terrorists have designed chemical dispersal devices fabricated from commonly available materials which are designed to asphyxiate victims. The device, in its simplest form, produces hydrogen cyanide (**HCN**) gas; however, it can be modified to produce both HCN and cyanogen chloride (**CICN**) gas. Little or no training is required to assemble and deploy such a device, due to its simplicity.

This improvised chemical device can simply consist of a pierced container or canister, such as a large milk container or paint can. The holes would presumably allow the toxic gas to escape. The acidic materials are likely to be in glass bottles or vials. The bottom of the container, around the bottles, would be partially filled with a crystalline solid. If cyanide salts are used, the color will be white or yellow. A slightly modified device would also use potassium permanganate ( $\text{KMnO}_4$ ) crystals, which are purple.

The device can be used with or without a detonator. A detonator, or other means, is used to break the inner container(s), releasing the acid and allowing the chemicals to mix, creating a gas.

The device could be placed near air intakes or ventilation systems, in crowded open spaces, or in enclosed spaces. It is most effective in enclosed spaces. In most cases, use of a ventilation system for dispersal would sufficiently dilute the gas from one or several smaller versions of these devices; therefore, mass fatalities would be unlikely to occur. HCN and CICN have a relatively low toxicity; therefore, a large concentration of either gas is needed to produce lethality.

However, lower concentrations are potentially fatal to the vulnerable such as children, the elderly, and people already in respiratory distress. The gas readily dissipates and would need to be generated quickly in order to deliver lethal levels of gas. In most cases, HCN and CICN would not be effective in large open areas with good ventilation.

Security personnel should be aware of the variety of symptoms related to the chemical substances described below. In any case where chemicals or a suspected chemical device is encountered in an investigation with a potential terrorism nexus, security personnel should contact the appropriate law enforcement/safety personnel in their jurisdiction.

The chemical device consists of a container or canister, such as a large milk container or paint can and :

- (1). Some of the materials are likely to be in glass bottles or vials.
- (2). The bottom of the container, around the bottles, would be partially filled with white/yellow crystals.
- (3). A more sophisticated device would also use purple crystals.
- (4). The device could be used with or without a detonator.
- (5). The device might be positioned near air intakes or a ventilation system.

### Cyanogen chloride

The cyanogen chloride will be irritating to lungs and eyes before it reaches a lethal concentration, and it emits a dense smoke. Both effects could slow evacuation and cause panic-related injuries. It is likely that all reactants will not be totally consumed at first, and the device may reactivate when disturbed, which could severely impair emergency responders.

## Description

Various transportation systems may be vulnerable to attack using these improvised chemical devices, particularly where security screening procedures are minimal. One or more assembled devices could easily be brought aboard a train or subway. These gases would also be effective when released in confined spaces of buildings or other indoor facilities. It is difficult to judge the number of casualties that would result from the use of multiple devices; however, such an attack will likely generate fear and panic among the local population.

An airplane is a more difficult location for terrorists to penetrate with a chemical device. However, most if not all of the components could be easily disguised as ordinary household items and mixed in-flight to produce toxic gases. For example, an acid solution, such as hydrochloric acid (**HCl**), might be stored in plastic or glass containers, such as thermoses, soda bottles, liquor bottles, and juice or baby bottles. It could not be stored in most metal containers due to its corrosive nature. HCl used in such a device would be colorless or slightly yellow—appearing like water or a commercially available beverage.

However, a noxious odor is easily detectable once the container is opened. Solid powder components could be smuggled aboard using the same concealment techniques as those used for drugs or explosives.

### **These concealment techniques may include, but are not limited to:**

- Electronic equipment.
- Clothing.
- Luggage and briefcases.
- Books.
- Children's toys.
- Medication, toiletries, and containers of consumable products.
- Casts or bandages on broken or injured limbs, prosthetic devices, wheelchairs, and walkers.
- Religious objects.

These materials could be brought onto an airplane in carry-on baggage. Multiple individuals could bring separate components aboard and assemble the device during flight in a lavatory. Cyanide is one of the main chemical poisons in which terrorist groups have shown an interest, both because of its ease of dissemination and its availability.

Cyanide salts, such as sodium cyanide (NaCN) or potassium cyanide (KCN), may be combined with a strong acid, HCl, to form a binary (two-part) chemical device. A simple mixing of the two components generates HCN gas, which can cause dozens of casualties if used at high concentrations in an enclosed area.

- NaCN and KCN are white to pale yellow salts.
- HCN is a colorless liquid that boils near room temperature. A slightly modified device may also incorporate KMnO<sub>4</sub> along with the cyanide salt and HCl. The KMnO<sub>4</sub> converts the chloride ion (Cl<sup>-</sup>) to chlorine (Cl<sub>2</sub>), which, in turn, converts some of the cyanide gas to ClCN, a blood agent similar to HCN but also a highly effective irritant to the eyes and lungs.
- KMnO<sub>4</sub> is a deep purple solid.
- ClCN is a colorless to pale yellow liquid, which boils below room temperature. Note that other strong acids, such as sulfuric acid H<sub>2</sub>SO<sub>4</sub>, can be used to react with cyanide salts to produce HCN gas; however, an acid with a (Cl<sup>-</sup>), such as HCl, is needed to produce ClCN gas.



### **Indicators of an Attack**

According to the Center for Disease Control (**CDC**), HCN is sometimes described as having a “bitter almond” smell, but it does not always give off an odor, and not everyone can detect this odor. Responders should not rely on odor detection alone to determine whether a dangerous concentration of HCN is present. CICN has an acrid, choking odor and causes burning pain in the victim’s eyes below lethal concentrations. These warning properties may make it possible to evacuate or ventilate the attack site before the agent reaches a lethal concentration. HCN produced by the reaction of cyanide salts and acid generates a white cloud around the device generating the gas.

Both HCN and CICN need to be at high concentration to be effective, so evacuating or ventilating the target area will significantly reduce the agent’s lethal potential. Cyanide compounds disrupt cells’ ability to utilize oxygen, leading to suffocation. Exposure to high concentrations of cyanide may produce nausea, vomiting, palpitations, confusion, hyperventilation, anxiety, and vertigo, which may progress to agitation, stupor, coma, and death. These symptoms will appear first in the most susceptible: the elderly, children, and the infirm. Medical countermeasures for cyanide poisoning include: high doses of oxygen, inhalation of amyl nitrite while a solution of sodium nitrate/sodium thiosulfate is prepared for intravenous use, and hyperbaric oxygenation if the victim does not respond to initial treatments. Prompt treatment is of the utmost importance.

### **SUGGESTED PROTECTIVE MEASURES**

Terrorists continue to select soft targets for attack--particularly those that will yield a high casualty count. There are two categories of soft targets that a terrorist may choose for attack, those being soft targets with controlled access and soft targets with uncontrolled access. Examples of soft targets with controlled access include sports stadiums, arenas, and office buildings (with security guards). Examples of soft targets with uncontrolled access include hospitals, malls, restaurants, and schools without elaborate security procedures.

All available antiterrorism measures, to include physical security perimeters, personnel awareness, and reporting mechanisms, should be rigorously reexamined.

### **General Protective Measures for Controlled and Uncontrolled Access**

The following are the recommended general protective measures that apply to both categories and specific protective measures recommended for soft targets with controlled access:

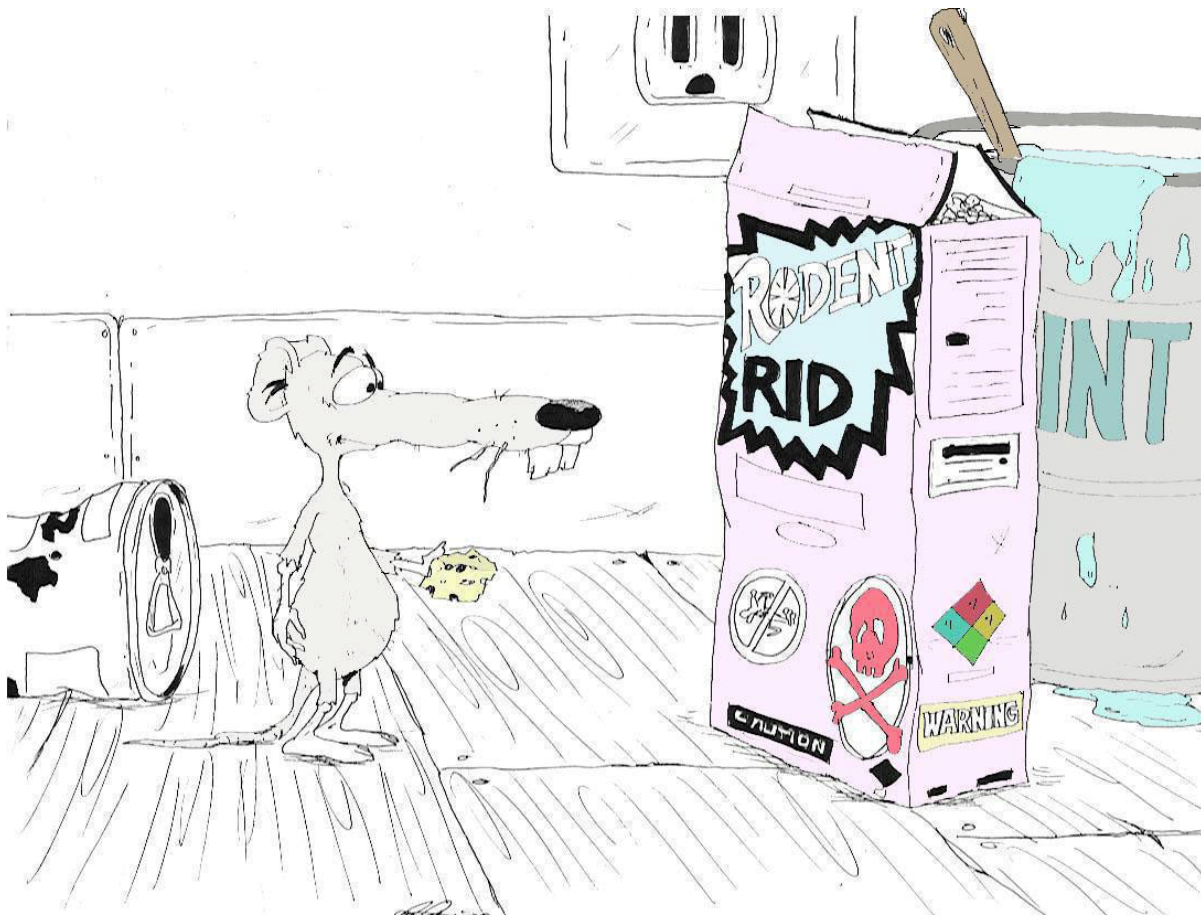
- Encourage personnel to take notice of and report unattended packages, devices, briefcases, or other unusual materials immediately; inform them not to handle or attempt to move any such object, especially near air intakes.
- Encourage personnel to know emergency exits and stairwells and the locations of rally points to ensure the safe egress of people present.
- Increase the number of visible security personnel wherever possible.
- Institute/increase vehicle, foot, and roving security patrols varying in size, timing, and routes.
- Enclosed spaces, such as restrooms, should be regularly inspected.
- Deliveries to concessions in stadiums, arenas, and conference centers should be inspected prior to scheduled events.
- Implement random security guard shift changes.
- Limit the number of access points and strictly enforce access control procedures.
- Deploy visible security cameras and motion sensors.
- Arrange for law enforcement vehicles to be parked randomly near entrances and exits.

- Review current contingency plans and, if not already in place, develop and implement procedures for receiving and acting on threat information, alert notification procedures, terrorist incident response procedures, evacuation procedures, bomb threat procedures, hostage and barricade procedures, chemical, biological, radiological and nuclear (CBRN) procedures, consequence and crisis management procedures, accountability procedures, and media procedures.
- Conduct internal training exercises and invite local emergency responders (fire, rescue, medical, and bomb squads) to participate in joint exercises.

#### **Additional Specific Protective Measures for Soft Targets with Controlled Access**

- Inspect vendor items being brought into soft target areas prior to event.
- Inspect all items being carried in by patrons accessing soft target areas.
- Ensure proper badging and identification of all staff working the event.
- Conduct security sweep of soft target area prior to event. Information on suspicious activities potentially related to terrorism should be forwarded immediately to the local FBI JTTF and the DHS HSOC.

For comments or questions related to the content or dissemination of this Information Bulletin, please contact the DHS/Information Analysis and Infrastructure Protection Directorate's Requirements Division at [HTUDHS.IAIP@DHS.GOV](mailto:HTUDHS.IAIP@DHS.GOV) UTH.

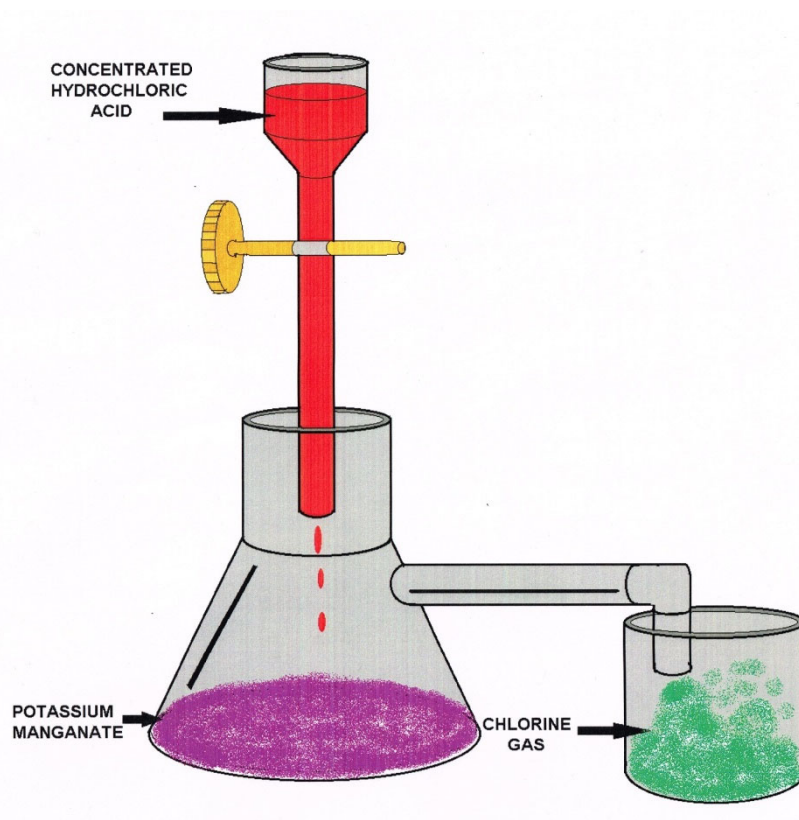


## CHAPTER 3 SUMMARY

Today, emergency responders and others in emergency services who support them face new challenges that seriously imperil not only the public but those very persons whose job it is to protect and help the public. The risks faced in today's world pose threats for which the average emergency responder may not be prepared. These threats go far beyond the usual ones associated with residential fires, vehicular accidents, or even hazardous materials incidents.

It is critical that emergency responders understand the implications of these modern threats and know proper response procedures and the limits of safe and prudent response. This knowledge will help prevent further fatalities. Responders need to translate this knowledge into SOPs/SOGs written to make safety the paramount consideration. Injured or incapacitated responders are no help to anyone.

The emergency services community has tremendous knowledge and resources available from the Federal government, military, public health, and law enforcement agencies, to name some of the more obvious. These resources can be a great help in writing prudent and safe SOPs/SOGs.





## Glossary

Acute Exposure	An exposure, often intense, over a relatively short period of time.
Alpha Radiation	The least penetrating type of nuclear radiation; not considered dangerous unless alpha-contaminated particles enter the body.
Asphyxiation	One of the six types of harm (see <b>TRACEM</b> ) that can be encountered at a terrorist incident. Asphyxiants interfere with oxygen flow during normal breathing. There are two types of asphyxiants: simple and chemical.
B-NICE	The acronym for identifying the five categories of terrorist incidents: Biological, Nuclear, Incendiary, Chemical, and Explosives.
Bacteria	Single-celled organisms that multiply by cell division and can cause disease in humans, plants, or animals. Examples include anthrax, cholera, plague, tularemia, and Q fever.
Beta Radiation	A type of nuclear radiation that is more penetrating than alpha radiation and can damage skin tissue and harm internal organs.
Biological Agent	Living organisms, or the materials derived from them, which cause disease in, or harm, humans, animals, or plants, or cause deterioration of material. Biological agents may be found as liquid droplets, aerosols, or dry powders. A biological agent can be adapted and used as a terrorist weapon, such as anthrax, tularemia, cholera, encephalitis, plague, and botulism. There are three different types of biological agents: bacteria, viruses, and toxins.
Biological Incident	An event in which a biological agent is used as a terrorist weapon.
Blister Agent	A chemical agent, also called a vesicant, which causes severe blistering and burns to eyes, skin, and tissues of the respiratory tract. Exposure is through liquid or vapor contact. Also referred to as mustard agents; examples include mustard and lewisite.
Blood Agent	A chemical agent that interferes with the ability of blood to transport oxygen and causes asphyxiation. These substances injure a person by interfering with cell respiration (the exchange of oxygen and carbon dioxide between blood and tissues). Common examples are hydrogen cyanide and cyanogen chloride.

Chemical Agent	There are five classes of chemical agents, all of which produce incapacitation, serious injury, or death: (1) nerve agents, (2) blister agents, (3) blood agents, (4) choking agents, and (5) irritating agents. A chemical substance used in military operations is intended to kill, seriously injure, or incapacitate people through its physiological effects.
Chemical Harm	One of the six types of harm (see <b>TRACEM</b> ) that can be encountered at a terrorist incident. There are two broad types of chemical agents that can cause harm: toxic and corrosive materials.
Chemical Incident	An event in which a chemical agent is used as a terrorist weapon.
Chemical Asphyxiant	Referred to as blood poisons, these are compounds that interrupt the flow of oxygen in the blood or the tissues in three ways: (1) They react more readily than oxygen with the blood. Carbon monoxide is the best-known example. (2) They liberate the hemoglobin from red blood cells, resulting in a lack of transport for oxygen. Hydrazine is one such asphyxiant. (3) They cause a malfunction in the oxygen-carrying ability of the red blood cells. Benzene and toluene are two of these.
Choking Agent	A chemical agent that causes physical injury to the lungs. In extreme cases, membranes swell and lungs become filled with liquid, which can result in asphyxiation resembling drowning. Death results from lack of oxygen; hence, the victim is " <b>choked.</b> " Common examples are chlorine and phosgene.
Chronic	An exposure, often mild, over a long period of time.
Consequence Management	As described in PDD-39, consequence management is the response to the disaster, and focuses on alleviating damage, loss, hardship, or suffering. The Federal Emergency Management Agency ( <b>FEMA</b> ) has the lead in consequence management.
Corrosive Materials	One type of chemical agent that can cause chemical harm at an incident scene. They are liquids or solids causing visible destruction or irreversible alterations in human skin tissue at the site of contact.
Crisis Management	As described in PDD-39, crisis management is the law enforcement response, and focuses on the criminal aspects of the incident. The Federal Bureau of Investigation ( <b>FBI</b> ) has the lead in crisis management.
Distance	One of the three components of the time, distance, and shielding ( <b>TDS</b> ) response; refers to the recommendation that

one maintain distance from a hazard if at all possible. Refer to the North American Emergency Response Guide (NAERG) as an appropriate resource.

Emergency Operations Plan (EOP)

An EOP is a document that (1) assigns responsibility to organizations and individuals for carrying out specific actions at projected times and places in an emergency that exceeds the capability or routine responsibility of any one agency; (2) sets forth lines of authority and organizational relationships, and shows how all actions will be coordinated; (3) describes how people and property will be protected in emergencies and disasters; (4) identifies personnel, equipment, facilities, supplies, and other recourses available for use during response and recovery operations; and (5) identifies steps to address mitigation concerns during response and recovery activities.

Emergency Support Functions (ESF)

The Federal Response Plan (**FRP**) details 12 ESFs in place to coordinate operations during Federal involvement in an incident: transportation, communications, public works and engineering, firefighting, information and planning, mass care, resource support, health and medical services, urban search and rescue, hazardous materials, food, and energy.

Etiological Harm

One of the six types of harm (see **TRACEM**) that can be encountered at a terrorist incident. Involves exposure to a living microorganism, or its toxins, which causes, or may cause, human disease. Biological agents are the most obvious examples of etiological agents.

Explosive

As defined by the U.S. Department of Transportation, "a substance fitting into one of these two categories: (1) any substance or article, including a device, designed to function by explosion; or (2) any substance or article, including a device, which, by chemical reaction within itself, can function in a similar manner even if not designed to function by explosion.

Explosive Incident

An event in which an explosives device is used as a terrorist weapon.

Federal Response Plan (FRP)

Developed to help expedite Federal support to disasters. Generally, the FRP is activated when the State's resources are not sufficient to cope with a disaster, and the governor has requested Federal assistance.

GEDAPER	An acronym used to describe an incident analysis process. The steps include (1) Gathering information, (2) Estimating course and harm, (3) Determining strategic goals, (4) Assessing tactical options and resources, (5) Planning and implementing actions, (6) Evaluating, and (7) Reviewing.
Gamma Radiation	Gamma rays are high-energy, ionizing radiation that travel at the speed of light and have great penetrating power. They can cause skin burns, severely injure internal organs, and have long-term, physiological effects.
Incendiary Device	Any mechanical, electrical, or chemical device used intentionally to initiate combustion and start a fire.
Incendiary Incident	An event in which an incendiary device is used as a terrorist weapon.
Irritating Agent	A chemical agent, also known as riot control agents or tear gas, which causes respiratory distress and tearing designed to incapacitate. Common examples include chloropicrin, MACE, tear gas, pepper spray, and dibenzoxazepine.
Local EOP	The local EOP focuses on essential measures for protecting the public, to include warning, emergency public information, evacuation, and shelter. To be included in a local EOP should be a mechanism for emergency responders and managers to notify and activate State resources.
Mechanical Harm	One of the six types of harm (see <b>TRACEM</b> ) that can be encountered at a terrorist incident. Causes trauma from contact with mechanical or physical hazards. One form of mechanical injury can result from an explosive device. Other types include routine slip, trip, and fall hazards.
NAERG	The North American Emergency Response Guidebook.
Nerve Agent	A substance that interferes with the central nervous system. Exposure is primarily through contact with the liquid (skin and eyes) and secondarily through inhalation of the vapor. Three distinct symptoms associated with nerve agents are pinpoint pupils, an extreme headache, and severe tightness in the chest. Examples of nerve agents are sarin, Soman, tabun, and VX agent.
Nuclear Incident	An event in which a nuclear agent is used as a terrorist weapon. There are two fundamentally different threats in the area of nuclear terrorism: (1) the use, or threatened use, of a nuclear bomb; and (2) the detonation of a conventional explosive incorporating nuclear materials.
PPE	Personal protective equipment.



Plan of Action	A written document that consolidates all of the operational actions to be taken by various personnel in order to stabilize the incident.
Presidential Decision Directive 39 (PDD-39)	Issued in June 1995, PDD-39, United States Policy on Counterterrorism, directed a number of measures to reduce the Nation's vulnerability to terrorism, to deter and respond to terrorist acts, and to strengthen capabilities to prevent and manage the consequences of terrorist use of nuclear, biological, and chemical weapons. Please see Appendix B for a copy of this document.
Radiological Dispersal Devices	(RDD) A conventional explosive incorporating nuclear materials.
Radiation	In this self-study program, refers to nuclear radiation, not radiation as a type of heat transfer. There are three types of nuclear radiation: (1) alpha, (2) beta, and (3) gamma. Radiation is the cause of one of the six types of harm (see TRACEM) that can be encountered at a terrorist incident.
Robert T. Stafford Disaster Relief and Emergency Assistance Act, Public Law 93-288	Authorizes the Federal government to respond to disasters and emergencies in order to help State and local governments save lives, and to protect public health, safety, and property.
Shielding	One of the three components of TDS; refers to maintaining significant physical barriers between you and the hazard. Examples include vehicles, buildings, walls, and PPE.
Simple Asphyxiant	Generally, an inert gas that displaces the oxygen necessary for breathing, and dilutes the oxygen concentration below the level that is useful for the human body.
Sizeup	The rapid mental evaluation of the factors that influence an incident. Sizeup is the first step in determining a course of action.
Stafford Act	See Robert T. Stafford Disaster Relief and Emergency Assistance Act.
State EOP	The State EOP is the framework within which local EOPs are created and through which the Federal government becomes involved. The States play three roles: (1) they assist local jurisdictions whose capabilities are overwhelmed by an emergency; (2) they themselves respond first to certain emergencies; and (3) they work with the Federal government when Federal assistance is necessary.

Strategic Goals	Strategic goals are broad, general statements of intent.
TRACEM	The acronym used to identify the six types of harm one may encounter at a terrorist incident: Thermal, Radioactive, Asphyxiation, Chemical, Etiological, and Mechanical.
Terrorism	As defined by the FBI, "the unlawful use of force against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in the furtherance of political or social objectives." This definition includes three elements: (1) Terrorist activities are illegal and involve the use of force. (2) The actions are intended to intimidate or coerce. (3) The actions are committed in support of political or social objectives.
Terrorism Incident Annex	The annex to the FRP that describes the Federal concept of operations to implement PDD-39 when necessary to respond to terrorist incidents within the U.S. Please see Appendix A for a copy of the annex.
Thermal Harm	One of the six types of harm (see <b>TRACEM</b> ) that can be encountered at a terrorist incident. Thermal harm is the result of exposure to the extremes of heat and cold.
Time	One of the three components of TDS; refers to the amount of time a responder should be exposed to an incident. It is recommended that one spend the shortest amount of time possible in the hazard area.
Time, Distance, and Shielding (TDS)	Three types of protective measures commonly associated with hazardous materials training.
Toxic Materials	A type of chemical that can cause chemical harm at an incident scene. They produce harmful effects depending on the concentration of the materials and the length of exposure to them. An individual can have chronic or acute exposures to toxic materials.
Toxins	Toxic substances of natural origin produced by an animal, plant, or microbe. They differ from chemical substances in that they are not manmade. Toxins may include botulism, Ricin, and mycotoxins.
Vesicants	Chemical agents, also called blister agents, which cause severe burns to eyes, skin, and tissues of the respiratory tract. Also referred to as mustard agents, examples include mustard and lewisite.

## CHAPTER 3 EXERCISE

---

This is a chapter review, you can find the final exam on TLC's website under Assignments.

1. As one involved in emergency services, you already may have responded to a terrorist or emergency incident. If you have, what were your key concerns or worries as you responded to the uncertainties of the situation?
2. In retrospect, do you think your anxiety level was higher than in the more customary responses such as to a house fire, a vehicle accident or even a hazardous materials incident? Why or why not?
3. If you have never been associated with a terrorist incident, what would be some of your anxieties or concerns as an emergency services provider in dealing with a situation like this?
4. Suggest some consequences for emergency services responders if it were suddenly realized that terrorists had contaminated the public water supply.
5. Does your department or organization have standard operating procedures/standard operating guidelines (SOPs/SOGs) to deal with a potential biological incident? Yes No If not, what would you do?
6. To whom would you turn in your community for help (such as monitoring training) in becoming better prepared to handle a radiological threat?
7. Does your department or organization have SOPs/SOGs for responding to an incendiary incident?
8. Does your department or organization have SOPs/SOGs for responding to a chemical incident?
9. What would be your specific role if you had to respond to a chemical threat?
10. What are some Federal and State agencies in your area to which you might turn for assistance in preparing SOPs/SOGs for the events discussed in this Chapter?
11. How different would these SOPs/SOGs be from existing ones for the more usual and customary emergencies?
12. If any one of the incidents discussed in this Chapter happened tomorrow, are you and your emergency services colleagues sufficiently prepared to deal with it?
13. What are some of the implications of your state of readiness?

### Chapter 3 Assignment

# 14 Describe one or two practical, achievable steps you will take as a result of studying this Chapter to help you to be better prepared to deal with one of the incidents described here.
Step One:
Step Two:
<b>HOW I WILL ACCOMPLISH STEP ONE</b>
<b>HOW I WILL ACCOMPLISH STEP TWO</b>

### LEARNING CHECK

True or False: Circle either T or F.

15.    T    F    The Federal Bureau of Investigation defines terrorism as "the unlawful use of force against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in the furtherance of political or social objectives."
16.    T    F    Nerve agents are similar in nature to organophosphate pesticides.
17.    T    F    The criminal component is the least important element separating a terrorist organization and its actions from a legitimate organization.
18.    T    F    Experts generally agree that there are five categories of terrorist incidents.
19.    T    F    Alpha radiation is the most penetrating kind.
20.    T    F    THE INTENT TO INTIMIDATE OR COERCE PEOPLE THROUGH RANDOM ACTS OF VIOLENCE IS A CHARACTERISTIC OF TERRORIST ACTIVITIES.

Multiple Choice: Circle your answer.

21. Of the following targets, which one would probably be the least appealing to a group plotting an attack?
- a. An urban complex of Federal facilities.
  - b. A major urban seaport serviced by two interstate highways.
  - c. An urban area in need of rehabilitation.
  - d. An urban family planning clinic.
22. Currently the most common terrorist threat is
- a. a biological agent.
  - b. an explosive device.
  - c. a chemical agent.
  - d. a nuclear device.
23. Which of the following would be identified as part of a biological incident?
- a. Radiation.
  - b. Irritants.
  - c. Toxins.
  - d. Blood agents.
24. It is estimated that the percentage of terrorist activities involving explosives is about
- a. 80 percent.
  - b. 70 percent.
  - c. 60 percent.
  - d. 50 percent.

Think about how your mail and packages are handled--do you need a Vulnerability Assessment in this area?



## Chapter 4: Incidents and Indicators

---

**Section Focus:** You will learn the basics of terrorism incidents and various indicators. At the end of this section, you the student will be able to understand and describe the unusual attacks upon your facility. There is a post quiz at the end of this section to review your comprehension and a final examination in the Assignment for your contact hours.

**Scope/Background:** *Incidents and Indicators* identifies criteria for recognizing suspicious incidents; presents on-scene key indicators, including those for locating terrorist incidents; and lists outward warning signs and detection clues.



### **ASSURING A SAFE RESPONSE TO A POTENTIAL CRIME SCENE**

There are many similarities between terrorism scene responses and the more common crime scenes to which public safety agencies respond. While law enforcement officers are well versed in crime scene investigations, the majority of fire, EMS, and emergency management personnel are not. It is critical that you understand the special demands placed upon you and your activities when responding to crime scenes.

Any response to an incident other than a natural disaster may be a response to a crime scene. Firefighters may be first responders to arson scenes. EMS personnel may be called upon to administer aid to victims of a violent crime.

Hazardous materials teams frequently respond to sites of clandestine dumping or intentional releases of chemicals. At a terrorism crime scene, you will need to coordinate closely with other first-responding fire, EMS, and law enforcement personnel to ensure that you and the other responders do not destroy important evidence.

Remember that even when the emergency phase of the incident is over, the incident itself has not ended. The incident ends only when there is successful prosecution of the guilty person(s).

As a first responder, you should be aware of warning signs that indicate criminal activity, because some incidents will involve criminal acts.



Harden all of your locks and fences, it would take 5 seconds to cut the above lock and less time to jump off this trash container and over the fence, double the size of your existing fences, harden locks, remove multiple locking devices. Install key pads or equivalent security devices. Rake areas adjacent to fences to see foot travel.

Harden doors with solid steel, install bulletproof or ballistic quality glass windows.





## Avoid Impeding the Investigation

Be sure to coordinate your actions with law enforcement operations. Basically, there are three ways to help solve a crime: the confession of the perpetrator, statements provided by witnesses or victims, and incriminating information obtained through physical evidence.

Of these, only physical evidence provides incontestable, impartial facts. Only physical evidence can overcome the conflicting and confusing statements of witnesses who, observing the same incident at essentially the same time, nonetheless have different perceptions of what took place.

Physical evidence may be crucial to connect the perpetrator to the scene. The recognition, collection, and preservation of physical evidence may be the only means to identify, and successfully prosecute, those responsible. Keep this in mind when arriving at any potential crime scene.

If you are involved with a terrorist incident as a first responder, you essentially become part of the crime scene. As they do with any material witness, law enforcement personnel likely will interview you at some point. You may be required to testify in court as to what you saw, did, and did not do.

Sometimes doing something inappropriate is more detrimental to solving the crime than doing nothing at all. Keep in mind that cases have been lost in court due to the imprudent actions of first responders--whether fire, police, or emergency medical responders.

---

### Scene Considerations

Your response to the scene of a potential terrorist attack could involve entry into a hazardous area. Deadly radioactive, chemical, or biological agents already may have contaminated the atmosphere around the scene. The presence of fires or collapsed building sections may intensify thermal and mechanical risk.

You can hope to survive only by entering this area very carefully--by moving cautiously and by wearing the appropriate personal protective equipment (**PPE**).



## Delaying Entry May Be Wisest

When you suspect hazardous substances or conditions, use only qualified personnel to secure the scene. Hazardous materials teams may have sufficient detection and monitoring equipment to define the hazard. Otherwise, it may be necessary for you to await the arrival of additional resources before you can attempt entry into the hazardous area.

Any appropriate response to the site of a determined mass biological, chemical, or radiological attack may require decontamination of equipment, entry personnel, survivors, and casualties. The emergency decontamination process may be the single most important task that the public safety community can perform during a terrorist incident, but it will certainly tax the abilities of any locality or state. Therefore it makes sense for all communities to preplan for mass decontamination.

Your response to large-scale explosions and fires requires that you pay just as much attention to hazardous conditions as you would at a potential chemical or biological incident. Be aware of the possible presence of a secondary device intended to injure or kill you and other first responders.

Often, these secondary devices are referred to as "**sucker punch**" devices. Bombs produce large-scale trauma due to shock waves, projectiles, and structural collapse. When arriving on the scene of a highly damaged structure, be aware of the structural conditions causing unsafe buildings to collapse, the types of injuries resulting from these incidents, and the specialized precautions you need to take.

Whatever type of threat you respond to, the description that you provide to investigators reconstructing the early minutes of activity at the incident scene can be the key to successful prosecution of the case. At the scene, be aware of persons coming or going on foot or by vehicle. Jot down the license plate numbers, and brief descriptions of those present in order to refresh your memory.

Encourage witnesses and bystanders to remain at the scene until investigators have interviewed them. Note any other unusual circumstances.

Your documentation of the incident will prove invaluable in prosecuting the case.

Whenever possible, provide photographs and videotape to show the "**big picture**" of the scene. Include as many details as possible. Use rough sketches to pinpoint the location of victims and their wounds, as well as the locations of potential evidence.



Take notes on what you see and organize them, and provide them to investigators as soon as possible after the response.

## Leave Things As You Find Them

At a potential crime scene, it is critical that you disturb the scene as little as possible. If you absolutely must move something, make sure you remember where it was originally, its orientation and condition, and anything else notable about its position and natural state. If possible, photograph the object before you move it. Take notes on any holes, breaks, or scratches that you caused, and pass this information on to the crime scene investigators. Law enforcement officers must be able to differentiate between the results of the crime and what responders might have done to those results.

Following your response, you may have to write an after-action report summarizing your activities and observations during the incident. Be sure to document the report thoroughly using your notes. Remember that your report can be used in court, both in your favor and against you.

### Locating the Potential Terrorist--Threat and Risk Target Assessment

In order to determine potential terrorist groups active in your jurisdiction, someone needs to conduct a threat analysis in cooperation with local, regional, State, and Federal law enforcement officials to identify groups that may pose a threat to your community. This person may be the emergency management coordinator or director, or someone else in the community associated with emergency response.

#### Terrorist groups may include, but are not limited to, the following:

- ethnic separatist and emigre groups;
- left-wing radical organizations;
- right-wing racist, anti-authority, survivalist groups;
- foreign terrorist organizations; and
- issue-oriented groups (including animal rights groups, extremist environmental groups, extremist religious groups, anti-authority, etc.).



Vehicle Inspection

## Threat Assessment

Once such groups are known (threat assessment) the next step is to identify potential facilities or activities that may become targets of terrorist acts. These facilities may include the following:

- civilian or military government installations;
- industries that are part of the "**military-industrial complex**," manufacture environmentally sensitive products, operate in politically sensitive countries, or generally represent capitalist endeavors;
- financial institutions that support the above;
- infrastructure components (i.e., transportation, communications, utilities, or energy systems on which the above depend);
- explosive magazine storage facilities (construction sites, quarries, etc.);
- sports arenas, parks (theme and others);
- schools, hospitals, shopping centers; and
- venues for special events.

**Identifying these potential targets is part of risk assessment.**



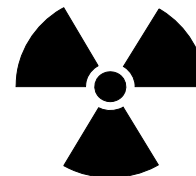
Concealed Handguns are everywhere, even in his purse.

## Outward Warning Signs and Indicators

At the scene, initial responders need to be on the lookout for the following common warning signs indicating the presence of lethal agents from the five threat categories.

### Biological Indicators

Biological incidents will present themselves in two ways. The first could be a community public health emergency, while the second could be a focused response to an incident, such as that involving a toxin.



In the case of a biological incident, the onset of some symptoms may take days to weeks, and typically there will be no characteristic signatures, because biological agents are usually odorless and colorless. Because of the delayed onset of symptoms, the number of victims and the areas affected may be greater due to the migration of infected individuals. On the other hand, some effects may be very rapid (as short as four to six hours).

Exact indicators of a biological event may follow:



include any of the

- unusual numbers of sick or dying people or animals;
- dissemination of unscheduled and unusual sprays, especially outdoors and/or at night; and
- abandoned spray devices with no distinct odors.

Any number of symptoms may occur. As a first responder, you should consider calling local hospitals to see if they have admitted additional casualties with similar symptoms. Casualties may occur within minutes or hours, or may not occur until many days or weeks after an incident has occurred. The agent used determines the time during which the symptoms appear.



### Nuclear Indicators

Short of an actual detonation or obvious accident involving radiological materials, there are a couple of ways to be certain that radiation is present. One is to observe the Department of Transportation (**DOT**) placards and labels. The other is to use the monitoring devices that most fire department hazardous materials teams now carry routinely. If the fire department does not have ready access to these instruments, the local or State office of emergency management should be able to provide them.

### Incendiary Indicators

Multiple fires may indicate the use of accelerants such as gasoline, rags, or other incendiary devices. Remains of incendiary device components, odors of accelerants, unusually heavy burning, or fire volume also are key indicators.

### **Chemical Indicators**

Once released, a nerve agent's outward warning signs are easy to spot. Within minutes, the most significant sign will be rapid onset of similar symptoms in a large group of people. Dermal exposure (clammy skin) and pinpoint pupils (miosis) are the best symptomatic indications of nerve agent use. Because nerve agents are so lethal, mass fatalities without other signs of trauma are common. Other outward signs of nerve agent release include

- hazardous materials or lab equipment that is not relevant to the occupancy;
- exposed individuals reporting unusual odors or tastes;
- explosions dispersing liquids, mists, or gases;
- explosions seeming only to destroy a package or bomb device;
- unscheduled dissemination of an unusual spray;
- abandoned spray devices;
- numerous dead animals, fish, and birds;
- absence of insect life in a warm climate;
- mass casualties without obvious trauma;
- distinct pattern of casualties and common symptoms; and
- civilian panic in potential target areas, i.e., government buildings, public assemblies, subway systems, etc.

### **Explosive Indicators**

Signs of explosive incidents may be obvious, such as large-scale damage to a building, or may be difficult to detect initially. Blown-out windows and widely scattered debris also serve as indicators.



Victims may exhibit effects of the blast, such as obvious shrapnel-induced trauma, appearance of shock-like symptoms, and/or damage to their eardrums.

## **Bomb Threats and General Evacuation Procedures**

Bombing and the threat of being bombed are harsh realities in today's world. The public is becoming more aware of those incidents of violence that are perpetrated by vicious, nefarious segments of our society through the illegal use of explosives.

Law enforcement agencies are charged with providing protection for life and property, but law enforcement alone cannot be held responsible. Every citizen must do his or her part to ensure a safe environment.

The following information is designed to help both the public and private sectors prepare for the potential threat of explosives-related violence. While the ideas set forth herein are applicable in most cases, they are intended only as a guide. The information provided is compiled from a wide range of sources, including the actual experiences of special agents of the Bureau of Alcohol, Tobacco and Firearms (**ATF**).

If there is one point that cannot be overemphasized, it is the value of being prepared. Do not allow a bomb incident to catch you by surprise. By developing a bomb incident plan and considering possible bomb incidents in your physical security plan, you can reduce the potential for personal injury and property damage. In making this information available to you, we hope to help you better prepare to deal with bomb threats and the illegal use of explosives.

Bombs can be constructed to look like almost anything and can be placed or delivered in any number of ways. The probability of finding a bomb that looks like the stereotypical bomb is almost nonexistent. The only common denominator that exists among bombs is that they are designed or intended to explode.

Most bombs are homemade and are limited in their design only by the imagination of, and resources available to, the bomber. Remember, when searching for a bomb, suspect anything that looks unusual. Let the trained bomb technician determine what is or is not a bomb.

Bomb threats are delivered in a variety of ways. The majority of threats are called in to the target. Occasionally these calls are through a third party. Sometimes a threat is communicated in writing or by a recording.

### **Two logical explanations for reporting a bomb threat are:**

1. The caller has definite knowledge or believes that an explosive or incendiary bomb has been or will be placed and he/she wants to minimize personal injury or property damage. The caller may be the person who placed the device or someone who has become aware of such information.
2. The caller wants to create an atmosphere of anxiety and panic which will, in turn, result in a disruption of the normal activities at the facility where the device is purportedly placed.

Whatever the reason for the report, there will certainly be a reaction to it. Through proper planning, the wide variety of potentially uncontrollable reactions can be greatly reduced. If you accept the two aforementioned explanations for reporting that a bomb is about to go off, you can better prepare to foil the bomber or threat maker.

Through proper preparation, you can reduce the accessibility of your business or building and identify those areas that can be "**hardened**" against the potential bomber. This will limit the amount of time lost to searching, if you determine a search is necessary. If a bomb incident occurs, proper planning will instill confidence in the leadership, reinforce the notion that those in charge do care, and reduce the potential for personal injury and property loss.

Proper planning can also reduce the threat of panic, the most contagious of all human emotions. Panic is sudden, excessive, unreasoning, infectious terror. Once a state of panic has been reached, the potential for injury and property damage is greatly increased. In the context of a bomb threat, panic is the ultimate achievement of the caller.

Be prepared! There is no excuse for not taking every step necessary to meet the threat.

### **How to Prepare**

In preparing to cope with a bomb incident, it is necessary to develop two separate but interdependent plans, namely a physical security plan and a bomb incident plan.

Physical security provides for the protection of property, personnel, facilities, and material against unauthorized entry, trespass, damage, sabotage, or other illegal or criminal acts. The physical security plan deals with prevention and control of access to the building. In most instances, some form of physical security may be already in existence, although not necessarily intended to prevent a bomb attack.

The bomb incident plan provides detailed procedures to be implemented when a bombing attack is executed or threatened. In planning for the bomb incident, a definite chain of command or line of authority must be established. Only by using an established organization and procedures can the bomb incident be handled with the least risk to all concerned. A clearly defined line of authority will instill confidence and avoid panic.

Establishing a chain of command is easy if there is a simple office structure, one business, one building. However, if a complex situation exists, a multi-occupant building for example, a representative from each occupant entity should attend the planning conference. A leader should be appointed and a clear line of succession delineated. This chain of command should be printed and circulated to all concerned parties.

In planning, you should designate a command center to be located in the switchboard room or other focal point of telephone or radio communications. The management personnel assigned to operate the center should have the authority to decide whatever action should be taken during the threat. Only those with assigned duties should be permitted in the center. Make some provision for alternates in the event someone is absent when a threat is received. Obtain an updated blueprint or floor plan of your building and maintain it in the command center.

Contact the police department, fire department, or local government agencies to determine if any assistance is available to you for developing your physical security plan or bomb incident plan. If possible, have police and/or fire department representatives and members of your staff inspect the building for areas where explosives are likely to be concealed. (Make a checklist of these areas for inclusion in command center materials.)



Determine whether there is a bomb disposal unit available, how to contact the unit, and under what conditions it is activated. In developing your bomb incident plan, you must also ascertain whether the bomb disposal unit, in addition to disarming and removing the explosives, will assist in searching the building in the event of a threat.

### **Training**

Training is essential to deal properly with a bomb threat incident. Instruct all personnel, especially those at the telephone switchboard, what to do if a bomb threat is received. Be absolutely certain that all personnel assigned to the command center are aware of their duties. The positive aspects of planning will be lost if the leadership is not apparent. It is also very important to organize and train an evacuation unit which will be responsive to the command center and has a clear understanding of the importance of its role.

We have suggested that the command center be located near the switchboard or focal point of communications. It is critical that lines of communication be established between the command center and the search or evacuation teams. The center must have the flexibility to keep up with the search team progress. In a large facility, if the teams go beyond the communications network, the command center must have the mobility to maintain contact and track search or evacuation efforts.

We mentioned earlier that, in dealing with bomb incidents or potential bomb incidents, two interrelated plans must be developed, the bomb incident plan and the physical security plan. Heretofore, we have primarily addressed the bomb incident plan. Now, before continuing with that plan, we will discuss security measures as they apply to "**hardening**" against the bomb attack.

Most commercial structures and individual residences already have some security in place, planned or unplanned, realized or not. Locks on windows and doors, outside lights, etc., are all designed and installed to contribute toward the security of a facility and the protection of its occupants.

In considering measures to increase security for your building or office, it is highly recommended that you contact your local police department for guidance regarding a specific plan for your facility. There is no single security plan that is adaptable to all situations. The following recommendations are offered because they may contribute to reducing your vulnerability to bomb attacks.

The exterior configuration of a building or facility is very important. Unfortunately, in most instances, the architect has given little or no consideration to security, particularly toward thwarting or discouraging a bomb attack. However, by the addition of fencing and lighting, and by controlling access, the vulnerability of a facility to a bomb attack can be reduced significantly.

Bombs being delivered by car or left in a car are a grave reality. Parking should be restricted, if possible, to 300 feet from your building or any building in a complex. If restricted parking is not feasible, properly identified employee vehicles should be parked closest to your facility and visitor vehicles parked at a distance.

Heavy shrubs and vines should be kept close to the ground to reduce their potential to conceal criminals or bombs. Window boxes and planters are perfect receptacles for the bomber.

Unless there is an absolute requirement for such ornamentation, window boxes and planters are better removed. If they must remain, a security patrol should be employed to check them regularly.

A highly visible security patrol can be significant deterrent. Even if this "**patrol**" is only one security guard/night guard, he/she is optimally utilized outside the building. If an interior guard is utilized, consider the installation of closed-circuit television cameras that cover exterior building perimeters.

Have an adequate burglar alarm system installed by a reputable company that can service and properly maintain the equipment. Post signs indicating that such a system is in place.

Entrance/exit doors with hinges and hinge pins on the inside to prevent removal should be installed. Solid wood or sheet metal faced doors provide extra integrity that a hollow-core wooden door cannot provide. A steel door frame that properly fits the door is as important as the construction of the door.

The ideal security situation is a building with no windows. However, bars, grates, heavy mesh screens, or steel shutters over windows offer good protection from otherwise unwanted entry. It is important that the openings in the protective coverings are not too large. Otherwise, a bomb may be introduced into the building while the bomber remains outside.

Floor vents, transoms, and skylights should also be covered. Please note that fire safety considerations preclude the use of certain window coverings. Municipal ordinances should be researched and safety considered before any of these renovations are undertaken.

Controls should be established for positively identifying personnel who are authorized access to critical areas and for denying access to unauthorized personnel. These controls should extend to the inspection of all packages and materials being taken into critical areas.

### **Security and Maintenance Personnel**

Security and maintenance personnel should be alert for people who act in a suspicious manner, as well as objects, items, or parcels which look out of place or suspicious. Surveillance should be established to include potential hiding places (e.g., stairwells, rest rooms, and any vacant office space) for unwanted individuals.

Doors or access ways to such areas as boiler rooms, mail rooms, computer areas, switchboards, and elevator control rooms should remain locked when not in use. It is important to establish a procedure for the accountability of keys. If keys cannot be accounted for, locks should be changed.

Good housekeeping is also vital. Trash or dumpster areas should remain free of debris.

A bomb or device can easily be concealed in the trash. Combustible materials should be properly disposed of, or protected if further use is anticipated.

### **Install Detection Devices**

Install detection devices at all entrances and closed-circuit television in those areas previously identified as likely places where a bomb may be placed. This, coupled with the posting of signs indicating such measures are in place, is a good deterrent.

The ATF recognizes the necessity for businesses to maintain good public relations. Corporate responsibility however, also encompasses the safety and protection of the public. The threatened use of explosives necessitates that in the interest of safety and security, some inconvenience may have to be imposed on visitors to public buildings.

The public is becoming more accustomed to routine security checks and will readily accept these minor inconveniences.

### **Minimal Expenditure**

Perhaps entrances and exits can be modified with a minimal expenditure to channel all visitors through someone at a reception desk. Individuals entering the building would be required to sign a register indicating the name and room number of the person whom they wish to visit. Employees at these reception desks could contact the person to be visited and advise him/her that a visitor, by name, is in the lobby. The person to be visited may decide to come to the lobby to ascertain that the purpose of the visit is valid.

A system for signing out when the individual departs could be integrated into this procedure.

Such a procedure may result in complaints from the public. If the reception desk clerk explains to the visitor that these procedures were implemented in his/her best interest and safety, the complaints would be reduced. The placement of a sign at the reception desk informing visitors of the need for safety is another option.

### **Decision Time**

The most serious of all decisions to be made by management in the event of a bomb threat is whether to evacuate the building. In many cases, this decision may have already been made during the development of the bomb incident plan. Management may pronounce a *carte blanche* policy that, in the event of a bomb threat, total evacuation will be effective immediately. This decision circumvents the calculated risk and demonstrates a deep concern for the safety of personnel in the building. However, such a decision can result in costly loss of time.

### ***Essentially, there are three alternatives when faced with a bomb threat:***

- 1. Ignore the threat.**
- 2. Evacuate immediately.**
- 3. Search and evacuate if warranted.**

Ignoring the threat completely can result in some problems. While a statistical argument can be made that very few bomb threats are real, it cannot be overlooked that bombs have been located in connection with threats. If employees learn that bomb threats have been received and ignored, it could result in morale problems and have a long-term adverse effect on your business.

Also, there is the possibility that if the bomb threat caller feels that he/she is being ignored, he/she may go beyond the threat and actually plant a bomb.

### **Disruptive Effect**

Evacuating immediately on every bomb threat is an alternative that on face value appears to be the preferred approach. However, the negative factors inherent in this approach must be considered. The obvious result of immediate evacuation is the disruptive effect on your business.

If the bomb threat caller knows that your policy is to evacuate each time a call is made, he/she can continually call and force your business to a standstill. An employee, knowing that the policy is to evacuate immediately, may make a threat in order to get out of work. A student may use a bomb threat to avoid a class or miss a test.

Also, a bomber wishing to cause personal injuries could place a bomb near an exit normally used to evacuate and then call in the threat.

Initiating a search after a threat is received and evacuating a building after a suspicious package or device is found is the third, and perhaps most desired, approach. It is certainly not as disruptive as an immediate evacuation and will satisfy the requirement to do something when a threat is received. If a device is found, the evacuation can be accomplished expeditiously while at the same time avoiding the potential danger areas of the bomb.

### **Evacuation**

An evacuation unit consisting of management personnel should be organized and trained. The organization and training of this unit should be coordinated with the development of the bomb incident plan, as well as with all tenants of a building.

The evacuation unit should be trained in how to evacuate the building during a bomb threat. You should consider priority of evacuation, e.g., evacuation by floor level. Evacuate the floor levels above and below the danger area in order to remove those persons from danger as quickly as possible. Training in this type of evacuation is usually available from police, fire or other units within the community.

You may also train the evacuation unit in search techniques, or you may prefer a separate search unit. Volunteer personnel should be solicited for this function. Assignment of search wardens, team leaders, etc., can be employed. To be proficient in searching the building, search personnel must be thoroughly familiar with all hallways, rest rooms, false ceiling areas, and every location in the building where an explosive or incendiary device may be concealed. When police officers or firefighters arrive at the building, the contents and the floor plan will be unfamiliar to them if they have not previously reconnoitered the facility.

Thus, it is extremely important that the evacuation or search unit be thoroughly trained and familiar with the floor plan of the building and immediate outside areas. When a room or particular area is searched, it should be marked or sealed with a piece of tape and reported to the supervisor of that area.

The evacuation or search unit should be trained only in evacuation and search techniques and not in the techniques of neutralizing, removing or otherwise having contact with the device. If a device is located, it should not be disturbed. However, its location should be well marked and a route back to the device noted.

## **Search Team**

It is advisable to use more than one individual to search any area or room, no matter how small. Searches can be conducted by supervisory personnel, area occupants or trained explosive search teams. There are advantages and disadvantages to each method of staffing the search teams.

Using supervisory personnel to search is a rapid approach and causes little disturbance. There will be little loss of employee working time, but a morale problem may develop if it is discovered that a bomb threat has been received and workers were left unaware.

Using a supervisor to search will usually not be as thorough because of his/her unfamiliarity with many areas and his/her desire to get on with business.

Using area occupants to search their own areas is the best method for a rapid search. The occupants' concern for their own safety will contribute toward a more thorough search. Furthermore, the personnel conducting the search are familiar with what does or does not belong in a particular area.

Using occupants to search will result in a shorter loss of worktime than if all were evacuated prior to search by trained teams. Using the occupants to search can have a positive effect on morale, given a good training program to develop confidence. Of course, this would require the training of an entire work force, and ideally the performance of several practical training exercises. One drawback of this search method is the increased danger to unevacuated workers.

The search conducted by a trained team is the best for safety, morale and thoroughness, though it does take the most time. Using a trained team will result in a significant loss of production time. It is a slow operation that requires comprehensive training and practice.

The decision as to who should conduct searches lies with management, and should be considered and incorporated into the bomb incident plan.

## **Search Techniques**

The following room search technique is based on the use of a two-person searching team. There are many minor variations possible in searching a room. The following contains only the basic techniques.

When the two-person search team enters the room to be searched, they should first move to various parts of the room and stand quietly with their eyes closed and listen for a clockwork device. Frequently, a clockwork mechanism can be quickly detected without use of special equipment. Even if no clockwork mechanism is detected, the team is now aware of the background noise level within the room itself.

Background noise or transferred sound is always disturbing during a building search. If a ticking sound is heard but cannot be located, one might become unnerved. The ticking sound may come from an unbalanced air-conditioner fan several floors away or from a dripping sink down the hall. Sound will transfer through air-conditioning ducts, along water pipes, and through walls. One of the most difficult buildings to search is one that has steam or hot water heat.

## **Background Noise**

This type of building will constantly thump, crack, chatter, and tick due to the movement of the steam or hot water through the pipes and the expansion and contraction of the pipes. Background noise may also include outside traffic sounds, rain, and wind.

The individual in charge of the room searching team should look around the room and determine how the room is to be divided for searching and to what height the first searching sweep should extend. The first searching sweep will cover all items resting on the floor up to the selected height.

You should divide the room into two virtually equal parts. This equal division should be based on the number and type of objects in the room to be searched and not on the size of the room. An imaginary line is then drawn between two objects in the room; e.g., the edge of the window on the north wall to the floor lamp on the south wall.

## **First Room-Searching Sweep**

Look at the furniture or objects in the room and determine the average height of the majority of items resting on the floor. In an average room, this height usually includes table or desk tops and chair backs. The first searching height usually covers the items in the room up to hip height.

After the room has been divided and a searching height has been selected, both individuals go to one end of the room division line and start from a back-to-back position. This is the starting point, and the same point will be used on each successive searching sweep. Each person now starts searching his/her way around the room, working toward the other person, checking all items resting on the floor around the wall area of the room.

When the two individuals meet, they will have completed a "**wall sweep**." They should then work together and check all items in the middle of the room up to the selected hip height, including the floor under the rugs. This first searching sweep should also include those items which may be mounted on or in the walls, such as air-conditioning ducts, baseboard heaters, and built-in wall cupboards, if these fixtures are below hip height.

The first searching sweep usually consumes the most time and effort. During all the searching sweeps, use the electronic or medical stethoscope on walls, furniture items, and floors.

## **Second Room-Searching Sweep**

The individual in charge again looks at the furniture or objects in the room and determines the height of the second searching sweep. This height is usually from the hip to the chin or top of the head. The two persons return to the starting point and repeat the searching technique at the second selected searching height. This sweep usually covers pictures hanging on the walls, built bookcases, and tall table lamps

## **Third Room-Searching Sweep**

When the second searching sweep is completed, the person in charge again determines the next searching height, usually from the chin or the top of the head up to the ceiling.

The third sweep is then made. This sweep usually covers high mounted air-conditioning ducts and hanging light fixtures.

### **Fourth Room-Searching Sweep**

If the room has a false or suspended ceiling, the fourth sweep involves investigation of this area. Check flush or ceiling-mounted light fixtures, air conditioning or ventilation ducts, sound or speaker systems, electrical wiring, and structural frame members.

Have a sign or marker indicating "**Search Completed**" conspicuously posted in the area. Place a piece of colored Scotch tape across the door and door jamb approximately 2 feet above floor level if the use of signs is not practical.

The room searching technique can be expanded. The same basic technique can be applied to search any enclosed area. Encourage the use of common sense or logic in searching. If a guest speaker at a convention has been threatened, common sense would indicate searching the speaker's platform and microphones first, but always return to the searching technique. Do not rely on random or spot checking of only logical target areas. ***The bomber may not be a logical person.***

**In conclusion, the following steps should be taken in order to search a room:**

1. Divide the area and select a search height
2. Start from the bottom and work up.
3. Start back-to-back and work toward each other.
4. Go around the walls and proceed toward the center of the room.

### **Suspicious Objects Located**

It is imperative that personnel involved in a search be instructed that their only mission is to search for and report suspicious objects. Under no circumstances should anyone move, jar or touch a suspicious object or anything attached to it.

### **Removal or Disarming**

The removal or disarming of a bomb must be left to the professionals in explosive ordnance disposal. When a suspicious object is discovered, the following procedures are recommended:

1. Report the location and an accurate description of the object to the appropriate warden. This information should be relayed immediately to the command center, which will notify the police and fire departments, and rescue squad. These officers should be met and escorted to the scene.
2. If absolutely necessary, place sandbags or mattresses, never metal shields, around the suspicious object. Do not attempt to cover the object.
3. Identify the danger area, and block it off with a clear zone of at least 300 feet, including floors below and above the object.
4. Check to see that all doors and windows are open to minimize primary damage from blast and secondary damage from fragmentation.
5. Evacuate the building.
6. Do not permit re-entry into the building until the device has been removed/disarmed, and the building declared safe for re-entry.

## **Handling the Media**

It is of paramount importance that all inquiries from the news media be directed to one individual appointed as spokesperson. All other persons should be instructed not to discuss the situation with outsiders, especially the news media. The purpose of this provision is to furnish the news media with accurate information and to see that additional bomb threat calls are not precipitated by irresponsible statements from uninformed sources.

## **Summary**

The individual in charge again looks at the furniture or objects in the room and determines the height of the second searching sweep. This height is usually from the hip to the chin or top of the head. The two persons return to the starting point and repeat the searching technique at the second selected searching height. This sweep usually covers pictures hanging on the walls, built bookcases, and tall table lamps

## **Bomb Incident Plan**

Designate a chain of command.

1. Establish a command center.
2. Decide what primary and alternate communications will be used.
3. Establish clearly how and by whom a bomb threat will be evaluated.
4. Decide what procedures will be followed when a bomb threat is received or device discovered.
5. Determine to what extent the available bomb squad will assist and at what point the squad will respond.
6. Provide an evacuation plan with enough flexibility to avoid a suspected danger area.
7. Designate search teams.
8. Designate areas to be searched.
9. Establish techniques to be utilized during search.
10. Establish a procedure to report and track progress of the search and a method to lead qualified bomb technicians to a suspicious package.
11. Have a contingency plan available if a bomb should go off.
12. Establish a simple-to-follow procedure for the person receiving the bomb threat.
13. Review your physical security plan in conjunction with the development of your bomb incident plan.

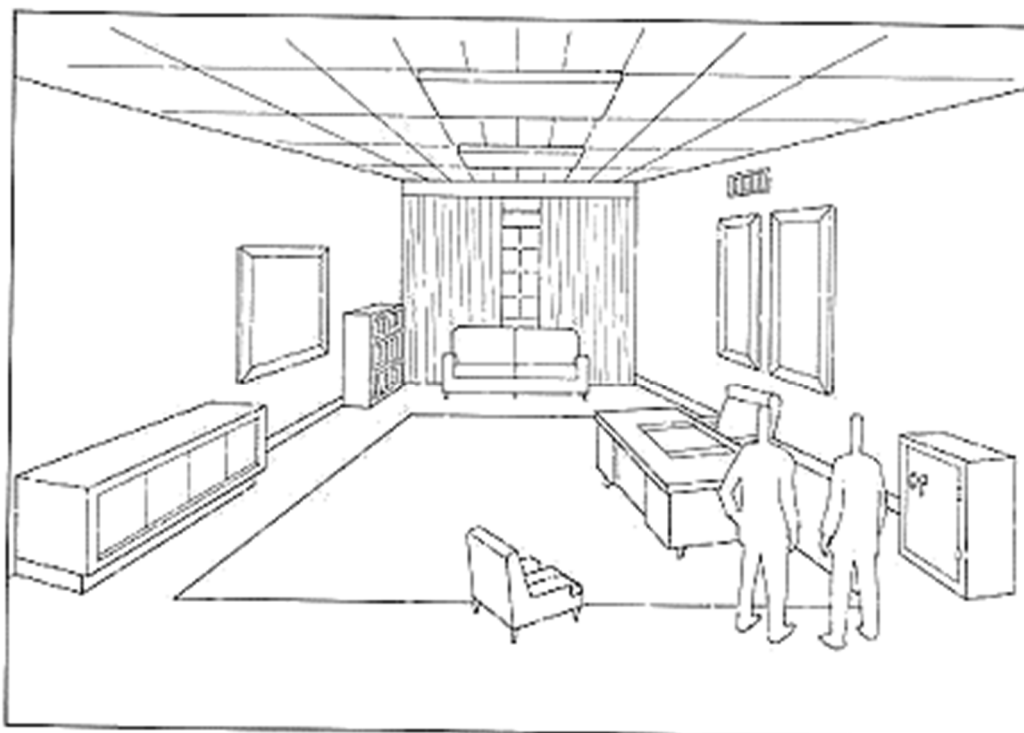
## **Command Center**

Designate a primary location and an alternate location.

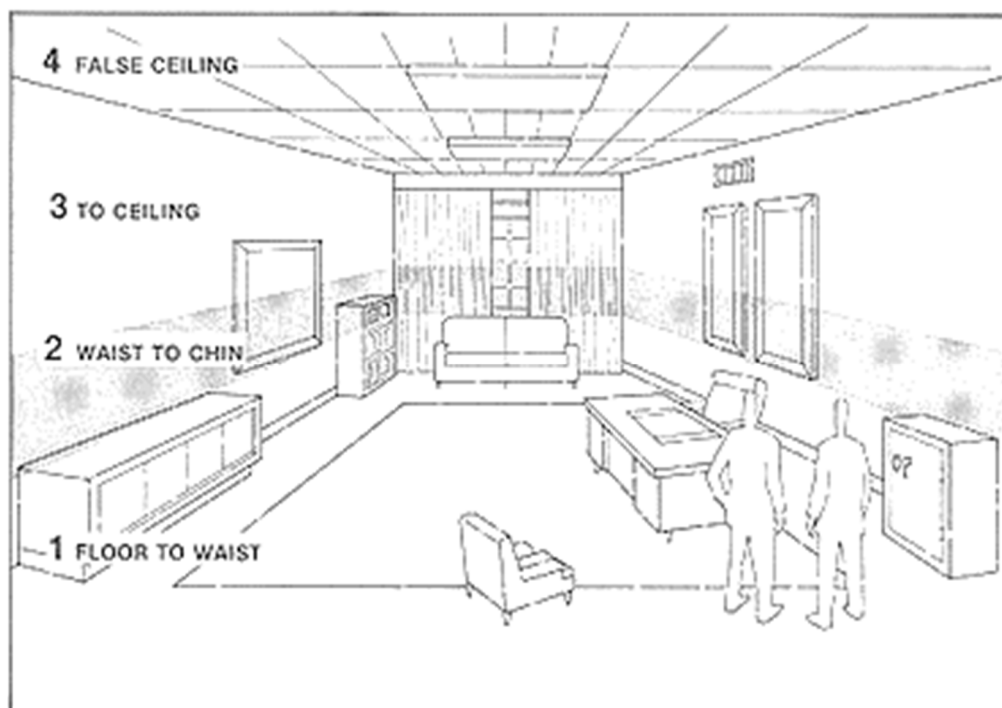
1. Assign personnel and designate decision-making authority.
2. Establish a method for tracking search teams.
3. Maintain a list of likely target areas.
4. Maintain a blueprint of floor diagrams in the center.
5. Establish primary and secondary methods of communication. (Caution-the use of two-way radios during a search can cause premature detonation of an electric blasting cap.)
6. Formulate a plan for establishing a command center, if a threat is received after normal work hours.
7. Maintain a roster of all necessary telephone numbers.



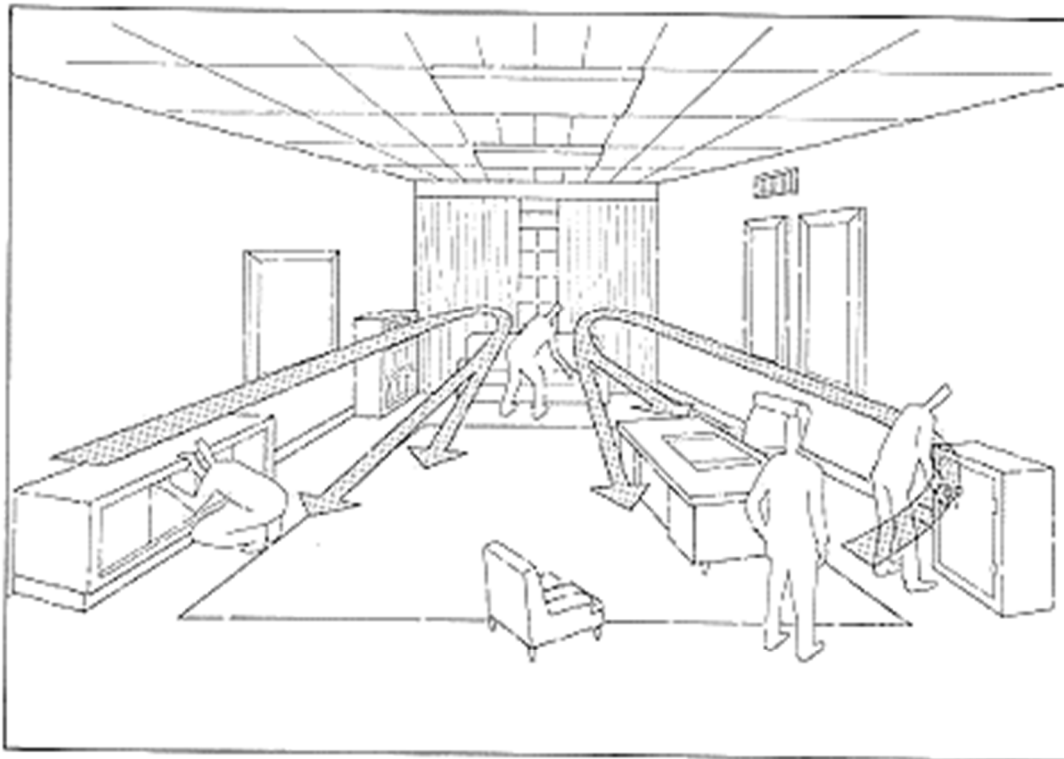
## Bomb Search Illustrations



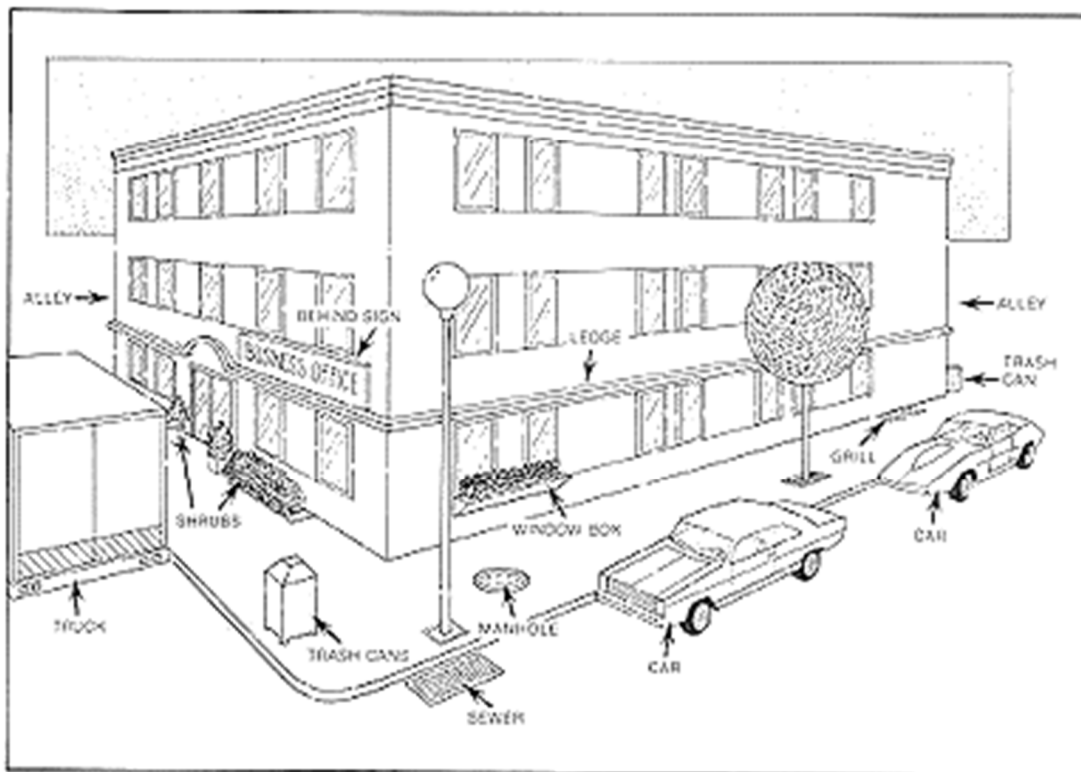
#1 ROOM SEARCH-STOP, LISTEN



#2 DIVIDE ROOM BY HEIGHT FOR SEARCH



#3 SEARCH ROOM BY HEIGHT & ASSIGNED AREA,  
OVERLAP FOR BETTER COVERAGE



#5 SEARCH OUTSIDE AREAS

# ATF BOMB THREAT CHECKLIST

Exact time of call:

Exact words of caller:

## QUESTIONS TO ASK

1. When is bomb going to explode?
2. Where is the bomb?
3. What does it look like?
4. What kind of bomb is it?
5. What will cause it to explode?
6. Did you place the bomb?
7. Why?
8. Where are you calling from?
9. What is your address?
10. What is your name?

## CALLER'S VOICE (circle)

Calm	Slow	Crying	Slurred
Stutter	Deep	Loud	Broken
Giggling	Accent	Angry	Rapid
Stressed	Nasal	Lisp	Excited
Disguised	Sincere	Squeaky	Normal

If voice is familiar, whom did it sound like?

Were there any background noises?

Remarks:

Person receiving call:

Telephone number call received at:

Date:

Report call immediately to:  
(Refer to bomb incident plan)





## Detecting Suspicious Packages/Letters

### REMEMBER

The item does not have to be delivered by a carrier.

Most bombers set up and deliver the bomb themselves.

1. If delivered by carrier, inspect for lumps, bulges, or protrusions, without applying pressure.
2. If delivered by carrier, balance check if lopsided or heavy sided.
3. Handwritten addresses or labels from companies are improper. Check to see if the company exists and if they sent a package or letter.
4. Packages wrapped in string are automatically suspicious, as modern packaging materials have eliminated the need for twine or string.
5. Excess postage on small packages or letters indicates that the object was not weighed by the Post Office.
6. No postage or non-canceled postage.
7. Any foreign writing, addresses, or postage.
8. Handwritten notes, such as: "**To Be Opened in the Privacy of**" "**CONFIDENTIAL**" - "**Your Lucky Day is Here**" - "**Prize Enclosed**".
9. Improper spelling of common names, places, or titles.
10. Generic or incorrect titles.
11. Leaks, stains, or protruding wires, string, tape, etc.
12. Hand delivered or dropped off for a friend packages or letters.
13. No return address or nonsensical return address.
14. Any letters or packages arriving before or after a phone call from an unknown person asking if the item was received.
15. If you have a suspicious letter or package.

Call: 911-ISOLATE-EVACUATE

## Bombs

Bombs can be constructed to look like almost anything and can be placed or delivered in any number of ways.

The probability of finding a bomb that looks like the stereotypical bomb is almost nonexistent. The only common denominator that exists among bombs is that they are designed or intended to explode.



Most bombs are homemade and are limited in their design only by the imagination of, and resources available to, the bomber.

Remember, when searching for a bomb, suspect anything that looks unusual. Let the trained bomb technician determine what is or is not a bomb.

## Pipe bombs: low-tech, lethal tools of terror

July 27, 1996

Web posted at: 10:25 p.m. EDT

ATLANTA (CNN) -- Explosives experts call it an "**anti-personnel fragmentation device**," but in Georgia, the pipe bomb that exploded in Centennial Olympic Park Saturday is an all-too-familiar instrument of terror.

In Georgia, the pipe bomb has a long and murderous history as a low-tech tool of mayhem favored by white supremacists and other political extremists.



Homemade, often sloppy, pipe bombs can be more dangerous than military weapons (CNN)

It was a nail-studded pipe bomb that killed a civil rights attorney in Savannah, Georgia, and a federal judge in neighboring Alabama in 1989. Pipe bombs have also turned up in the arsenals of many of Georgia's homegrown political warriors.

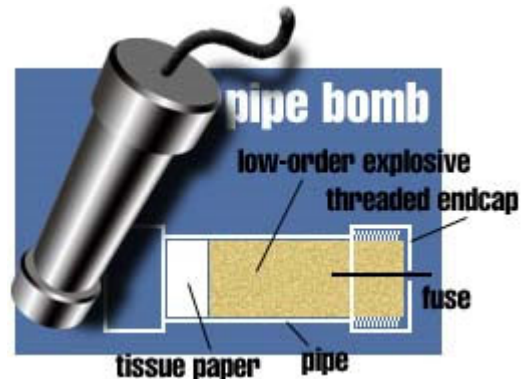
Earlier this year, police arrested three members of a Georgia-based anti-government "**militia**" group amid reports that they may have had plans to attack the Olympic Games. Among the weapons seized in the arrest was a pipe bomb.

### Simple and deadly

A pipe bomb is a fairly simple device -- literally a length of pipe capped at both ends and filled with an explosive.

Often they are packed with nails and screws to heighten damage, as was the case with the pipe bomb that exploded Saturday killing one person and injuring 111 others. A cameraman died of a heart attack after the bombing.

Investigators initially described the bomb as a crude device, although sources tell CNN it contained a timer, which may suggest greater expertise.



Experts warn that simple devices, while not the weapons of sophisticated terrorists, can cause considerable damage.

"The fact that it was an unsophisticated device doesn't mean it was an unsophisticated threat," said security consultant Martin Vitch. **"Even though they may be simple, because (they) are homemade, they are sloppy, and sloppy can make it very, very dangerous."**

The bomb that exploded in the park Saturday was actually three pipe bombs packed with black gun powder, nails and screws, sources told CNN.

**"I would venture to say that that was between two pounds and maybe five or six pounds of explosive,"** said security expert Jack McGeorge. He described the bomb as **"not very big at all."**

Pipe bombs come in all shapes and sizes. They are simple and cheap to make and potentially more unstable than military bombs.

***"Essentially it's a pipe,"*** McGeorge said, ***"a plain old plumbing pipe, threaded ends with caps screwed to both ends. The components are available in any hardware store in the country."***

### **It could happen again**

With bomb instruction manuals available from the Internet or many bookstores, bomb experts say another incident could easily happen again.

The pipes can be filled with low-order gunpowder or higher-order plastique. It can be rigged to go off instantly or with a timer.

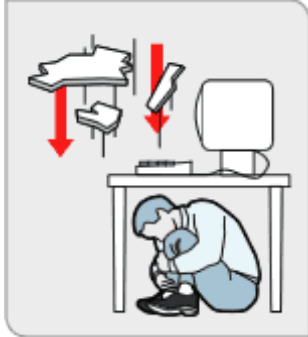
Based on the information investigators have disclosed, the pipe bomb that exploded in Atlanta had little in common with the powerful bombs that destroyed the federal building in Oklahoma City or damaged the World Trade Center in New York -- where shock waves caused most of the damage and deaths.

It was the shrapnel, tiny bits of the bomb itself that caused the most injuries at Olympic Park, according to Vitch. Vitch says there may be more like it out there.

***"I would not be completely surprised if we didn't see another incident before the Olympics are over,"*** he said. ***"This is too rich a target."***



## If there is an explosion...



1. Take shelter against your desk or a sturdy table.



2. Exit the building as quickly as possible.



3. Do not use elevators.



4. Check for fire and other hazards.



5. Take your emergency kit if time allows.



## SUMMARY

The responsibility of the first responder trained to the awareness level is relatively limited when dealing with the incidents being discussed in this course.

A basic consideration is always to help assure the preservation of evidence at the crime scene so as not to impede the investigation or prejudice ensuing litigation. The wisest course of action, although not the easiest, might be to delay entry and await the arrival of more highly trained personnel.

Responders in the habit of making quick responses will need to exercise a great deal of self-control in these situations, especially if human life is at stake. Specific steps that can be taken by the first responder at the awareness level are to isolate the scene, deny entry, notify additional resources, and recognize key indicators of a potential terrorist incident.



---

Bomb Disposal Unit



Contraband  
Interdiction



Obstructed Cargo Area Search  
w/Pole. Quick Connect Trolley  
For Under Vehicle Search (in  
foreground)



Covert Surveillance



WalkAbout with Portable  
Video Microscope

## CHAPTER 4 EXERCISE

This is a chapter review, you can find the final exam on TLC's website under Assignments.

1. Does your department have SOPs/SOGs for incidents involving mass decontamination?
2. Does the jurisdiction's emergency operations plan have such SOPs/SOGs?
3. How would you find out?
4. Obtain a copy of your community's emergency response plan and check that section of the plan dealing with hazard or vulnerability assessment. Do you find anything in the plan that identifies potentially threatening groups?
5. If yes, what are some of the groups named?
6. If none are named, what steps can you take to identify them?
7. Identify six different facilities or elements in your jurisdiction that might be targets of terrorist activities.
8. Do you think the occupants of those facilities really think they are at risk? Why or why not?
9. For each of the facilities you named, use a scale of 1 to 10 to indicate your level of preparedness to respond to a terrorist incident at that facility (1 = low; 10 = high).

Facility 1 \_\_\_ Facility 2 \_\_\_ Facility 3 \_\_\_ Facility 4 \_\_\_ Facility 5 \_\_\_ Facility 6 \_\_\_

#10 Describe one or two practical, achievable steps you will take as a result of studying this Chapter to help you to be better prepared to deal with one of the incidents described here.
Step One:
Step Two:
HOW I WILL ACCOMPLISH STEP ONE

HOW I WILL ACCOMPLISH STEP TWO

LEARNING CHECK

True or False: Circle either T or F.

11. T F At a potential crime scene, it is critical that you disturb the scene as little as possible.
12. T F In responding to an incident other than a natural disaster, first responders could possibly be dealing with a potential crime scene.
13. T F At a potential crime scene, protection of physical evidence is not a concern to first responders.
14. T F The actions of initial responders could in some situations jeopardize the successful prosecution of a crime.
15. T F At a potential crime scene, specific steps that can be taken by the first responder at the awareness level are to isolate the scene, deny entry, and notify additional resources.

***More on the next page***

Multiple Choice: Circle your answer.

16. Of the following incidents involving first responders, the least likely to be a crime scene is
- a. The fourth of six fires in a four-block area in one night.
  - b. Emergency responders respond to a structural collapse immediately following an earthquake.
  - c. EMS personnel administering first aid to burn victims resulting from a Molotov Cocktail.
  - d. Emergency responders are faced with large numbers of patients exhibiting symptoms of pesticide poisoning.
- 
17. A first responder at an explosion that damaged the foundation of a tall office building in a financial district should be primarily concerned about
- a. a secondary explosion.
  - b. a chemical incident.
  - c. mass decontamination.
  - d. numerous fatalities.
- 
18. A terrorism incident ends when
- a. you leave the scene.
  - b. there is successful prosecution of the terrorist(s).
  - c. you finish the incident report.
  - d. you have communicated with law enforcement officials.
- 
19. Hazard assessment includes
- a. threat assessment and risk assessment.
  - b. threat assessment and damage assessment.
-



Prepare redundant power systems. Prepare for a power outage of more than 7 days. Do not keep generators together. Prepare and simulate a complete power/gas/water failure.

Is this power center vulnerable to an attack? No locks or alarms. How about yours?

Right picture, or how about this potable water tank with the ladder access unlocked?



## Chapter 5: Self-Protection

**Section Focus:** You will learn the basics of self-protection and self-preservation. At the end of this section, you the student will be able to understand and describe the protection process. There is a post quiz at the end of this section to review your comprehension and a final examination in the Assignment for your contact hours.

**Scope/Background:** *Self-Protection* includes the types of potential harm encountered at the scene of an incident, and means of protection.



### SELF-PROTECTION

As already mentioned in this course, your self-protection as an initial responder is critical so that you can do your job effectively and not become a victim. Your exercise of sound judgment and use of your personal protective equipment (**PPE**) according to design specifications are your initial steps to protecting yourself.

However, there are various protective countermeasures for the six common types of hazards. In this Chapter you will learn how these countermeasures, depending on the type of incident, are useful allies of the first responder.

## RECOGNIZING HAZARDS AND THEIR PHYSICAL EFFECTS

You could arrive at a potential terrorist incident and not really know what you're up against. Your first concern must be self-protection. You must recognize the various hazards that may be present at any kind of incident: biological, nuclear, incendiary, chemical, or explosive. You need to remember, too, that a single incident can present a variety of hazards, and exposure can be fatal.

One commonly accepted classification identifies six types of harm you can encounter at an incident: thermal, radiological, asphyxiative, chemical, etioloical, and mechanical. The acronym, **TRACEM**, is an easy way to remember them. Since each has different harmful effects, let's take a brief look at each.



## COMMON GENERAL HAZARD SYMBOLS



# TRACEM

## Thermal

Thermal harm is the result of exposure to the extremes of heat and cold. Here we will examine only heat, but cold can be equally harmful. As you have learned elsewhere, heat travels by one of four methods: conduction, convection, radiation, and direct flame contact.

## Radiological

Radiation, as used in this section, refers to nuclear radiation, not radiation as a type of heat transfer. There are three types of nuclear radiation that the first responder should be familiar with: alpha, beta, and gamma. Alpha and beta radiation are found as particles, while gamma radiation is found in the form of rays.

Alpha radiation is the least penetrating of the three, and is not considered dangerous unless alpha-contaminated particles enter the body. Once inside the body, alpha radiation will damage internal organs.

Beta radiation is more penetrating than alpha radiation. Beta-contaminated particles can damage skin tissue, and can harm internal organs if they enter the body.

The use of PPE including SCBA will greatly enhance the emergency responder's safety when dealing with alpha or beta radiation.

Gamma radiation has great penetrating power. Gamma rays are high-energy, ionizing radiation that travel at the speed of light. They can cause skin burns, severely injure internal organs, and have long-term, physiological effects.

---

If your department, utility or jurisdiction is within the evacuation zones of a nuclear generating plant, no doubt there are plans for dealing with a radiological event. You may have received training on how to respond.

You might want to check to see how current the plans are, how recently your jurisdiction has had an exercise, what equipment you have, etc.

Specifically, try to answer these questions.

What standard operating procedures/standard operating guidelines (SOPs/SOGs) exist to protect the responders from radiation in case of an accident?

---

---

---

Does the facility transport its spent nuclear fuels through the jurisdiction? How?

---

---

---

Has the jurisdiction ever had a joint exercise with the facility? [ ] Yes [ ] No

If so, what were some of the lessons learned?

---

---

---

### Asphyxiation

Asphyxiants interfere with oxygen flow during normal breathing. There are two types of asphyxiants: **simple and chemical**.

Simple asphyxiants generally are inert gases that displace the oxygen necessary for breathing, and dilute the oxygen concentration below the level that is useful to the human body.

Chemical asphyxiants are far more serious. Referred to as blood poisons, they are compounds that interrupt the flow of oxygen in the blood or to the tissues. The asphyxiants prevent proper oxygen distribution and starve the body's cells of oxygen.

In all cases, the cells of the body are starved for oxygen. The asphyxiants prevent proper oxygen distribution.

Examples of chemical asphyxiants include hydrogen cyanide (**AC**), cyanogen chloride (**CR**), phosgene, carbon monoxide (**CO**), aniline, and hydrogen sulfide.

List some asphyxiants you have encountered in your experiences as a first responder.

Did you or any of your colleagues suffer harmful effects? [ ] Yes [ ] No

If yes, why?

## Chemical

There are two broad types of chemicals used that can cause harm: toxic and corrosive materials. Both of these can exist as solids, liquids, or gases.

Toxic materials produce harmful effects depending on the concentration of the materials and the length of exposure to them. An individual can have chronic or acute exposures to toxic materials. Nerve agents are examples of toxic materials.

Corrosive materials are liquids or solids causing visible destruction or irreversible alterations in human skin tissue at the site of contact. They may be liquids that have a severe corrosion rate on steel or aluminum. Sulfuric acid is an example of a corrosive material. Blister agents also behave like corrosives.

Of all the hazards that fall under the umbrella of hazardous materials, chemical hazards are probably the ones you most frequently deal with because they are so common.

## Etiological

This type of harm involves exposure to a living microorganism, or its toxin, which causes, or may cause, human disease. Biological agents are the most obvious examples of etiological agents.

Once again, refer to your department's or jurisdiction's emergency response plan.

Is there any provision for dealing with an etiological hazard? [ ] Yes [ ] No

IF THERE IS A PLAN, WHAT PROVISIONS ARE THERE FOR CONTACTING THE NUMEROUS HEALTH AND BIOLOGICAL SERVICES AVAILABLE THROUGH THE STATE AND FEDERAL GOVERNMENTS?

If there is no plan, what are some possible implications for you as an emergency responder?

## Mechanical

This most common type of harm causes trauma from contact with mechanical or physical hazards. One form of mechanical injury can result from an explosive device, in the form of shrapnel or antipersonnel materials, such as nails, contained in the explosion. Advanced planning and forethought are required to avoid this type of harm. Other examples of mechanical harm include routine slip, trip, and fall hazards that are common to emergency response.



***Emergency Preparedness and Response.*** We must prepare to minimize the damage and recover from any future terrorist attacks that may occur despite our best efforts at prevention. An effective response to a major terrorist incident—as well as a natural disaster—depends on being prepared. Therefore, we need a comprehensive national system to bring together and coordinate all necessary response assets quickly and effectively.

## Time, Distance, and Shielding (TDS)--The Keys to Self-protection

Much of the traditional training in hazardous materials response builds on these three methods, even though often the explicit link is not made.

### Time

You should spend the shortest amount of time possible in the hazard area and minimize the time of exposure to the hazard. Time is an ally when the hazard can be expected to become gradually less hazardous. Use time to protect yourself at a crime scene. Use techniques such as rapid entries to execute reconnaissance or rescue. Minimizing time spent in the affected area also will reduce the chance of contaminating the crime scene.



### Distance

Whenever you can distance yourself from the hazard, you should. It should be an absolute rule always to maintain a safe distance from the hazard area or projected hazard area.



Use of the Table of Initial Isolation and Protective Action Distances as found in the North American Emergency Response Guidebook (**NAERG**) is advisable. Remember that the greater the distance from the source of harm, the less the exposure. Finally, it is advisable to be upwind and uphill of the source, if at all possible.

### Shielding

As it makes good sense for you to let time and distance work in your favor, maintaining significant physical barriers between you and the hazard makes equally good sense. Shielding can take various forms: vehicles, buildings, walls, personal protective equipment (**PPE**), etc. Use of PPE, including SCBA, will greatly increase your chances of a safe and successful response.

However, you need to remember that no matter how much shielding is available and how safe you think it is, always take full advantage of time and distance.

### Implementing the Protective Measures of Time, Distance, and Shielding

#### WHAT IS THE APPROPRIATE COURSE OF ACTION FOR YOU TO AVOID THE RANGE OF POTENTIAL HAZARDS AT TERRORIST INCIDENTS?

#### Recognizing Psychological Effects

As with any mass casualty/fatality incident, the psychological effect on first responders is an issue that must be addressed. Some individuals may be unable to deal with the trauma involved in the incident. In such a case, appropriate psychological assistance, debriefing, and alternate work assignments can be helpful in handling individual needs. Most emergency response agencies have assistance available to personnel in the areas of critical incident stress and post-traumatic types of incidents.

## SUMMARY

When dealing with a potential terrorist incident, you are facing something unusual, something that, perhaps, you never have faced before. This could prove fatal, given the potential complexity of hazards and the specialized response skills needed. The situation may require atypical responses.

Before making any kind of response, you should evaluate the types of hazards involved and match to them the most appropriate response methods available to you.



Ask your local police department to assist you in drills and evaluations. Usually the police and state agencies will assist you and have funds set aside just for first response practice drills. There are several Homeland Security grants available for training and equipment, like: satellite telephones, Level A suits, decontamination equipment and training. Most police officers love to play cops and terrorists.

## CHAPTER 5 EXERCISE

This is a chapter review, you can find the final exam on TLC's website under Assignments.

### LEARNING CHECK

#### True or False: Circle either T or F.

1.    T    F    The harmful effects of etiologic hazards usually result from interference with oxygen flow during normal breathing.
2.    T    F    Gamma radiation is a type of asphyxiative hazard.
3.    T    F    Whenever you can distance yourself from a hazard you should.
4.    T    F    Asphyxiants are liquids or solids that usually cause visible destruction or irreversible alterations in human skin tissue at the site of contact.

#### MULTIPLE CHOICE: CIRCLE YOUR ANSWER.

5.    Hazard causing first responders the most injury.
  - a.    Thermal.
  - b.    Chemical.
  - c.    Biological.
  - d.    Mechanical.
6.    When in a hazardous area, responders should avoid
  - a.    rushing.
  - b.    wearing PPE.
  - c.    shielding.
  - d.    self-protection.
7.    When determining a safe distance from a projected hazard area, responders should refer to the Table of Initial Isolation and Protection Action Distances as found in the
  - a.    SOP.
  - b.    SOG.
  - c.    NAERG.
  - d.    RUN.
8.    PPE provides critical shielding during
  - a.    situations involving radioactive materials only.
  - b.    all hazard situations.
  - c.    situations involving toxic materials only.
  - d.    most hazard situations.

9. The responder's safest position at an incident scene is
  - a. upwind and uphill.
  - b. upwind and downhill.
  - c. crosswind and uphill.
  - d. downwind and downhill.
  
10. Which of the following is an example of inappropriate shielding?
  - a. Vehicles.
  - b. Wire fencing.
  - c. Walls.
  - d. Buildings.



### **Special Operation Team**

As you have read in the newspapers, these highly trained individuals have been practicing for every type of event, from school shootings to presidential protection. You will usually find ex-military personnel in these units. You will also find the use of dogs as part of a Special Operations Team.

One problem with highly trained operators as in the above photo, once in a while, one of these people will wash out of the police or fire program and have the training and skills and possibly enough personal problems to use their training against your facility. Public safety officials do not like to discuss this matter, but some officers do washout of the system and make excellent terrorists.



## Chapter 6: Emergency Planning

**Section Focus:** You will learn the basics of emergency planning. At the end of this section, you the student will be able to understand and describe emergency planning for utilities. There is a post quiz at the end of this section to review your comprehension and a final examination in the Assignment for your contact hours.

**Scope/Background:** *Scene Control* describes initial response and arrival considerations and the appropriate course of action for scene isolation and evacuation.



### Emergency Planning

#### **4 STEPS IN THE PLANNING PROCESS**

**Step 1 -- Establish a Planning Team**

**Step 2 -- Analyze Capabilities and Hazards**

**Step 3 -- Develop the Plan**

**Step 4 -- Implement the Plan**

**STEP 1 -- ESTABLISH A PLANNING TEAM.** There must be an individual or group in charge of developing the emergency management plan. The following is guidance for making the appointment.

1. **Form the Team** - the size of the planning team will depend on the facility's operations, requirements and resources. Usually involving a group of people is best because:
  - a. It encourages participation and gets more people invested in the process.
  - b. It increases the amount of time and energy participants are able to give.

- c. It enhances the visibility and stature of the planning process.
- d. It provides for a broad perspective on the issues.

Determine who can be an active member and who can serve in an advisory capacity. In most cases, one or two people will be doing the bulk of the work. At the very least, you should obtain input from all functional areas:

- a. Upper management
- b. Line management
- c. Labor
- d. Human Resources
- e. Engineering and maintenance
- f. Safety, health and environmental affairs
- g. Public information officer
- h. Security
- i. Community relations
- j. Sales and marketing
- k. Legal
- l. Finance and purchasing

Have participants appointed in writing by upper management. Their job descriptions could also reflect this assignment.

**2. Establish Authority** - demonstrate management's commitment and promote an atmosphere of cooperation by "authorizing" the planning group to take the steps necessary to develop a plan. The group should be led by the chief executive or the plant manager. Establish a clear line of authority between group members and the group leader, though not so rigid as to prevent the free flow of ideas.

**3. Issue a Mission Statement** - have the chief executive or plant manager issue a mission statement to demonstrate the company's commitment to emergency management. The statement should:

Define the purpose of the plan and indicate that it will involve the entire organization

#### **Define the authority and structure of the planning group**

**4. Establish a Schedule and Budget** - establish a work schedule and planning deadlines. Timelines can be modified as priorities become more clearly defined. Develop an initial budget for such things as research, printing, seminars, consulting services and other expenses that may be necessary during the development process.

**STEP 2 -- ANALYZE CAPABILITIES AND HAZARDS.** This step entails gathering information about current capabilities and about possible hazards and emergencies, and then conducting a vulnerability analysis to determine the facility's capabilities for handling emergencies.



## **FBI: 100 Percent Chance of WMD Attack**

Feb. 14, 2011

***By Ronald Kessler***

The probability that the U.S. will be hit with a weapons of mass destruction attack at some point is 100 percent, Dr. Vahid Majidi, the FBI's assistant director in charge of the FBI's Weapons of Mass Destruction Directorate, tells Newsmax.

Such an attack could be launched by foreign terrorists, lone wolves who are terrorists, or even by criminal elements, Majidi says. It would most likely employ chemical, biological, or radiological weapons rather than a nuclear device.

As it is, Majidi says, American intelligence picks up hundreds of reports each year of foreign terrorists obtaining WMD. When American forces invaded Afghanistan, they found that al-Qaida was working on what Majidi calls a "nascent" weapons of mass destruction effort involving chemical and biological weapons.

In every other case so far, the reports of foreign terrorists obtaining WMD have turned out to be unfounded. However, Majidi's directorate within the FBI investigates more than a dozen cases in the U.S. each year where there was intent to use WMD. For example, in 2008, the FBI arrested Roger Bergendorff, who was found to have ricin and anarchist literature. Ricin kills cells by inhibiting protein synthesis. Within several days, the liver, spleen, and kidneys of a person who inhales or ingests ricin stop working, resulting in death.

"The notion of probability of a WMD attack being low or high is a moot point because we know the probability is 100 percent," Majidi says. "We've seen this in the past, and we will see it in the future. There is going to be an attack using chemical, biological or radiological material."

Even a WMD attack that does not kill a great number of people would have a crushing psychological impact. "A singular lone wolf individual can do things in the dark of the night with access to a laboratory with low quantities of material and could hurt a few people but create a devastating effect on the American psyche," Majidi says.

As described by Majidi, who was previously the chemistry division leader at Los Alamos

National Laboratory, the WMD Directorate was established in 2006 to coordinate all elements of the FBI that deal with WMD cases. Regarding a subject that is full of hype and misinformation, it is rare for an official who is an expert in the field and has full access to current classified information to talk about it for publication. Majidi says the kind of threat that keeps him awake at night is one from a lone wolf. That's because the FBI, along with the CIA and foreign partners, has developed a number of ways to detect plots by al-Qaida and other foreign terrorists. Besides intercepting their communications and infiltrating their organizations, the FBI gets reports when people purchase materials that could be used in a WMD attack. These techniques are known as trip wires.

For my book "The Terrorist Watch: Inside the Desperate Race to Stop the Next Attack," Arthur M. "Art" Cummings II, who headed FBI counterterrorism and counterintelligence investigations, gave an example of the FBI's use of trip wires. When the FBI got a report of a man buying chemicals that could be used for explosives, it investigated. In this case, it would have been easy to dismiss the purchases as innocent, since the man was buying the supplies from a swimming pool company, and his business shipped pool supplies.

"That explanation wasn't good enough," Cummings says. "It's not OK to say, 'It looks like pool supplies, we're done. You don't finish there. Who at the pool company, specifically, did he buy them from? What specifically was the transaction, and what happened from there? Is it a friend; is it an associate; is it somebody who wants to do us harm? There was a day we would have said, 'It's a commercial transaction, don't worry about it. Each and every lead is followed all the way down to the most minute detail.'"

Majidi says three agents from his directorate have been assigned to FBI offices overseas — known as legal attaché offices or legats — in countries like Georgia to work with foreign intelligence authorities on possible attacks. Currently, Majidi is working to develop ways to detect development of new organisms that could be used in a biological attack. By definition, there would be no way to detect a new organism or to develop an antidote before it is unleashed.

"We are not sitting on our hands waiting to predict what will happen based on what happened yesterday," Majidi says. As an example, he says, "You can design an organism de novo that never existed before. While there is no known articulated threat, this is something that we feel is a technology or science that potentially can be misused, either accidentally or on purpose."

The FBI is working with the synthetic biology community to develop ways to zero in on any hint that someone could be developing such an organism that could become a threat. "We're not there to stop the science but to integrate our activities within their portfolio so that when the threat does develop or may develop over a long arc of time, we are ahead of those issues," Majidi explains.

Majidi says the most remote threat is an attack with a nuclear device. A terrorist bent on detonating a nuclear weapon would have to successfully negotiate a series of steps, Majidi says. He would have to find an expert with the right knowledge. He would have to find the right material. He would have to bring the device into the country, and he would have to evade detection programs. "While the net probability is incredibly low, a 10 kiloton device would be of enormous consequence," Majidi says. "So even with those enormously low probabilities, we still have to have a very effective and integrated approach trying to fight the possibility."

Experts are constantly being quoted with estimates of the amount of enriched uranium that could be unaccounted for from Soviet Union stockpiles and could be used to make nuclear weapons. Majidi says no one knows the actual amount. "I know there is a hobby of guessing, and different folks give you a different number," he says. "All I can tell you is that from the interdictions that we have had in the past decade, the quantities have been sufficient of highly enriched uranium that I clearly worry about this material on a global scale. How much is there? Any amount is too much."

A terrorist who stole a nuclear weapon from a country that has one would have an easier time than if he tried to make one. "One of the things you have to understand is that nuclear markets are very ambiguous markets," Majidi says. "There are as many bad guys trying to sell material as there are good guys trying to make sure that that doesn't happen." While terrorists talk about using WMD, the preferred method for attack so far has been explosives. Majidi cites two examples: the Christmas Day bomber, Umar Farouk Abdulmutallab, a Nigerian citizen who boarded a Northwest Airlines flight to Detroit on Dec. 25, 2009, and tried to detonate explosives sewn into his underwear; and the Times Square bomber, Faisal Shahzad, a Pakistani immigrant who attempted to set off a car bomb in Times Square.

"While all of these guys are still interested in potentially using chemical, biological, or radiological weapons wherever it is possible, the pragmatic approach that they have taken is to use what has worked for them best, which is various forms of explosives and improvised explosives," Majidi says. "The latest round is concealing explosives coming through the commercial shipping environment," Majidi notes. "That brings to the fore the fact that explosives are something that we're not going to get away from any time soon. It's the modality that is most often preferred by a pragmatic adversary."

Given the sensitivity and complexity of the subject, Majidi says he tries to present all the issues in context: "One of my jobs is to make sure I put all of these things in an appropriate light, because if you were in my job you would see that everyone always tries to elevate things to a tremendous level." Of one thing Majidi is sure: "There's a probability of 100 percent that a WMD event will happen."

## **Man Who Plotted Terror Attack Sentenced to Life**

NEW YORK – An immigrant from Guyana, accused of planning an attack against gasoline mains that supply airplanes at New York’s John F. Kennedy International Airport, was sentenced to life imprisonment by a federal judge.

Russell Defreitas, a former cargo handler at JFK, was found guilty last year along with Guyanese politico Abdul Kadir, who has also been given a life sentence.

Prosecutors said that Defreitas and Kadir belonged to a “terrorist cell of Islamist extremists” which since January 2006 had been gathering photos and videos to plan the attack, and which was in its initial phase when they were arrested.

The plotters intended to cause a series of explosions in the pipelines that supply JFK and which cross New York.

These gasoline mains are some 60 kilometers (37 miles) long, beginning in the state of New Jersey and going through the boroughs of Staten Island and Brooklyn before finally reaching La Guardia and JFK airports, both in Queens.

The authorities detected the plan thanks to a convicted drug dealer acting as an informant for the FBI, who struck up several conversations with the accused.

In one of those conversations, according to the complaint, Defreitas said that “anytime you hit Kennedy, it is the most hurtful thing to the United States.” He also said that the destruction would have been greater than the attacks on Sept. 11, 2001. EFE

## **2011 January Snow Storm Exposes Flaws Ideal for Terrorist Attack**

WASHINGTON, DC (WUSA) -- Not a month has passed since a January 26 snow storm crippled much of the Washington Metro area. Now, among other flaws a failure in communication with 9-1-1 calls is coming under the criticism of many including officials with the Federal Communications Commission.

Various jurisdictions including DC, and Montgomery County are reporting that during the height of the storm, many 9-1-1 emergency calls made by cell phones went dead. The callers heard busy signals, and in other cases, nothing at all. Emergency officials say the disruption in communication was caused by Verizon wireless trunk lines that went down as a result of an extremely high call volume and snow damage to actual phone towers and lines.

Jamie Barnett, the chief of the FCC public safety and homeland security bureau said that problem may be occurring nationwide. In Washington, a local anti-terrorism expert says failed 9-1-1 calls are a clear weakness that could be exploited by those wanting to cause us harm.

"We still don't have the communications systems we need with ordinary people. The system is going to go down if it gets overloaded. That's just a fact," Neil Livingstone said. "We should be looking at snow storms as an opportunity to test and perfect our systems. If we can't handle a snow storm, there is a very good likelihood that we can't handle a terrorist attack, and that's the problem."

Another example of public safety vulnerabilities exposed during the snow storm, he said, is the massive grid lock that congested roads and streets throughout Washington and surrounding cities. He said that is a clear indication of how chaotic an evacuation may be in the event of a catastrophic event. According to Livingstone, that's something else that is of interest to terrorist.

While emergency agencies work to solve the problem of 9-1-1 calls, Livingstone told 9NEWS NOW, "It's not a matter of if, but a matter of when" about the possibility of terrorist striking again. He said Washington remains a top target.





## WHERE DO YOU STAND RIGHT NOW?

### Review Internal Plans and Policies

Documents to look for include:

- a. Evacuation plan
- b. Fire protection plan
- c. Safety and health program
- d. Environmental policies
- e. Security procedures
- f. Insurance programs
- g. Finance and purchasing procedures
- h. Plant closing policy
- i. Employee manuals
- j. Hazardous materials plan
- k. Process safety assessment
- l. Risk management plan
- m. Capital improvement program
- n. Mutual aid agreements



### 1. Meet with Outside Groups

Meet with government agencies, community organizations and utilities. Ask about potential emergencies and about plans and available resources for responding to them. Sources of information include:

- a. Community emergency management office
- b. Mayor or Community Administrator's office
- c. Local Emergency Planning Committee (LEPC)
- d. Fire Department
- e. Police Department
- f. Emergency Medical Services organizations
- g. American Red Cross
- h. National Weather Service
- i. Public Works Department
- j. Planning Commission
- k. Telephone companies
- l. Electric utilities
- m. Neighboring businesses

*Think about this item and remember 911 and future attacks or emergencies... While researching potential emergencies, one facility discovered that a dam -- 50 miles away -- posed a threat to its community. The facility was able to plan accordingly.*

### 2. Identify Codes and Regulations

Identify applicable Federal, State and local regulations such as:

- a. Occupational safety and health regulations
  - b. Environmental regulations
  - c. Fire codes
  - d. Seismic safety codes
  - e. Transportation regulations
  - f. Zoning regulations
  - g. Corporate policies

### 3. **Identify Critical Products, Services and Operations**

You'll need this information to assess the impact of potential emergencies and to determine the need for backup systems. Areas to review include:

- a. Company products and services and the facilities and equipment needed to produce them
- b. Products and services provided by suppliers, especially sole source vendors
- c. Lifeline services such as electrical power, water, sewer, gas, telecommunications and transportation
- d. Operations, equipment and personnel vital to the continued functioning of the facility

### 4. **Identify Internal Resources and Capabilities**

Resources and capabilities that could be needed in an emergency include:

- a. **Personnel** -- fire brigade, hazardous materials response team, emergency medical services, security, emergency management group, evacuation team, public information officer
- b. **Equipment** -- fire protection and suppression equipment, communications equipment, first aid supplies, emergency supplies, warning systems, emergency power equipment, decontamination equipment
- c. **Facilities** -- emergency operating center, media briefing area, shelter areas, first-aid stations, sanitation facilities
- d. **Organizational capabilities** -- training, evacuation plan, employee support system
- e. **Backup systems** -- arrangements with other facilities to provide for:
  - (1) Payroll
  - (2) Communications
  - (3) Production
  - (4) Customer services
  - (5) Shipping and receiving
  - (6) Information systems support
  - (7) Emergency power
  - (8) Recovery support

*Think about this item and remember 911 and future attacks or emergencies...*

One way to increase response capabilities is to identify employee skills (medical, engineering, communications, foreign language) that might be needed in an emergency.

#### **Identify External Resources**

There are many external resources that could be needed in an emergency. In some cases, formal agreements may be necessary to define the facility's relationship with the following:

- a. Local emergency management office
- b. Fire Department
- c. Hazardous materials response organization
- d. Emergency medical services
- e. Hospitals
- f. Local and State police
- g. Community service organizations
- h. Utilities
- i. Contractors
- j. Suppliers of emergency equipment and Insurance carriers

- **Do an Insurance Review**

Meet with insurance carriers to review all policies. (See Section 2: Recovery and Restoration.)

- **Conduct a vulnerability analysis**

The next step is to assess the vulnerability of your facility -- the probability and potential impact of each emergency. Use the Vulnerability Analysis Chart in the appendix section to guide the process, which entails assigning probabilities, estimating impact and assessing resources, using a numerical system. The lower the score the better.

- **List Potential Emergencies**

In the first column of the chart, list all emergencies that could affect your facility, including those identified by your local emergency management office. Consider both:

- a. Emergencies that could occur within your facility
- b. Emergencies that could occur in your community

*Below are some other factors to consider:*

**Historical** -- What types of emergencies have occurred in the community, at this facility and at other facilities in the area?

- a. Fires
- b. Severe weather
- c. Hazardous material spills
- d. Transportation accidents
- e. Earthquakes
- f. Hurricanes
- g. Tornadoes
- h. Terrorism
- i. Utility outages
- j. Backflow

**Geographic** -- What can happen as a result of the facility's location? Keep in mind:

- a. Proximity to flood plains, seismic faults and dams
- b. Proximity to companies that produce, store, use or transport hazardous materials
- c. Proximity to major transportation routes and airports
- d. Proximity to nuclear power plants

**Technological** -- What could result from a process or system failure? Possibilities include:

- a. Fire, explosion, hazardous materials incident
- b. Safety system failure
- c. Telecommunications failure
- e. Computer system failure
- f. Power failure
- g. Heating/cooling system failure
- h. Emergency notification system failure

**Human Error** -- What emergencies can be caused by employee error? Are employees trained to work safely? Do they know what to do in an emergency?

Human error is the single largest cause of workplace emergencies and can result from:

- a. Poor training
- b. Poor maintenance
- c. Carelessness
- d. Misconduct
- e. Substance abuse
- f. Fatigue

**Physical** -- What types of emergencies could result from the design or construction of the facility? Does the physical facility enhance safety? Consider:

- a. The physical construction of the facility
- b. Hazardous processes or byproducts
- c. Facilities for storing combustibles
- d. Layout of equipment
- e. Lighting
- f. Evacuation routes and exits
- g. Proximity of shelter areas

**Regulatory** -- What emergencies or hazards are you regulated to deal with? Analyze each potential emergency from beginning to end. Consider what could happen as a result of:

- a. Prohibited access to the facility
- b. Loss of electric power
- c. Communication lines down
- e. Ruptured gas mains
- f. Water damage
- g. Smoke damage
- h. Structural damage
- i. Air or water contamination
  - j. Explosion
  - k. Building collapse
  - l. Trapped persons
  - m. Chemical release

- **Estimate Probability**

In the Probability column, rate the likelihood of each emergency's occurrence. This is a subjective consideration, but useful nonetheless.

Use a simple scale of 1 to 5 with 1 as the lowest probability and 5 as the highest.

- **Assess the Potential Human Impact**

Analyze the potential human impact of each emergency -- the possibility of death or injury. a 1 to 5 scale with 1 as the lowest impact and 5 as the highest.

- **Assess the Potential Property Impact**

Consider the potential property for losses and damages. Again, assign a rating in the Property Impact column, 1 being the lowest impact and 5 being the highest.

## **Considerations**

- a. Cost to replace**
- b. Cost to set up temporary replacement**
- c. Cost to repair**

*Think about this item and remember 911 and future attacks or emergencies...*  
A bank's vulnerability analysis concluded that a "small" fire could be as catastrophic to the business as a computer system failure. The planning group discovered that bank employees did not know how to use fire extinguishers, and that the bank lacked any kind of evacuation or emergency response system.

- **Assess the Potential Business Impact**

Consider the potential loss of market share. Assign a rating in the Business Impact column. Again, 1 is the lowest impact and 5 is the highest. Assess the impact of:

- a. Business interruption
- b. Employees unable to report to work
- c. Customers unable to reach facility
- d. Company in violation of contractual agreements
- e. Imposition of fines and penalties or legal costs
- f. Interruption of critical supplies
- g. Interruption of product distribution

- **Assess Internal and External Resources**

Next, assess your resources and ability to respond. Assign a score to your Internal Resources and External Resources. The lower the score the better.

To help you do this, consider each potential emergency from beginning to end and each resource that would be needed to respond. For each emergency ask these questions:

- Do we have the needed resources and capabilities to respond?
  - Will external resources be able to respond to us for this emergency as quickly as we may need them, or will they have other priority areas to serve?
- a. Develop additional emergency procedures
  - b. Conduct additional training
  - c. Acquire additional equipment
  - d. Establish mutual aid agreements
  - e. Establish agreements with specialized contractors

- **Add the Columns**

Total the scores for each emergency. The lower the score the better. While this is a subjective rating, the comparisons will help determine planning and resource priorities -- the subject of the pages to follow.

*Think about this item and remember 911 and future attacks or emergencies...*

When assessing resources, remember that community emergency workers -- police, paramedics, firefighters -- will focus their response where the need is greatest. Or they may be victims themselves and be unable to respond immediately. That means response to your facility may be delayed.



## STEP 3 -- DEVELOP THE PLAN

You are now ready to develop an emergency management plan. This section describes how.

### PLAN COMPONENTS

Your plan should include the following basic components.

#### 1. Executive Summary

The executive summary gives management a brief overview of the purpose of the plan; the facility's emergency management policy; authorities and responsibilities of key personnel; the types of emergencies that could occur; and where response operations will be managed.

#### 2. Emergency Management Elements

This section of the plan briefly describes the facility's approach to the core elements of emergency management, which are:

- a. Direction and control
- b. Communications
- c. Life safety
- d. Property protection
- e. Community outreach
- f. Recovery and restoration
- g. Administration and logistics.

These elements, which are described in detail in Section 2, are the foundation for the emergency procedures that your facility will follow to protect personnel and equipment and resume operations.

#### 3. Emergency Response Procedures

The procedures spell out how the facility will respond to emergencies. Whenever possible, develop them as a series of checklists that can be quickly accessed by senior management, department heads, response personnel and employees.

#### Determine what actions would be necessary to:

- a. Assess the situation
- b. Protect employees, customers, visitors, equipment, vital records and other assets, particularly during the first three days
- c. Get the business back up and running.



**Specific procedures** might be needed for any number of situations such as bomb threats or tornadoes, and for such functions as:

- a. Warning employees and customers
- b. Communicating with personnel and community responders
- c. Conducting an evacuation and accounting for all persons in the facility
- d. Managing response activities
- e. Activating and operating an emergency operations center
- f. Fighting fires
- g. Shutting down operations
- h. Protecting vital records
- i. Restoring operations

#### **4. Support Documents**

**Documents that could be needed in an emergency include:**

**Emergency call lists** -- lists (wallet size if possible) of all persons on and off site who would be involved in responding to an emergency, their responsibilities and their 24-hour telephone numbers

**Building and site maps that indicate:**

- a. Utility shutoffs
- b. Water hydrants
- c. Water main valves
- d. Water lines
- e. Gas main valves
- f. Gas lines
- g. Electrical cutoffs
- h. Electrical substations
- i. Storm drains
- j. Sewer lines
- k. Location of each building (include name of building, street name and number)
- l. Floor plans
- m. Alarm and enunciators
- n. Fire extinguishers
- o. Fire suppression systems
- p. Exits
- q. Stairways
- r. Designated escape routes
- s. Restricted areas
- t. Hazardous materials (including cleaning supplies and chemicals)
- u. High-value items

**Resource lists** -- lists of major resources (equipment, supplies, services) that could be needed in an emergency; mutual aid agreements with other companies and government agencies.

*Think about this item and remember 911 and future attacks or emergencies...*

In an emergency, all personnel should know:

1. What is my role?
2. Where should I go?



**Some facilities are required to develop:**

1. Emergency escape procedures and routes
2. Procedures for employees who perform or shut down critical operations before an evacuation
3. Procedures to account for all employees, visitors and contractors after an evacuation is completed
4. Rescue and medical duties for assigned employees
5. Procedures for reporting emergencies
6. Names of persons or departments to be contacted for information regarding the plan

**THE DEVELOPMENT PROCESS**

The following is guidance for developing the plan.

**1. Identify Challenges and Prioritize Activities**

Determine specific goals and milestones. Make a list of tasks to be performed, by whom and when. Determine how you will address the problem areas and resource shortfalls that were identified in the vulnerability analysis.

**2. Write the Plan**

Assign each member of the planning group a section to write. Determine the most appropriate format for each section.

**Establish an aggressive timeline** with specific goals. Provide enough time for completion of work, but not so much as to allow assignments to linger. Establish a schedule for:

- a. First draft
- b. Review
- c. Second draft
- d. Tabletop exercise
- e. Final draft
- f. Printing
- g. Distribution

**3. Establish a Training Schedule**

Have one person or department responsible for developing a training schedule for your facility. For specific ideas about training, refer to Step 4.

**4. Coordinate with Outside Organizations**

Meet periodically with local government agencies and community organizations. Inform appropriate government agencies that you are creating an emergency management plan.

While their official approval may not be required, they will likely have valuable insights and information to offer.

**Determine State** and local requirements for reporting emergencies, and incorporate them into your procedures.

**Determine protocols** for turning control of a response over to outside agencies. Some details that may need to be worked out are:

- a. Which gate or entrance will responding units use?
  - b. Where and to whom will they report?
  - c. How will they be identified?
  - d. How will facility personnel communicate with outside responders?
  - e. Who will be in charge of response activities?
- Determine what kind of identification authorities will require to allow your key personnel into your facility during an emergency.

*Think about this item and remember 911 and future attacks or emergencies...*  
Determine the needs of disabled persons and non-English-speaking personnel. For example, a blind employee could be assigned a partner in case an evacuation is necessary.

The Americans with Disabilities Act (**ADA**) defines a disabled person as anyone who has a physical or mental impairment that substantially limits one or more major life activities, such as seeing, hearing, walking, breathing, performing manual tasks, learning, caring for oneself or working.

*Think about this item and remember 911 and future attacks or emergencies...*  
Your emergency planning priorities may be influenced by government regulation. To remain in compliance you may be required to address specific emergency management functions that might otherwise be a lower priority activity for that given year.

## **5. Maintain Contact with Other Corporate Offices**

Communicate with other offices and divisions in your company to learn:

- a. Their emergency notification requirements
- b. The conditions where mutual assistance would be necessary
- c. How offices will support each other in an emergency
- d. Names, telephone numbers and pager numbers of key personnel

Incorporate this information into your procedures.

## **6. Review, Conduct Training and Revise**

Distribute the first draft to group members for review. Revise as needed.

For a second review, conduct a tabletop exercise with management and personnel who have a key emergency management responsibility. In a conference room setting, describe an emergency scenario and have participants discuss their responsibilities and how they would react to the situation.

Based on this discussion, identify areas of confusion and overlap, and modify the plan accordingly.

## **7. Seek Final Approval**

Arrange a briefing for the chief executive officer and senior management and obtain written approval.

## **8. Distribute the Plan**

Place the final plan in three-ring binders and number all copies and pages. Each individual who receives a copy should be required to sign for it and be responsible for posting subsequent changes.

Determine which sections of the plan would be appropriate to show to government agencies (some sections may refer to corporate secrets or include private listings of names, telephone numbers or radio frequencies). Distribute the final plan to:

- a. Chief executive and senior managers
- b. Key members of the company's emergency response organization
- c. Company headquarters
- d. Community emergency response agencies (appropriate sections)

Have key personnel keep a copy of the plan in their homes. Inform employees about the plan and training schedule.

*Think about this item and remember 911 and future attacks or emergencies...* Consolidate emergency plans for better coordination. Stand-alone plans, such as a Spill Prevention Control and Countermeasures (**SPCC**) plan, fire protection plan or safety and health plan, should be incorporated into one comprehensive plan.

## **STEP 4 -- IMPLEMENT THE PLAN.**

Implementation means more than simply exercising the plan during an emergency. It means acting on recommendations made during the vulnerability analysis, integrating the plan into company operations, training employees and evaluating the plan.

## **INTEGRATE THE PLAN INTO COMPANY OPERATIONS**

Emergency planning must become part of the corporate culture.

Look for opportunities to build awareness; to educate and train personnel; to test procedures; to involve all levels of management, all departments and the community in the planning process; and to make emergency management part of what personnel do on a day-to-day basis.

### **Test How Completely The Plan Has Been Integrated By Asking:**

- a. How well does senior management support the responsibilities outlined in the plan?
- b. Have emergency planning concepts been fully incorporated into the facility's accounting, personnel and financial procedures?
- c. How can the facility's processes for evaluating employees and defining job classifications better address emergency management responsibilities?
- d. Are there opportunities for distributing emergency preparedness information through corporate newsletters, employee manuals or employee mailings?
- e. What kinds of safety posters or other visible reminders would be helpful?
- f. Do personnel know what they should do in an emergency?
- g. How can all levels of the organization be involved in evaluating and updating the plan?

## **CONDUCT TRAINING, DRILLS AND EXERCISES**

Everyone who works at or visits the facility requires some form of training. This could include periodic employee discussion sessions to review procedures, technical training in equipment use for emergency responders, evacuation drills and full-scale exercises. On the next page are basic considerations for developing a training plan.



## Planning Considerations

Assign responsibility for developing a training plan. Consider the training and information needs for employees, contractors, visitors, managers and those with an emergency response role identified in the plan.

### **Determine for a 12 month period:**

- a. Who will be trained?
- b. Who will do the training?
- c. What training activities will be used?
- d. When and where each session will take place?
- e. How the session will be evaluated and documented?

Use the Training Drills and Exercises Chart in the appendix section to schedule training activities or create one of your own. Consider how to involve community responders in training activities.

Conduct reviews after each training activity. Involve both personnel and community responders in the evaluation process.

## 1. Training Activities

### ***Training can take many forms:***

**a. Orientation and Education Sessions** -- These are regularly scheduled discussion sessions to provide information, answer questions and identify needs and concerns.

**b. Tabletop Exercise** -- Members of the emergency management group meet in a conference room setting to discuss their responsibilities and how they would react to emergency scenarios. This is a cost-effective and efficient way to identify areas of overlap and confusion before conducting more demanding training activities.

**c. Walk-through Drill** -- The emergency management group and response teams actually perform their emergency response functions. This activity generally involves more people and is more thorough than a tabletop exercise.

**d. Functional Drills** -- These drills test specific functions such as medical response, emergency notifications, warning and communications procedures and equipment, though not necessarily at the same time. Personnel are asked to evaluate the systems and identify problem areas.

**e. Evacuation Drill** -- Personnel walk the evacuation route to a designated area where procedures for accounting for all personnel are tested. Participants are asked to make notes as they go along of what might become a hazard during an emergency, e.g., stairways cluttered with debris, smoke in the hallways. Plans are modified accordingly.

**f. Full-scale Exercise** -- A real-life emergency situation is simulated as closely as possible. This exercise involves company emergency response personnel, employees, management and community response organizations.

## **2. Employee Training**

- a. Individual roles and responsibilities
- b. Information about threats, hazards and protective actions
- c. Notification, warning and communications procedures
- d. Means for locating family members in an emergency
- e. Emergency response procedures
- f. Evacuation, shelter and accountability procedures
- g. Location and use of common emergency equipment
- h. Emergency shutdown procedures

The scenarios developed during the vulnerability analysis can serve as the basis for trains.

*Think about this item and remember 911 and future attacks or emergencies...*

OSHA training requirements are a minimum standard for many facilities that have a fire brigade, hazardous materials team, rescue team or emergency medical response team.

## **3. Evaluate and Modify the Plan**

Conduct a formal audit of the entire plan at least once a year. Among the issues to consider are:

- a. How can you involve all levels of management in evaluating and updating the plan?
- b. Are the problem areas and resource shortfalls identified in the vulnerability analysis being sufficiently addressed?
- c. Does the plan reflect lessons learned from drills and actual events?
- d. Do members of the emergency management group and emergency response team understand their respective responsibilities? Have new members been trained?
- e. Does the plan reflect changes in the physical layout of the facility? Does it reflect new facility processes?
- f. Are photographs and other records of facility assets up to date?
- g. Is the facility attaining its training objectives?
- h. Have the hazards in the facility changed?
- i. Are the names, titles and telephone numbers in the plan current?
- j. Are steps being taken to incorporate emergency management into other facility processes?
  - a. After each training drill or exercise
  - b. After each emergency
  - c. When personnel or their responsibilities change
  - d. When the layout or design of the facility changes
  - e. When policies or procedures change
  - f. Remember to brief personnel on changes to the plan.

*Think about this item and remember 911 and future attacks or emergencies...*

Conduct a formal audit of the entire plan at least once a year.

## Incident Command Section



Experience has shown that those incidents managed in a systematic way are the most successful at achieving the intended goals. Incident command deals with the Incident Commander (IC) and his/her staff making operational decisions, some strategic, others tactical in nature, and carefully allocating resources to implement them. As a first responder you need to understand the role of the IC as the ultimate decision maker responsible for the outcome of the incident.

The ICS is the framework necessary to manage the resources, personnel, apparatus, and equipment used to mitigate the incident. Strategic decisions identify the overall approach to the incident, and operational decisions spell out the best use of those resources.

During routine emergencies, most firefighters follow a standard approach: performing size-up, choosing a strategy, implementing various tactics, and conducting ongoing evaluation.

In recent years with an increased emphasis on non-routine incidents such as hazardous materials, and now terrorist events, other methods have been developed to address new aspects related to non-routine situations. In these situations it is especially critical to know exactly what steps to take and the sequence in which they must occur because of the presence of hazards other than those traditionally encountered.

For example, during a bombing you may find it difficult to determine an appropriate course of action due to the nature or the magnitude of the incident. Furthermore, you may feel extreme pressure to act.

Regardless of the specific process used, responders go through a number of similar steps in dealing with their response.

Five common steps include conducting size up, evaluating the situation, setting incident priorities, estimating potential incident course and harm, and choosing strategic goals and tactical objectives.

<p>Have you ever been in a situation where you were, even for a short time, the IC? [ ] Yes [ ] No</p> <hr/> <p>If so, did you consciously handle the incident using an ICS or did you operate without one?</p> <hr/> <hr/> <hr/>
<p>What are the risks of operating without an ICS?</p> <hr/>



Command Center and Dispatch



## Conducting Size-Up

Size-up, the rapid mental evaluation of the factors that influence an incident, is the first step in determining a course of action. For many responders it begins even before the incident in the form of preplanning. The more information you have prior to the incident, the greater the chances of having a safe and successful response.

### Evaluating the Situation

Incident factors are dynamic and must be evaluated continually. Therefore, in a sense, size-up continues throughout the incident. In the same way that the military studies its enemy prior to battle and constantly evaluates its battle plans, so should you.

Incident situation refers to the type, the cause, and the status of the incident.

The type of incident refers to whether it is one of the five types of incidents discussed in Chapter 3 (a chemical attack, an explosion, a fire, etc.). The cause of the incident refers to whether it is an accident, such as a system failure, or something intentional, such as a bombing. The incident status refers to whether the incident is in a somewhat controlled state (static) or is still uncontrolled (dynamic or expanding).

---

#### Thinking About My Situation...

Do you agree with this statement? "Evaluating the situation is not something a responder does consciously. By virtue of training, the responder is constantly evaluating." [ ] Yes [ ] No

Do you think injury and fatalities could result from a lack of proper evaluation? Do you know of any instances where this may have occurred?

---

---

---

What might have prevented the injuries?

---

---

---

## Setting Incident Priorities

Incident priorities include life safety (for the responders as well as the public); protecting critical systems (such as the infrastructure, including transportation, public services, and communication networks); and incident stabilization.

### Estimating Potential Incident Course and Harm

Potential incident course and harm includes a series of predictions based upon the incident situation and available information. The responders estimate the probable course that the incident will take and the probable harm or damage that is likely to occur. For example, if faced with an explosion, you should be concerned about the possible presence of a secondary device that may cause harm to personnel or create additional property damage.

### Choosing Strategic Goals and Tactical Objectives

Strategic goals are broad, general statements of the desired outcome. An example of a strategic goal would be **"to prevent loss of life for both civilians and responders."**

Tactical objectives are specific operations or functions to meet the goal. For example, to meet the strategic goal of preventing loss of life, you should **"isolate the hazard area and deny entry into that area."**

Tactics are the specific steps and actions taken by the assigned personnel to meet the determined objectives. For example, to accomplish the tactical objective of isolation, you could **"position apparatus in such a fashion as to block the area, and cordon off the area with banner tape."** Notice that at each level there are more specifics involved. In the case of the tactical methods, using the apparatus and cordoning off the area are only two possible approaches.

### Influence of Hazardous Materials

In recent years the Federal government has enacted laws and developed regulations that require emergency services personnel to receive proper training. This legislation grew out of the realization that hazardous materials incidents differ from the more traditional incidents that historically have been the **"bread and butter"** of the fire service. This training is organized around five levels: Awareness, Operations, Technician, Specialist, and Incident Manager.

In implementing its training programs, the National Fire Academy (**NFA**) has followed these classifications. Furthermore, the **NFA** has adopted for its hazardous materials curriculum an incident analysis process called **GEDAPER** (developed by David M. Lesak). In doing so, the **NFA** is saying that the seven steps of **GEDAPER** provide the responders the needed processes for analyzing and handling a hazardous materials incident safely and prudently.

It also is the view of the **NFA** that this same tool, although not the only one available, can be very helpful in dealing with the range of potential incidents that are the focus of this course.

## GEDAPER

***There are seven steps to this process:***

1. Gathering information.
2. Estimating course and harm.
3. Determining strategic goals.
4. Assessing tactical options and resources.
5. Planning and implementing actions.
6. Evaluating.
7. Reviewing.

### **Gathering Information**

As a first responder, you need to gather as much information about the incident as possible (***a first responder in PPE, including positive pressure SCBA, could only use sight and hearing***) through observation, using the senses. Given the likelihood of the presence of hazardous materials at a terrorist incident, it would be in your best interest to observe from a distance, using only the senses of sight and hearing. The use of touch, taste, or smell could result in exposure.

Your education, training, and experience will help you evaluate this information before going any further. Today, there are numerous information resources available in hard copy or electronic format. If you cannot access this information at the scene, contact those who can access it for you.

For instance, when the term "**mass casualty incident**" is used to describe an incident scene, you can relate to the situation automatically. The term triggers a mental assessment based on education, training, and experience. This is unavoidable. On top of this there are other layers--perhaps many--of technical information (data) provided by other sources, commonly including texts, computers, preplans, floor plans, etc. For example, if responding to an incident involving hazardous materials (**B-NICE**), the first responder may consult the North American Emergency Response Guidebook for recommendations on initial isolation and protective action distances.

**There are other types of information that will assist you as first responder:**

- ✓ Information received from the dispatcher, such as type of incident, incident location, number of reported casualties, etc., that could indicate a possible terrorist incident;
- ✓ Information obtained during sizeup, such as unusual signs and symptoms, presence of dead animals or people, unexplained odors, unusual metal debris, placards or labels, etc. (outward warning signs and detection clues); and
- ✓ Environmental information, such as time of day or night, location (address, neighborhood, and occupancy), weather (temperature, wind direction, relative humidity), topography (lay of the land, hills, bodies of water), and exposures (people, property, environment).

Regardless of the incident, the first step is to collect all the information possible as quickly as you can before you go any further. Then, once you have made some initial decisions, you need to continue to collect information and reassess it.

### Thinking About My Situation...

Recall a recent incident that you have participated in as a first responder, preferably a hazardous materials incident. List a few specific steps of information gathering that you took.

---

---

---

Did you consult any printed sources? If so, name two or three.

---

---

---

Did you refer to any other resources that were not at the scene for additional information using a radio, telephone, or other electronic device? If you did, how helpful was this?

---

---

---

### Estimating Course and Harm

Estimating the course of an incident involves using the information you have gathered to make a series of predictions and to assess the potential harm. This involves damage assessment, hazard identification, vulnerability assessment, and risk determination. Damage assessment involves figuring the damage that has already occurred.

Hazard identification means determining what product is involved, where it is, what it can do, how much there is, etc. Vulnerability assessment is figuring out who and what is at risk--in other words, all persons and things the hazard may affect.

Risk determination involves estimating the probability that the situation might get worse before it is controlled. Initially, strategic goals and tactical options should be based on the most likely situation outcome.

### Determining Strategic Goals

Strategic goals are broad, general statements of intent. Always to be included in determining strategic goals are the incident priorities of life safety (responder and civilian), protection of critical systems (anything that is in place for the betterment of the community, such as public utilities and transportation, hospitals, etc.), and incident stabilization.

## Assessing Tactical Options and Resources

In order to meet the strategic goals, you need to select appropriate tactical objectives and methods. For instance, if the strategic goal is isolation, then the tactical objectives must include establishing perimeters and operational zones, denying entry into the "hot zone," and removing the public and emergency personnel far from the "hot zone."

Perimeters and zones represent a safety factor, or buffer, against the hazards presented by the incident. The establishment of zones, or perimeters, is critical to protect both first responders and civilians. Denial of entry includes the use of physical barriers, such as tape, rope, barricades, etc. These tasks are within the scope of responsibilities of a first responder trained to the awareness level.

Public protection involves establishing an area of safe refuge for those who are contaminated, thus reducing the chances of secondary contamination. It also involves assisting those individuals who are in harm's way to safety. Doing so will set the stage for decontamination and subsequent medical treatment.

All of these objectives require the use of resources, including personnel and equipment. The level of effort required, coupled with the amount of resources available, will determine if the goals and objectives can be attained. If the resources are adequate, or if other assistance is available, then the next step, planning and implementing actions, becomes possible.

Withdrawal is an option where the situation is too dangerous or too large for intervention. The best course of action may be to evacuate the area, deny entry, and allow the incident to run its course.

### Thinking About My Situation...

Do your local SOPs/SOGs address issues such as establishing operational zones and perimeters (public protection)? If so, what specific issues are addressed that involve the efforts of first responders?

---

---

---

### Planning and Implementing Actions

The plan of action is a written document that consolidates all of the operational actions to be taken by various personnel in order to stabilize the incident. It is important for you to appreciate the purposes of the written plan. It helps pinpoint the exact actions planned.

Standard operating procedures/ standard operating guidelines (**SOPs/SOGs**) are linked to the plan of action. They spell out the functions, roles, and responsibilities of personnel on the incident scene.

They should be agreed upon long before the incident, and the staff must be trained in implementing them. The plan of action references SOPs/SOGs, it does not create them.

Another important planning step is to create a **"site safety and health plan."** If the incident involves hazardous materials, which most terrorist incidents will, Federal regulations (**OSHA 1910.120**) require that you create one. A site safety and health plan is a series of checklists used to manage an incident and to assure the safety of all involved. Like SOPs/SOGs, the checklists are developed before the incident and are implemented during the incident.

The site safety and health plan identifies the health and safety hazards faced at the incident scene. It further identifies appropriate PPE, decontamination considerations, EMS concerns, and similar safety issues. When the incident involves chemical or biological hazards it assists in fulfilling employee right-to-know requirements.

The site safety and health plan helps to document the specific actions and safety procedures used. It will assist in documenting whether the chosen plan of action and the specific procedures are followed. In addition, the site safety and health plan tracks activities and performances and assures that personnel safely perform those tasks for which they received appropriate training. Someone trained only to the Awareness Level should not perform tasks specific to the Operations or Technician Levels, for example.

Included in the site safety and health plan are the location and the extent of zones, the nature of the hazards found on the scene, the types of personal protective equipment (**PPE**) worn by personnel, and the type(s) of decontamination procedures followed. Your local or State hazardous materials responders should have examples of existing site safety and health plans that can be adjusted to fit a terrorist scenario.

<b>Thinking About My Situation...</b>
To which level are you trained? _____
Have you ever operated beyond your level of training either of your own volition or because an officer told you to? [ ] Yes [ ] No
Apart from the legal implications, what are the safety implications?
_____
_____
_____

## Evaluating

The goal of the evaluation process is to determine whether the plan of action is working as intended. Evaluation will help identify possible errors and allow the responders to correct them. You should monitor and evaluate all incident scenes, terrorist or not. If your plan is failing rapidly, you will need an alternate plan of action that can be implemented quickly and, depending on the available resources, used to solve the problem. It is foolish to stick with a plan that is not working.

### Reviewing

The review process involves revisiting and confirming the **GEDAPER** process. Review occurs either when strategic goals are accomplished or when there is an extended response period and it is not wise to wait until the entire operation has concluded. If the entire process is managed effectively from the start, there should be no problems with the plan of action.

Specifically, if the information gathered initially is thorough, comprehensive, and well managed, the estimate of course and harm should be accurate and the strategic goals and tactical objectives chosen also should be appropriate.

If problems are discovered with the plan, then the existing plan should be modified to reflect the appropriate changes, or a new plan should be developed to replace the flawed one. In summary, the plan tells what should be, the evaluation tells what is not, and the review makes the corrections. Ongoing evaluation assures that the plan is working or alerts you that the plan is failing.

How often have you been involved in reviewing the incident action plans? \_\_\_\_\_

What were some of the benefits of this review process?

---

---

---

Did it make a difference on the final outcome?

---

---

---

## SUMMARY

While you may not be faced with being the IC, it should be obvious that your role as a first responder is critical to the management of the incident. Remember that the actions you take and the decisions you make early in the incident will have a dramatic effect on the outcome of the event. One of the first concerns you should address is your safety.

Dependent upon the situation you find upon your arrival, coupled with pre-arrival information such as the incident location and situation as dispatched, you will need to make early decisions that will affect the incident.

Always keep in mind the outward warning signs and detection clues mentioned in Chapter 4. On scene considerations should be similar to your existing response guidelines dealing with hazardous materials.

While it would be easy to become overwhelmed, keep in mind the following key points:

- Your safety and that of your fellow personnel is paramount; otherwise you cannot possibly mitigate the incident.
- The initial steps of gaining control of the scene will greatly affect incident management. Simple procedures, such as staging apparatus uphill and upwind, performing isolation, and establishing perimeters, will help immensely. This may be all you can do prior to the arrival of additional resources, but do not minimize its importance.
- You need to be proactive, not reactive. In other words, try to stay a few steps ahead of the current situation to be better prepared for what may occur next.
- Remember also that you are only human and that you can do only a limited number of tasks simultaneously. Although you may be overwhelmed initially, eventually your actions should overcome the seemingly chaotic situation and the incident will be under control.
- Plan to be a part of the solution, not part of the problem.
- Do not hesitate to seek additional assistance.





## CHAPTER 6 EXERCISE

This is a chapter review, you can find the final exam on TLC's website under Assignments.

### LEARNING CHECK

True or False: Circle either T or F.

1.    T    F    AS A FIRST RESPONDER, YOUR INITIAL CONCERN SHOULD BE THE SAFETY OF OTHERS, NOT YOURSELF.
2.    T    F    ALL EMERGENCY OPERATIONS MUST BE ORGANIZED TO BE SUCCESSFUL.
3.    T    F    A SYSTEM IS A COLLECTION OF UNRELATED, INDEPENDENT PARTS DESIGNED WITH NO PARTICULAR PURPOSE.
4.    T    F    IMPROPER EMERGENCY SCENE MANAGEMENT CAN RESULT IN LOSS OF SCENE CONTROL, BUT NOT GREATER LOSS OF LIFE OR INJURY.
5.    T    F    STRATEGIC GOALS ARE BROAD GENERAL STATEMENTS OF THE DESIRED OUTCOME.

### MULTIPLE CHOICE: CIRCLE YOUR ANSWER.

6.    This plan documents specific actions and safety procedures used. Tracks activities and performances, and assures that personnel safely perform those tasks for which they received appropriate training.
  - a.    Plan of action.
  - b.    SOP/SOG.
  - c.    Site safety plan.
  - d.    Employers Emergency Response Plan.
7.    During the review step in the GEDAPER process, you should
  - a.    determine the location and extent of zones, the nature of hazards found on the scene, and the types of PPE required.
  - b.    develop a site safety and operational plan.
  - c.    revisit and confirm the proceeding steps in the GEDAPER process.
  - d.    establish the cause and status of the incident.
8.    When estimating course and harm during the GEDAPER process, you would
  - a.    assess damage.
  - b.    establish perimeters.
  - c.    determine life safety priorities.
  - d.    assess resources.

9. When gathering information during the GEDAPER process, you would
  - a. develop SOPs.
  - b. establish the number of casualties.
  - c. develop SOGs.
  - d. select appropriate tactical objectives and methods.
  
10. If an incident involves hazardous materials, which most terrorist incidents will, Federal regulations require you to create
  - a. an evaluation tool.
  - b. a site safety plan.
  - c. a risk determination.
  - d. none of the above.
  
11. Describe one or two practical, achievable steps you will take as a result of studying this Chapter to help you to be better prepared to deal with one of the incidents described here.

Step One:

Step Two:

How I will accomplish Step One

How I will accomplish Step Two

## Chapter 7: Notification and Coordination

**Section Focus:** You will learn the basics of proper notification and coordination with public protection services. At the end of this section, you the student will be able to understand and describe the communication process. There is a post quiz at the end of this section to review your comprehension and a final examination in the Assignment for your contact hours.

**Scope/Background:** *Notification and Coordination* provides procedures for activating response resources.



### ACTIVATING RESOURCES

The first responder at the local level plays a critical role in the communication link. It is vitally important that you are able to realize the need for additional resources, and make the appropriate notifications to your communication center.

Your locality should have an emergency operations plan (**EOP**) in place to deal with incidents of such magnitude. In jurisdictions that use a functional planning approach, hazard-specific appendices can be developed to describe the unique provisions and procedures associated with performing response functions (e.g., direction and control; communications; alert, notification, and warning; emergency public information; evacuation and movement; mass care; health and medical; and resource management, among others) in a situation involving terrorism.

Occasionally, a natural or manmade disaster occurs which overwhelms resources and capabilities at the local level. When such a disaster occurs, it becomes the State's responsibility to provide assistance to the affected jurisdiction(s).

If the State's resources and capabilities are not adequate to mitigate the incident, Federal assistance would be requested through the governor.

The first step in explaining this process involves your understanding of local, county, State, and Federal planning.

### What is an EOP?

*An EOP is a document that:*

- assigns responsibility to organizations and individuals for carrying out specific actions at projected times and places in an emergency that exceeds the capability or routine responsibility of any one agency, e.g., the fire department;
- sets forth lines of authority and organizational relationships, and shows how all actions will be coordinated;
- describes how people and property will be protected in emergencies and disasters;
- identifies personnel, equipment, facilities, supplies, and other resources available—within the jurisdiction or by agreement with other jurisdictions—for use during response and recovery operations; and
- identifies steps to address mitigation concerns during response and recovery activities.

### Local EOPs

In our country's system of emergency management, local government must act first to attend to the public's emergency needs (Realistically, first responders act on behalf of the local government at incident scenes). Depending on the nature and size of the emergency, State and Federal assistance may be provided to the local jurisdiction. The local EOP focuses on essential measures for protecting the public. These include warning, emergency public information, evacuation, and shelter. Included in your local EOP should be a mechanism for emergency responders and managers to notify and activate State resources.

### State EOPs

States play three roles: (1) they assist local jurisdictions whose capabilities are overwhelmed by an emergency; (2) they themselves respond first to certain emergencies; and (3) they work with the Federal government when Federal assistance is necessary. The State EOP is the framework within which local EOPs are created and through which the Federal government becomes involved. As such, the State EOP ensures that all levels of government are able to mobilize as a unified emergency organization to safeguard the well-being of the State's citizens.

State whether you agree or disagree with the following statement, and why.

As a first responder trained to the awareness level, it is unlikely I would be involved in a major emergency operation requiring State resources. However, as a member of the local emergency management community, there still is some value in my being familiar with the State Emergency Operations Plan.

## Linking Federal and State Response

The Robert T. Stafford Disaster Relief and Emergency Assistance Act, Public Law 93-288, as amended, authorizes the Federal government to respond to disasters and emergencies in order to help State and local governments save lives, and to protect public health, safety, and property.

The Federal Response Plan (**FRP**) was developed to help expedite Federal support to disasters. Generally, the FRP is implemented when the State's resources are not sufficient to cope with a disaster, and the governor has requested Federal assistance.

The FRP details what the Federal government will do to provide emergency assistance to a State and its local governments affected by a large-scale disaster. It also describes an organizational structure for providing this assistance. It is built on the principle of functionality, in that 12 emergency support functions (**ESFs**) are arranged with a lead Federal agency to coordinate operations within each area. This is shown below.

<b>ESF</b>	<b>Function</b>	<b>Lead Agency</b>
	Transportation	U.S. Department Of Transportation
	Communications	National Communication System
	Public works and engineering	U.S. Department of Defense, Army Corps of Engineers
	Firefighting	U.S. DEPARTMENT OF AGRICULTURE, FOREST SERVICE
	Information and planning	Federal Emergency Management Agency
	Mass care	American Red Cross
	Resource support	General Services Administration
<b>ESF</b>	<b>Function</b>	<b>Lead Agency</b>
	Health and medical services	U.S. Department of Health and Human Services, Public Health Service
	Urban search and rescue	Federal Emergency Management Agency
	Hazardous materials	Environmental Protection Agency
	Food	U.S. Department of Agriculture, Food and Nutrition Service
	Energy	U.S. Department of Energy

## Presidential Decision Directive 39 (PDD-39)

In June 1995, the White House issued Presidential Decision Directive 39 (PDD-39), United States Policy on Counterterrorism. PDD-39 directed a number of measures to reduce the Nation's vulnerability to terrorism, to deter and respond to terrorist acts, and to strengthen capabilities to prevent and manage the consequences of terrorist use of nuclear, biological, and chemical (**NBC**) weapons, including weapons of mass destruction (**WMD**). PDD-39 discusses crisis management and consequence management.

Crisis management is the law-enforcement response, and focuses on the criminal aspects of the incident. Specific components of crisis management include activities to anticipate, prevent, and/or resolve a threat or incident; identify, locate, and apprehend the perpetrators; and investigate and gather evidence to support prosecution. Crisis management involves local, State, and Federal law-enforcement agencies, with the Federal Bureau of Investigation (**FBI**) having the lead role.



Consequence management is the response to the disaster, and focuses on alleviating damage, loss, hardship, or suffering. Specific components of consequence management include activities to protect public health and safety; restore essential government services; and provide emergency assistance to affected governments, businesses, and individuals. Consequence management includes Federal, State, and local volunteer and private agencies.



The Federal Emergency Management Agency (**FEMA**) has the lead role in consequence management. The laws of the United States assign primary authority to the States to respond to the consequences of terrorism; the Federal government provides assistance as required.

Contrast the roles you would play as a first responder in crisis management and consequence management. In which area do you think you would have a bigger role as a first responder?

---

---

---

---

## **Federal Response Plan: Terrorism Incident Annex**

In the event that Federal assistance is needed at a terrorist incident, FEMA would use the newly developed Terrorism Incident Annex of the Federal Response Plan.

This describes the Federal concept of operations to implement PDD-39 when necessary to respond to terrorist incidents within the U.S. Included in the Appendix are copies of an unclassified abstract of PDD-39 and the FRP: Terrorism Incident Annex.

### **Chain of Events**

If a terrorist incident that exceeded available resources and capabilities were to occur within your locality, your jurisdiction would notify your appropriate State emergency management agency. In the event that State resources and capabilities were exceeded, the governor would place the call to FEMA for Federal assistance.

Under the Robert T. Stafford Act, once a Presidential Declaration of Disaster is made, the following actions would be taken, many concurrently, in response to a terrorist incident:

- FEMA would use its emergency authorities to notify the Federal agencies, activate the FRP, begin coordinating the delivery of Federal assistance, and establish liaison operations with the FBI.
- The FEMA Director would consult with the governor of the affected State to determine the scope and extent of the incident.
- An emergency response team, made up of representatives from each of the primary Federal agencies, would be assembled and deployed to the field to establish a Disaster Field Office and initiate operations.

### **SUMMARY**

The first responder must understand what happens when an incident, natural or manmade, overwhelms local and State capabilities and becomes a Federal response.

Your role in the notification process is the first link in the communications chain. As soon as possible after you suspect criminal activity or a potential act of terrorism, you should notify the appropriate authorities.

For most of you, however, this does not extend beyond your dispatch or communications center. This will assist in activating available response resources, and increase the likelihood of success.

Given the likely increase in terrorism-related incidents in the U.S., your familiarity with local, State, and Federal plans will enable you and your agency to respond more effectively in the event that terrorism strikes in your jurisdiction.





## CHAPTER 7 EXERCISE

This is a chapter review, you can find the final exam on TLC's website under Assignments.

### LEARNING CHECK

#### MULTIPLE CHOICE: CIRCLE YOUR ANSWER.

1. An EOP
  - a. covers specific actions occurring at projected times and places during an emergency. It does not assign responsibilities to organizations and individuals for implementing these actions.
  - b. designates responsibility for setting lines of authority and organizational relationships to any first responder assigned to an incident.
  - c. describes alternative approaches for apprehending and convicting would-be terrorists.
  - d. identifies personnel, equipment, facilities, supplies, and other resources available for use during response and recovery operations.
  
2. Crisis management includes activities to
  - a. protect public health and safety.
  - b. restore essential government services.
  - c. provide emergency assistance to affected governments, businesses, and individuals.
  - d. anticipate, prevent, and/or resolve a threat or incident.
  
3. Consequence management
  - a. includes activities to identify, locate, and apprehend the perpetrators.
  - b. includes Federal, state, and local volunteer and private agencies.
  - c. involves local, state, and Federal law enforcement agencies.
  - d. focuses on criminal aspects of the incident.
  
4. When a Presidential Declaration of Disaster is announced, which of the following occurs?
  - a. FEMA suspends FRP activities.
  - b. An emergency response team is deployed to establish a Disaster Field Office and initiate operations.
  - c. The President confers directly with first responders to determine the scope and extent of the incident.
  - d. FEMA assumes command of the incident scene.
  
5. The \_\_\_\_\_ authorizes the Federal Government to respond to disasters and emergencies in order to provide State and local governments with assistance.
  - a. Federal Response Plan
  - b. Robert T. Stafford Act
  - c. State EOP
  - d. SARA Title III

True or False: Circle either T or F.

- 6.    T    F    The first responder plays a critical role in the communications link.
- 7.    T    F    In our country's system of emergency management, local government (first responders) must act first to attend to the public's emergency needs.
- 8.    T    F    According to PDD-39, FEMA is given the lead role in crisis management.
- 9.    T    F    As soon as you suspect criminal activity as a potential act of terrorism, you should notify the appropriate authorities.
- 10.   T    F    A first responder does not need to be familiar with local emergency operations plans.

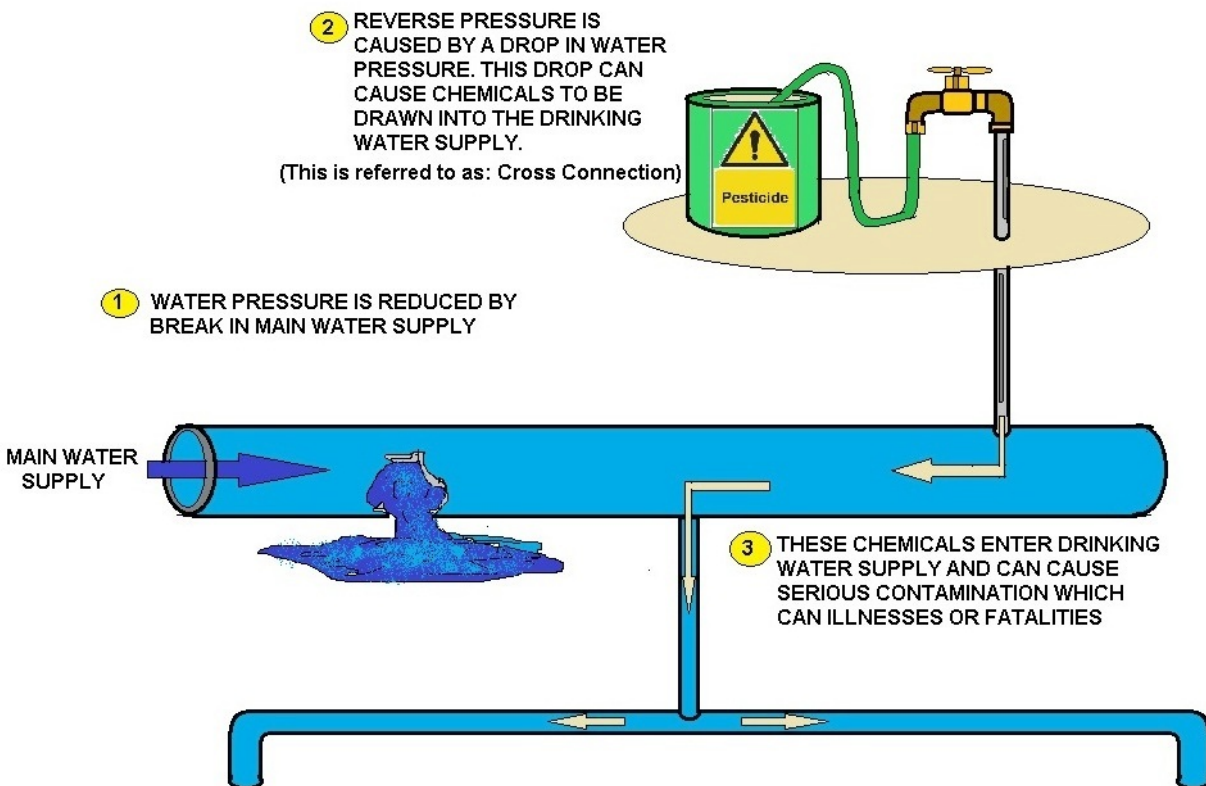
11.    Refer to your local and State EOPs. List resources identified in the plan that could help you in a B-NICE incident.

12.    Where or how do you contact FEMA?

## Chapter 8 Backflow - Backflow Events

**Section Focus:** You will learn the basics of conventional water treatment. At the end of this section, you the student will be able to understand and describe the water treatment process. There is a post quiz at the end of this section to review your comprehension and a final examination in the Assignment for your contact hours.

**Scope/Background:** Review of water distribution related fundamentals. This course will cover the basics of backflow prevention, water quality and hydraulic fundamentals. Backflow Familiarization, Definitions, and Terms.



### Paraquat

In June 1983, "yellow gushy stuff" poured from some faucets in the Town of Woodsboro, Maryland. Town personnel notified the County Health Department and the State Water Supply Division. The State dispatched personnel to take water samples for analysis and placed a ban on drinking the Town's water.

Firefighters warned residents not to use the water for drinking, cooking, bathing, or any other purpose except flushing toilets. The Town began flushing its water system. An investigation revealed that the powerful agricultural herbicide Paraquat had backflowed into the Town's water system.

Someone left open a gate valve between an agricultural herbicide holding tank and the Town's water system and, thus, created a cross-connection. Coincidentally, water pressure in the Town temporarily decreased due to failure of a pump in the Town's water system. The herbicide Paraquat was backsiphoned into the Town's water system. Upon restoration of pressure in the Town's water system, Paraquat flowed throughout much of the Town's water system.

Fortunately, this incident did not cause any serious illness or death. The incident did, however, create an expensive burden on the Town. Tanker trucks were used temporarily to provide potable water, and the Town flushed and sampled its water system extensively.

### **Mortuary**

The chief plumbing inspector in a large southern city received a telephone call advising that blood was coming from drinking fountains at a mortuary (i.e., a funeral home). Plumbing and health inspectors went to the scene and found evidence that blood had been circulating in the potable water system within the funeral home. They immediately ordered the funeral home cut off from the public water system at the meter.

City water and plumbing officials did not think that the water contamination problem had spread beyond the funeral home, but they sent inspectors into the neighborhood to check for possible contamination. Investigation revealed that blood had backflowed through a hydraulic aspirator into the potable water system at the funeral home.

The funeral home had been using a hydraulic aspirator to drain fluids from bodies as part of the embalming process. The aspirator was directly connected to a faucet at a sink in the embalming room. Water flow through the aspirator created suction used to draw body fluids through a needle and hose attached to the aspirator. When funeral home personnel used the aspirator during a period of low water pressure, the potable water system at the funeral home became contaminated. Instead of body fluids flowing into the wastewater system, they were drawn in the opposite direction--into the potable water system.

*U.S. Environmental Protection Agency, Cross-Connection Control Manual, 1989*

## **Recent Backflow Situations**

### **Oregon 1993**

Water from a drainage pond, used for lawn irrigation, is pumped into the potable water supply of a housing development.

### **California 1994**

A defective backflow device in the water system of the County Courthouse apparently caused sodium nitrate contamination that sent 19 people to the hospital.

### **New York 1994**

An 8-inch reduced pressure principle backflow assembly in the basement of a hospital discharged under backpressure conditions, dumping 100,000 gallons of water into the basement.

### **Nebraska 1994**

While working on a chiller unit of an air conditioning system at a nursing home, a hole in the coil apparently allowed Freon to enter the circulating water and from there into the city water system.

### **California 1994**

The blue tinted water in a pond at an amusement park backflowed into the city water system and caused colored water to flow from homeowner's faucets.

### **California 1994**

A film company shooting a commercial for television accidentally introduced a chemical into the potable water system.

### **Iowa 1994**

A backflow of water from the Capitol Building chilled water system contaminates potable water with Freon.

### **Indiana 1994**

A water main break caused a drop in water pressure allowing anti-freeze from an air conditioning unit to backsiphon into the potable water supply.

### **Washington 1994**

An Ethylene Glycol cooling system was illegally connected to the domestic water supply at a veterinarian hospital.

### **Ohio 1994**

An ice machine connected to a sewer sickened dozens of people attending a convention.



# Hydraulics

**Definition:** **Hydraulics** is a branch of engineering concerned mainly with moving liquids. The term is applied commonly to the study of the mechanical properties of water, other liquids, and even gases when the effects of compressibility are small. Hydraulics can be divided into two areas, hydrostatics and hydrokinetics.

**Hydraulics: *The Engineering science pertaining to liquid pressure and flow.***

The word **hydraulics** is based on the Greek word for water, and originally covered the study of the physical behavior of water at rest and in motion. Use has broadened its meaning to include the behavior of all liquids, although it is primarily concerned with the motion of liquids.

Hydraulics includes the manner in which liquids act in tanks and pipes, deals with their properties, and explores ways to take advantage of these properties.

Hydrostatics, the consideration of liquids at rest, involves problems of buoyancy and flotation, pressure on dams and submerged devices, and hydraulic presses. The relative incompressibility of liquids is one of its basic principles.

Hydrodynamics, the study of liquids in motion, is concerned with such matters as friction and turbulence generated in pipes by flowing liquids, the flow of water over weirs and through nozzles, and the use of hydraulic pressure in machinery.

## Hydrostatics

Hydrostatics is about the pressures exerted by a fluid at rest. Any fluid is meant, not just water. Research and careful study on water yields many useful results of its own, however, such as forces on dams, buoyancy and hydraulic actuation, and is well worth studying for such practical reasons. Hydrostatics is an excellent example of deductive mathematical physics, one that can be understood easily and completely from a very few fundamentals, and in which the predictions agree closely with experiment.

There are few better illustrations of the use of the integral calculus, as well as the principles of ordinary statics, available to the student. A great deal can be done with only elementary mathematics. Properly adapted, the material can be used from the earliest introduction of school science, giving an excellent example of a quantitative science with many possibilities for hands-on experiences.

The definition of a fluid deserves careful consideration. Although time is not a factor in hydrostatics, it enters in the approach to hydrostatic equilibrium. It is usually stated that a fluid is a substance that cannot resist a shearing stress, so that pressures are normal to confining surfaces. Geology has now shown us clearly that there are substances which can resist shearing forces over short time intervals, and appear to be typical solids, but which flow like liquids over long time intervals. Such materials include wax and pitch, ice, and even rock.



A ball of pitch, which can be shattered by a hammer, will spread out and flow in months. Ice, a typical solid, will flow in a period of years, as shown in glaciers, and rock will flow over hundreds of years, as in convection in the mantle of the earth.

Shear earthquake waves, with periods of seconds, propagate deep in the earth, though the rock there can flow like a liquid when considered over centuries. The rate of shearing may not be strictly proportional to the stress, but exists even with low stress.

Viscosity may be the physical property that varies over the largest numerical range, competing with electrical resistivity. There are several familiar topics in hydrostatics which often appears in expositions of introductory science, and which are also of historical interest and can enliven their presentation. Let's start our study with the principles of our atmosphere.

## **Atmospheric Pressure**

The atmosphere is the entire mass of air that surrounds the earth. While it extends upward for about 500 miles, the section of primary interest is the portion that rests on the earth's surface and extends upward for about 7 1/2 miles. This layer is called the troposphere.

If a column of air 1-inch square extending all the way to the "top" of the atmosphere could be weighed, this column of air would weigh approximately 14.7 pounds at sea level. Thus, atmospheric pressure at sea level is approximately 14.7 psi.

As one ascends, the atmospheric pressure decreases by approximately 1.0 psi for every 2,343 feet. However, below sea level, in excavations and depressions, atmospheric pressure increases. Pressures under water differ from those under air only because the weight of the water must be added to the pressure of the air.

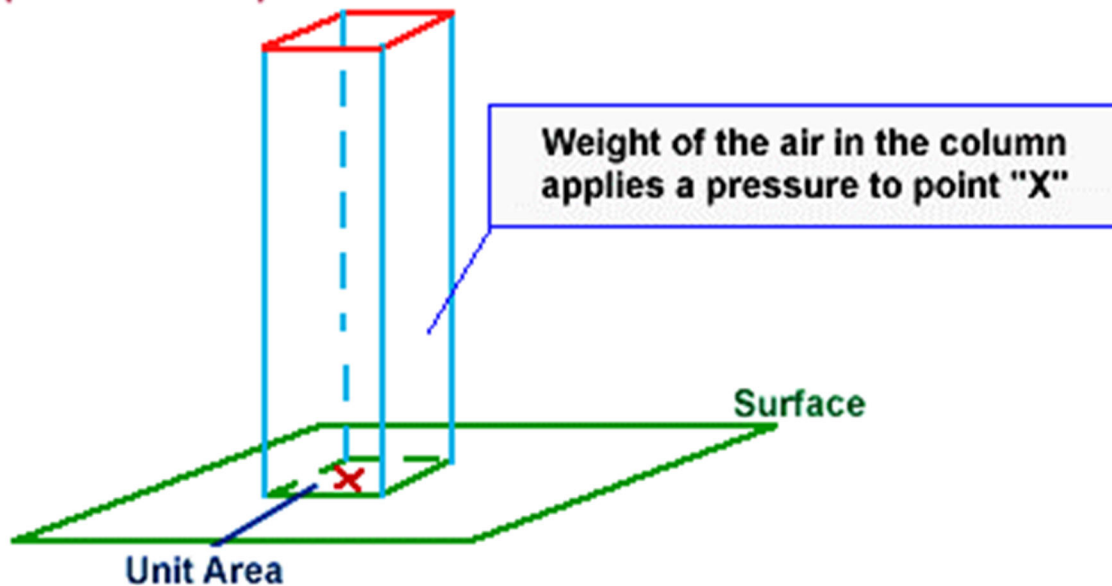
Atmospheric pressure can be measured by any of several methods. The common laboratory method uses the mercury column barometer. The height of the mercury column serves as an indicator of atmospheric pressure. At sea level and at a temperature of 0° Celsius (**C**), the height of the mercury column is approximately 30 inches, or 76 centimeters. This represents a pressure of approximately 14.7 psi. The 30-inch column is used as a reference standard.

Another device used to measure atmospheric pressure is the aneroid barometer. The aneroid barometer uses the change in shape of an evacuated metal cell to measure variations in atmospheric pressure. The thin metal of the aneroid cell moves in or out with the variation of pressure on its external surface. This movement is transmitted through a system of levers to a pointer, which indicates the pressure.

The atmospheric pressure does not vary uniformly with altitude. It changes very rapidly. Atmospheric pressure is defined as the force per unit area exerted against a surface by the weight of the air above that surface. In the diagram on the following page, the pressure at point "X" increases as the weight of the air above it increases. The same can be said about decreasing pressure, where the pressure at point "X" decreases if the weight of the air above it also decreases.



## Top of the Atmosphere



### Barometric Loop

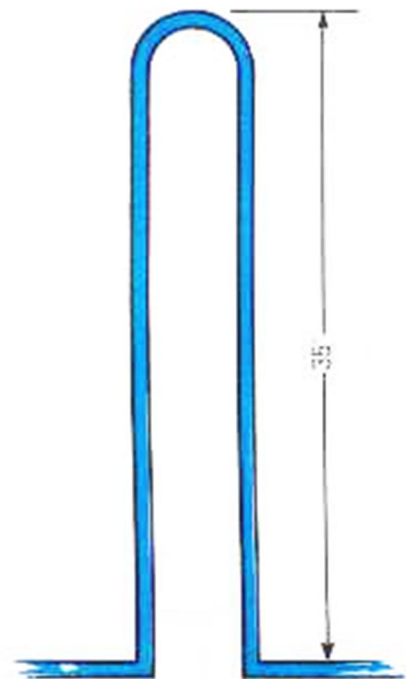
The barometric loop consists of a continuous section of supply piping that abruptly rises to a height of approximately 35 feet and then returns back down to the originating level. It is a loop in the piping system that effectively protects against backsiphonage. It may not be used to protect against back-pressure.

Its operation, in the protection against backsiphonage, is based upon the principle that a water column, at sea level pressure, will not rise above 33.9 feet. In general, barometric loops are locally fabricated, and are 35 feet high.

Pressure may be referred to using an absolute scale, pounds per square inch absolute (**psia**), or gauge scale, (**psig**). Absolute pressure and gauge pressure are related.

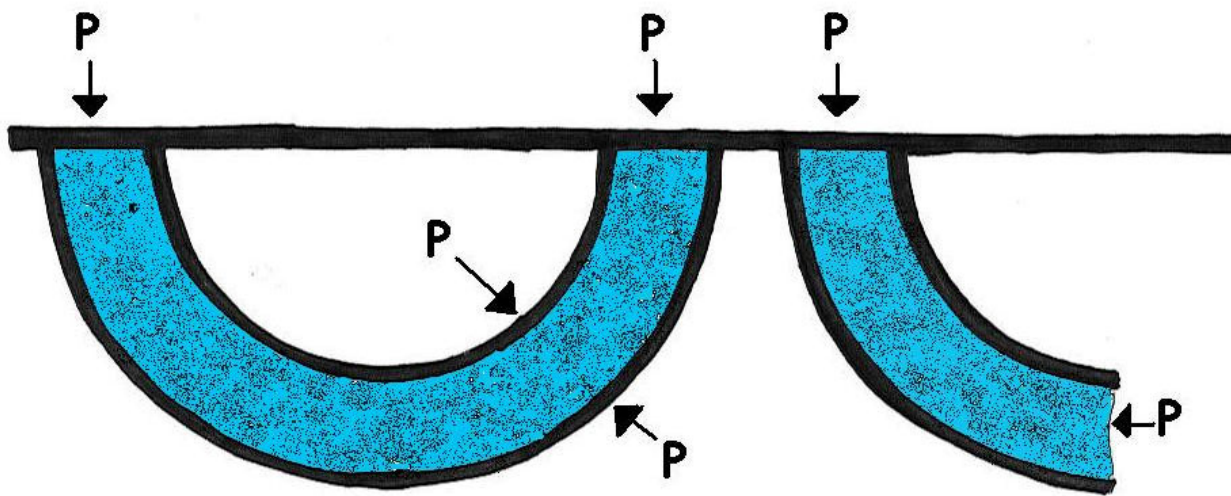
Absolute pressure is equal to gauge pressure plus the atmospheric pressure. At sea level, the atmospheric pressure is 14.7 psai.

Absolute pressure is the total pressure. Gauge pressure is simply the pressure read on the gauge. If there is no pressure on the gauge other than atmospheric, the gauge will read zero. Then the absolute pressure would be equal to 14.7 psi, which is the atmospheric pressure.



## Pressure

By a fluid, we have a material in mind like water or air, two very common and important fluids. Water is incompressible, while air is very compressible, but both are fluids. Water has a definite volume; air does not. Water and air have low viscosity; that is, layers of them slide very easily on one another, and they quickly assume their permanent shapes when disturbed by rapid flows. Other fluids, such as molasses, may have high viscosity and take a long time to come to equilibrium, but they are no less fluids. The coefficient of viscosity is the ratio of the shearing force to the velocity gradient. Hydrostatics deals with permanent, time-independent states of fluids, so viscosity does not appear, except as discussed in the Introduction.



### Equality of Pressure

A fluid, therefore, is a substance that cannot exert any permanent forces tangential to a boundary. Any force that it exerts on a boundary must be normal to the boundary. Such a force is proportional to the area on which it is exerted, and is called a pressure. We can imagine any surface in a fluid as dividing the fluid into parts pressing on each other, as if it were a thin material membrane, and so think of the pressure at any point in the fluid, not just at the boundaries. In order for any small element of the fluid to be in equilibrium, the pressure must be the same in all directions (or the element would move in the direction of least pressure), and if no other forces are acting on the body of the fluid, the pressure must be the same at all neighboring points.

Therefore, in this case the pressure will be the same throughout the fluid, and the same in any direction at a point (Pascal's Principle). Pressure is expressed in units of force per unit area such as dyne/cm<sup>2</sup>, N/cm<sup>2</sup> (pascal), pounds/in<sup>2</sup> (psi) or pounds/ft<sup>2</sup> (psf). The axiom that if a certain volume of fluid were somehow made solid, the equilibrium of forces would not be disturbed is useful in reasoning about forces in fluids.

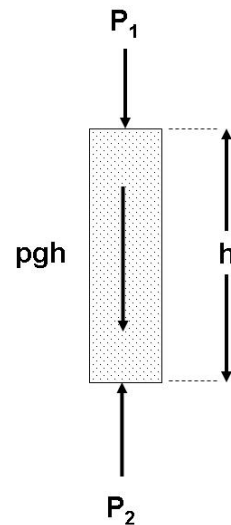
On earth, fluids are also subject to the force of gravity, which acts vertically downward, and has a magnitude  $\gamma = \rho g$  per unit volume, where  $g$  is the acceleration of gravity, approximately  $981 \text{ cm/s}^2$  or  $32.15 \text{ ft/s}^2$ ,  $\rho$  is the density, the mass per unit volume, expressed in  $\text{g/cm}^3$ ,  $\text{kg/m}^3$ , or  $\text{slug/ft}^3$ , and  $\gamma$  is the specific weight, measured in  $\text{lb/in}^3$ , or  $\text{lb/ft}^3$  (pcf). Gravitation is an example of a body force that disturbs the equality of pressure in a fluid. The presence of the gravitational body force causes the pressure to increase with depth, according to the equation  $dp = \rho g dh$ , in order to support the water above. We call this relation the barometric equation, for when this equation is integrated, we find the variation of pressure with height or depth. If the fluid is incompressible, the equation can be integrated at once, and the pressure as a function of depth  $h$  is  $p = \rho gh + p_0$ .

The density of water is about  $1 \text{ g/cm}^3$ , or its specific weight is  $62.4 \text{ pcf}$ . We may ask what depth of water gives the normal sea-level atmospheric pressure of  $14.7 \text{ psi}$ , or  $2117 \text{ psf}$ .

This is simply  $2117 / 62.4 = 33.9 \text{ ft}$  of water. This is the maximum height to which water can be raised by a suction pump, or, more correctly, can be supported by atmospheric pressure. Professor James Thomson (brother of William Thomson, Lord Kelvin) illustrated the equality of pressure by a "curtain-ring" analogy shown in the diagram. A section of the toroid was identified, imagined to be solidified, and its equilibrium was analyzed.

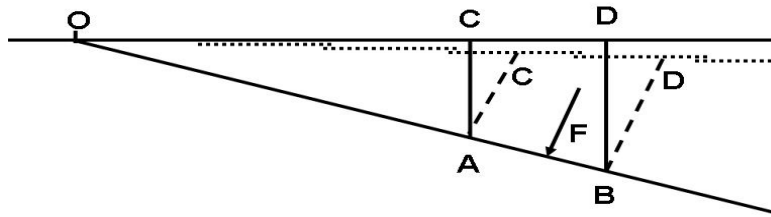
The forces exerted on the curved surfaces have no component along the normal to a plane section, so the pressures at any two points of a plane must be equal, since the fluid represented by the curtain ring was in equilibrium.

Free Surface

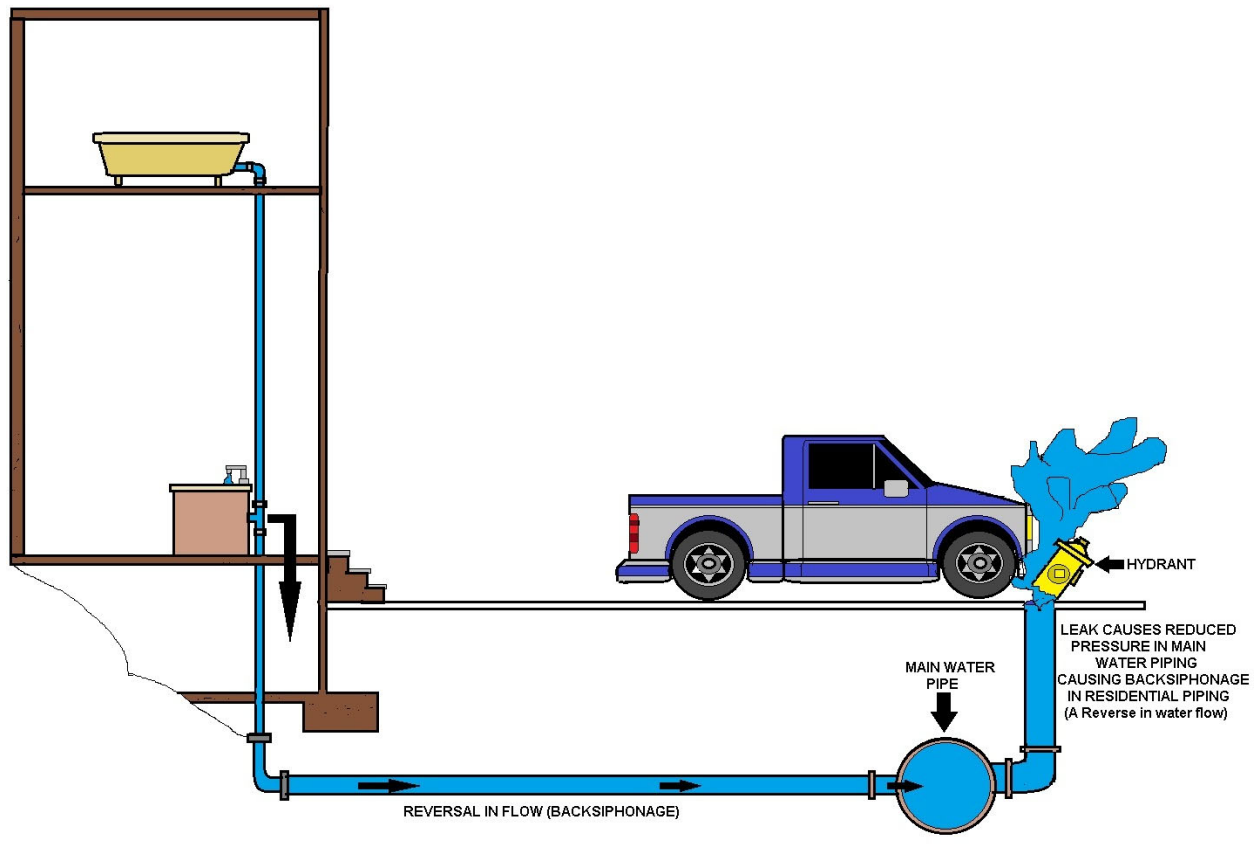


Increase of Pressure with Depth

The diagram illustrates the equality of pressures in orthogonal directions. This can be extended to any direction whatever, so Pascal's Principle is established. This demonstration is similar to the usual one using a triangular prism and considering the forces on the end and lateral faces separately.



Thrust on a Plane



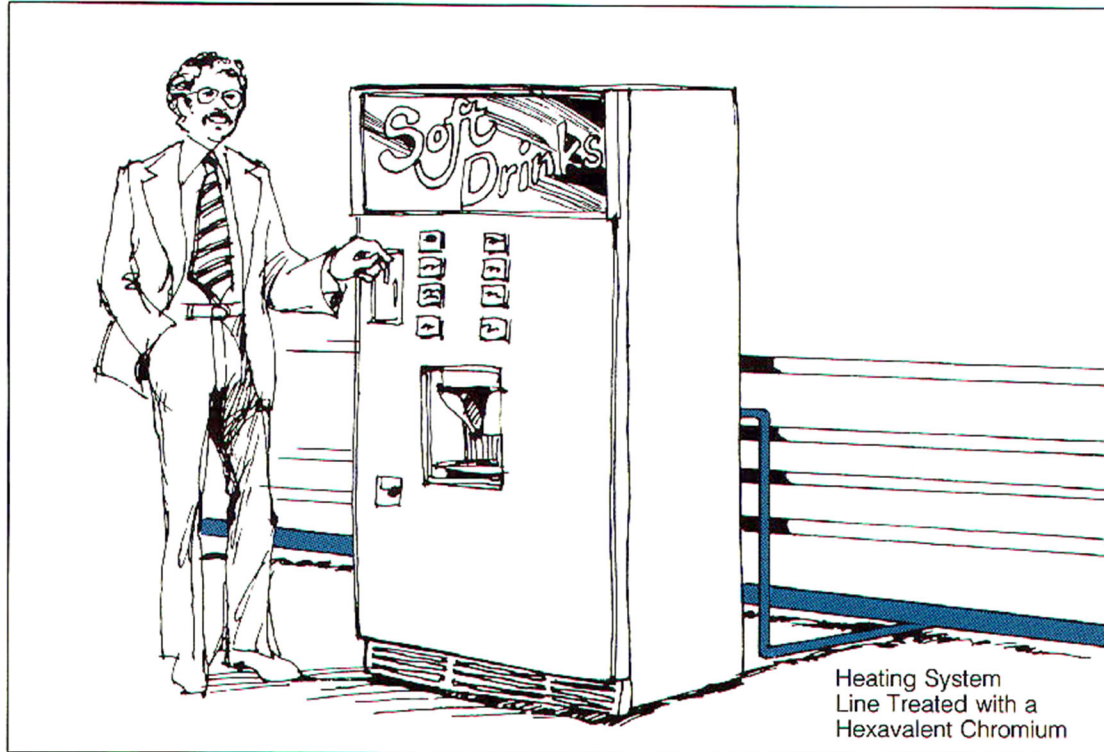
## BACKSIPHONAGE

## Common Cross-Connection Terms

### Cross-Connection

A cross-connection is any temporary or permanent connection between a public water system or consumer's potable (i.e., drinking) water system and any source or system containing nonpotable water or other substances.

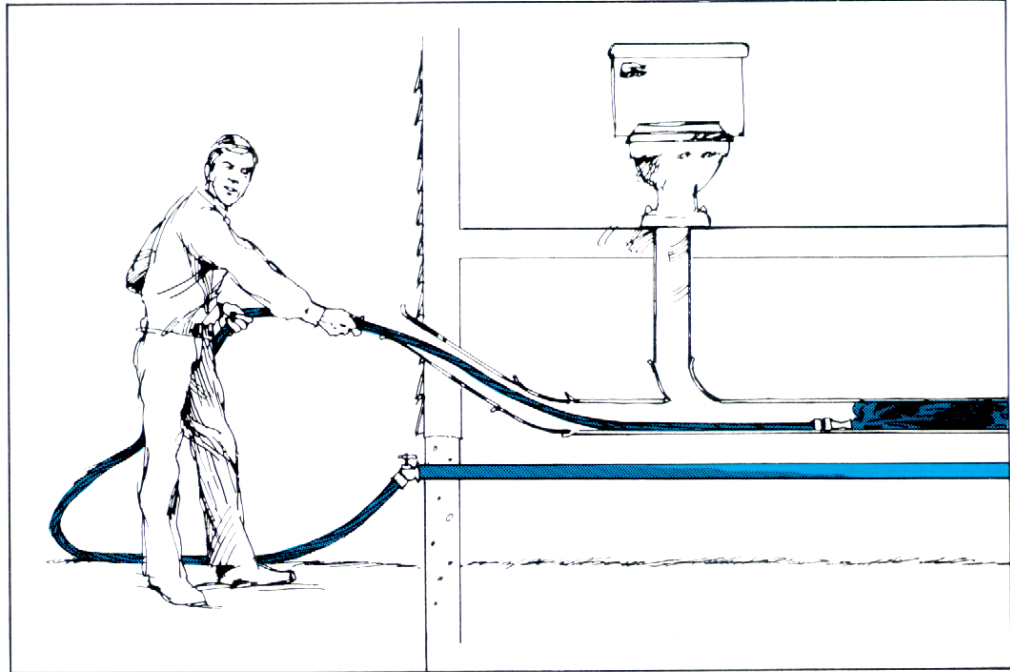
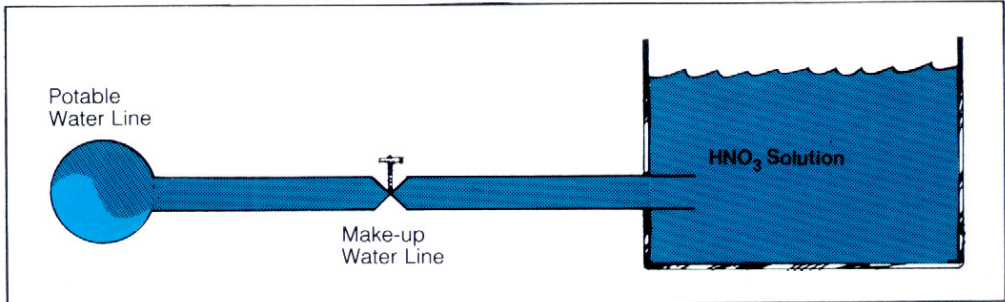
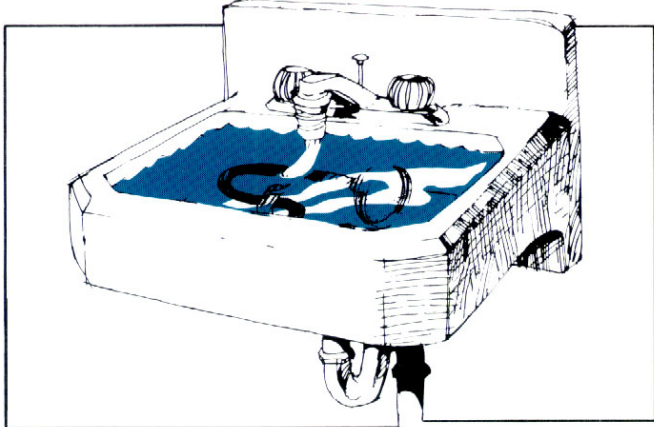
An example is the piping between a public water system or consumer's potable water system and an auxiliary water system, cooling system, or irrigation system.



Several cross-connection have been made to soda machines, the one to worry about is when you have a copper water line hooked to CO<sub>2</sub> without a backflow preventer.

The reason is that the CO<sub>2</sub> will mix in the water and create copper carbonic acid which can be deadly. This is one reason that you will see clear plastic lines at most soda machines and no copper lines. Most codes require a stainless steel RP backflow assembly at soda machines.

**Common Cross-Connections**

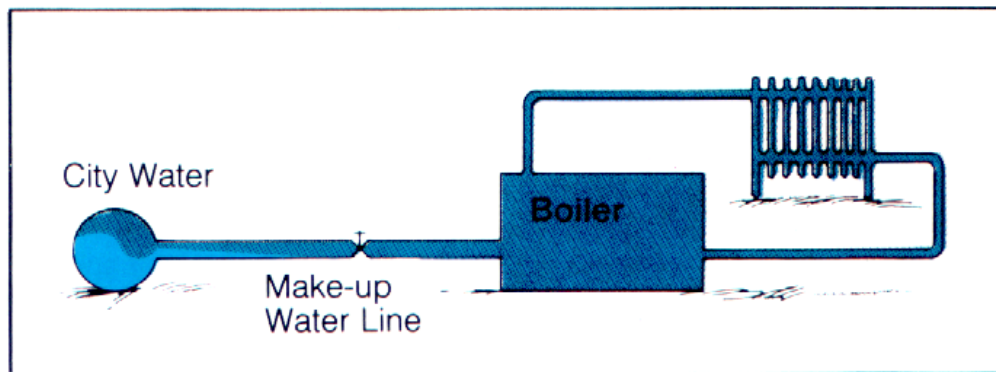


Bottom, a direct connection between water and sewage. *A perfect cross-connection and it happens all day long.*

## Backflow

Backflow is the undesirable reversal of flow of nonpotable water or other substances through a cross-connection and into the piping of a public water system or consumer's potable water system. There are two types of backflow--**backpressure** and **backsiphonage**.

### *Backsiphonage*



Backpressure caused by heat.



If you ever need to prove for a need for backflow protection, visit your local fair grounds or trailer park. I guarantee that you'll find all you need at the concession stand and most health departments and plumbing officials either do not know or could care less. Here is a photograph of a drinking water and sewer connection in the same meter box with the sewer backing up. The white hose is for drinking water and it is back siphoning the sewage water, the sheen is a reflection of the water pulsating in and out of the meter box.

### **What is backflow? *Reverse flow condition.***

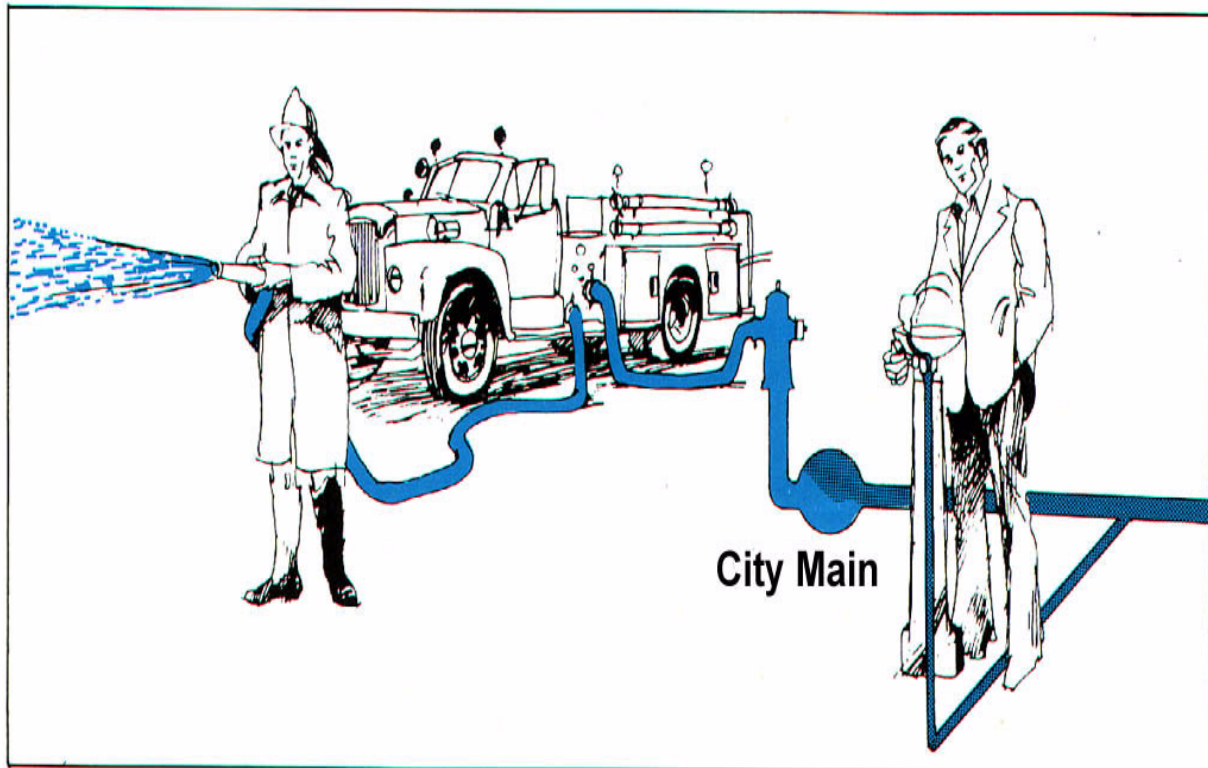
Backflow is the undesirable reversal of flow of nonpotable water or other substances through a cross-connection and into the piping of a public water system or consumer's potable water system. There are two types of backflow--**backpressure** and **backsiphonage**.



## Backsiphonage

Backsiphonage is backflow caused by a negative pressure (i.e., a vacuum or partial vacuum) in a public water system or consumer's potable water system. The effect is similar to drinking water through a straw.

Backsiphonage can occur when there is a stoppage of water supply due to nearby fire fighting, a break in a water main, etc.



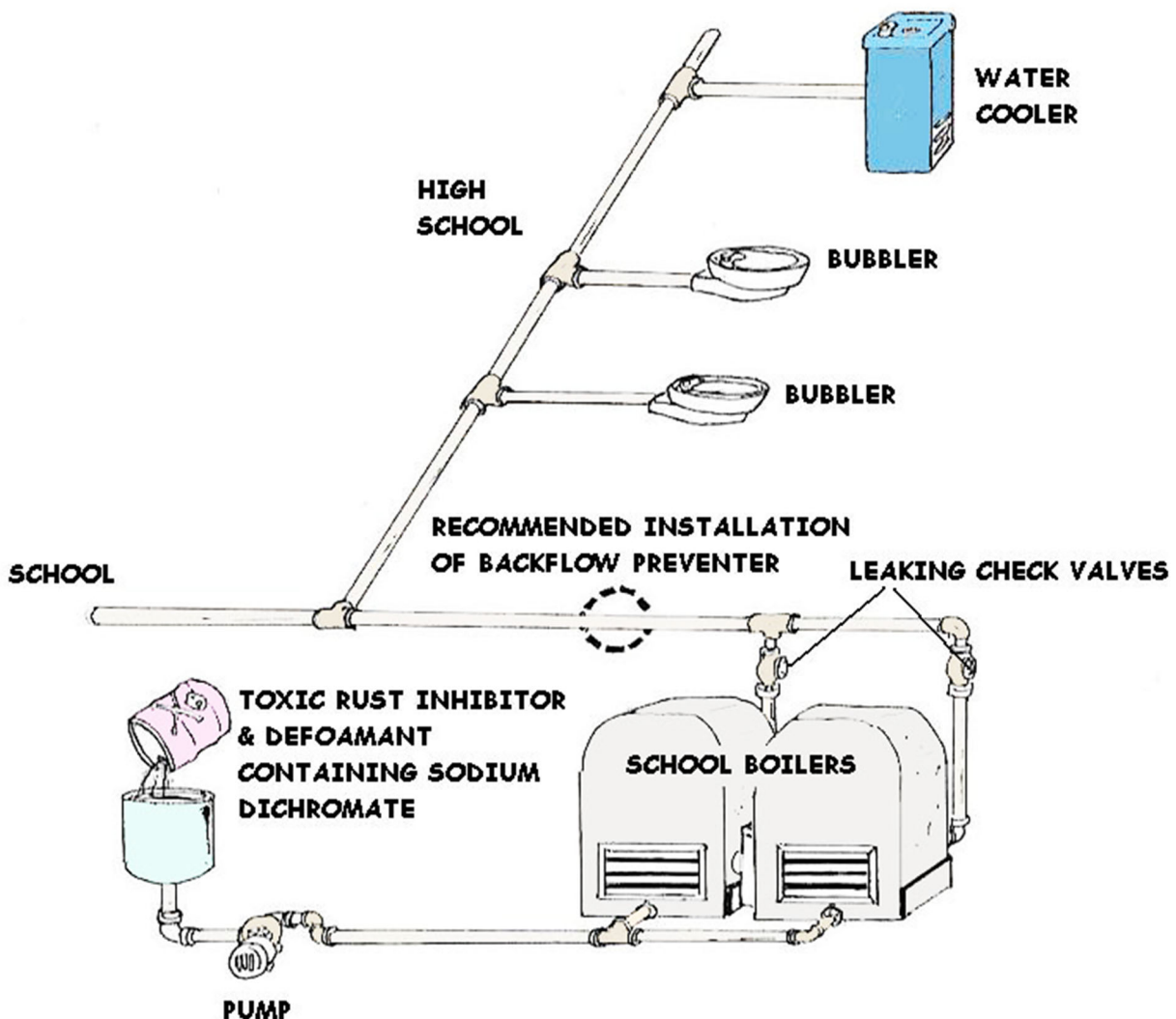
Every day, our public water system has several backsiphonage occurrences, Think of people that use water driven equipment, from a device that drains water-beds to pesticide applicators.

Backpressure is rarer, but does happen in areas of high elevation, like tall buildings or buildings with pumps. A good example is the pressure exerted by a building that is 100 feet tall is about 43 PSI, the water main feeding the building is at 35 PSI. The water will flow back to the water main. Never drink water or coffee inside a funeral home, vet clinic or hospital.

## Backpressure

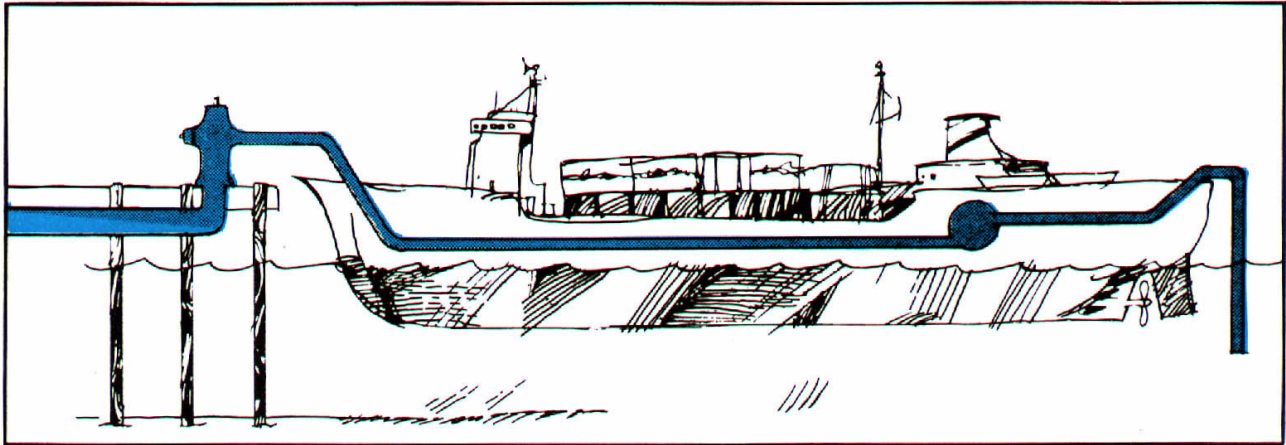
Backpressure backflow is backflow caused by a downstream pressure that is greater than the upstream or supply pressure in a public water system or consumer's potable water system. Backpressure (i.e., downstream pressure that is greater than the potable water supply pressure) can result from an increase in downstream pressure, a reduction in the potable water supply pressure, or a combination of both. Increases in downstream pressure can be created by pumps, temperature increases in boilers, etc.

Reductions in potable water supply pressure occur whenever the amount of water being used exceeds the amount of water being supplied, such as during water line flushing, firefighting, or breaks in water mains.



## Backpressure Examples

*Booster pumps, pressure vessels, elevation, heat*



Here we see the backpressure of salt water back into the public water system from a ship's pressure pump. Most water providers are now requiring a RP assembly at the hydrant.

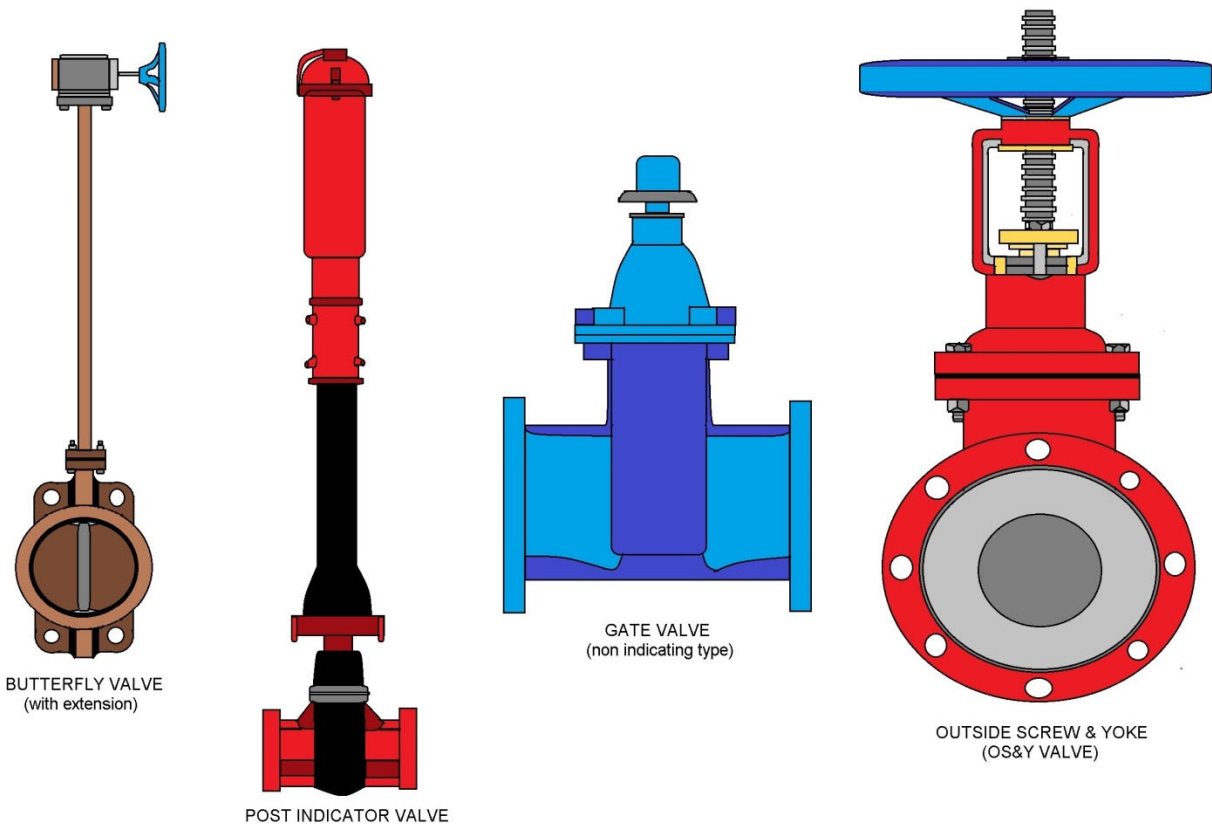
### What is a backflow preventer?

A backflow preventer is a means or mechanism to prevent backflow. The basic means of preventing backflow is an air gap, which either eliminates a cross-connection or provides a barrier to backflow. The basic mechanism for preventing backflow is a mechanical backflow preventer, which provides a physical barrier to backflow. The principal types of mechanical backflow preventer are the reduced-pressure principle assembly, the pressure vacuum breaker assembly, and the double check valve assembly.

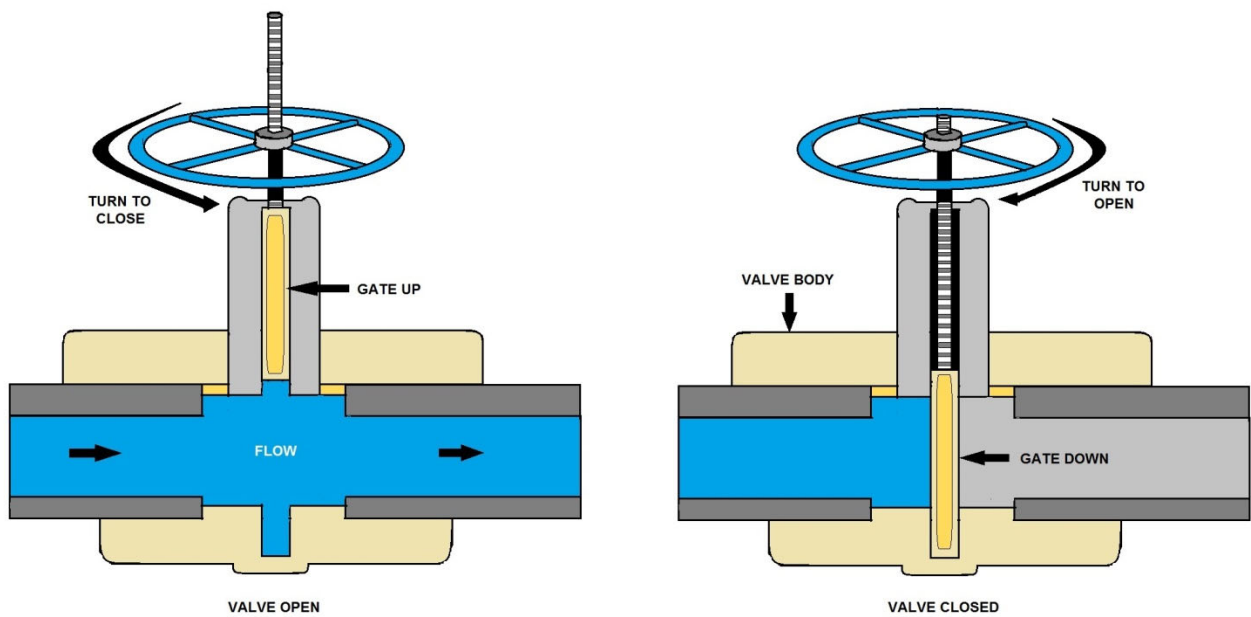
### Residential Dual Check Valve

A secondary type of mechanical backflow preventer is the residential dual check valve. We do not recommend the installation of dual checks because there is no testing method or schedule for these devices. Once these devices are in place, they, like all mechanical devices, are subject to failure and will probably be stuck open.

Some type of debris will keep the device from working properly.



## TYPES OF VALVES



## OS&Y VALVE

## Types of Backflow Prevention Methods and Assemblies

### Backflow Devices

Cross connections must either be physically disconnected or have an approved backflow prevention device installed to protect the public water system. There are five types of approved devices/methods:

1. Air gap- *Is not really a device but is a method.*
2. Atmospheric vacuum breaker
3. Pressure vacuum breaker
4. Double check valve
5. Reduced pressure principle backflow preventer (RP device)

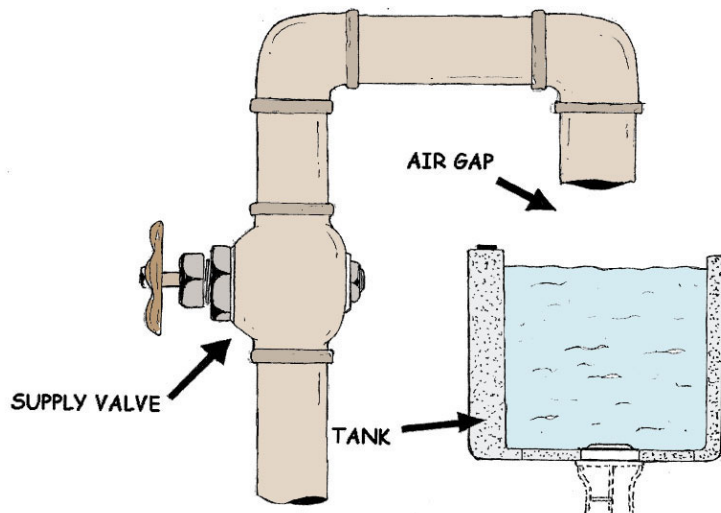
The type of device selected for a particular installation depends on several factors. First, the degree of hazard must be assessed. A high hazard facility is one in which a cross connection could be hazardous to health, such as a chrome plating shop or a sewage treatment plant. A low hazard situation is one in which a cross connection would cause only an aesthetic problem such as a foul taste or odor.

Second, the plumbing arrangement must be considered.

Third, it must be determined whether protection is needed at the water meter or at a location within the facility. A summary of these factors and the recommended device selection is given in Table 7-1.

### Approved Air Gap Separation (AG)

An approved air gap is a physical separation between the free flowing discharge end of a potable water supply pipeline, and the overflow rim of an open or non-pressure receiving vessel. These separations must be vertically orientated a distance of at least twice the inside diameter of the inlet pipe, but never less than one inch.



An obstruction around or near an air gap may restrict the flow of air into the outlet pipe and nullify the effectiveness of the air gap to prevent backsiphonage. When the air flow is restricted, such as the case of an air gap located near a wall, the air gap separation must be increased. Also, within a building where the air pressure is artificially increased above atmospheric, such as a sports stadium with a flexible roof kept in place by air blowers, the air gap separation must be increased.



Which of these ice machine drains has an approved air gap? Here is a better question; would you use the ice from this ice machine? Here is where all those stories about cockroaches and stomach flu originate. The stories are true.

### **Air Gap**

An air gap is a physical disconnection between the free flowing discharge end of a potable water pipeline and the top of an open receiving vessel. The air gap must be at least two times the diameter of the supply pipe and not less than one inch.

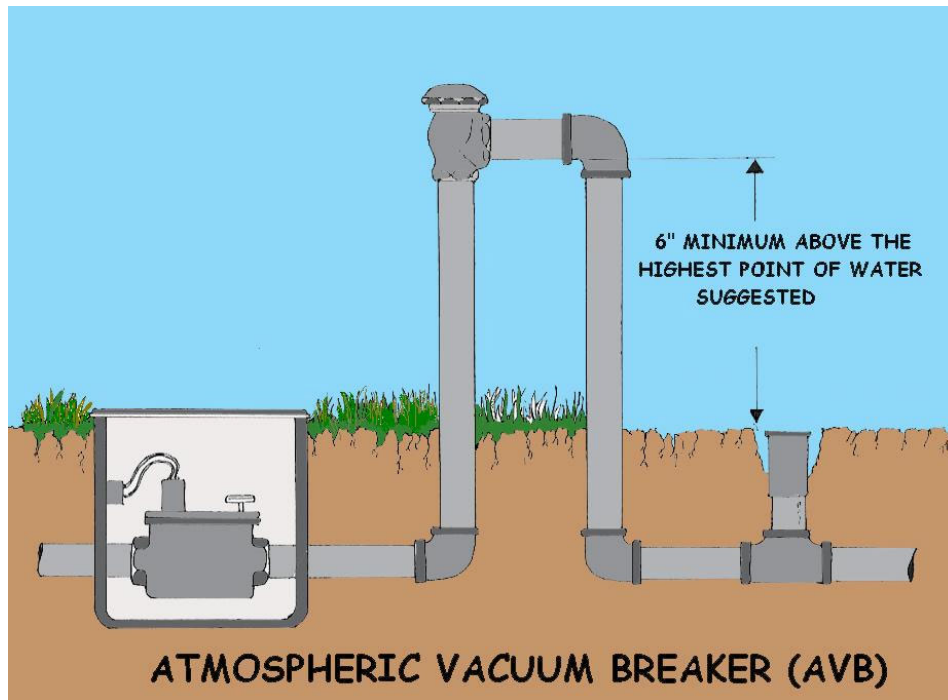
This type of protection is acceptable for high hazard installations and is theoretically the most effective protection.

However, this method of prevention can be circumvented if the supply pipe is extended.



## Vacuum Breakers

There are two types of vacuum breakers, atmospheric and pressure. The difference between them is that the pressure vacuum breaker is spring loaded to assist the device's opening. Both devices open the pipeline to atmosphere in the event of backsiphonage only. Neither device is approved for backpressure conditions. Both devices are only suitable for low hazard applications. Their primary purpose is to protect the water system from cross connections due to submerged inlets, such as irrigation systems and tank applications. Shutoff valves may not be installed downstream of atmospheric vacuum breakers but are allowed on pressure vacuum breakers. The devices must be installed above the highest downstream piping.

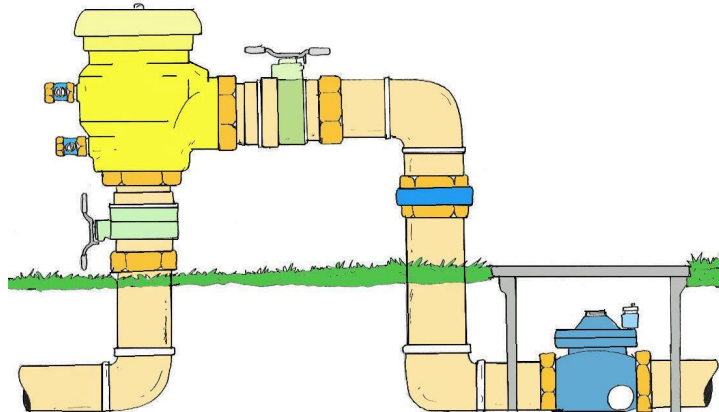


**Atmospheric Vacuum Breaker (AVB)** The Atmospheric Vacuum Breaker contains a float check (poppet), a check seat, and an air inlet port. The device allows air to enter the water line when the line pressure is reduced to a gauge pressure of zero or below. The air inlet valve is not internally loaded. To prevent the air inlet from sticking closed, the device must not be installed on the pressure side of a shutoff valve, or wherever it may be under constant pressure more than 12 hours during a 24 hour period.

Atmospheric vacuum breakers are designed to prevent backflow caused by backsiphonage only from low health hazards. Atmospheric Vacuum Breaker Uses: Irrigation systems, commercial dishwasher and laundry equipment, chemical tanks and laboratory sinks (backsiphonage only, non-pressurized connections.) (Note: hazard relates to the water purveyor's risk assessment; plumbing codes may allow AVB for high hazard fixture isolation).

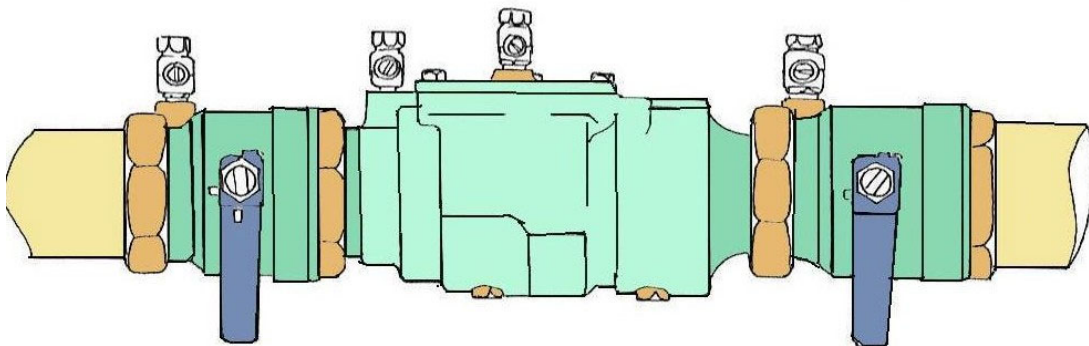
**Pressure Vacuum Breaker Assembly (PVB)** The Pressure Vacuum Breaker Assembly consists of a spring loaded check valve, an independently operating air inlet valve, two resilient seated shutoff valves, and two properly located resilient seated test cocks. It shall be installed as a unit as shipped by the manufacturer. The air inlet valve is internally loaded to the open position, normally by means of a spring, allowing installation of the assembly on the pressure side of a shutoff valve. The PVB needs to be installed 12 inches above the highest downstream outlet to work correctly.

PRESSURE VACUUM BREAKER ASSEMBLY



### **Double Check Valve Assembly (DC)**

The Double Check Valve Assembly consists of two internally loaded check valves, either spring loaded or internally weighted, two resilient seated full ported shutoff valves, and four properly located resilient seated test cocks. This assembly shall be installed as a unit as shipped by the manufacturer. The double check valve assembly is designed to prevent backflow caused by backpressure and backsiphonage from low health hazards or polluttional concerns only. The double check valve should be installed in an accessible location and protected from freezing. The DC needs to be installed 12 inches above the ground for testing purposes only.



DOUBLE CHECK VALVE ASSEMBLY



## Reduced Pressure Backflow Assembly (RP)

The reduced pressure backflow assembly consists of two independently acting spring loaded check valves separated by a spring loaded differential pressure relief valve, two resilient seated full ported shutoff valves, and four properly located resilient seated test cocks. This assembly shall be installed as a unit shipped by the manufacturer.

During normal operation, the pressure between the two check valves, referred to as the zone of reduced pressure, is maintained at a lower pressure than the supply pressure. If either check valve leaks, the differential pressure relief valve maintains a differential pressure of at least two (2) psi between the supply pressure and the zone between the two check valves by discharging water to atmosphere.

The reduced pressure backflow assembly is designed to prevent backflow caused by backpressure and backsiphonage from low to high health hazards. The RP needs to be installed 12 inches above the ground for testing purposes only.



Two brand new RPs.

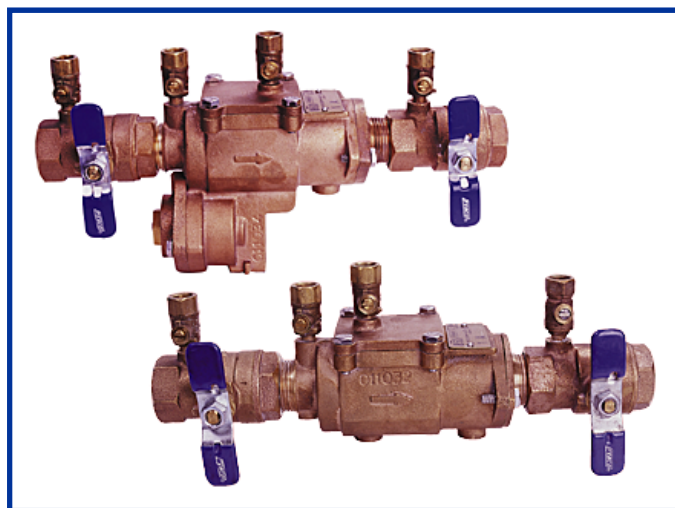
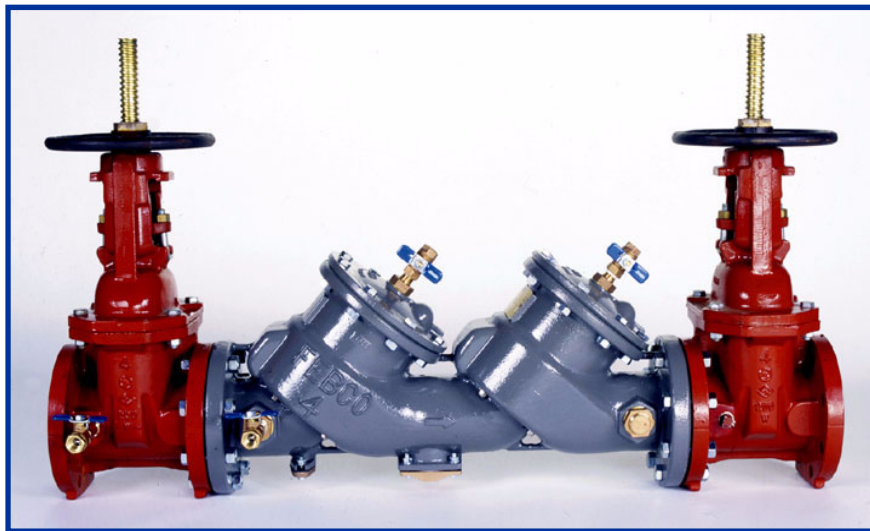
## Different Types of RPs

The RP consists of two internally loaded (weighted or spring loaded) check valves separated by a reduced pressure zone with a relief port to vent water to the atmosphere.

The reduced pressure device can be used for high hazard situations under both backpressure and backsiphonage conditions. Under normal conditions, the second check valve should prevent backflow.

However, if the second check valve fails or becomes fouled and backflow into the reduced pressure zone occurs, the relief port vents the backflow to atmosphere.

The reduced pressure zone port opens anytime pressure in the zone comes within 2 psi of the supply pressure.

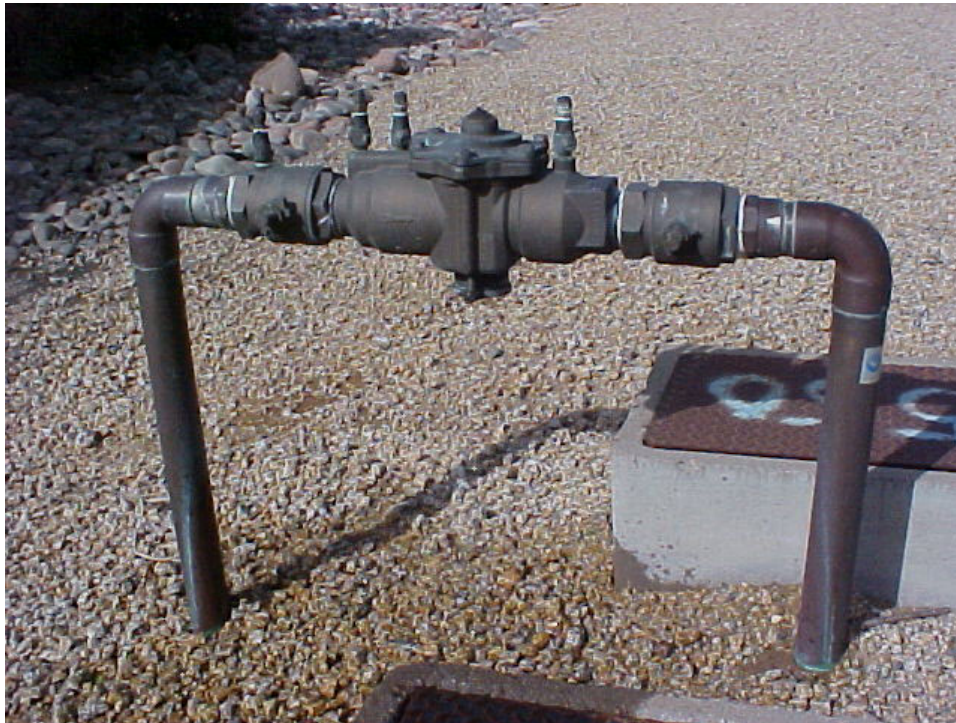


## Why do Backflow Preventors have to be Tested Periodically?

Mechanical backflow preventors have internal seals, springs, and moving parts that are subject to fouling, wear, or fatigue. Also, mechanical backflow preventors and air gaps can be bypassed. Therefore, all backflow preventors have to be tested periodically to ensure that they are functioning properly. A visual check of air gaps is sufficient, but mechanical backflow preventors have to be tested with properly calibrated gauge equipment.

Backflow prevention devices must be tested annually to ensure that they work properly. It is usually the responsibility of the property owner to have this test done and to make sure that a copy of the test report is sent to the Public Works Department or Water Purveyor.

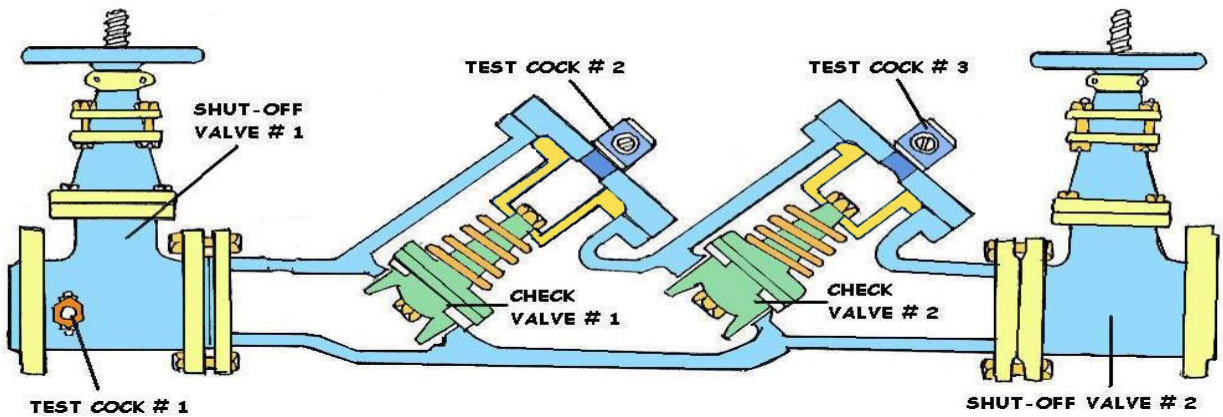
If a device is not tested annually, Public Works or the Water Purveyor will notify the property owner, asking them to comply. If the property owner does not voluntarily test their device, the City may be forced to turn off water service to that property. State law requires the City to discontinue water service until testing is complete.



Leaky RP--have your assemblies tested annually or more often. Re-test after repairs and problems. A RP should not leak more than 1 or 2 minute—any more than that, there is a problem; a piece of debris or stuck check is causing the RP's hydraulic relief port to dump.



Here is an RP that had never been tested and leaked every day until the grass was 3 feet high and the owner notified the Water Department of a water leak. The water meter reader should have caught this problem in the first couple months.



**DOUBLE - CHECK BACKFLOW ASSEMBLY DIAGRAM**

## Fireline Backflow Assemblies



Example of an inline and vertical Reduced Pressure Backflow Assembly.

## Fire Suppression Systems

- ✓ Properly designed and installed fixed fire suppression systems enhance fire safety in the workplace. Automatic sprinkler systems throughout the workplace are among the most reliable firefighting means. The fire sprinkler system detects the fire, sounds an alarm and puts the water where the fire and heat are located.
- ✓ Automatic fire suppression systems require proper maintenance to keep them in serviceable condition. When it is necessary to take a fire suppression system out of service while business continues, the employer must temporarily substitute a fire watch of trained employees standing by to respond quickly to any fire emergency in the normally protected area. The fire watch must interface with the employers' fire prevention plan and emergency action plan.
- ✓ Signs must be posted about areas protected by total flooding fire suppression systems which use agents that are a serious health hazard such as carbon dioxide, Halon 1211, etc. Such automatic systems must be equipped with area pre-discharge alarm systems to warn employees of the impending discharge of the system and allow time to evacuate the area. There must be an emergency action plan to provide for the safe evacuation of employees from within the protected area. Such plans are to be part of the overall evacuation plan for the workplace facility.



Halon Systems

## Fire System Classifications

Industrial fire protection systems will usually consist of sprinklers, hose connections, and hydrants. Sprinkler system may be dry or wet, open or closed. Systems of fixed-spray nozzles may be used indoors or outdoors for protection of flammable-liquid and other hazardous processes. It is standard practice, especially in cities, to equip automatic sprinkler systems with fire department pumper connections.

For cross-connection control, fire protection systems may be classified on the basis of water source and arrangement of supplies as follows:

1. **Class 1**--direct connections from public water mains only; no pumps, tanks, or reservoirs; no physical connection from other water supplies; no antifreeze or other additives of any kind; all sprinkler drains discharging to atmosphere, dry wells, or other safe outlets.
2. **Class 2**--same as class 1, except that booster pumps may be installed in the connections from the street mains (Booster pumps do not affect the potability of the system; it is necessary, however, to avoid drafting so much water that pressure in the water main is reduced below 10 psi.)
3. **Class 3**--direct connection from public water supply main plus one or more of the following: elevated storage tanks; fire pumps taking suction from above-ground covered reservoirs or tanks; and pressure tanks (All storage facilities are filled or connected to public water only, the water in the tanks to be maintained in potable conditions. Otherwise, Class 3 systems are the same as Class 1.)
4. **Class 4**--directly supplied from public mains similar to Classes 1 and 2, and with an auxiliary water supply on or available to the premises; or an auxiliary water supply may be located within 1,700 ft. of the pumper connection.
5. **Class 5**--directly supplied from public mains, and interconnected with auxiliary supplies, such as: pumps taking suction from reservoirs exposed to contamination, or rivers and ponds; driven wells; mills or other industrial water systems; or where antifreeze or other additives are used.
6. **Class 6**--combined industrial and fire protection systems supplied from the public water mains only, with or without gravity storage or pump suction tanks.

**Industrial Fluids** - shall mean any fluid or solution which may chemically, biologically or otherwise contaminated or polluted in a form or concentration such as would constitute a health, system, pollutional or plumbing hazard if introduced into an approved water supply.

This may include, but not be limited to: polluted or contaminated used water; all types of process waters and "used waters" originating from the public water system which may deteriorate in sanitary quality; chemicals in fluids from: plating acids and alkalies; circulated cooling waters connected to an open cooling tower and/or cooling waters that are chemically or biologically treated or stabilized with toxic substances; contaminated natural waters such as from wells, springs, streams, rivers, bays, harbors, seas, irrigation canals or systems, etc.; oils, gases, glycerin, paraffins, caustic and acid solutions and other liquid and gaseous fluids used in industrial or other processes or for firefighting purposes.

In some states, Fire lines need backflow prevention assemblies for certain criteria: a. Class 1 and 2 fire systems are not currently required to have any backflow prevention equipment at the service connection other than the equipment that is required for those systems under the state fire code standards. b. Class 3 fire systems may be converted to Class 1 or 2 systems by removing the tank. However, you must have the approval of the fire authority. c. Class 4 and 5 must comply with backflow requirements. Class 5 includes those fire systems that use antifreeze or other additives (RPDA required). This may apply to residential homes over 3,000 sq. ft. d. Class 6 fire systems require an on-site review to determine backflow requirements.



Double Check Backflow Assembly (Notice chain common on OS&Y).



## Common Backflow Questions and Answers

### 1. What is a cross connection, what two types of backflow can cause one, and what methods of protection can be used to prevent them?

**Backflow:** Water that flows back to the distribution system. It is sometimes caused by a loss of pressure in the water system. A reverse flow condition.

**Cross-Connection:** A physical connection between potable water and any other source or non-potable water.

**Backpressure:** Backpressure backflow is backflow caused by a downstream pressure that is greater than the upstream or supply pressure in a public water system or consumer's potable water system. Backpressure (i.e., downstream pressure that is greater than the potable water supply pressure) can result from an increase in downstream pressure, a reduction in the potable water supply pressure, or a combination of both. Increases in downstream pressure can be created by pumps, temperature increases in boilers, etc. Reductions in potable water supply pressure occur whenever the amount of water being used exceeds the amount of water being supplied, such as during water line flushing, firefighting, or breaks in water mains.

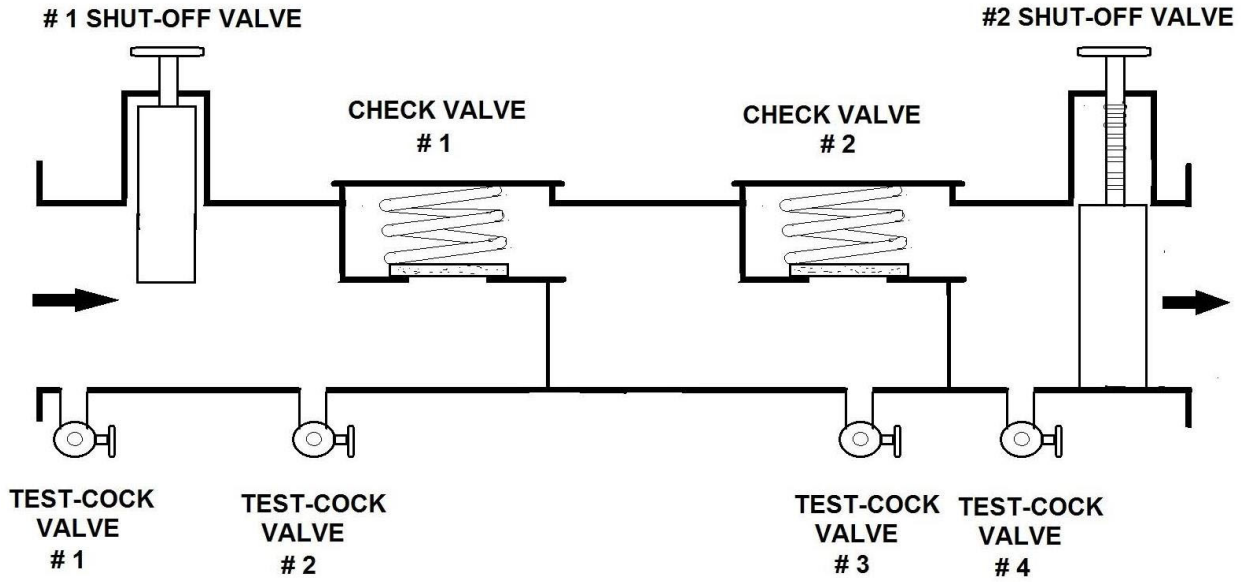
**Backsiphonage:** Backsiphonage is backflow caused by a negative pressure (i.e., a vacuum ~ or partial vacuum) in a Public water system or consumer's potable water system. The effect is similar to drinking water through a straw. Backsiphonage can occur when there is a stoppage of water supply due to nearby firefighting, a break in a water main, etc.

### 2. Why do water suppliers need to control cross-connections and protect their public water systems against backflow?

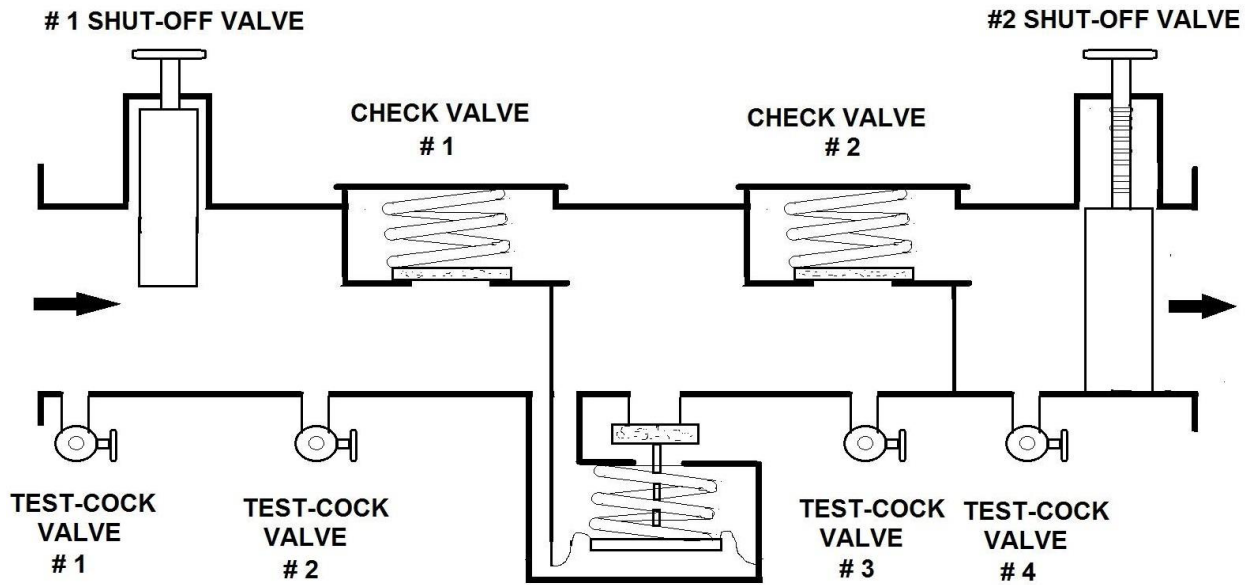
**Backflow:** Backflow into a public water system can pollute or contaminate the water in that system (i.e., backflow into a public water system can make the water in that system unusable or unsafe to drink), and each water supplier has a responsibility to provide water that is usable and safe to drink under all foreseeable circumstances. Furthermore, consumers generally have absolute faith that water delivered to them through a public water system is always safe to drink. For these reasons, each water supplier must take reasonable precautions to protect its public water system against backflow.

### 3. What should water suppliers do to control cross-connections and protect their public water systems against backflow?

Water suppliers usually do not have the authority or capability to repeatedly inspect every consumer's premises for cross-connections and backflow protection. Alternatively, each water supplier should ensure that a proper backflow preventer is installed and maintained at the water service connection to each system or premises that poses a significant hazard to the public water system.



**DOUBLE- CHECK BACKFLOW ASSEMBLY DIAGRAM**



**REDUCED PRESSURE PRINCIPLE BACKFLOW PREVENTION ASSEMBLY**

## CHAPTER 8 EXERCISE

---

The following assignment is Fill-in-the-Blank type answers.

1. \_\_\_\_\_: A group of bacteria commonly found in the environment. They are an indicator of potential contamination of water. Adequate and appropriate disinfection effectively destroys coliform bacteria.
2. \_\_\_\_\_: A virus whose presence may indicate contaminated water; a virus which may infect the gastrointestinal tract of humans.
3. \_\_\_\_\_: A group of bacteria that may indicate the presence of human or animal fecal matter in water.
4. \_\_\_\_\_: A pathogenic parasite which may be found in contaminated water.
5. \_\_\_\_\_: An atmosphere which by reason of being explosive, flammable, poisonous, corrosive, oxidizing, irritating, oxygen deficient, toxic, or otherwise harmful, may cause death, illness, or injury.
6. \_\_\_\_\_: A broad group of bacteria including non-pathogens, pathogens, and opportunistic pathogens; they may be an indicator of poor general biological quality of drinking water. Often referred to as HPC.
7. \_\_\_\_\_: Disease-producing bacteria, viruses and other microorganisms.
8. \_\_\_\_\_: To reverse the natural and normal directional flow of liquids, gases, or solid substances back in to the public potable (drinking) water supply. This is normally an undesirable effect.
9. \_\_\_\_\_: Any natural or man-made physical, chemical, biological, or radiological substance or matter in water, which is at a level that may have an adverse effect on public health, and which is known or anticipated to occur in public water systems.
10. \_\_\_\_\_: To make something bad. To pollute or infect something. To reduce the quality of the potable (drinking) water and create an actual hazard to the water supply by poisoning or through spread of diseases.
11. \_\_\_\_\_: If water flows through a pipeline at a high velocity, the pressure in the pipeline is reduced. Velocities can be increased to a point that a partial vacuum is created.
12. \_\_\_\_\_: To stop or prevent the occurrence of, the unnatural act of reversing the normal direction of the flow of liquids, gases, or solid substances back in to the public potable (drinking) water supply.

13. \_\_\_\_\_: A liquid substance that is carried over a higher point. It is the method by which the liquid substance may be forced by excess pressure over or into a higher point.
14. \_\_\_\_\_: A disease, caused by a virus, bacterium, protozoan, or other microorganism, capable of being transmitted by water (e.g., typhoid fever, cholera, amoebic dysentery, gastroenteritis).
15. \_\_\_\_\_: A physical separation space that is present between the discharge vessel and the receiving vessel, for an example, a kitchen faucet. The best form of backflow protection.
16. \_\_\_\_\_: A physical separation which may be a low inlet into the indirect waste receptor from the fixture, or device that is indirectly connected. You will most likely find this on waste fixtures or on non-potable lines. You should never allow one on an ice machine.
17. \_\_\_\_\_: A disease-causing parasite, resistant to chlorine disinfection. It may be found in fecal matter or contaminated drinking water.
18. \_\_\_\_\_: To kill and inhibit growth of harmful bacterial and viruses in drinking water.
19. \_\_\_\_\_: The treatment of water to inactivate, destroy, and/or remove pathogenic bacteria, viruses, protozoa, and other parasites.
20. \_\_\_\_\_: The maximum allowable level of a contaminant that federal or state regulations allow in a public water system. If it is exceeded, the water system must treat the water so that it meets it, or provide adequate backflow protection.
21. \_\_\_\_\_: Any minute, simple, single-celled form of life, especially one that causes disease.
22. \_\_\_\_\_: Microscopic organisms present in untreated water that can cause waterborne diseases.
23. \_\_\_\_\_: To make something unclean or impure. Some states will have a definition of pollution that relates to non-health related water problems, like taste and odors.
24. \_\_\_\_\_: disease-causing; waterborne. A bacterium, virus or parasite that causes or is capable of causing disease. They may contaminate water and cause waterborne disease.
25. \_\_\_\_\_: Good water which is safe for drinking or cooking purposes.  
Non-Potable: A liquid or water that is not approved for drinking.
26. \_\_\_\_\_: chemical which disinfects (kills bacteria), kills algae and oxidizes organic matter.

27. \_\_\_\_\_: Also known as superchlorination or break point chlorination. Ridding a pool of organic waste by the addition of significant quantities of a halogen. Often the best cure for ridding a water line of contamination after a backflow incident.

28. Can Backflow happen in a gas or sewer line or is backflow limited to water?

29. Is a Backflow Incident possible at your facility? Explain

30. How can you prepare or guard against a backflow incident?

31. Are you prepared for your potable water system to become contaminated?

32. How would you disinfect or prepare for non-potable water during an emergency?

Think about how long your facility could survive without potable water.



## Chapter 9: Cyber-Terrorism or Cyber-Crime

**Section Focus:** You will learn the basics of cyber-terrorism. At the end of this section, you the student will be able to understand and describe various cyber-terrorism attacks. There is a post quiz at the end of this section to review your comprehension and a final examination in the Assignment for your contact hours.

**Scope/Background:** Review of the different methods of destroying and protection of your computer files including SCADA and Internet systems.



**Cyberterrorism** is the use of the Internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation. It is also sometimes considered an act of Internet terrorism where terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet by means of tools such as computer viruses, computer worms, phishing, and other malicious software and hardware methods and programming scripts.

Cyberterrorism is a controversial term. Some authors opt for a very narrow definition, relating to deployment by known terrorist organizations of disruption attacks against information systems for the primary purpose of creating alarm, panic, or physical disruption. Other authors prefer a broader definition, which includes cybercrime. Participating in a cyberattack affects the terror threat perception, even if it isn't done with a violent approach. By some definitions, it might be difficult to distinguish which instances of online activities are cyberterrorism or cybercrime.

Cyberterrorism can be also defined as the intentional use of computers, networks, and public internet to cause destruction and harm for personal objectives.

Experienced cyberterrorists, who are very skilled in terms of hacking can cause massive damage to government systems, hospital records, and national security programs, which might leave a country, community or organization in turmoil and in fear of further attacks. The objectives of such terrorists may be political or ideological since this can be considered a form of terror.



There is much concern from government and media sources about potential damage that could be caused by cyberterrorism, and this has prompted efforts by government agencies such as the Federal Bureau of Investigations (FBI) and the Central Intelligence Agency (CIA) to put an end to cyber-attacks and cyberterrorism.



## Newspaper Article

February 11, 2021 Aaron Weaver

### Hacker Tries to Poison Drinking Water in Small Florida Town

Remember the name, “Oldsmar, Florida.” You probably won’t. But if hackers had been able to carry out their plans, it would likely be a name you would never forget. That’s because the 15,000 residents of this town were nearly poisoned by a cybercriminal who hacked into their water treatment facility.



**Marco Rubio** @marcorubio · Feb 8

I will be asking the @FBI to provide all assistance necessary in investigating an attempt to poison the water supply of a #Florida city.

This should be treated as a matter of national security.

[vice.com/en/article/88a...](https://www.vice.com/en/article/88a...) via @vice



Hacker Tried to Poison Florida City's Water Supply, Police Say  
The hacker tried to drastically increase sodium hydroxide levels in the water, Pinellas County, Florida, officials said on Monday.

[vice.com](https://www.vice.com)

Sheriff Bob Gualtieri of Pinellas County said that the main ingredient in drain cleaner, sodium hydroxide, was increased 100-fold from 100 parts per million to 11,100. Those high levels could’ve made victims severely ill or worse. Gualtieri called this “dangerous stuff.” He continued: It’s a bad act. It’s a bad actor. It’s not just a little chlorine, or a little fluoride — you’re basically talking about lye.

Florida Senator Marco Rubio said this event should be treated as a “matter of national security.” Marco Rubio is not taking this lightly. | Source: Twitter  
And he’s absolutely right. As Joe Biden pushes for more funding into national cybersecurity, events like this prove why it’s so important.

### **How Did This Happen?**

Last Friday, an employee noticed that someone was controlling his computer. Apparently, the water treatment facility operates with software that allows supervisors to access computers remotely. But it hadn’t in some time. According to CNN, the hacked software TeamViewer had been dormant for about six months, even though it was still on the system.

After about five and a half hours, however, the employee realized that the foreign actor was accessing different programs and changing the levels of lye. Thank goodness. Because of that employee’s awareness, the drinking supply in Oldsmar was not compromised by the time it reached residents. Robert M. Lee, the CEO of the cybersecurity company Dragos Inc., told CNN that “it’s exactly what folks worry about.”

### **It’s Not the First Time**

If 2020 was one of the most significant years ever for cybercriminals, 2021 is off to a hot start. After the massive attacks on FireEye and SolarWinds (collectively known as the Sunburst hack) last year, Joe Biden and his new regime have pushed for more cybersecurity funding. And they absolutely should. While the Sunburst attack was devastating and the fallout is still being assessed, it was not an outright attack on U.S. infrastructure. The same can’t be said about the water treatment hack.

## Hackers force water utilities to sink or swim

Blake Sobczak, E&E News reporter Published: Thursday, March 28, 2019

Last month, hackers tied computers into knots at a small Colorado water utility. It wasn't the first time the Fort Collins-Loveland Water District and its wastewater counterpart had been hit by "ransomware," a type of malware that encrypts victims' computer files and demands online payment to unlock them.

While operations weren't harmed, the infection prompted the water district to switch out its information technology service provider and call in the FBI. The case, first reported by the *Coloradoan*, remains under active investigation. FCLWD and the South Fort Collins Sanitation District treat and distribute water to 45,000 customers in northern Colorado.

Colorado water officials aren't alone in their cybersecurity woes. The nation's nearly 70,000 water and wastewater utilities are struggling to keep their heads above a rising tide of online threats, based on interviews with security experts and water company operators.

As one IT manager at a midsize water utility put it, "It's not a question of if, it's a question of when" hackers disrupt vital U.S. water systems. "Most small and midsize utilities are overstressed," said the manager, who requested anonymity.

Some larger utilities are well-positioned to thwart an attack by hackers backed by a foreign government, said Michael Arceneaux, managing director for the Water Information Sharing and Analysis Center, the industry's clearinghouse for getting the word out about the latest hacking threats and vulnerabilities. But in a sector that encompasses tens of thousands of local water systems, securing America's vast and disparate drinking water supply remains a significant challenge.

"Drinking water utilities run the gamut in terms of cybersecurity preparedness," Arceneaux said. "What we try to do to compensate for that is make sure people are aware of the threats, so they have some motivation to invest the resources that should be invested."

He said the ISAC and its membership recently reached the level of maturity needed to start partnering with other sharing and analysis centers, including the multistate government ISAC and the electric power sector's E-ISAC.

Water utilities and power distributors share similar industrial control systems, rely on many of the same equipment providers and can encounter similar cyberthreats. While the water system is inherently not as interconnected as the U.S. electricity system, "it's very plausible that the water sector is less prepared than the power sector for dealing with cybersecurity threats," Arceneaux said. "We are so fractured, so the water sector as a whole is at a little bit of a disadvantage."

### What keeps you up at night?

The decentralized nature of the U.S. water industry has left policymakers with a dilemma. Cybersecurity for water treatment and supply networks is only loosely monitored at the federal level and is often ignored by state utility commissions that may have limited cybersecurity expertise and tend to focus on water quality.

"Water cybersecurity is not on everyone's — or certainly not every commissioner's — radar screen, although I've tried to make it that way," said Mary-Anna Holden, a commissioner on the New Jersey Board of Public Utilities.

In many emergency planning exercises, it isn't the lack of electricity that triggers chaos and widespread casualties. It's the lack of clean water that forces people from their homes.

"Nobody thinks about wastewater systems until they break," said Holden, who chairs the Committee on Water at the National Association of Regulatory Utility Commissioners.

## Hackers

A slang term for a computer enthusiast, i.e., a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s). Among professional programmers, depending on how it used, the term can be either complimentary or derogatory, although it is developing an increasingly derogatory connotation. The pejorative sense of hacker is becoming more prominent largely because the popular press has co-opted the term to refer to individuals who gain unauthorized access to computer systems for the purpose of stealing and corrupting data. Hackers, themselves, maintain that the proper term for such individuals is cracker.

### Why Would Someone Hack Your Computer?

Besides gaining access to your private information, such as financial records or password files, intruders can, and do, use individuals' computers to:

- Launch denial of service (**DoS**) attacks against a high profile Web site. Once gaining control, the hacker can direct your computer, and hundreds or thousands of other so-called "**zombies**," to act simultaneously, which overloads and effectively shuts down a popular site.
- Distribute software illegally. After appropriating space on your hard drive, they enable others to access your computer as a "**warez**" site and download pirated entertainment or business applications.

### America's Most Wanted Computer Outlaw

Kevin Mitnick, "**America's Most Wanted Computer Outlaw**," eluded the police, US Marshals, and FBI for over two years after vanishing while on probation for his 1989 conviction for computer and access device fraud. His downfall was his Christmas 1994 break-in to Tsutomu Shimomura's computers in San Diego, California. Less than two months later, Tsutomu had tracked him down after a cross-country electronic pursuit. Mitnick was arrested by the FBI in Raleigh, North Carolina, on February 15th, 1995.



While he was on the run, he broke into countless computers, intercepted private electronic communications, and copied off personal and confidential materials. Among the materials he copied off and stashed in readily accessible locations around the Net were personal electronic mail, stolen passwords, and proprietary software. Much of the stolen software was the trade secret source code to key products in which companies had invested many millions of dollars of development effort in order to maintain their competitive edge.

His activities on the systems he broke into, often altering information, corrupting system software, and eavesdropping on users, sometimes prevented or impeded legitimate use. He tried to stay a step ahead of the law by using cloned cellular telephones and stolen cellular and internet service for many of his intrusions. Mitnick was charged in North Carolina with 23 counts of access device fraud for his activities shortly before his arrest. In order to expedite his return to California, he agreed to plead guilty to one count and have his case consolidated in Los Angeles. In California, he was charged with an additional 25 counts of access device, wire, and computer fraud.

On March 16, 1999, Mitnick plead guilty to five of these counts and two additional counts from the Northern District of California. He was sentenced to 46 months and three years' probation, to be served in addition to eight months for his North Carolina plea and 14 months for his probation violation. He was released from prison on January 21, 2000, being eligible for early release after serving almost 60 months of his 68 month sentence.

***Here are some of Kevin Mitnick's and other Hacker's tricks in their language and attitude:***

### **Basic Hacking Skills**

The hacker attitude is vital, but skills are even more vital. Attitude is no substitute for competence, and there's a certain basic toolkit of skills which you have to have before any hacker will dream of calling you one.

This toolkit changes slowly over time as technology creates new skills and makes old ones obsolete. For example, it used to include programming in machine language, and didn't until recently involve HTML. But right now it pretty clearly includes the following:

#### **1. Learn how to Program.**

This, of course, is the fundamental hacking skill. If you don't know any computer languages, I recommend starting with Python. It is cleanly designed, well documented, and relatively kind to beginners. Despite being a good first language, it is not just a toy; it is very powerful, flexible and well suited for large projects. Good tutorials are available at the Python web site.

Java is also a good language for learning to program in. It is more difficult than Python, but produces faster code than Python. I think it makes an excellent second language.

Be aware that you won't reach the skill level of a hacker or even merely a programmer if you only know one or two languages -- you need to learn how to think about programming problems in a general way, independent of any one language. To be a real hacker, you need to get to the point where you can learn a new language in days by relating what's in the manual to what you already know. This means you should learn several very different languages.

If you get into serious programming, you will have to learn C, the core language of Unix. C++ is very closely related to C; if you know one, learning the other will not be difficult. Neither language is a good one to try learning as your first, however. And, actually, the more you can avoid programming in C the more productive you will be.

C is very efficient, and very sparing of your machine's resources. Unfortunately, C gets that efficiency by requiring you to do a lot of low-level management of resources (like memory) by hand. All that low-level code is complex and bug-prone, and will soak up huge amounts of your time on debugging. With today's machines as powerful as they are, this is usually a bad tradeoff -- it's smarter to use a language that uses the machine's time less efficiently, but your time much more efficiently. Thus, Python.

## Julian Assange

In 1987, after turning 16, Assange began hacking under the name "Mendax" (derived from a phrase of Horace: "splendide mendax", or "nobly untruthful"). He and two other hackers joined to form a group which they named the International Subversives. Assange wrote down the early rules of the subculture: "Don't damage computer systems you break into (including crashing them); don't change the information in those systems (except for altering logs to cover your tracks); and share information". The Personal Democracy Forum said he was "Australia's most famous ethical computer hacker."



The Australian Federal Police became aware of this group and set up "Operation Weather" to investigate their hacking. In September 1991 Mendax was discovered in the act of hacking into the Melbourne master terminal of Nortel, the Canadian telecommunications company. In response the Australian Federal Police tapped Assanges' phonenumber and subsequently raided his Melbourne home in 1991. He was also reported to have accessed computers belonging to an Australian university, the USAF 7th Command Group in the Pentagon and other organizations, via modem. It took three years to bring the case to court, where he was charged with 31 counts of hacking and related crimes. Nortel claimed his incursions cost them more than \$100,000 dollars.

Despite representing hacking as a victimless crime, he nonetheless pleaded guilty to 25 charges of hacking. Six charges were dropped. He was released on bond for good conduct after being fined \$2100. The judge said "there is just no evidence that there was anything other than sort of intelligent inquisitiveness and the pleasure of being able to—what's the expression—surf through these various computers" and stated that Assange would have gone to jail for up to 10 years if he had not had such a disrupted childhood.

Assange later commented, "It's a bit annoying, actually. Because I co-wrote a book about [being a hacker], there are documentaries about that, people talk about that a lot. They can cut and paste. But that was 20 years ago. It's very annoying to see modern day articles calling me a computer hacker. I'm not ashamed of it, I'm quite proud of it. But I understand the reason they suggest I'm a computer hacker now. There's a very specific reason."

In 2011 court records revealed that in 1993 Assange helped Victoria Police Child Exploitation Unit by providing technical advice and assisted in prosecuting persons.

In 1993, Assange was involved in starting one of the first public internet service providers in Australia, Suburbia Public Access Network. Starting in 1994, he lived in Melbourne as a programmer and a developer of free software. In 1995, he wrote Strobe, the first free and open source port scanner. He contributed several patches to the PostgreSQL project in 1996. He helped to write the book *Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier* (1997), which credits him as a researcher and reports his history with International Subversives.

Starting around 1997, he co-invented the Rubberhose deniable encryption system, a cryptographic concept made into a software package for Linux designed to provide plausible deniability against rubber-hose cryptanalysis; he originally intended the system to be used "as a tool for human rights workers who needed to protect sensitive data in the field." Other free software that he has authored or co-authored includes the Usenet caching software NNTPCache and Surfraw, a command-line interface for web-based search engines.

In 1999, he registered the domain leaks.org; "But", he says, "then I didn't do anything with it." From 2003 to 2006, Assange pursued a bachelor of science degree from the University of Melbourne. He also studied philosophy and neuroscience. He never graduated and received the minimum passing grades in most of his math courses. The fact that his fellow students were doing research for Pentagon's DARPA was reportedly a factor in motivating him to drop out and start WikiLeaks.

WikiLeaks was founded in 2006. That year, Assange wrote two essays setting out the philosophy behind WikiLeaks: "To radically shift regime behavior we must think clearly and boldly for if we have learned anything, it is that regimes do not want to be changed. We must think beyond those who have gone before us and discover technological changes that embolden us with ways to act in which our forebears could not." In his blog he wrote, "the more secretive or unjust an organization is, the more leaks induce fear and paranoia in its leadership and planning coterie.... Since unjust systems, by their nature induce opponents, and in many places barely have the upper hand, mass leaking leaves them exquisitely vulnerable to those who seek to replace them with more open forms of governance."

Assange is a prominent media spokesman on WikiLeaks' behalf. While newspapers have described him as a "director" or "founder" of Wikileaks, Assange has said, "I don't call myself a founder"; he does describe himself as the editor in chief of WikiLeaks, and has stated that



he has the final decision in the process of vetting documents submitted to the site. Assange says that Wikileaks has released more classified documents than the rest of the world press combined: "That's not something I say as a way of saying how successful we are – rather, that shows you the parlous state of the rest of the media.

How is it that a team of five people has managed to release to the public more suppressed information, at that level, than the rest of the world press combined? It's disgraceful." He advocates a "transparent" and "scientific" approach to journalism, saying that "you can't publish a paper on physics without the full experimental data and results; that should be the standard in journalism." In 2006, CounterPunch called him "Australia's most infamous former computer hacker." The Age has called him "one of the most intriguing people in the world" and "internet's freedom fighter." Assange has called himself "extremely cynical". He has been described as being largely self-taught and widely read on science and mathematics, and as thriving on intellectual battle.

WikiLeaks has been involved in the publication of material documenting extrajudicial killings in Kenya, a report of toxic waste dumping on the coast of Côte d'Ivoire, Church of Scientology manuals, Guantanamo Bay procedures, the 12 July 2007 Baghdad airstrike video, and material involving large banks such as Kaupthing and Julius Baer among other documents. In 2008, Assange published an article entitled "The Hidden Curse of Thomas Paine", in which he wrote "What does it mean when only those facts about the world with economic powers behind them can be heard, when the truth lays naked before the world and no one will be the first to speak without payment or subsidy?"

In late 2010, Assange was in the process of completing his memoirs for publication in 2011. On 28 November 2010, WikiLeaks began releasing some of the 251,000 American diplomatic cables in their possession, of which over 53 percent are listed as unclassified, 40 percent are "Confidential" and just over six percent are classified "Secret". The following day, the Attorney-General of Australia, Robert McClelland, told the press that Australia would inquire into Assange's activities and WikiLeaks. He said that "from Australia's point of view, we think there are potentially a number of criminal laws that could have been breached by the release of this information. The Australian Federal Police are looking at that". McClelland would not rule out the possibility that Australian authorities will cancel Assange's passport, and warned him that he might face charges should he return to Australia. The Federal Police inquiry found that Assange had not committed any crime.

The United States Department of Justice launched a criminal investigation related to the leak. US prosecutors are reportedly considering charges against Assange under several laws, but any prosecution would be difficult. In relation to its ongoing investigations of WikiLeaks, on 14 December 2010 the US DoJ issued a subpoena ordering Twitter to release information relating to Assange's account, amongst others. Pentagon Papers whistleblower Daniel Ellsberg said that Assange "is serving our [American] democracy and serving our rule of law precisely by challenging the secrecy regulations, which are not laws in most cases, in this country." On the issue of national security considerations for the US, Ellsberg added that "He's obviously a very competent guy in many ways. I think his instincts are that most of this material deserves to be out. We are arguing over a very small fragment that doesn't. He has not yet put out anything that hurt anybody's national security". Assange told London reporters that the leaked cables showed US ambassadors around the world were ordered "to engage in espionage behavior" which he said seemed to be "representative of a gradual shift to a lack of rule of law in US institutions that needs to be exposed and that we have been exposing."



## Virus Protection

Ensure your computer has anti-virus software installed and that you are familiar with its operation. If you are not sure, check the documentation or consult your unit's technical staff. ***Most important, make sure it is updated!***

Where possible, cut viruses off at the network before they can even reach an individual user's workstation. There are many methods available to allow system administrators to detect and eliminate viruses before they reach the corporate desktop.

There are publicly available additions to the primary configuration file for UNIX's Sendmail program that can configure Sendmail to either block the attachments, or to forward e-mails containing them through a virus scanner. In addition, most major firewall vendors provide some mechanism for virus screening at the network perimeter. These tools can be configured to either strip attachments from e-mails or to pass them through a virus scanner.

Remember, it doesn't necessarily take a person with bad intent to trash your systems -- just a destructive virus allowed to run wild.

### ***Password Use***

Your password is a vital component of the security of any system, since an unscrupulous person could use your account to damage other systems or impersonate you. Therefore, ensure that your password is chosen well and kept secure. Basically, passwords are almost zero protection but keep honest people out of your information.

### **Safe Passwords:**

- Are composed of at least six letters and numbers (upper and lowercase).
- Do not use guessable information such as names, phone numbers, license plates or birthdates (all of which can be easily obtained through other means).
- Do not use words which may be found in dictionaries (English, foreign languages or other) since these are easily cracked.

Passwords should be changed on a defined, regular basis. Passwords should be different for every system one uses.

### **Victim of Identity Theft?**

If you suspect your identity has been stolen, take immediate action:

- Change your passwords.
- Notify customer service for those online accounts.
- Notify your bank or financial institution.
- Request a credit report from credit bureaus.

If you've ever lost your wallet, you know the sense of vulnerability—that someone else could be walking around with your identification, pretending to be you. If someone were to get your passwords—log on to your computer or your online accounts—they could ultimately assume your digital identity, pass themselves off as you, and have fun at your expense.

## Fun for Bad Guys: Bad News for You

What could someone do if they have your passwords?

- Access information on your computer, such as your financial records, e-mail messages, stored lists of passwords, and private information.
- Open new accounts and buy, buy, buy.
- Change your mailing address, and have items they purchase (and bills) sent to them.
- Withdraw money from your bank.
- Buy or sell stocks.
- Apply for loans, including mortgages.
- Pretend to be you in online chats or other online activities, such as auctions.

Think of your password as if it were a key to your home and everything you own, including your reputation.

### How Would You Know if Your Password Has Been Compromised?

You'll only know for sure that someone else is using your password to your online accounts; if you spot unusual activity in your accounts or if you don't receive a monthly bill or bank statement.

If an identity thief changes the mailing address for your accounts, you may not know you have a problem until you get a phone call from a collections agency.

### Checklist for Password Protection

Hackers use "**dictionary**" and other software tools that run rapidly through thousands of likely passwords, looking for easy marks. Protect yourself by using unlikely or strong passwords, managing your password carefully, and monitoring your accounts.

### Computer Usage

Do not leave login sessions, such as on library or administrative systems, unattended even for short periods, and remember to terminate all sessions. This will prevent others from obtaining unauthorized access to these systems or your files.

### Separation of Duties

The phrase "**separation of duties**" is most often associated to the business practice of separating job functions among various individuals. Among other benefits, this can help prevent malicious actions from occurring and help catch those that do occur. The same theory can apply to information systems and servers.

In the case of a Web server and e-commerce infrastructure, separation of duties can be critical to the integrity and protection of information.

## **Watch Your Visitors**

Temporary workers, contractors and consultants represent a unique security threat in that they are generally not subject to the same scrutiny as a firm's full-time employees but may be granted the same high levels of system access.

In addition, they will sometimes know the applications and operating systems running on your network better than your own employees will. Watch these ad-hoc employees closely until you are familiar with their qualifications, the caliber of their work and, most importantly, the degree of trust that it is safe to allow.

Though usually honest and competent, these outside resources must be monitored closely to ensure that their work is sound and that they are truly working in your company's interest. Vendors, for example, will sometimes leave behind trap doors into your systems with the purest intentions of using them only to protect you from yourself or to make future modifications or updates -- guard against this and make it expressly known that these mechanisms will not be tolerated.

These security holes can then be used by intruders to break in, steal information or plant viruses on your systems. In addition, it's not unheard of for a vendor's employee to suddenly become a disgruntled ex-employee and decide to embarrass their former employer by wreaking havoc on your systems.

Don't be afraid to ask consulting firms and contract agencies for details about their hiring policies and standards and be very leery if they are reluctant to discuss such issues.

Clients have a reasonable right to find out just how much outside vendors know about the employees they will be putting in close contact with your company's information assets. Make sure you know in detail what these temporary employees are doing when operating on your systems and monitor all of their activities.

### **Don't Forget to Lock the House**

Another fundamental but frequently overlooked aspect of sound internal security is the physical restrictions put on access to systems and data. Having good physical security in place is a necessary follow-up to whatever office building security your organization may have in place.

Know who is coming into your offices at all times and make sure that your secure computing areas are locked and all access is strictly controlled.

Many complex and expensive network security measures can easily be rendered irrelevant if a thief can bluff their way past the lobby guard, walk into your computer room and simply leave with diskettes, tapes or servers themselves.

In addition, all employees should be instructed to keep laptop computers locked at all times and to log off of any company systems when leaving their workstations.



Shred all of your trash; do not leave any information that can be used to gain access to your facility. Assign individual alarm codes to each employee and change the code on a regular schedule. Change radio communication frequencies every other month or purchase a secure radio frequency. Remember, anybody can obtain a radio scanner to listen in on you and with today's technology, any type of document can be forged or reproduced from your trash.



## Electronic Attack Slows Internet

**WASHINGTON (AP) -- Traffic on the many parts of the Internet slowed dramatically for hours early Saturday, the apparent effects of a fast-spreading, virus-like infection that overwhelmed the world's digital pipelines and interfered with Web browsing and delivery of e-mail.**

Sites monitoring the health of the Internet reported significant slowdowns globally. Experts said the electronic attack bore remarkable similarities to the "Code Red" virus during the summer of 2001 which also ground traffic to a halt on much of the Internet.

"It's not debilitating," said Howard Schmidt, President Bush's No. 2 cyber-security adviser. "Everybody seems to be getting it under control." Schmidt said the FBI's National Infrastructure Protection Center and private experts at the CERT Coordination Center were monitoring the attacks.

The virus-like attack, which began about 12:30 a.m. EST, sought out vulnerable computers on the Internet to infect using a known flaw in popular database software from Microsoft Corp., called "SQL Server 2000." But the attacking software code was scanning for victim computers so randomly and so aggressively -- sending out thousands of probes each second -- that it overwhelmed many Internet data pipelines.

"This is like Code Red all over again," said Marc Maiffret, an executive with eEye Digital Security, whose engineers were among the earliest to study samples of the attack software. "The sheer number of attacks is eating up so much bandwidth that normal operations can't take place."

"The impact of this worm was huge," agreed Ben Koshy of W3 International Media Ltd., which operates thousands of Web sites from its computers in Vancouver. "It's a very significant attack."

Koshy added that, about six hours after the attack, commercial Web sites that had been overwhelmed were starting to come back online as engineers began effectively blocking the malicious data traffic.

"People are recovering from it," Koshy said.

Symantec Corp., an antivirus vendor, estimated that at least 22,000 systems were affected worldwide.

"Traffic itself seems to have leveled off a little bit, so likely only so many systems are exposed out there," said Oliver Friedrichs, senior manager with Symantec Security Response. The attacking software, technically known as a worm, was overwhelming Internet traffic-directing devices known as routers.

"The Internet is still usable, but we're definitely receiving reports from some of our customers who have had it affect their routers specifically," Friedrichs said. The attack sought to take advantage of a software flaw discovered by researchers in July 2002 that permits hackers to seize control of corporate database servers. Microsoft deemed the problem "critical" and offered a free repairing patch, but it was impossible to know how many computer administrators applied the fix.

"People need to do a better job about fixing vulnerabilities," Schmidt said. The latest attack was likely to revive debate within the technology industry about the need for an Internet-wide monitoring center, which the Bush administration has proposed. Some Internet industry executives and lawyers said they would raise serious civil liberties concerns if the U.S. government, not an industry consortium, operated such a powerful monitoring center.



## Shred What You Toss

A determined crook, intruder or competitor will seldom waste valuable time with fancy hacking techniques if they can simply dig through your trash for printed versions of critical data and information.

Shred all papers and documentation containing sensitive company information, network diagrams and systems data to guard against "**Dumpster Diving**", in which the bad guys breach your firm's security by rummaging through your trash.

Also, advise employees against writing down user IDs or passwords at all -- much less discarding them intact in their trash can.

### Watch for Rogue Modems

The best firewall on the market won't protect you if you maintain scores of unprotected modems open to the outside world within the confines of your office. With what they believe to be the best of intentions, workers will sometimes hook up unauthorized modems to their workstations to avoid your officially sanctioned dial-in mechanism and make it easier for them to access their desktop data.

IT employees who should be familiar with the dangers of such configurations will often plant a modem (with a publicly accessible incoming phone line attached) on a server to allow for access by an outside vendor.

Whatever the cause of these unauthorized access mechanisms, it is imperative that organizations carefully control the extent to which modems are used to allow for remote access to your systems. All external access to networks, systems and data should be done through a centrally administered, tested and sanctioned remote access solution.

Policy should exist that prohibits the establishment of any unauthorized inroads to your systems and any discovered mechanisms of this sort should be removed immediately.

### Install a Firewall

If you work in a managed IT environment, always check with your system administrator before making changes to your computer at work.

### Checklist for Firewalls

Firewalls have the same deterring effect as a home alarm system—would-be perpetrators usually look elsewhere for an easier target.

### How does a firewall protect your computer?

Firewalls safeguard your computer by enforcing restrictions on incoming traffic. Firewalls can also mask your computer's identity, so hackers' attempts to probe or scan your computer cannot return the type of information that makes it easy to invade.



### **Good fences make good neighbors.**

You can add an important layer of protection between your computer and the Internet by using a firewall system. Potential intruders scan computers on the Internet probing for a "port" where they can break and enter. A firewall can block unauthorized entry into your computer, as well as restrict outbound traffic.

The FBI and the Computer Security Institute (**CSI**) reported that 85 percent of large corporations had detected a security breach. But why would you be at risk?

### **Suit Yourself**

Security is a trade-off. The more features and functionalities you enable on a computer connected to the Internet, the greater your exposure to risk. The more restrictive your settings, however, the less you can experience through the Web. As one support professional said, "***the only way to be completely secure is not to take the computer out of the box.***"

### **Checklist for Checking Your Settings**

#### **1. Is your software up-to-date?**

Before making changes to your settings, always make sure your software patches are up-to-date.

#### **2. Check your Internet Explorer browser settings**

You can adjust settings for the four Web content zones, set preferences about receiving cookies, and activate the Content Advisor.

- Check the Security Tab settings. Internet Explorer divides your online world into four zones: intranet, Trusted, Restricted, and Internet. You can assign Web sites to each zone and can set each zone's level of security. For example, you might put well-known entertainment or shopping sites in the Trusted Zone, and set the security level lower than you would for unknown sites in the Internet Zone.

For how-to details, look up "security zones" in Internet Explorer Help.

- ✓ Check the Privacy Tab settings. Define your preferences for handling cookies and your standards for releasing personal information. See how to in Internet Explorer and Web Privacy.
- ✓ Activate the Content Advisor in Internet Explorer 5.5 and 6.0. Use the Content Advisor to set rules about which Web sites your children can access. Use the rating system or set you own criteria. Read about Content Advisor.

### **Want a cookie?**

Cookies are small text files that some Web sites create when you visit, and use to store information on your computer. Some sites use this data to deliver customized content, such as local news or stock quotes.

You can use the Internet Explorer privacy settings to specify how the browser should handle cookies, such as allowing all, preventing all, or prompting you before placing a cookie on your computer (so you can allow or block each time).

### 3. Check your Outlook settings

The most common method by which viruses spread is by attachments sent through e-mail. To find out which version of Microsoft Outlook® you are using, on the task bar click on Help, then click on About Microsoft Outlook.

### Teach Your Employees Well

One of the most important and often overlooked elements of a successful information security program is having employees trained to a higher degree of security awareness.

Employees should be trained to appreciate the importance of data that they handle daily and not be lulled into a sense of ambivalence based on the routine of working with such information. Formal information security awareness training should be provided that reinforces the need to keep all information on your company's information assets confidential -- even data that appears the most innocuous.

Workers should be further trained to not reveal this information until the requesting party is identified and their need to know authenticated.

An important follow-up measure is to have a written information security policy that explains the company's security philosophy and the business rationale behind it. This policy should be imparted to all new employees as a part of new-hire orientation.

How can having security savvy employees help protect your organization? Many hackers make ample use of "**social engineering**" skills in which they attempt to convince employees that they have a legitimate right to obtain and know information about your company. For example, a clever intruder may call your information services department claiming to be an outside vendor and simply ask for the name of your systems and what operating system they are running.

He may follow up by asking for the names of key employees at your company. Armed with that basic information, this unwelcome visitor now knows how to identify your systems, what operating system holes they may be able to exploit and what potential user IDs they can try to use to access those systems.

Having employees who are mindful of such ruses and are prepared to respond appropriately moves any company miles closer to a secure information security infrastructure.

## Who's the New Guy?



Do thorough pre-employment background checks on employees before hiring them to work with your company's vital information assets and check references religiously.

You need to find out if that new programmer or systems administrator you've hired into a critical position was fired from their last three jobs for computer fraud before their start date, not after you have been similarly victimized.

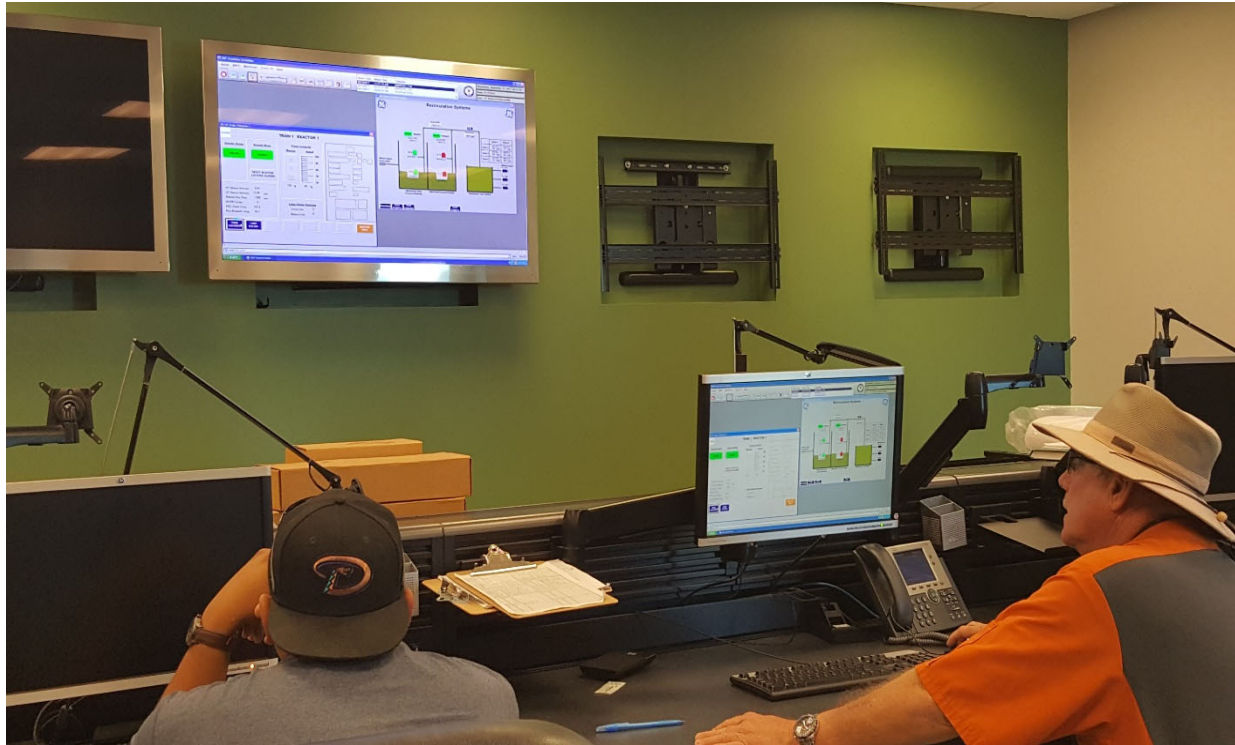
Once hired, make sure that employees can only access data to which they have a legitimate need based on their written job description.

While the vast majority of employees would never do intentional damage to their employer's data or systems, damage can also be done through error or carelessness.

An accountant who accidentally erases vital financial information means no harm but can still cause considerable trouble. Limiting who has access to critical data will not eliminate this risk, but it can at least serve to minimize its potential.

Strict data segmentation and need-to-know access will also help in ensuring that a minimal amount of proprietary information can find its way to a competitor should one of your trusted employees leave to work for another company in the same business.

## SCADA Introduction



### What is SCADA and Who Uses It?

Supervisory control and data acquisition (SCADA) is a system of software and hardware elements that allows industrial organizations to:

- Control industrial processes locally or at remote locations
- Monitor, gather, and process real-time data
- Directly interact with devices such as sensors, valves, pumps, motors, and more through human-machine interface (HMI) software
- Record events into a log file

SCADA systems are crucial for industrial organizations since they help to maintain efficiency, process data for smarter decisions, and communicate system issues to help mitigate downtime.

The basic SCADA architecture begins with programmable logic controllers (PLCs) or remote terminal units (RTUs). PLCs and RTUs are microcomputers that communicate with an array of objects such as factory machines, HMIs, sensors, and end devices, and then route the information from those objects to computers with SCADA software. The SCADA software processes, distributes, and displays the data, helping operators and other employees analyze the data and make important decisions.

For example, the SCADA system quickly notifies an operator that a batch of product is showing a high incidence of errors. The operator pauses the operation and views the SCADA system data via an HMI to determine the cause of the issue. The operator reviews the data and discovers that Machine 4 was malfunctioning. The SCADA system's ability to notify the operator of an issue helps him to resolve it and prevent further loss of product.

SCADA systems are used by industrial organizations and companies in the public and private sectors to control and maintain efficiency, distribute data for smarter decisions, and communicate system issues to help mitigate downtime.

SCADA systems work well in many different types of enterprises because they can range from simple configurations to large, complex installations. SCADA systems are the backbone of many modern industries, including:

- Energy
- Food and beverage
- Manufacturing
- Oil and gas
- Power
- Recycling
- Transportation
- Water and wastewater
- And many more

Virtually anywhere you look in today's world, there is some type of SCADA system running behind the scenes: maintaining the refrigeration systems at the local supermarket, ensuring production and safety at a refinery, achieving quality standards at a waste water treatment plant, or even tracking your energy use at home, to give a few examples.

Effective SCADA systems can result in significant savings of time and money. Numerous case studies have been published highlighting the benefits and savings of using a modern SCADA software solution such as Ignition.

## SCADA Explained



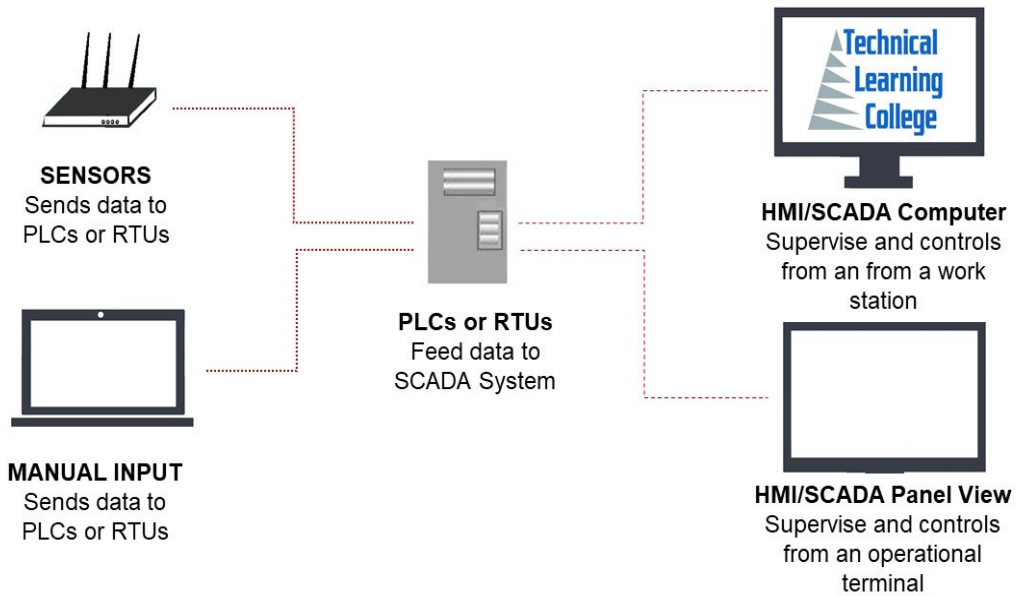
Supervisory control and data acquisition – SCADA refers to ICS (industrial control systems) used to control infrastructure processes (water treatment, wastewater treatment, gas pipelines, wind farms, etc.), facility-based processes (airports, space stations, ships, etc.), or industrial processes (production, manufacturing, refining, power generation, etc.).

Supervisory Control and Data Acquisition (SCADA) is a control system architecture that uses computers, networked data communications and graphical user interfaces for high-level process supervisory management, but uses other peripheral devices such as programmable logic controller (PLC) and discrete PID controllers to interface with the process plant or machinery. The use of SCADA has been also considered for management and operations of project-driven-process in construction.

### **The following subsystems are usually present in SCADA systems:**

- The apparatus used by a human operator; all the processed data are presented to the operator
- A supervisory system that gathers all the required data about the process
- Remote Terminal Units (RTUs) connected to the sensors of the process, which helps to convert the sensor signals to the digital data and send the data to supervisory stream.
- Programmable Logic Controller (PLCs) used as field devices
- Communication infrastructure connects the Remote Terminal Units to supervisory system.

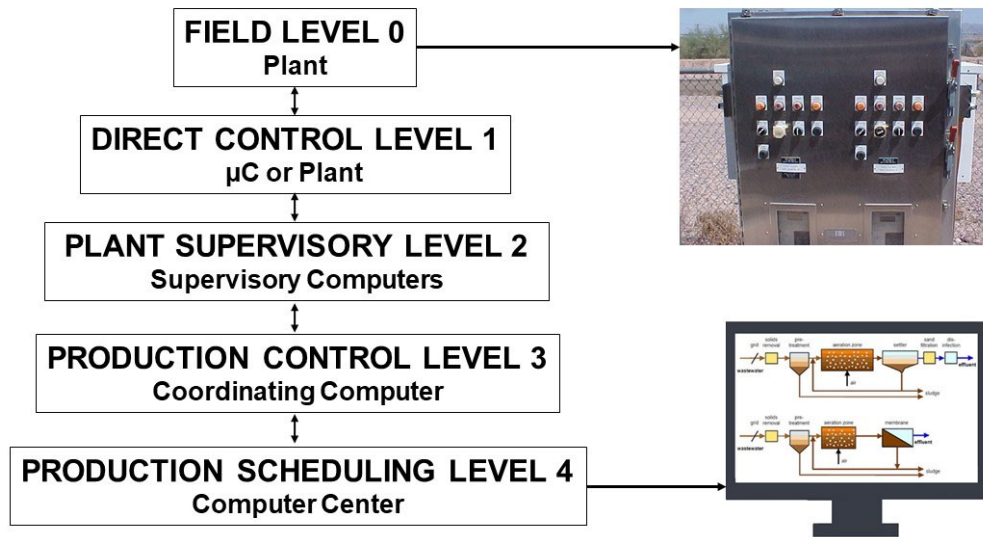
Generally, a SCADA system does not control the processes in real time – it usually refers to the system that coordinates the processes in real time.



## BASIC SCADA DIAGRAM



## SCADA Systems Concepts



### FUNCTION LEVELS OF CONTROL OPERATION

SCADA refers to the centralized systems that control and monitor the entire sites, or they are the complex systems spread out over large areas. Nearly all the control actions are automatically performed by the remote terminal units (RTUs) or by the programmable logic controllers (PLCs). The restrictions to the host control functions are supervisory level intervention or basic overriding. For example, the PLC (in an industrial process) controls the flow of cooling water, the SCADA system allows any changes related to the alarm conditions and set points for the flow (such as high temperature, loss of flow, etc.) to be recorded and displayed.

Data acquisition starts at the PLC or RTU level, which includes the equipment status reports, and meter readings. Data is then formatted in such way that the operator of the control room can make the supervisory decisions to override or adjust normal PLC (RTU) controls, by using the HMI.

SCADA systems mostly implement the distributed databases known as tag databases, containing data elements called points or tags. A point is a single output or input value controlled or monitored by the system. Points are either 'soft' or 'hard'.

The actual output or input of a system is represented by a hard point, whereas the soft point is a result of different math and logic operations applied to other points. These points are usually stored as timestamp-value pairs.

Series of the timestamp-value pairs gives history of the particular point. Storing additional metadata with the tags is common (these additional data can include comments on the design time, alarm information, path to the field device or the PLC register).

The key attribute of a SCADA system is its ability to perform a supervisory operation over a variety of other proprietary devices.

The accompanying diagram is a general model which shows functional manufacturing levels using computerized control.

SCADA systems typically use a tag database, which contains data elements called tags or points, which relate to specific instrumentation or actuators within the process system according to such as the Piping and instrumentation diagram.

Data is accumulated against these unique process control equipment tag references.

**Referring to the diagram,**

**Level 0** contains the field devices such as flow and temperature sensors, and final control elements, such as control valves.

**Level 1** contains the industrialized input/output (I/O) modules, and their associated distributed electronic processors.

**Level 2** contains the supervisory computers, which collate information from processor nodes on the system, and provide the operator control screens.

**Level 3** is the production control level, which does not directly control the process, but is concerned with monitoring production and targets.

**Level 4** is the production scheduling level.

Level 1 contains the programmable logic controllers (PLCs) or remote terminal units (RTUs).

Level 2 contains the SCADA software and computing platform. The SCADA software exists only at this supervisory level as control actions are performed automatically by RTUs or PLCs. SCADA control functions are usually restricted to basic overriding or supervisory level intervention.

For example, a PLC may control the flow of cooling water through part of an industrial process to a set point level, but the SCADA system software will allow operators to change the set points for the flow.

The SCADA also enables alarm conditions, such as loss of flow or high temperature, to be displayed and recorded. A feedback control loop is directly controlled by the RTU or PLC, but the SCADA software monitors the overall performance of the loop.

Levels 3 and 4 are not strictly process control in the traditional sense, but are where production control and scheduling takes place.

Data acquisition begins at the RTU or PLC level and includes instrumentation readings and equipment status reports that are communicated to level 2 SCADA as required.

Data is then compiled and formatted in such a way that a control room operator using the HMI (Human Machine Interface) can make supervisory decisions to adjust or override normal RTU (PLC) controls. Data may also be fed to a historian, often built on a commodity database management system, to allow trending and other analytical auditing.

## **Considerations of SCADA System**

Typical considerations when putting a SCADA system together are:

- Overall control requirements
- Sequence logic
- Analog loop control
- Ratio and number of analog to digital points
- Speed of control and data acquisition
- Master/operator control stations
- Type of displays required
- Historical archiving requirements
- System consideration
- Reliability/availability
- Speed of communications/update time/system scan rates
- System redundancy
- Expansion capability
- Application software and modeling

## **Benefits of a SCADA System**

Obviously, a SCADA system's initial cost has to be justified.

A few typical reasons for implementing a SCADA system are:

1. Improved operation of the plant or process resulting in savings due to optimization of the system
2. Increased productivity of the personnel
3. Improved safety of the system due to better information and improved control
4. Protection of the plant equipment
5. Safeguarding the environment from a failure of the system
6. Improved energy savings due to optimization of the plant
7. Improved and quicker receipt of data so that clients can be invoiced more quickly and accurately
8. Government regulations for safety and metering of gas (for royalties etc.)

## Human Machine Interface Introduction

The HMI, or Human Machine Interface, is an apparatus that gives the processed data to the human operator. A human operator uses HMI to control processes.

The HMI is linked to the SCADA system's databases, to provide the diagnostic data, management information and trending information such as logistic information, detailed schematics for a certain machine or sensor, maintenance procedures and troubleshooting guides.

The information provided by the HMI to the operating personnel is graphical, in the form of mimic diagrams. This means the schematic representation of the plant that is being controlled is available to the operator.

For example, a photograph of the pump that is connected to the pipe shows that this pump is running and it also shows the amount of fluid pumping through the pipe at the particular moment. The pump can then be switched off by the operator.

The software of the HMI shows the decrease in the flow rate of fluid in the pipe in the real time. Mimic diagrams either consist of digital photographs of process equipment with animated symbols, or schematic symbols and line graphics that represent various process elements.

HMI package of the SCADA systems consist of a drawing program used by the system maintenance personnel or operators to change the representation of these points in the interface.

These representations can be as simple as on-screen traffic light that represents the state of the actual traffic light in the area, or complex, like the multi-projector display that represents the position of all the trains on railway or elevators in skyscraper.

SCADA systems are commonly used in alarm systems. The alarm has only two digital status points with values ALARM or NORMAL.

When the requirements of the Alarm are met, the activation will start. For example, when the fuel tank of a car is empty, the alarm is activated and the light signal is on. To alert the SCADA operators and managers, text messages and emails are sent along with alarm activation.

## **Supervisory Station Introduction**

A 'supervisory Station' refers to the software and servers responsible for communication with the field equipment (PLCs, RTUs etc.), and after that, to HMI software running on the workstations in the control room, or somewhere else.

A master station can be composed of only one PC (in small SCADA systems). Master station can have multiple servers, disaster recovery sites and distributed software applications in larger SCADA systems. For increasing the system integrity, multiple servers are occasionally configured in hot standby or dual-redundant formation, providing monitoring and continuous control during server failures.

## **SCADA Hardware**

SCADA system may have the components of the Distributed Control System. Execution of easy logic processes without involving the master computer is possible because 'smart' PLCs or RTUs. IEC61131-3(Ladder Logic) is used, (this is a functional block programming language, commonly used in creating programs running on PLCs and RTUs.) IEC 61131-3 has very few training requirements, unlike procedural languages like FORTRAN and C programming language.

The SCADA system engineers can perform implementation and design of programs being executed on PLC or RTU. The compact controller, Programmable automation controller (PAC), combines the capabilities and features of a PC-based control system with a typical PLC.

'Distributed RTUs', in various electrical substation SCADA applications, use station computers or information processors for communicating with PACs, protective relays, and other I/O devices. Almost all big PLC manufacturers offer integrated HMI/SCADA systems, since 1998. Many of them are using non-proprietary and open communication protocols.

Many skilled third party HMI/SCADA packages have stepped into the market, offering in-built compatibility with several major PLCs, which allows electrical engineers, mechanical engineers or technicians to configure HMIs on their own, without requiring software-developer-written custom-made program.

## **Remote Terminal Unit (RTU)**

The RTU is connected to the physical equipment. Often, the RTU converts all electrical signals coming from the equipment into digital values like the status- open/closed – from a valve or switch, or the measurements like flow, pressure, current or voltage. By converting and sending the electrical signals to the equipment, RTU may control the equipment, like closing or opening a valve or a switch, or setting the speed of the pump.



## **SCADA Operational Philosophy**

The costs resulting from control system failures are very high. Even lives may be lost. For a few SCADA systems, hardware is ruggedized, to withstand temperature, voltage and vibration extremes, and reliability is increased, in many critical installations, by including communications channels and redundant hardware. A part which is failing can be identified and the functionality taken over automatically through backup hardware. It can be replaced without any interruption of the process.

### **Communication Methods and Infrastructure**

SCADA systems initially used modem connections or combinations of direct and radio serial to meet communication requirements, even though IP and Ethernet over SONET/SDH can also be used at larger sites like power stations and railways. The monitoring function or remote management of the SCADA system is called telemetry.

SCADA protocols have been designed to be extremely compact and to send information to the master station only when the RTU is polled by the master station. Typically, the legacy of SCADA protocols consists of Conitel, Profibus, Modbus RTU and RP-570. These protocols of communication are specifically SCADA-vendor. Standard protocols are IEC 61850, DNP3 and IEC 60870-5-101 or 104. These protocols are recognized and standardized by all big SCADA vendors. Several of these protocols have extensions for operating through the TCP/IP.

The development of many automatic controller devices and RTUs had started before the advent of industry standards for the interoperability.

For better communication between different software and hardware, PLE for Process Control is a widely accepted solution that allows communication between the devices that originally weren't intended to be part of the industrial network.

### **Alarm Management Introduction**

An important part of most SCADA implementations is alarm handling. The system monitors whether certain alarm conditions are satisfied, to determine when an alarm event has occurred. Once an alarm event has been detected, one or more actions are taken (such as the activation of one or more alarm indicators, and perhaps the generation of email or text messages so that management or remote SCADA operators are informed).

In many cases, a SCADA operator may have to acknowledge the alarm event; this may deactivate some alarm indicators, whereas other indicators remain active until the alarm conditions are cleared.

Alarm conditions can be explicit—for example, an alarm point is a digital status point that has either the value NORMAL or ALARM that is calculated by a formula based on the values in other analogue and digital points—or implicit: the SCADA system might automatically monitor whether the value in an analogue point lies outside high and low- limit values associated with that point.

Examples of alarm indicators include a siren, a pop-up box on a screen, or a colored or flashing area on a screen (that might act in a similar way to the "fuel tank empty" light in a car); in each case, the role of the alarm indicator is to draw the operator's attention to the part of the system 'in alarm' so that appropriate action can be taken.

### **PLC/RTU Programming**

"Smart" RTUs, or standard PLCs, are capable of autonomously executing simple logic processes without involving the supervisory computer. They employ standardized control programming languages such as under, IEC 61131-3 (a suite of 5 programming languages including function block, ladder, structured text, sequence function charts and instruction list), is frequently used to create programs which run on these RTUs and PLCs.

Unlike a procedural language such as the C programming language or FORTRAN, IEC 61131-3 has minimal training requirements by virtue of resembling historic physical control arrays. This allows SCADA system engineers to perform both the design and implementation of a program to be executed on an RTU or PLC.

A programmable automation controller (PAC) is a compact controller that combines the features and capabilities of a PC-based control system with that of a typical PLC. PACs are deployed in SCADA systems to provide RTU and PLC functions.

In many electrical substation SCADA applications, "distributed RTUs" use information processors or station computers to communicate with digital protective relays, PACs, and other devices for I/O, and communicate with the SCADA master in lieu of a traditional RTU.

### **PLC Commercial Integration**

Since about 1998, virtually all major PLC manufacturers have offered integrated HMI/SCADA systems, many of them using open and non-proprietary communications protocols.

Numerous specialized third-party HMI/SCADA packages, offering built-in compatibility with most major PLCs, have also entered the market, allowing mechanical engineers, electrical engineers and technicians to configure HMIs themselves, without the need for a custom-made program written by a software programmer.

The Remote Terminal Unit (RTU) connects to physical equipment. Typically, an RTU converts the electrical signals from the equipment to digital values such as the open/closed status from a switch or a valve, or measurements such as pressure, flow, voltage or current. By converting and sending these electrical signals out to equipment the RTU can control equipment, such as opening or closing a switch or a valve, or setting the speed of a pump.



## **SCADA Architectures**

### **Monolithic: The First Generation**

In the first generation, mainframe systems were used for computing. At the time SCADA was developed, networks did not exist. Therefore, the SCADA systems did not have any connectivity to other systems, meaning they were independent systems. Later on, RTU vendors designed the Wide Area Networks that helped in communication with RTU. The usage of communication protocols at that time was proprietary. If the mainframe system failed, there was a back-up mainframe, connected at the bus level.

### **Distributed: The Second Generation**

The information between multiple stations was shared in real time through LAN and the processing was distributed between various multiple stations. The cost and size of the stations were reduced in comparison to the ones used in the first generation. The protocols used for the networks were still proprietary, which caused many security issues for SCADA systems. Due to the proprietary nature of the protocols, very few people actually knew how secure the SCADA installation was.

### **Networked: The Third Generation**

The SCADA system used today belong to this generation. The communication between the system and the master station is done through the WAN protocols like the Internet Protocols (IP). Since the standard protocols used and the networked SCADA systems can be accessed through the internet, the vulnerability of the system is increased. However, the usage of security techniques and standard protocols means that security improvements can be applied in SCADA systems.

### **The Evolution of SCADA**

The first iteration of SCADA started off with mainframe computers. Networks as we know them today were not available and each SCADA system stood on its own. These systems were what would now be referred to as monolithic SCADA systems.

In the 80s and 90s, SCADA continued to evolve thanks to smaller computer systems, Local Area Networking (LAN) technology, and PC-based HMI software. SCADA systems soon were able to be connected to other similar systems. Many of the LAN protocols used in these systems were proprietary, which gave vendors control of how to optimize data transfer. Unfortunately, these systems were incapable of communicating with systems from other vendors. These systems were called distributed SCADA systems.

In the 1990s and early 2000s, building upon the distributed system model, SCADA adopted an incremental change by embracing an open system architecture and communications protocols that were not vendor-specific. This iteration of SCADA, called a networked SCADA system, took advantage of communications technologies such as Ethernet. Networked SCADA systems allowed systems from other vendors to communicate with each other, alleviating the limitations imposed by older SCADA systems, and allowed organizations to connect more devices to the network.

While SCADA systems have undergone substantial evolutionary changes, many industrial organizations continued to struggle with industrial data access from the enterprise level. By the late 1990s to the early 2000s, a technological boom occurred and personal computing and IT technologies accelerated in development.

Structured query language (SQL) databases became the standard for IT databases but were not adopted by SCADA developers. This resulted in a rift between the fields of controls and IT, and SCADA technology became antiquated over time.

Traditional SCADA systems still use proprietary technology to handle data. Whether it is a data historian, a data connector, or other means of data transfer, the solution is messy and incredibly expensive. Modern SCADA systems aim to solve this problem by leveraging the best of controls and IT technology.

### **Communication Infrastructure and Methods**

SCADA systems have traditionally used combinations of radio and direct wired connections, although SONET/SDH is also frequently used for large systems such as railways and power stations. The remote management or monitoring function of a SCADA system is often referred to as telemetry. Some users want SCADA data to travel over their pre-established corporate networks or to share the network with other applications. The legacy of the early low-bandwidth protocols remains, though.

SCADA protocols are designed to be very compact. Many are designed to send information only when the master station polls the RTU. Typical legacy SCADA protocols include Modbus RTU, RP-570, Profibus and Conitel. These communication protocols, with the exception of Modbus (Modbus has been made open by Schneider Electric), are all SCADA-vendor specific but are widely adopted and used. Standard protocols are IEC 60870-5-101 or 104, IEC 61850 and DNP3. These communication protocols are standardized and recognized by all major SCADA vendors. Many of these protocols now contain extensions to operate over TCP/IP. Although the use of conventional networking specifications, such as TCP/IP, blurs the line between traditional and industrial networking, they each fulfill fundamentally differing requirements.[7] Network simulation can be used in conjunction with SCADA simulators to perform various 'what-if' analyses.

With increasing security demands (such as North American Electric Reliability Corporation (NERC) and critical infrastructure protection (CIP) in the US), there is increasing use of satellite-based communication. This has the key advantages that the infrastructure can be self-contained (not using circuits from the public telephone system), can have built-in encryption, and can be engineered to the availability and reliability required by the SCADA system operator. Earlier experiences using consumer-grade VSAT were poor. Modern carrier-class systems provide the quality of service required for SCADA.

RTUs and other automatic controller devices were developed before the advent of industry wide standards for interoperability. The result is that developers and their management created a multitude of control protocols. Among the larger vendors, there was also the incentive to create their own protocol to "lock in" their customer base. A list of automation protocols is compiled here.

OLE for process control (OPC) can connect different hardware and software, allowing communication even between devices originally not intended to be part of an industrial network. Standardization in the field of mySCADA protocols resulted into the vendor independent protocol called OPC UA (Unified Architecture). OPC UA is starting to be widely adopted among multiple SCADA vendors.

## **SCADA Trends**

In the late 1990s instead of using the RS-485, manufacturers used open message structures like Modbus ASCII and Modbus RTU (both developed by Modicon). By 2000, almost all I/O makers offered fully open interfacing like Modbus TCP instead of the IP and Ethernet.

SCADA systems are now in line with the standard networking technologies. The old proprietary standards are being replaced by the TCP/IP and Ethernet protocols. However, due to certain characteristics of frame-based network communication technology, Ethernet networks have been accepted by the majority of markets for HMI SCADA.

The 'Next Generation' protocols using XML web services and other modern web technologies, make themselves more IT supportable. A few examples of these protocols include Wonderware's SuiteLink, GE Fanuc's Proficy, I Gear's Data Transport Utility, Rockwell Automation's FactoryTalk and OPC-UA.

Some vendors have started offering application-specific SCADA systems that are hosted on remote platforms all over the Internet. Hence, there is no need to install systems at the user-end facility. Major concerns are related to the Internet connection reliability, security and latency. The SCADA systems are becoming omnipresent day by day. However, there are still some security issues.

## **SCADA Security Issues**

Security of SCADA-based systems is being questioned, as they are potential targets to cyberterrorism/cyberwarfare attacks.

There is an erroneous belief that SCADA networks are safe enough because they are secured physically. It is also wrongly believed that SCADA networks are safe enough because they are disconnected from the Internet.

SCADA systems also are used for monitoring and controlling physical processes, like distribution of water, traffic lights, electricity transmissions, gas transportation and oil pipelines and other systems used in the modern society. Security is extremely important because destruction of the systems would have very bad consequences.

There are two major threats. The first one is unauthorized access to software, be it human access or intentionally induced changes, virus infections or other problems that can affect the control host machine. The second threat is related to the packet access to network segments that host SCADA devices. In numerous cases, there remains less or no security on actual packet control protocol; therefore, any person sending packets to SCADA device is in position to control it. Often, SCADA users infer that VPN is sufficient protection, and remain oblivious to the fact that physical access to network switches and jacks related to SCADA provides the capacity to bypass the security on control software and control SCADA networks.

SCADA vendors are addressing these risks by developing specialized industrial VPN and firewall solutions for SCADA networks that are based on TCP/IP. In addition, white-listing solutions have been implemented due to their ability to prevent unauthorized application changes.

SCADA systems that tie together decentralized facilities such as power, oil, gas pipelines, water distribution and wastewater collection systems were designed to be open, robust, and easily operated and repaired, but not necessarily secure.

The move from proprietary technologies to more standardized and open solutions together with the increased number of connections between SCADA systems, office networks and the Internet has made them more vulnerable to types of network attacks that are relatively common in computer security. For example, United States Computer Emergency Readiness Team (US-CERT) released a vulnerability advisory warning that unauthenticated users could download sensitive configuration information including password hashes from an Inductive Automation Ignition system utilizing a standard attack type leveraging access to the Tomcat Embedded Web server. Security researcher Jerry Brown submitted a similar advisory regarding a buffer overflow vulnerability in a Wonderware InBatchClient ActiveX control. Both vendors made updates available prior to public vulnerability release. Mitigation recommendations were standard patching practices and requiring VPN access for secure connectivity. Consequently, the security of some SCADA-based systems has come into question as they are seen as potentially vulnerable to cyber-attacks.

**In particular, security researchers are concerned about**

- the lack of concern about security and authentication in the design, deployment and operation of some existing SCADA networks
- the belief that SCADA systems have the benefit of security through obscurity through the use of specialized protocols and proprietary interfaces
- the belief that SCADA networks are secure because they are physically secured
- the belief that SCADA networks are secure because they are disconnected from the Internet

SCADA systems are used to control and monitor physical processes, examples of which are transmission of electricity, transportation of gas and oil in pipelines, water distribution, traffic lights, and other systems used as the basis of modern society. The security of these SCADA systems is important because compromise or destruction of these systems would impact multiple areas of society far removed from the original compromise. For example, a blackout caused by a compromised electrical SCADA system would cause financial losses to all the customers that received electricity from that source. How security will affect legacy SCADA and new deployments remains to be seen.

There are many threat vectors to a modern SCADA system. One is the threat of unauthorized access to the control software, whether it is human access or changes induced intentionally or accidentally by virus infections and other software threats residing on the control host machine. Another is the threat of packet access to the network segments hosting SCADA devices. In many cases, the control protocol lacks any form of cryptographic security, allowing an attacker to control a SCADA device by sending commands over a network.

In many cases, SCADA users have assumed that having a VPN offered sufficient protection, unaware that security can be trivially bypassed with physical access to SCADA-related network jacks and switches. Industrial control vendors suggest approaching SCADA security like Information Security with a defense in depth strategy that leverages common IT practices

The reliable function of SCADA systems in our modern infrastructure may be crucial to public health and safety. As such, attacks on these systems may directly or indirectly threaten public health and safety. Such an attack has already occurred, carried out on Maroochy Shire Council's sewage control system in Queensland, Australia. Shortly after a contractor installed a SCADA system in January 2000, system components began to function erratically. Pumps did not run when needed and alarms were not reported.

More critically, sewage flooded a nearby park and contaminated an open surface-water drainage ditch and flowed 500 meters to a tidal canal. The SCADA system was directing sewage valves to open when the design protocol should have kept them closed. Initially this was believed to be a system bug.

Monitoring of the system logs revealed the malfunctions were the result of cyber-attacks. Investigators reported 46 separate instances of malicious outside interference before the culprit was identified. The attacks were made by a disgruntled ex-employee of the company that had installed the SCADA system. The ex-employee was hoping to be hired by the utility full-time to maintain the system.

In April 2008, the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack issued a Critical Infrastructures Report which discussed the extreme vulnerability of SCADA systems to an electromagnetic pulse (EMP) event. After testing and analysis, the Commission concluded: "SCADA systems are vulnerable to an EMP event.

The large numbers and widespread reliance on such systems by all of the Nation's critical infrastructures represent a systemic threat to their continued operation following an EMP event. Additionally, the necessity to reboot, repair, or replace large numbers of geographically widely dispersed systems will considerably impede the Nation's recovery from such an assault."

### **SCADA System Summary**

A SCADA (or supervisory control and data acquisition) system means a system consisting of a number of remote terminal units (or RTUs) collecting field data connected back to a master station via a communications system.

The master station displays the acquired data and allows the operator to perform remote control tasks.

The accurate and timely data (normally real-time) allows for optimization of the operation of the plant and process. A further benefit is more efficient, reliable and most importantly, safer operations. This all results in a lower cost of operation compared to earlier non-automated systems.

There is a fair degree of confusion between the definition of SCADA systems and process control system. SCADA has the connotation of remote or distant operation.



## SUMMARY

---

Information Security isn't necessarily easy -- but it is an involuntary element in doing business in the new century. While some organizations are entirely information intensive or based purely on the Internet, all business entities have in the last 20 years come to rely on networks, systems and electronic data as vital components of their core business.

Some SCADA users feel secure as their systems are very proprietary in nature. But these systems are no match for determined terrorists. Anyone who is willing to invest the time can figure out proprietary systems.

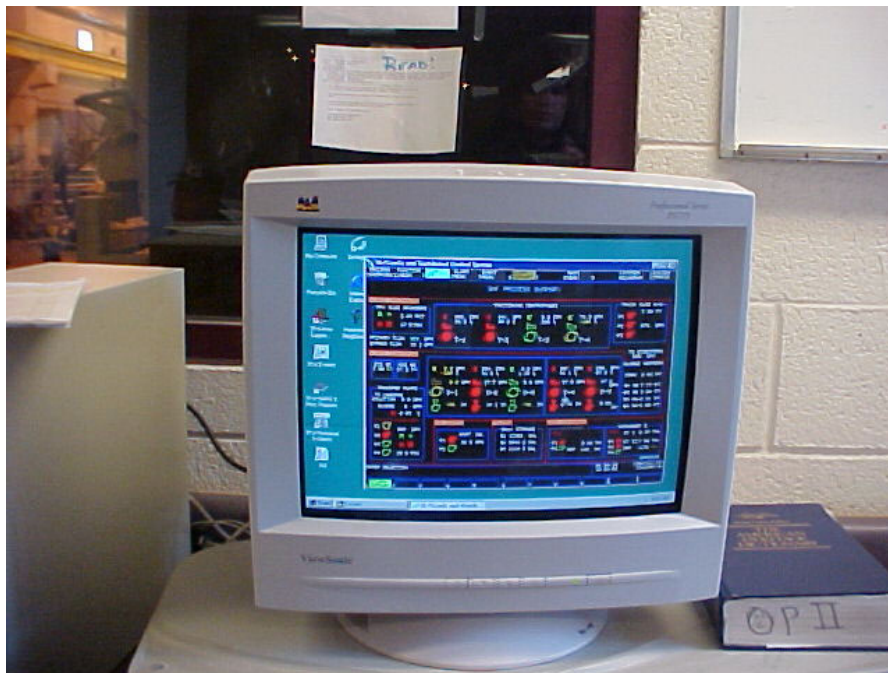
While it would be folly to ignore the threat from the outside world, it is equally foolish to be vulnerable and open to serious damage to business interests based on ignorance of internal security issues.

Pay more attention to what's going on in-house to achieve a sound, bedrock security posture that will allow you to protect your organization's information assets, and maybe even help you sleep better at night.



## Resources

1. IT Security for Industrial Control Systems Joe Falco, Keith Stouffer, Albert Wavering, Frederick Proctor Intelligent Systems Division National Institute of Standards and Technology (NIST) Gaithersburg, MD
2. Roy E. Fraser, Process Measurement and Control - Introduction to Sensors, Communication, Adjustment, and Control, Prentice-Hall, Inc., 2001.
3. Information Security Primer, EPRI Report TR-100797, September 2000
4. Bruce Schneier, Secrets & Lies - Digital Security in a Networked World, John Wiley & Sons, Inc., 2000.
5. Information Assurance Task Force, Electric Power Risk Assessment, National Security Telecommunications Advisory Committee, [http://www.ncs.gov/n5\\_hp/Reports/EPRA/EPRA.html](http://www.ncs.gov/n5_hp/Reports/EPRA/EPRA.html).
6. Understanding SCADA System Security Vulnerabilities, Riptech, <http://www.riptidech.com/industry/energy.html>
7. Paul Oman et al, Safeguarding IEDS, Substations, and SCADA Systems Against Electronic Intrusions, <http://www.selinc.com/techpprs/6118.pdf>.
8. Common Criteria for Information Technology Security Evaluation, Part1: Introduction and general model, CCIMB-99-031, Version 2.1, 1999. Intrusions, <http://www.selinc.com/techpprs/6118.pdf>.
9. Common Criteria Toolbox, Version 6.0f, <http://niap.nist.gov/tools/cctool.html>.



SCADA



## SCADA References

- Antunes, Ricardo; Poshdar, Mani (2018). "Envision of an integrated information system for project-driven production in construction". Proc. 26th Annual Conference of the International Group for Lean Construction (IGLC): 134–143. doi:10.24928/2018/0511. Retrieved 27 December 2018.
- Boys, Walt (18 August 2009). "Back to Basics: SCADA". Automation TV: Control Global - Control Design.
- "Cyberthreats, Vulnerabilities and Attacks on SCADA Networks" (PDF). Rosa Tang, berkeley.edu. Archived from the original (PDF) on 13 August 2012. Retrieved 1 August 2012.
- Boyer, Stuart A. (2010). SCADA Supervisory Control and Data Acquisition. USA: ISA - International Society of Automation. p. 179. ISBN 978-1-936007-09-7.
- Jeff Hieb (2008). Security Hardened Remote Terminal Units for SCADA Networks. University of Louisville.
- Aquino-Santos, Raul (30 November 2010). Emerging Technologies in Wireless Ad-hoc Networks: Applications and Future Development: Applications and Future Development. IGI Global. pp. 43–. ISBN 978-1-60960-029-7.
- "Introduction to Industrial Control Networks" (PDF). IEEE Communications Surveys and Tutorials. 2012.
- Bergan, Christian (August 2011). "Demystifying Satellite for the Smart Grid: Four Common Misconceptions". Electric Light & Powers. Utility Automation & Engineering T&D. Tulsa, OK: PennWell. 16 (8). Four. Retrieved 2 May 2012. satellite is a cost-effective and secure solution that can provide backup communications and easily support core smart grid applications like SCADA, telemetry, AMI backhaul and distribution automation
- OFFICE OF THE MANAGER NATIONAL COMMUNICATIONS SYSTEM October 2004. "Supervisory Control and Data Acquisition (SCADA) Systems" (PDF). NATIONAL COMMUNICATIONS SYSTEM.
- J. Russel. "A Brief History of SCADA/EMS (2015)". Archived from the original on 11 August 2015.
- Security Hardened Remote Terminal Units for SCADA Networks. ProQuest. 2008. pp. 12–. ISBN 978-0-549-54831-7.
- "SCADA as a service approach for interoperability of micro-grid platforms". Sustainable Energy, Grids and Network. 2016. doi:10.1016/j.segan.2016.08.001.
- "SCADA as a service approach for interoperability of micro-grid platforms", Sustainable Energy, Grids and Network, 2016, doi:10.1016/j.segan.2016.08.001
- "ICSA-11-231-01—INDUCTIVE AUTOMATION IGNITION INFORMATION DISCLOSURE VULNERABILITY" (PDF). 19 Aug 2011. Retrieved 21 Jan 2013.
- "ICSA-11-094-01—WONDERWARE INBATCH CLIENT ACTIVEX BUFFER OVERFLOW" (PDF). 13 Apr 2011. Retrieved 26 Mar 2013.
- D. Maynor and R. Graham (2006). "SCADA Security and Terrorism: We're Not Crying Wolf" (PDF).
- Robert Lemos (26 July 2006). "SCADA system makers pushed toward security". Security Focus. Retrieved 9 May 2007.
- "Industrial Security Best Practices" (PDF). Rockwell Automation. Retrieved 26 Mar 2013.
- Slay, J.; Miller, M. (November 2007). "Chpt 6: Lessons Learned from the Maroochy Water Breach". Critical infrastructure protection (Online-Ausg. ed.). Springer Boston. pp. 73–82. ISBN 978-0-387-75461-1. Retrieved 2 May 2012.
- [http://www.empcommission.org/docs/A2473-EMP\\_Commission-7MB.pdf](http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf)
- "Security for all". InTech. June 2008. Retrieved 2 May 2012.

## **CHAPTER 9 EXERCISE *LAST ASSIGNMENT***

---

1. Do you believe that your computer systems are vulnerable to attack?
2. How would you plan to protect your computer systems?
3. Give an example of a hard or difficult “password”

***You are finished with all of your exercises. Please find the final assignment on the Assignment webpage and complete and e-mail or fax it to us. Thank you.***

## **Bibliography**

Burdick, Brett A., ed. Hazardous Materials Training Public Safety Response to Terrorism. Student Manual. Richmond, VA: Virginia Department of Emergency Services, 1997.

Emergency Management Institute. Radiological Emergency Management Independent Study Course. Emmitsburg, MD: author, 1994.

Federal Emergency Management Agency. The Federal Response Plan for Public Law 93-288. Washington, DC: author, as amended, 1992.

The Federal Response Plan for Public Law 93-288: Terrorism Incident Annex. Washington, DC: author, 1996.

Medici, John and Steve Patrick. Emergency Response to Incidents Involving Chemical & Biological Warfare Agents. Richmond, VA: Virginia Dept. of Emergency Services, 1996.

National Fire Academy. Command and Control of Fire Department Major Operations. Student Manual. Emmitsburg, MD: author, 1988.

Initial Response to Hazardous Materials Incidents: Concept Implementation. Student Manual. Emmitsburg, MD: author, 1992.

Terrorism Training Needs Assessment Meeting Report. Emmitsburg, MD: author, 1996.

Preparedness, Training, and Exercises Directorate. Guide for All-Hazard Emergency Operations Planning. Washington, DC: Federal Emergency Management Agency, 1996.

U.S. Army. Material Safety Data Sheets for: GA, GB, VX, GD, CS, Lewisite, and HD. U.S. Army Edgewood Research, Development and Engineering Center.

U.S. Army Medical Research Institute of Chemical Defense. Medical Management of Chemical Casualties Handbook, 2nd ed. Aberdeen Proving Ground, MD: U.S. Army, 1995.

U.S. Army Medical Research Institute of Infectious Diseases. Medical Management of Biological Casualties Handbook, 2nd ed. Frederick, MD: U.S. Army, 1996.

U.S. Department of Transportation. North American Emergency Response Guidebook. Washington, DC: author, 1996.

White House. Presidential Decision Directive 39. United States Policy on Counterterrorism. Washington, DC: author, 1995.

***For more information please visit the following web sites:***

<http://www.epa.gov/ebtpages/ecounterterrorism.html>

EPA Alert on Chemical Accident Prevention and Site Security:

<http://www.epa.gov/ceppo/pubs/secale.pdf>

U.S. Centers for Disease Control & Prevention: <http://www.bt.cdc.gov>

Association of Metropolitan Water Agencies: <http://www.amwa.net/isac/amwacip.html>

American Water Works Association: <http://awwa.org>

National League of Cities: [http://www.nlc.org/nlc\\_org/site/newsroom/terrorism\\_response](http://www.nlc.org/nlc_org/site/newsroom/terrorism_response)

Operator Certification Information <http://www.tlch2o.com>

Julie Desai, State of New Mexico, 11/27/01

Department of Alcohol, Tobacco and Firearms



What damage could a Terrorist do in a chemical sensitive area? Little or no security. Personnel are only there during the day. How about a high powered rifle with a homemade silencer? How about the damage that could happen to a power transformer? Are you prepared? If not, get a grant from Department of Homeland Security and start to guard against incidents.

# Security Vulnerability Self-Assessment

## Record of Security Vulnerability Self-Assessment Completion

*The following information should be completed by the individual conducting the self-assessment and/or any additional revisions.*

Name: \_\_\_\_\_  
Title: \_\_\_\_\_  
Area of  
Responsibility: \_\_\_\_\_  
Water System  
Name: \_\_\_\_\_  
Water System  
PWSID: \_\_\_\_\_  
Address: \_\_\_\_\_  
City: \_\_\_\_\_  
County: \_\_\_\_\_  
State: \_\_\_\_\_  
Zip Code: \_\_\_\_\_  
Telephone: \_\_\_\_\_  
Fax: \_\_\_\_\_  
E-mail: \_\_\_\_\_  
Date Completed: \_\_\_\_\_

Date Revised: \_\_\_\_\_

Date Revised: \_\_\_\_\_



## Inventory of Small Water System Critical Components

<b>Component</b>	<b>Number &amp; Location (if applicable)</b>	<b>Description</b>	<b>Critical Asset or Single Point of Failure (H/M/L)</b>
<b>Source Water Type</b>			
Ground Water			
Surface Water			
Purchased			
<b>Treatment Plant</b>			
Buildings			
Pumps			
Treatment Equipment (e.g., basin, clear well, filter)			
Process Controls			
Treatment Chemicals and Storage			
Laboratory Chemicals and Storage			
<b>Storage</b>			
Storage Tanks			
Pressure Tanks			
<b>Power</b>			
Primary Power			
Auxiliary Power			
<b>Distribution System</b>			
Pumps			
Pipes			
Valves			
Appurtenances (e.g., flush hydrants, backflow preventers, meters)			
Other Vulnerable Points			
<b>Offices</b>			
Buildings			
Computers			
Files			
Transportation/ Work Vehicles			
Personnel			
<b>Communications</b>			
Telephone			
Cell Phone			
Radio			
Computer Control Systems (SCADA)			

<b>Critical Facilities Served</b>			
Power Plant Facilities			
Hospitals			
Schools			
Waste Water Treatment Plants			
Food/Beverage Processing Plants			
Nursing Homes			
Prisons/Other Institutions			



**General Questions for the Entire Water System**

**Security Vulnerability Self-Assessment for Small Water Systems**

*The first 15 questions in this vulnerability self-assessment are general questions designed to apply to all components of your system (wellhead or surface water intake, treatment plant, storage tank(s), pumps, distribution system, and offices). These are followed by more specific questions that look at individual system components in greater detail.*

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
1. Do you have a written emergency response plan (ERP)?	Yes <input type="checkbox"/> No <input type="checkbox"/>	<p>Under the provisions of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 you are required to develop and/or update an ERP within six months after completing this assessment. If you do not have an ERP, you can obtain a sample from your state drinking water primacy agency. As a first step in developing your ERP, you should develop your Emergency Contact List (see Attachment 2).</p> <p>A plan is vital in case there is an incident that requires immediate response. Your plan should be reviewed at least annually (or more frequently if necessary) to ensure it is up-to-date and addresses security emergencies including ready access to laboratories capable of analyzing water samples. You should coordinate with your LEPC.</p> <p>You should designate someone to be contacted in case of emergency regardless of the day of the week or time of day. This contact information should be kept up-to-date and made available to all water system personnel and local officials (if applicable).</p> <p>Share this ERP with police, emergency personnel, and your state primacy agency. Posting contact information is a good idea only if authorized personnel are the only ones seeing the information. These signs could pose a security risk if posted for public viewing since it gives people information that could be used against the system.</p>	
2. Have you reviewed U.S. EPA's Baseline Threat Information Document?	Yes <input type="checkbox"/> No <input type="checkbox"/>	The U.S. EPA baseline threat document is available through the Water Information Sharing and Analysis Center at <a href="http://www.waterisac.org">www.waterisac.org</a> . It is important you use this document to determine potential threats to your system and to obtain additional security related information. U.S. EPA should have provided a certified letter to your system that provided instructions on obtaining the threat document.	

<p>3. Is access to the critical components of the water system (i.e., a part of the physical infrastructure of the system that is essential for water flow and/or water quality) restricted to authorized personnel only?</p>	<p>Yes <input type="checkbox"/> No <input type="checkbox"/></p>	<p>You should restrict or limit access to the critical components of your water system to authorized personnel only. This is the first step in security enhancement for your water system. Consider the following:</p> <ul style="list-style-type: none"> <li>◆ Issue water system photo identification cards for employees, and require them to be displayed within the restricted area at all times.</li> <li>◆ Post signs restricting entry to authorized personnel and ensure that assigned staff escort people without proper ID.</li> </ul>	
<p>4. Are all critical facilities fenced, including wellhouses and pump pits, and are gates locked where appropriate?</p>	<p>Yes <input type="checkbox"/> No <input type="checkbox"/></p>	<p>Ideally, all facilities should have a security fence around the perimeter.</p> <p>The fence perimeter should be walked periodically to check for breaches and maintenance needs. All gates should be locked with chains and a tamper-proof padlock that at a minimum protects the shank. Other barriers such as concrete "jersey" barriers should be considered to guard certain critical components from accidental or intentional vehicle intrusion.</p>	
<p>5. Are all critical doors, windows, and other points of entry such as tank and roof hatches and vents kept closed and locked?</p>	<p>Yes <input type="checkbox"/> No <input type="checkbox"/></p>	<p>Lock all building doors and windows, hatches and vents, gates, and other points of entry to prevent access by unauthorized personnel. Check locks regularly. Dead bolt locks and lock guards provide a high level of security for the cost.</p> <p>A daily check of critical system components enhances security and ensures that an unauthorized entry has not taken place.</p> <p>Doors and hinges to critical facilities should be constructed of heavy-duty reinforced material. Hinges on all outside doors should be located on the inside.</p> <p>To limit access to water systems, all windows should be locked and reinforced with wire mesh or iron bars, and bolted on the inside. Systems should ensure that this type of security meets with the requirements of any fire codes. Alarms can also be installed on windows, doors, and other points of entry.</p>	
<p>6. Is there external lighting around all critical components of your water system?</p>	<p>Yes <input type="checkbox"/> No <input type="checkbox"/></p>	<p>Adequate lighting of the exterior of water systems' critical components is a good deterrent to unauthorized access and may result in the detection or deterrence of trespassers. Motion detectors that activate switches that turn lights on or trigger alarms also enhance security.</p>	

<p>7. Are warning signs (tampering, unauthorized access, etc.) posted on all critical components of your water system? (For example, well houses and storage tanks.)</p>	<p>Yes <input type="checkbox"/> No <input type="checkbox"/></p>	<p>Warning signs are an effective means to deter unauthorized access.</p> <p>“Warning - Tampering with this facility is a federal offense” should be posted on all water facilities. These are available from your state rural water association.</p> <p>“Authorized Personnel Only,” “Unauthorized Access Prohibited,” and “Employees Only” are examples of other signs that may be useful.</p>	
<p>8. Do you patrol and inspect all source intakes, buildings, storage tanks, equipment, and other critical components?</p>	<p>Yes <input type="checkbox"/> No <input type="checkbox"/></p>	<p>Frequent and random patrolling of the water system by utility staff may discourage potential tampering. It may also help identify problems that may have arisen since the previous patrol.</p> <p>All systems are encouraged to initiate personal contact with the local law enforcement to show them the drinking water facility. The tour should include the identification of all critical components with an explanation of why they are important. Systems are encouraged to review, with local law enforcement, the NRW/ASDWA Guide for Security Decisions or similar state document to clarify respective roles and responsibilities in the event of an incident. Also consider asking the local law enforcement to conduct periodic patrols of your water system.</p>	
<p>9. Is the area around all the critical components of your water system free of objects that may be used for breaking and entering?</p>	<p>Yes <input type="checkbox"/> No <input type="checkbox"/></p>	<p>When assessing the area around your water system’s critical components, look for objects that could be used to gain entry (e.g., large rocks, cement blocks, pieces of wood, ladders, valve keys, and other tools).</p>	
<p>10. Are the entry points to all of your water system easily seen?</p>	<p>Yes <input type="checkbox"/> No <input type="checkbox"/></p>	<p>You should clear fence lines of all vegetation. Overhanging or nearby trees may also provide easy access. Avoid landscaping that will permit trespassers to hide or conduct unnoticed suspicious activities.</p> <p>Trim trees and shrubs to enhance the visibility of your water system’s critical components.</p> <p>If possible, park vehicles and equipment in places where they do not block the view of your water system’s critical components.</p>	

11. Do you have an alarm system that will detect unauthorized entry or attempted entry at all critical components?	Yes <input type="checkbox"/> No <input type="checkbox"/>	<p>Consider installing an alarm system that notifies the proper authorities or your water system's designated contact for emergencies when there has been a breach of security. Inexpensive systems are available. An alarm system should be considered whenever possible for tanks, pump houses, and treatment facilities.</p> <p>You should also have an audible alarm at the site as a deterrent and to notify neighbors of a potential threat.</p>	
12. Do you have a key control and accountability policy?	Yes <input type="checkbox"/> No <input type="checkbox"/>	<p>Keep a record of locks and associated keys, and to whom the keys have been assigned. This record will facilitate lock replacement and key management (e.g., after employee turnover or loss of keys). Vehicle and building keys should be kept in a lockbox when not in use.</p> <p>You should have all keys stamped (engraved) "<b>DO NOT DUPLICATE.</b>"</p>	
13. Are entry codes and keys limited to water system personnel only?	Yes <input type="checkbox"/> No <input type="checkbox"/>	<p>Suppliers and personnel from co-located organizations (e.g., organizations using your facility for telecommunications) should be denied access to codes and/or keys. Codes should be changed frequently if possible. Entry into any building should always be under the direct control of water system personnel.</p>	
14. Do you have an updated operations and maintenance manual that includes evaluations of security systems?	Yes <input type="checkbox"/> No <input type="checkbox"/>	<p>Operation and maintenance plans are critical in assuring the on-going provision of safe and reliable water service. These plans should be updated to incorporate security considerations and the on-going reliability of security provisions – including security procedures and security related equipment.</p>	
15. Do you have a neighborhood watch program for your water system?	Yes <input type="checkbox"/> No <input type="checkbox"/>	<p>Watchful neighbors can be very helpful to a security program. Make sure they know whom to call in the event of an emergency or suspicious activity.</p>	

## Water Sources

*In addition to the above general checklist for your entire water system (questions 1-15), you should give special attention to the following issues, presented in separate tables, related to various water system components. Your water sources (surface water intakes or wells) should be secured. Surface water supplies present the greatest challenge. Typically they encompass large land areas. Where areas cannot be secured, steps should be taken to initiate or increase law enforcement patrols. Pay particular attention to surface water intakes. Ask the public to be vigilant and report suspicious activity.*

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
16. Are your wellheads sealed properly?	Yes <input type="checkbox"/> No <input type="checkbox"/>	A properly sealed wellhead decreases the opportunity for the introduction of contaminants. If you are not sure whether your wellhead is properly sealed, contact your well drilling/maintenance company, your state drinking water primacy agency, your state rural water association, or other technical assistance providers.	
17. Are well vents and caps screened and securely attached?	Yes <input type="checkbox"/> No <input type="checkbox"/>	Properly installed vents and caps can help prevent the introduction of a contaminant into the water supply.  Ensure that vents and caps serve their purpose, and cannot be easily breached or removed.	
18. Are observation/test and abandoned wells properly secured to prevent tampering?	Yes <input type="checkbox"/> No <input type="checkbox"/>	All observation/test and abandoned wells should be properly capped or secured to prevent the introduction of contaminants into the aquifer or water supply. Abandoned wells should be either removed or filled with concrete.	
19. Is your surface water source secured with fences or gates? Do water system personnel visit the source?	Yes <input type="checkbox"/> No <input type="checkbox"/>	Surface water supplies present the greatest challenge to secure. Often, they encompass large land areas. Where areas cannot be secured, steps should be taken to initiate or increase patrols by water utility personnel and law enforcement agents.	

## ***Treatment Plant and Suppliers***

***Some small systems provide easy access to their water system for suppliers of equipment, chemicals, and other materials for the convenience of both parties. This practice should be discontinued.***

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
20. Are deliveries of chemicals and other supplies made in the presence of water system personnel?	Yes <input type="checkbox"/> No <input type="checkbox"/>	Establish a policy that an authorized person, designated by the water system, must accompany all deliveries. Verify the credentials of all drivers. This prevents unauthorized personnel from having access to the water system.	
21. Have you discussed with your supplier(s) procedures to ensure the security of their products?	Yes <input type="checkbox"/> No <input type="checkbox"/>	Verify that your suppliers take precautions to ensure that their products are not contaminated. Chain of custody procedures for delivery of chemicals should be reviewed. You should inspect chemicals and other supplies at the time of delivery to verify they are sealed and in unopened containers. Match all delivered goods with purchase orders to ensure that they were, in fact, ordered by your water system.  You should keep a log or journal of deliveries. It should include the driver's name (taken from the driver's photo I.D.), date, time, material delivered, and the supplier's name.	
22. Are chemicals, particularly those that are potentially hazardous (e.g. chlorine gas) or flammable, properly stored in a secure area?	Yes <input type="checkbox"/> No <input type="checkbox"/>	All chemicals should be stored in an area designated for their storage only, and the area should be secure and access to the area restricted. Access to chemical storage should be available only to authorized employees. Pay special attention to the storage, handling, and security of chlorine gas because of its potential hazard.  You should have tools and equipment on site (such as a fire extinguisher, drysweep, etc.) to take immediate actions when responding to an emergency.	

<p>23. Do you monitor raw and treated water so that you can detect changes in water quality?</p>	<p>Yes <input type="checkbox"/> No <input type="checkbox"/></p>	<p>Monitoring of raw and treated water can establish a baseline that may allow you to know if there has been a contamination incident.</p> <p>Some parameters for raw water include pH, turbidity, total and fecal coliform, total organic carbon, specific conductivity, ultraviolet adsorption, color, and odor.</p> <p>Routine parameters for finished water and distribution systems include free and total chlorine residual, heterotrophic plate count (HPC), total and fecal coliform, pH, specific conductivity, color, taste, odor, and system pressure.</p> <p>Chlorine demand patterns can help you identify potential problems with your water. A sudden change in demand may be a good indicator of contamination in your system.</p> <p>For those systems that use chlorine, absence of chlorine residual may indicate possible contamination. Chlorine residuals provide protection against bacterial and viral contamination that may enter the water supply.</p>	
<p>24. Are tank ladders, access hatches, and entry points secured?</p>	<p>Yes <input type="checkbox"/> No <input type="checkbox"/></p>	<p>The use of tamper-proof padlocks at entry points (hatches, vents, and ladder enclosures) will reduce the potential for of unauthorized entry.</p> <p>If you have towers, consider putting physical barriers on the legs to prevent unauthorized climbing.</p>	
<p>25. Are vents and overflow pipes properly protected with screens and/or grates?</p>	<p>Yes <input type="checkbox"/> No <input type="checkbox"/></p>	<p>Air vents and overflow pipes are direct conduits to the finished water in storage facilities. Secure all vents and overflow pipes with heavy-duty screens and/or grates.</p>	
<p>26. Can you isolate the storage tank from the rest of the system?</p>	<p>Yes <input type="checkbox"/> No <input type="checkbox"/></p>	<p>A water system should be able to take its storage tank(s) out of operation or drain its storage tank(s) if there is a contamination problem or structural damage. Install shut-off or bypass valves to allow you to isolate the storage tank in the case of a contamination problem or structural damage.</p> <p>Consider installing a sampling tap on the storage tank outlet to test water in the tank for possible contamination.</p>	

## **Distribution**

***Hydrants are highly visible and convenient entry points into the distribution system. Maintaining and monitoring positive pressure in your system is important to provide fire protection and prevent introduction of contaminants.***

QUESTION	ANSWER	COMMENT	ACTION/NEEDED TAKEN
27. Do you control the use of hydrants and valves?	Yes <input type="checkbox"/> No <input type="checkbox"/>	<p>Your water system should have a policy that regulates the authorized use of hydrants for purposes other than fire protection. Require authorization and backflow devices if a hydrant is used for any purpose other than firefighting.</p> <p>Consider designating specific hydrants for use as filling station(s) with proper backflow prevention (e.g., to meet the needs of construction firms). Then, notify local law enforcement officials and the public that these are the only sites designated for this use.</p> <p>Flush hydrants should be kept locked to prevent contaminants from being introduced into the distribution system, and to prevent improper use.</p>	
28. Does your system monitor for, and maintain, positive pressure?	Yes <input type="checkbox"/> No <input type="checkbox"/>	Positive pressure is essential for fire fighting and for preventing backsiphonage that may contaminate finished water in the distribution system. Refer to your state primacy agency for minimum drinking water pressure requirements.	
29. Has your system implemented a backflow prevention program?	Yes <input type="checkbox"/> No <input type="checkbox"/>	In addition to maintaining positive pressure, backflow prevention programs provide an added margin of safety by helping to prevent the intentional introduction of contaminants. If you need information on backflow prevention programs, contact your state drinking water primacy agency.	



## ***Personnel***

***You should add security procedures to your personnel policies.***

<b>QUESTION</b>	<b>ANSWER</b>	<b>COMMENT</b>	<b>ACTION NEEDED/TAKEN</b>
30. When hiring personnel, do you request that local police perform a criminal background check, and do you verify employment eligibility (as required by the Immigration and Naturalization Service, Form I-9)?	Yes <input type="checkbox"/> No <input type="checkbox"/>	It is good practice to have all job candidates fill out an employment application. You should verify professional references. Background checks conducted during the hiring process may prevent potential employee-related security issues.  If you use contract personnel, check on the personnel practices of all providers to ensure that their hiring practices are consistent with good security practices.	
31. Are your personnel issued photo-identification cards?	Yes <input type="checkbox"/> No <input type="checkbox"/>	For positive identification, all personnel should be issued water system photo-identification cards and be required to display them at all times.  Photo identification will also facilitate identification of authorized water system personnel in the event of an emergency.	
32. When terminating employment, do you require employees to turn in photo IDs, keys, access codes, and other security-related items?	Yes <input type="checkbox"/> No <input type="checkbox"/>	Former or disgruntled employees have knowledge about the operation of your water system, and could have both the intent and physical capability to harm your system. Requiring employees who will no longer be working at your water system to turn in their IDs, keys, and access codes helps limit these types of security breaches.	
33. Do you use uniforms and vehicles with your water system name prominently displayed?	Yes <input type="checkbox"/> No <input type="checkbox"/>	Requiring personnel to wear uniforms, and requiring that all vehicles prominently display the water system name, helps inform the public when water system staff is working on the system. Any observed activity by personnel without uniforms should be regarded as suspicious. The public should be encouraged to report suspicious activity to law enforcement authorities.	
34. Have water system personnel been advised to report security vulnerability concerns and to report suspicious activity?	Yes <input type="checkbox"/> No <input type="checkbox"/>	Your personnel should be trained and knowledgeable about security issues at your facility, what to look for, and how to report any suspicious events or activity.  Periodic meetings of authorized personnel should be held to discuss security issues.	

35. Do your personnel have a checklist to use for threats or suspicious calls or to report suspicious activity?	Yes <input type="checkbox"/> No <input type="checkbox"/>	<p>To properly document suspicious or threatening phone calls or reports of suspicious activity, a simple checklist can be used to record and report all pertinent information. Calls should be reported immediately to appropriate law enforcement officials. Checklists should be available at every telephone. Sample checklists are included in Attachment 3.</p> <p>Also consider installing caller ID on your telephone system to keep a record of incoming calls.</p>	
---	--	--	--

## **Information/Storage/Computers/Controls/Maps**

**Security of the system, including computerized controls like a Supervisory Control and Data Acquisition (SCADA) system, goes beyond the physical aspects of operation. It also includes records and critical information that could be used by someone planning to disrupt or contaminate your water system.**

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
36. Is computer access "password protected?" Is virus protection installed and software upgraded regularly and are your virus definitions updated at least daily? Do you have Internet firewall software installed on your computer? Do you have a plan to back up your computers?	Yes <input type="checkbox"/> No <input type="checkbox"/>	<p>All computer access should be password protected. Passwords should be changed every 90 days and (as needed) following employee turnover. When possible, each individual should have a unique password that they do not share with others. If you have Internet access, a firewall protection program should be installed on your side of the computer and reviewed and updated periodically.</p> <p>Also consider contacting a virus protection company and subscribing to a virus update program to protect your records.</p> <p>Backing up computers regularly will help prevent the loss of data in the event that your computer is damaged or breaks. Backup copies of computer data should be made routinely and stored at a secure off-site location.</p>	
37. Is there information on the Web that can be used to disrupt your system or contaminate your water?	Yes <input type="checkbox"/> No <input type="checkbox"/>	<p>Posting detailed information about your water system on a Web site may make the system more vulnerable to attack. Web sites should be examined to determine whether they contain critical information that should be removed.</p> <p>You should do a Web search (using a search engine such as Google, Yahoo!, or Lycos) using key words related to your water supply to find any published data on the Web that is easily accessible by someone who may want to damage your water supply.</p>	
38. Are maps, records, and other information stored in a secure location?	Yes <input type="checkbox"/> No <input type="checkbox"/>	<p>Records, maps, and other information should be stored in a secure location when not in use. Access should be limited to authorized personnel only.</p> <p>You should make back-up copies of all data and sensitive documents. These should be stored in a secure off-site location on a regular basis.</p>	
39. Are copies of records, maps, and other sensitive information labeled confidential, and are all copies controlled and returned to the water system?	Yes <input type="checkbox"/> No <input type="checkbox"/>	<p>Sensitive documents (e.g., schematics, maps, and plans and specifications) distributed for construction projects or other uses should be recorded and recovered after use. You should discuss measures to safeguard your documents with bidders for new projects.</p>	

<p>40. Are vehicles locked and secured at all times?</p>	<p>Yes <input type="checkbox"/> No <input type="checkbox"/></p>	<p>Vehicles are essential to any water system. They typically contain maps and other information about the operation of the water system. Water system personnel should exercise caution to ensure that this information is secure.</p> <p>Water system vehicles should be locked when they are not in use or left unattended.</p> <p>Remove any critical information about the system before parking vehicles for the night.</p> <p>Vehicles also usually contain tools (e.g., valve wrenches) and keys that could be used to access critical components of your water system. These should be secured and accounted for daily.</p>	
--	---	--	--

## **Public Relations**

***You should educate your customers about your system. You should encourage them to be alert and to report any suspicious activity to law enforcement authorities.***

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
41. Do you have a program to educate and encourage the public to be vigilant and report suspicious activity to assist in the security protection of your water system?	Yes <input type="checkbox"/> No <input type="checkbox"/>	Advise your customers and the public that your system has increased preventive security measures to protect the water supply from vandalism. Ask for their help. Provide customers with your telephone number and the telephone number of the local law enforcement authority so that they can report suspicious activities. The telephone number can be made available through direct mail, billing inserts, notices on community bulletin boards, flyers, and consumer confidence reports.	
42. Does your water system have a procedure to deal with public information requests, and to restrict distribution of sensitive information?	Yes <input type="checkbox"/> No <input type="checkbox"/>	You should have a procedure for personnel to follow when you receive an inquiry about the water system or its operation from the press, customers, or the general public.  Your personnel should be advised not to speak to the media on behalf of the water system. Only one person should be designated as the spokesperson for the water system. Only that person should respond to media inquiries. You should establish a process for responding to inquiries from your customers and the general public.	
43. Do you have a procedure in place to receive notification of a suspected outbreak of a disease immediately after discovery by local health agencies?	Yes <input type="checkbox"/> No <input type="checkbox"/>	It is critical to be able to receive information about suspected problems with the water at any time and respond to them quickly. Written procedures should be developed in advance with your state drinking water primacy agency, local health agencies, and your local emergency planning committee and reviewed periodically.	

<p>44. Do you have a procedure in place to advise the community of contamination immediately after discovery?</p>	<p>Yes <input type="checkbox"/> No <input type="checkbox"/></p>	<p>As soon as possible after a disease outbreak, you should notify testing personnel and your laboratory of the incident. In outbreaks caused by microbial contaminants, it is critical to discover the type of contaminant and its method of transport (water, food, etc.). Active testing of your water supply will enable your laboratory, working in conjunction with public health officials, to determine if there are any unique (and possibly lethal) disease organisms in your water supply.</p> <p>It is critical to be able to get the word out to your customers as soon as possible after discovering a health hazard in your water supply. In addition to your responsibility to protect public health, you must also comply with the requirements of the Public Notification Rule. Some simple methods include announcements via radio or television, door-to-door notification, a phone tree, and posting notices in public places. The announcement should include accepted uses for the water and advice on where to obtain safe drinking water. Call large facilities that have large populations of people who might be particularly threatened by the outbreak: hospitals, nursing homes, the school district, jails, large public buildings, and large companies. Enlist the support of local emergency response personnel to assist in the effort.</p>	
<p>45. Do you have a procedure in place to respond immediately to a customer complaint about a new taste, odor, color, or other physical change (oily, filmy, burns on contact with skin)?</p>	<p>Yes <input type="checkbox"/> No <input type="checkbox"/></p>	<p>It is critical to be able to respond to and quickly identify potential water quality problems reported by customers. Procedures should be developed in advance to investigate and identify the cause of the problem, as well as to alert local health agencies, your state drinking water primacy agency, and your local emergency planning committee if you discover a problem.</p>	

***Now that you have completed the “Security Vulnerability Self-Assessment Guide for Small Water Systems Serving Populations between 3,300 and 10,000,” review your needed actions and then prioritize them based on the most likely threats. A Table to assist you in prioritizing actions is provided in Attachment 1.***







## Attachment 2. Emergency Contact List

All community water systems serving populations greater than 3,300 and less than 10,000 must adopt an emergency response plan (**ERP**) based on their vulnerability assessment. Emergency response plans are action steps to follow if a primary source of drinking water becomes contaminated or if the flow of water is disrupted. You can obtain sample ERPs from your state drinking water administrator, or from your state primacy agency.

This sample document is an “**Emergency Contact List.**” Although it can be an essential part of your ERP, **this will not satisfy the Bioterrorism Act requirement to develop or update your emergency response plan based on your vulnerability assessment.** It contains the names and telephone numbers of people you might need to call in the event of an emergency. This is a critical document to have at your disposal at all times. It gives you a quick reference to all names and telephone numbers that you need for support in the case of an emergency.

Filling out this Emergency Contact List reminds you to think about all of the people you might need to contact in an emergency. You should also talk with these people about what you and they would do if an emergency were to occur.

### **Section 1. System Identification**

Public Water System (PWS) ID Number		
System Name		
Town/City		
Telephone Numbers	System Telephone	Evening/Weekend Telephone
Other Contact Information	System Fax	Email
Population Served and Number of Service Connections	People Served	Connections
System Owner (The owner must be listed as a person’s name)		
Name, title, and telephone number of person responsible for maintaining this emergency contact list	Name and title	Telephone



**Section 2. Notification/Contact Information – Update regularly and display clearly next to telephones**

**Responders**

ORGANIZATION	CONTACT	PHONE (DAY)	PHONE (NIGHT)	E-MAIL
Fire Department				
Police Department				
FBI Field Office (for terrorism or sabotage)				
Emergency Medical Service				
Local Health Department				
National Spill Response Center	24 Hour Hotline	<b>1 (800) 424-8802</b>		
State Spill Hotline	24 Hour Hotline			
Local Hazmat Team (if any)				
Local/Regional Laboratory				
Water System Operators				



**Local Notification List**

ORGANIZATION	CONTACT NAME/TITLE	PHONE (DAY)	PHONE (NIGHT)	E-MAIL
Government Officials				
Emergency Planning Committee				
Hospitals				
Pharmacy				
Nursing Homes				
Schools				
Prisons				
Neighboring Water Systems				
Critical Industrial/Commercial Water Users				

### Service/Repair Notification List

ORGANIZATION	CONTACT NAME/TITLE	PHONE (DAY)	PHONE (NIGHT)	E-MAIL
Electrician				
Electric Utility Company				
Gas Utility Company				
Sewer Utility Company				
Telephone Utility Company				
Plumber				
Pump Specialist				
<b>"Dig Safe"</b> or local equivalent				
Soil Excavator/Backhoe				
Equipment Rental (Power Generators)				
Equipment Rental (Chlorinators)				
Equipment Rental (Portable Fencing)				
Equipment Repairman				
Equipment Repairman (Chlorinator)				
Radio/Telemetry Repair Service				
Bottled Water Source				
Bulk Water Hauler				
Pump Supplier				
Well Drillers				
Pipe Supplier				
Chemical Supplier				

**State Notification List**

<b>ORGANIZATION</b>	<b>CONTACT NAME/TITLE</b>	<b>PHONE (DAY)</b>	<b>PHONE (NIGHT)</b>	<b>E-MAIL</b>
Drinking Water Primacy Agency				
Department of Environmental Protection (or state equivalent)				
Department of Health				
Emergency Management Agency				
Hazmat Hotline				





**Media Notification List**

ORGANIZATION	CONTACT NAME/TITLE	PHONE (DAY)	PHONE (NIGHT)	E-MAIL
Designated Water System Spokesperson				
Newspaper - Local				
Newspaper – Regional/State				
Radio				
Television				



## **Section 3. Communication and Outreach**

### **Communication**

Communications during an emergency pose some special problems. A standard response might be to call “911” for local fire and police departments. But what if your emergency had disrupted telephone lines and overloaded cell phone lines?

Talk with your local Emergency Management Agency, Health Department representative, or your Local Emergency Planning Committee (**LEPC**) about local emergency preparedness and solutions to these problems. Increasingly, state emergency agencies are establishing secure lines of communication with limited access.

Learn how you can access those lines of communication if all others fail.

### **Outreach**

If there is an incident of contamination in your water supply, you will need to notify the public and make public health recommendations (e.g., boil water, or use bottled water). To do this, you need a plan.

- How will you reach all customers in the first 24 hours of an emergency?
- Appoint a media spokesperson—a single person in your water system who will be authorized to make all public statements to the media.
- Make arrangements for contacting institutions with large numbers of people, some of whom may be immuno-compromised:
  - ✓ Nursing homes
  - ✓ Hospitals
  - ✓ Schools
  - ✓ Prisons



## Attachment 3: Threat Identification Checklists

### Water System Telephone Threat Identification Checklist

In the event your water system receives a threatening phone call, remain calm and try to keep the caller on the line. Use the following checklist to collect as much detail as possible about the nature of the threat and the description of the caller.

<p><b>1. Types of Tampering/Threat:</b></p> <p><input type="checkbox"/> Contamination                      <input type="checkbox"/> Threat to tamper</p> <p><input type="checkbox"/> Biological                                <input type="checkbox"/> Bombs, explosives, etc.</p> <p><input type="checkbox"/> Chemical                                 <input type="checkbox"/> Other (explain)</p>
<p><b>2. Water System Identification:</b></p> <p>Name: Address:</p> <p>Telephone:</p> <p>PWS Owner or Manager's Name:</p>
<p><b>3. Alternate Water Source Available: Yes/No                      If yes, give name and location:</b></p>
<p><b>4. Location of Tampering:</b></p> <p><input type="checkbox"/> Distribution Line    <input type="checkbox"/> Water Storage Facilities    <input type="checkbox"/> Treatment Plant    <input type="checkbox"/> Raw Water Source    <input type="checkbox"/> Treatment Chemicals</p> <p><input type="checkbox"/> Other (explain):</p>
<p><b>5. Contaminant Source and Quantity:</b></p>
<p><b>7. Date and Time of Tampering/Threat:</b></p>
<p><b>8. Caller's Name/Alias, Address, and Telephone Number:</b></p>

**9. Is the Caller (check all that apply):**

- Female
- Male

**10. Is the Caller's Voice (check all that apply):**

- Soft
- Slurred
- Deep
- Old
- Calm
- Loud
- Nasal
- High
- Angry
- Laughing
- Clear
- Cracking
- Slow
- Crying
- Lisp
- Excited
- Rapid
- Normal
- Stuttering
- Young
- Familiar (who did it sound like?)
- Accented (which nationality or region?)

**11. Is the Connection Clear? (Could it have been a wireless or cell phone?)**

**12. Are There Background Noises?**

<input type="checkbox"/> Street noises (what kind?)	
<input type="checkbox"/> Machinery (what type?)	
<input type="checkbox"/> Voices (describe)	
<input type="checkbox"/> Children (describe)	
<input type="checkbox"/> Animals (what kind?)	
<input type="checkbox"/> Computer Keyboard, Office	
<input type="checkbox"/> Motors (describe)	
<input type="checkbox"/> Music (what kind?)	
<input type="checkbox"/> Other	

<b>13. Call Received By (Name, Address, and Telephone Number):</b>	
Date Call Received:	
Time of Call:	
<b>14. Call Reported to:</b>	<b>Date/Time</b>
<b>15. Action(s) Taken Following Receipt of Call:</b>	





# Water System Report of Suspicious Activity

In the event personnel from your water system (or neighbors of your water system) observe suspicious activity, use the following checklist to collect as much detail about the nature of the activity.

<b>1. Types of Suspicious Activity:</b>				
<input type="checkbox"/> Breach of security systems (e.g., lock cut, door forced open)	<input type="checkbox"/> Changes in water quality noticed by customers (e.g., change in color, odor, taste) that were not planned or announced by the water system			
<input type="checkbox"/> Unauthorized personnel on water system property.	<input type="checkbox"/> Other (explain)			
<input type="checkbox"/> Presence of personnel at the water system at unusual hours				
<b>2. Water System Identification:</b>				
Name:				
Address:				
Telephone:				
PWS Owner or Manager's Name:				
<b>3. Alternate Water Source Available: Yes/No</b>	<b>If yes, give name and location:</b>			
<b>4. Location of Suspicious Activity:</b>				
<input type="checkbox"/> Distribution Line	<input type="checkbox"/> Water Storage Facilities	<input type="checkbox"/> Treatment Plant	<input type="checkbox"/> RawWater Source	<input type="checkbox"/> Treatment Chemicals
<input type="checkbox"/> Other (explain):				

**5. If Breach of Security, What was the Nature of the Breach?**

- Lock was cut or broken, permitting unauthorized entry.

Specify location

- Lock was tampered with, but not sufficiently to allow unauthorized entry.

Specify location

- Door, gate, window, or any other point of entry (vent, hatch, etc.) was open and unsecured

Specify location

- Other

Specify nature and location

**6. Unauthorized personnel on site?**

Where were these people?

Specify location

What made them suspicious?

- Not wearing water system uniforms  
 Something else? (Specify)

What were they doing?

**7. Please describe these personnel (height, weight, hair color, clothes, facial hair, any distinguishing marks):**

**8. Call Received By (Name, Address, and Telephone Number):**

**Received:**

**Time of Call:**

**9. Call Reported to:**

**Date/Time:**

**10. Action(s) Taken Following Receipt of Call:**

## Freedom of Information Act Guide, May 2000 Exemption 2 Excerpts

Exemption 2 of the FOIA exempts from mandatory disclosure records that are "related solely to the internal personnel rules and practices of an agency." (1) Courts have interpreted the exemption to encompass two distinct categories of information:

(a) internal matters of a relatively trivial nature—sometimes referred to as "low 2" information; and

(b) more substantial internal matters, the disclosure of which would risk circumvention of a legal requirement--sometimes referred to as "high 2" information.

(2) For a long time, much confusion existed concerning the intended coverage of Exemption 2, due to the differing ways in which Exemption 2 was addressed in the Senate and House Reports when the FOIA was enacted. The Senate Report stated:

Exemption No. 2 relates only to the internal personnel rules and practices of an agency. Examples of these may be rules as to personnel's use of parking facilities or regulation of lunch hours, statements of policy as to sick leave, and the like.

(3) The House Report provided a more expansive interpretation of Exemption 2's coverage, stating that it was intended to include: [o]perating rules, guidelines, and manuals of procedure for Government investigators or examiners . . . but [that] this exemption would not cover all "matters of internal management" such as employee relations and working conditions and routine administrative procedures which are withheld under present law.

(4) The Supreme Court confronted the conflict in Exemption 2's coverage of routine internal matters in a case in which a requester sought to obtain case summaries of Air Force Academy ethics hearings, and it found the Senate Report to be more authoritative. In *Department of the Air Force v. Rose*,

(5) the Supreme Court construed Exemption 2's somewhat ambiguous language as protecting internal agency matters so routine or trivial that they could not be "subject to . . . a genuine and significant public interest."

(6) The Court declared that Exemption 2 was intended to relieve agencies of the burden of assembling and providing access to any "matter in which the public could not reasonably be expected to have an interest."

(7) At the same time, presaging the eventual development of "high 2," the Court also suggested in *Rose* that the policy enunciated by the House Report might permit an agency to withhold matters of some public interest "where disclosure may risk circumvention of agency regulation."

(8) The Supreme Court's ruling in *Rose* helped to define the contours of Exemption 2, but it did not dispel all the confusion about its scope. Early judicial opinions, particularly in the Court of Appeals for the District of Columbia Circuit, showed that courts were unsure whether the exemption covered only internal personnel rules and personnel practices of an agency or, on the other hand, an agency's internal personnel rules and more general internal practices.

(9) This confusion was finally laid to rest, at least in the D.C. Circuit, in *Founding Church of Scientology v. Smith*,

(10) which articulated the following test for Exemption 2 coverage: First, the material withheld should fall within the terms of the statutory language as a personnel rule or internal practice of the agency. Then, if the material relates to trivial administrative matters of no genuine public interest, exemption would be automatic under the statute. If withholding frustrates legitimate public interest, however, the material should be released unless the government can show that disclosure would risk circumvention of lawful agency regulation.

### **"High 2": Risk of Circumvention**

The second category of information covered by Exemption 2--internal matters of a more substantial nature the disclosure of which would risk the circumvention of a statute or agency regulation--has generated considerable controversy over the years. In *Department of the Air Force v. Rose*,<sup>(51)</sup> the Supreme Court specifically left open the question of whether such records fall within Exemption 2 coverage. Most of the cases first developed this aspect of the exemption in the context of law enforcement manuals containing sensitive staff instructions. For example, the position adopted by the Court of Appeals for the Eighth Circuit on this subject is that Exemption 2 does not relate to such matters, but that subsection (a)(2)(C) of the FOIA,<sup>(52)</sup> which arguably excludes law enforcement manuals from the automatic disclosure provisions of the FOIA, bars disclosure of manuals whose release to the public would significantly impede the law enforcement process.<sup>(53)</sup> Although tacitly approving the Eighth Circuit's argument, the Courts of Appeals for the Fifth and Sixth Circuits have an alternative rationale for withholding law enforcement manuals; disclosure would allow persons "simultaneously to violate the law and to avoid detection"<sup>(54)</sup> by impeding law enforcement efforts.<sup>(55)</sup>

The majority of the courts in other circuits, however, have placed greater weight on the House Report<sup>(56)</sup> in this respect and accordingly have held that Exemption 2 is applicable to internal administrative and personnel matters, including law enforcement manuals, to the extent that disclosure would risk circumvention of an agency regulation or statute or impede the effectiveness of an agency's law enforcement activities.<sup>(57)</sup>

The Court of Appeals for the District of Columbia Circuit adopted this majority approach when the full court addressed the issue in *Crooker v. ATF*, a case involving a law enforcement agents' training manual.<sup>(58)</sup> Although not explicitly overruling its earlier en banc decision in *Jordan v. United States Department of Justice*, which held that guidelines for the exercise of prosecutorial discretion were not properly withholdable,<sup>(59)</sup> the en banc decision in *Crooker* specifically rejected the rationale of *Jordan* that Exemption 2 cannot protect law enforcement manuals or other documents whose disclosure would risk circumvention of the law.<sup>(60)</sup>

In *Crooker*, the D.C. Circuit fashioned a two-part test for determining which sensitive materials are exempt from mandatory disclosure under Exemption 2.

This test requires both:

(1) that a requested document be "predominantly internal," and

(2) that its disclosure "significantly risks circumvention of agency regulations or statutes."<sup>(61)</sup>

Whether there is any public interest in disclosure is legally irrelevant under this "anti-circumvention" aspect of Exemption 2.(62) Rather, the concern under "high 2" is that a FOIA disclosure should not "benefit those attempting to violate the law and avoid detection."(63) Thus, this aspect of Exemption 2 fundamentally rests upon a determination of "foreseeable harm."(64)

In years past, it was often relatively easy to meet the first part of the Crooker test that the materials be "predominantly internal."(65) The D.C. Circuit established specific guidance on what constitutes an "internal" document in *Cox v. United States Department of Justice*, which held protectible information that

does not purport to regulate activities among members of the public . . . [and] does [not] . . . set standards to be followed by agency personnel in deciding whether to proceed against or to take action affecting members of the public. Differently stated, the unreleased information is not "secret law," the primary target of [the FOIA's] disclosure provisions.(66)

Reflecting a measure of deference that is implicitly accorded law enforcement activities under this substantive aspect of Exemption 2,(67) courts have treated a wide variety of information pertaining to such activities as "internal," including:

- (1) general guidelines for conducting investigations;(68)
- (2) guidelines for conducting post-investigation litigation;(69)
- (3) guidelines for identifying law violators;(70)
- (4) a study of agency practices and problems pertaining to undercover agents;(71) and
- (5) sections of a Bureau of Prisons manual which summarize procedures for security of prison control centers, including escape prevention plans, control of keys and locks within a prison, instructions regarding transportation of federal prisoners, and the arms and defensive equipment inventories maintained in the facility.(72)

Exemption 2's "circumvention" protection also should be readily applicable to vulnerability assessments, which are perhaps the quintessential type of record warranting protection on that basis; such records generally assess an agency's vulnerability (or that of another institution) to some form of outside interference or harm by identifying those programs or systems deemed the most sensitive and describing specific security measures that can be used to counteract such vulnerabilities.(91) A prime example of vulnerability assessments warranting protection under "high 2" are the computer security plans that all federal agencies are required by law to prepare.(92) In a decision involving such a document, *Schreibman v. United States Department of Commerce*,(93) Exemption 2 coverage was invoked to prevent unauthorized access to information which could result in "alternation [sic], loss, damage or destruction of data contained in the computer system."(94) It should be remembered, however, that even such a sensitive document must be reviewed to determine whether any "reasonably segregable" portion can be disclosed without harm.(95) See the further discussions of this under Procedural Requirements, "Reasonably Segregable "Obligation, above, and Litigation Considerations, "Reasonably Segregable" Requirements,

Release of various other categories of information also has been found likely to result in harmful circumvention:

- (1) information that would reveal the identities of informants;(96)
- (2) information that would reveal the identities of undercover agents;(97)
- (3) sensitive administrative notations in law enforcement files;(98)
- (4) security techniques used in prisons;(99)
- (5) agency audit guidelines;(100)
- (6) agency testing materials;(101)
- (7) codes that would identify intelligence targets;(102)
- (8) agency credit card numbers;(103) and
- (9) an agency's unclassified manual detailing the categories of information that are classified and their corresponding classification levels.(104)

Finally, under the Freedom of Information Reform Act of 1986,(124) many of the materials previously protectible only on a "high 2" basis may be protectible also under Exemption 7(E).(125) Several post-amendment cases have held such information to be exempt from disclosure under both Exemption 2 and Exemption 7(E).(126) While Exemption 2 must still be used if any information fails to meet Exemption 7's "law enforcement" threshold, Exemption 2's history and judicial interpretations should be helpful in applying Exemption 7(E).

## **Conclusion**

### **Priorities for the Future**

This National Strategy for Homeland Security has set a broad and complex agenda for the United States. The Strategy has defined many different goals that need to be met, programs that need to be implemented, and responsibilities that need to be fulfilled.

The principal purpose of a strategy, however, is to set priorities. It is particularly important for government institutions to set priorities explicitly, since these institutions generally lack a clear measure of how successfully they provide value to the citizenry.

Setting priorities is important to homeland security in two distinct respects. First, there is the question of the priority of homeland security compared to everything else the government does or might do.

There is a strong consensus that protecting the people from terrorist attacks of potentially catastrophic proportions is among the highest, if not the highest, priority any government can have.

There will, of course, be vigorous debate over how to achieve specific homeland security goals, who should pay, how much security is enough, and what the responsibilities of different entities should be, but there is little disagreement that securing the homeland is more important than just about every other government activity.

Americans will never forget the murderous events of September 11, 2001. Our Nation suffered great harm on that terrible morning.

The American people have responded magnificently with courage and compassion, strength and resolve. There should be no doubt that we will succeed in weaving an effective and permanent level of security into the fabric of a better, safer, stronger America.





## FBI Offices

FBI Albany  
200 McCarty Avenue  
Albany, New York 12209  
albany.fbi.gov  
(518) 465-7551

FBI Albuquerque  
Suite 300  
415 Silver Avenue, Southwest  
Albuquerque, New Mexico 87102  
albuquerque.fbi.gov  
(505) 224-2000

FBI Anchorage  
101 East Sixth Avenue  
Anchorage, Alaska 99501-2524  
anchorage.fbi.gov  
(907) 258-5322

FBI Atlanta  
Suite 400  
2635 Century Parkway, Northeast  
Atlanta, Georgia 30345-3112  
atlanta.fbi.gov  
(404) 679-9000

FBI Baltimore  
7142 Ambassador Road  
Baltimore, Maryland 21244-2754  
baltimore.fbi.gov  
(410) 265-8080

FBI Birmingham  
Room 1400  
2121 8th. Avenue N.  
Birmingham, Alabama 35203-2396  
birmingham.fbi.gov  
(205) 326-6166

FBI Boston  
Suite 600  
One Center Plaza  
Boston, Massachusetts 02108  
boston.fbi.gov  
(617) 742-5533

FBI Buffalo  
One FBI Plaza  
Buffalo, New York 14202-2698  
buffalo.fbi.gov  
(716) 856-7800

FBI Charlotte  
Suite 900, Wachovia Building  
400 South Tyron Street  
Charlotte, North Carolina 28285-0001  
charlotte.fbi.gov  
(704) 377-9200

FBI Chicago  
Room 905  
E.M. Dirksen Federal Office Building  
219 South Dearborn Street  
Chicago, Illinois 60604-1702  
chicago.fbi.gov  
(312) 431-1333

FBI Cincinnati  
Room 9000  
550 Main Street  
Cincinnati, Ohio 45202-8501  
cincinnati.fbi.gov  
(513) 421-4310

FBI Cleveland  
Room 3005  
Federal Office Building  
1240 East 9th Street  
Cleveland, Ohio 44199-9912  
cleveland.fbi.gov  
(216) 522-1400

FBI Columbia  
151 Westpark Blvd  
Columbia, South Carolina 29210-3857  
columbia.fbi.gov  
(803) 551-4200

FBI Dallas  
One Justice Way  
Dallas, Texas 75220  
dallas.fbi.gov  
(972) 559-5000

FBI Denver  
Federal Office Building, Room 1823  
1961 Stout Street, 18th. Floor  
Denver, Colorado 80294-1823  
denver.fbi.gov  
(303) 629-7171

FBI Detroit  
26th. Floor, P. V. McNamara FOB  
477 Michigan Avenue  
Detroit, Michigan 48226  
detroit.fbi.gov  
(313) 965-2323

FBI El Paso  
660 S. Mesa Hills Drive  
El Paso, Texas 79912-5533  
elpaso.fbi.gov  
(915) 832-5000

FBI Honolulu  
Room 4-230, Kalaniana'ole FOB  
300 Ala Moana Boulevard  
Honolulu, Hawaii 96850-0053  
honolulu.fbi.gov  
(808) 521-1411

FBI Houston  
2500 East TC Jester  
Houston, Texas 77008-1300  
houston.fbi.gov  
(713) 693-5000

FBI Indianapolis  
Room 679, FOB  
575 North Pennsylvania Street  
Indianapolis, Indiana 46204-1585  
indianapolis.fbi.gov  
(317) 639-3301

FBI Jackson  
Room 1553, FOB  
100 West Capitol Street  
Jackson, Mississippi 39269-1601  
jackson.fbi.gov  
(601) 948-5000

FBI Jacksonville  
Suite 200  
7820 Arlington Expressway  
Jacksonville, Florida 32211-7499  
jacksonville.fbi.gov  
(904) 721-1211

FBI Kansas City  
1300 Summit  
Kansas City, Missouri 64105-1362  
kansascity.fbi.gov  
(816) 512-8200

FBI Knoxville  
Suite 600, John J. Duncan FOB  
710 Locust Street  
Knoxville, Tennessee 37902-2537  
knoxville.fbi.gov  
(865) 544-0751

FBI Las Vegas  
John Lawrence Bailey Building  
700 East Charleston Boulevard  
Las Vegas, Nevada 89104-1545  
lasvegas.fbi.gov  
(702) 385-1281

FBI Little Rock  
Suite 200  
Two Financial Centre  
10825 Financial Centre Parkway  
Little Rock, Arkansas 72211-3552  
littlerock.fbi.gov  
(501) 221-9100

FBI Los Angeles  
Suite 1700, FOB  
11000 Wilshire Boulevard  
Los Angeles, California 90024-3672  
losangeles.fbi.gov  
(310) 477-6565

FBI Louisville  
Room 500  
600 Martin Luther King Jr. Place  
Louisville, Kentucky 40202-2231  
louisville.fbi.gov  
(502) 583-3941

FBI Memphis  
Suite 3000, Eagle Crest Bldg.  
225 North Humphreys Blvd.  
Memphis, Tennessee 38120-2107  
memphis.fbi.gov  
(901) 747-4300

FBI North Miami Beach  
16320 Northwest Second Avenue  
North Miami Beach, Florida 33169-6508  
miami.fbi.gov  
(305) 944-9101

FBI Milwaukee  
Suite 600  
330 East Kilbourn Avenue  
Milwaukee, Wisconsin 53202-6627  
milwaukee.fbi.gov  
(414) 276-4684

FBI Minneapolis  
Suite 1100  
111 Washington Avenue, South  
Minneapolis, Minnesota 55401-2176  
minneapolis.fbi.gov  
(612) 376-3200

FBI Mobile  
One St. Louis Centre  
1 St. Louis Street, 3rd. Floor  
Mobile, Alabama 36602-3930  
mobile.fbi.gov  
(334) 438-3674

FBI Newark  
1 Gateway Center, 22nd. Floor  
Newark, New Jersey 07102-9889  
newark.fbi.gov  
(973) 792-3000

FBI New Haven  
600 State Street  
New Haven, Connecticut 06511-6505  
(203) 777-6311

FBI New Orleans  
2901 Leon C. Simon Dr.  
New Orleans, Louisiana 70126  
neworleans.fbi.gov  
(504) 816-3000

FBI New York  
26 Federal Plaza, 23rd. Floor  
New York, New York 10278-0004  
newyork.fbi.gov  
(212) 384-1000

FBI Norfolk  
150 Corporate Boulevard  
Norfolk, Virginia 23502-4999  
norfolk.fbi.gov  
(757) 455-0100

FBI Oklahoma City  
3301 West Memorial Drive  
Oklahoma City, Oklahoma 73134  
oklahomacity.fbi.gov  
(405) 290-7770

FBI Omaha  
10755 Burt Street  
Omaha, Nebraska 68114-2000  
omaha.fbi.gov  
(402) 493-8688

FBI Philadelphia  
8th. Floor  
William J. Green Jr. FOB  
600 Arch Street  
Philadelphia, Pennsylvania 19106  
philadelphia.fbi.gov  
(215) 418-4000

FBI Phoenix  
Suite 400  
201 East Indianola Avenue  
Phoenix, Arizona 85012-2080  
phoenix.fbi.gov  
(602) 279-5511

FBI Pittsburgh  
3311 East Carson St.  
Pittsburgh, PA 15203  
pittsburgh.fbi.gov  
(412) 432-4000

FBI Portland  
Suite 400, Crown Plaza Building  
1500 Southwest 1st Avenue  
Portland, Oregon 97201-5828  
portland.fbi.gov  
(503) 224-4181

FBI Richmond  
1970 E. Parham Road  
Richmond, Virginia 23228  
richmond.fbi.gov  
(804) 261-1044

FBI Sacramento  
4500 Orange Grove Avenue  
Sacramento, California 95841-4205  
sacramento.fbi.gov  
(916) 481-9110

FBI St. Louis  
2222 Market Street  
St. Louis, Missouri 63103-2516  
stlouis.fbi.gov  
(314) 231-4324

FBI Salt Lake City  
Suite 1200, 257 Towers Bldg.  
257 East, 200 South  
Salt Lake City, Utah 84111-2048  
saltlakecity.fbi.gov  
(801) 579-1400

FBI San Antonio  
Suite 200  
U.S. Post Office Courthouse Bldg.  
615 East Houston Street  
San Antonio, Texas 78205-9998  
sanantonio.fbi.gov  
(210) 225-6741

FBI San Diego  
Federal Office Building  
9797 Aero Drive  
San Diego, California 92123-1800  
sandiego.fbi.gov  
(858) 565-1255

FBI San Francisco  
450 Golden Gate Avenue, 13th. Floor  
San Francisco, California 94102-9523  
sanfrancisco.fbi.gov  
(415) 553-7400

FBI San Juan  
Room 526, U.S. Federal Bldg.  
150 Carlos Chardon Avenue  
Hato Rey  
San Juan, Puerto Rico 00918-1716  
sanjuan.fbi.gov  
(787) 754-6000

FBI Seattle  
1110 Third Avenue  
Seattle, Washington 98101-2904  
seattle.fbi.gov  
(206) 622-0460

FBI Springfield  
Suite 400  
400 West Monroe Street  
Springfield, Illinois 62704-1800  
springfield.fbi.gov  
(217) 522-9675

FBI Tampa  
Room 610, FOB  
500 Zack Street  
Tampa, Florida 33602-3917  
tampa.fbi.gov  
(813) 273-4566

FBI Washington  
Washington Metropolitan Field Office  
601 4th Street, N.W.  
Washington, D.C. 20535-0002  
washingtondc.fbi.gov  
(202) 278-2000



Excellent example of a secure office environment



The Operator has complete access to employee photographs, policies, procedures and communications.



Obstructed Cargo Area Search w/Pole. Quick Connect Trolley For Under Vehicle Search (in foreground)

Zistos offers LOW COST portable Flex 'N Stay® Video camera INSPECTION systems to view or record or transmit condition-monitoring maintenance or rescue images from inside machines, inaccessible voids including underwater. Data recorded ON THE IMAGE (time/date/size/GPS location) helps identify the hidden problems or allows trend monitoring the internal machine/tank/pipe flaws. Other uses — search cargo containers, trucks, aircraft for contraband.

RESCUE or HAZMAT or EMERGENCY teams can SEARCH collapsed building voids, assess trapped accident victim extrication. Police TACTICAL OPERATIONS can COVERTLY SEE around corners, through windows, assess bombs, from a safe distance - in total darkness.

Then — transmit the image to a second remote Zistos display.



This “Clock” has a small video camera in the dot between the 1 and 2. It is best to keep a digital record of your video recordings. This type of camera is commonly found in Police or Security Departments and is usually accompanied by a “*Voice activated*” sound recorder, as well. These types of devices are not legal for employee surveillance.

## **WaterISAC – [www.waterisac.org](http://www.waterisac.org)**

*As a drinking water or wastewater utility manager, you have made some very important decisions related to the safety of your employees, the health of your customers and the continued reliability of your system.*

*You have improved security by constructing barriers, changing procedures and installing sophisticated security equipment.*

*You have conducted vulnerability assessments and developed security strategies and emergency response plans.*

### **What's missing from your security toolbox? The WaterISAC.**

*The WaterISAC is a constantly updated source of security information. By subscribing to this service, you will help to ensure your vulnerability assessment, security strategy and emergency response plan remain up-to-date.*

*Add the WaterISAC to your security toolbox today.*

#### **Products & Services**

- Alerts on potential terrorist activity.
- Information on water security from federal homeland security, intelligence, law enforcement, public health and environment agencies.
- Databases of chemical, biological and radiological agents.
- Physical vulnerabilities and security solutions.
- Research, reports and other information.
- Notification of cyber vulnerabilities and technical fixes.
- A secure means for reporting security incidents.
- Vulnerability assessment tools and resources.
- Secure electronic bulletin boards and chat rooms on security topics.
- Emergency preparedness and response resources.

#### **WaterISAC: The Next Level of Security**

Information is the key to protecting the nation's drinking water and wastewater infrastructure. In response to the need for sound security information, the *Water Information Sharing and Analysis Center*, or *WaterISAC*, was developed to provide America's drinking water and wastewater systems with a secure Web-based environment for early warning of potential physical, contamination and cyber threats and a source of knowledge about security — an information edge in the fight against terrorism.

The *WaterISAC* helps the water sector move to the next level of security, with its wide array of information and tools to assist in identifying and assessing threats, in taking measures to mitigate those threats and in analyzing incident reports.

The *Water/SAC* also serves as an important link between the water sector and federal environmental, homeland security, law enforcement, intelligence and public health agencies. In addition, the *Water/SAC* provides many resources to help utilities complete and continually improve their vulnerability assessments and emergency response plans, required by law for many systems.

### **A Federal Call For ISACs**

Presidential Decision Directive 63 and Executive Order 13231 designate the water sector and other industry sectors as critical to the nation's well-being. These presidential orders also call for the various sectors to establish Information Sharing and Analysis Centers, or ISACs, to promote the flow of security information. The water sector must protect its critical facilities from terrorist and other threats because safe and clean water is fundamental to the nation's health and economic prosperity.

### ***Water/SAC* Subscriptions and Users**

The *Water/SAC* is open to all U.S. drinking water and wastewater systems.

Subscription fees are based on the number of people served by the utility. The information on the *Water/SAC* is specifically geared to utility executives, managers, operators and security officers. Because of the sensitive nature of the information, subscribers must agree in advance to protect the *Water/SAC's* sensitive information from disclosure and establish protocols for handling the information within the utility.

Each utility will be allowed a certain number of users, depending on the size of the utility. To access the secure portal of the *Water/SAC*, users will be provided a smart card and card reader and a special access code.

Refer to the *Water/SAC* Service Agreement for details on subscription fees and users.

### **More Than A Clearinghouse**

The *Water/SAC* is much more than a security clearinghouse. While it gathers and distributes information on threats to the drinking water and wastewater industry, it takes the additional steps of analyzing information and identifying trends. This extremely sensitive and valuable information is then distributed to subscribers through encrypted e-mail and a secure portal, making the *Water/SAC* the one place where all sensitive security-related information is available to the drinking water and wastewater community.

Using secure electronic bulletin boards and chat rooms, for the first time drinking water and wastewater systems have a forum for sharing and discussing sensitive information and intelligence. These state-of-the-art forums will host discussions on current security topics, keeping the water sector informed with the latest knowledge.

Beyond these immediate objectives, the *Water/SAC* is also designed to offer a repository for security-related documents, a focal point for online training and education on security topics, a place where utility managers can share information and advice in a secure setting, a contact point for links and resources beyond the world of utilities and a security library tailored to the needs of the sector.

### **Potential Threats to Water Security International Terrorists**

- Domestic Terrorists
- Extreme Activists



- Lone Wolves
- Insiders
- Vandals

### **Secure Handling Of Sensitive Information**

Analysts for the *WaterISAC* have government security clearances and operate under strict protocols. The computers hosting the *WaterISAC* portal reside in a government-approved facility and are protected by security barriers and monitored by IT security experts. Communications from the *WaterISAC* to subscribers are conducted through encrypted e-mail.

Many different sources are used to gather information for the *WaterISAC*, including intelligence and law enforcement agencies, water utility incident reports, research foundations, federal public health and research agencies, publicly available information and private organizations, such as think tanks. *WaterISAC* analysts gather information from these sources, then assess, sanitize and disseminate it, enabling managers to make better-informed security decisions.

Within the *WaterISAC*'s organization, analysts investigate and disseminate threat reports and other security information. Subject-matter experts are on call and brought in on an as-needed basis. In conducting analysis for the *WaterISAC*, analysts look for patterns and trends in seemingly unrelated events and seek associations that may link several events together.

### **User-Friendly Web Interface**

The web interface for the *WaterISAC* is designed to be user-friendly, with a homepage that provides sensitive security information in an easy-to-find format.

Elements of the *WaterISAC* web site include:

- Contaminant Information
- Cyber Security Information
- Physical Threat Information
- Secure Bulletin Boards and Chat Rooms
- Vulnerability Assessment Tools and Training Aids
- Government Reports
- Case Studies
- Research Reports
- Incident Reporting Forms
- Key Web Site Links
- Federal Laws and Regulations

### ***WaterISAC* Governance**

The *WaterISAC* was developed for the drinking water and wastewater community under a grant from the U.S. Environmental Protection Agency by the Association of Metropolitan Water Agencies, with the advice of utility representatives. The *WaterISAC* is governed by a Board of Managers, comprised of water utility managers appointed by the national drinking water and wastewater organizations below. There are also two at-large seats, filled by the Board of Managers.

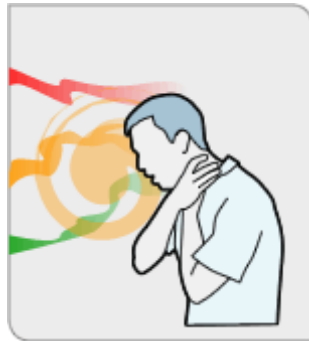
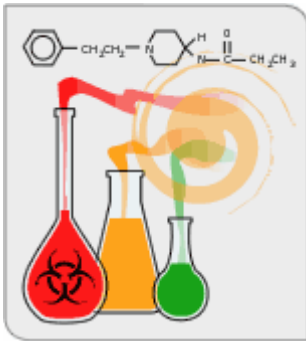
*American Water Works Association*  
*Association of Metropolitan Sewerage Agencies*  
*Association of Metropolitan Water Agencies*  
*Awwa Research Foundation*

*National Association of Water Companies*  
*National Rural Water Association*  
*Water Environment Federation*  
*Water Environment Research Foundation*

**System Requirements**

- 133 MHz or higher CPU, and Windows 2000 operating system (or XP)
- Min. 64 MB of RAM (128 MB of RAM preferred)
- Min. 2 GB hard disk (4 GB preferred) with 650 MB of free space
- A USB or Serial or PCMCIA port available
- Internet Explorer version 6.x or higher (preferred), or Netscape version 7.x or higher
- Floppy disk drive
- Adobe Acrobat Reader 5

# Chemical Attack



1. A chemical attack is the deliberate release of a toxic gas, liquid or solid that can poison people and the environment.
2. Watch for signs such as many people suffering from watery eyes, twitching, choking, having trouble breathing or losing coordination.
3. Many sick or dead birds, fish or small animals are also cause for suspicion.



4. If you see signs of a chemical attack, quickly try to define the impacted area or where the chemical is coming from, if possible.
5. Take immediate action to get away from any sign of a chemical attack.
6. If the chemical is inside a building where you are, try to get out of the building without passing through the contaminated area, if possible.



7. Otherwise, it may be better to move as far away from where you suspect the chemical release is and "shelter-in-place."

8. If you are outside when you see signs of a chemical attack, you must quickly decide the fastest way to get away from the chemical threat.

9. Consider if you can get out of the area or if it would be better to go inside a building and follow your plan to "shelter-in-place."

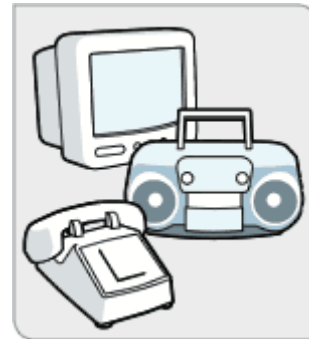
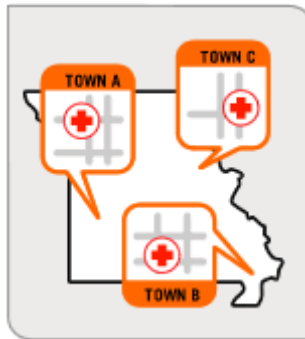
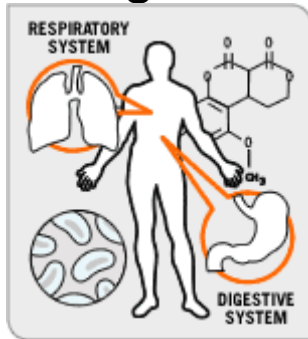


10. If your eyes are watering, your skin is stinging, you are having trouble breathing or you simply think you may have been exposed to a chemical, immediately strip and wash. Look for a hose, fountain, or any source of water.

11. Wash with soap and water, if possible, but do not scrub the chemical into your skin.

12. Seek emergency medical attention.

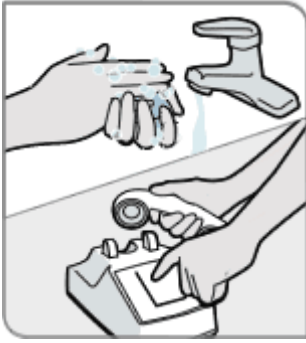
# Biological Attack



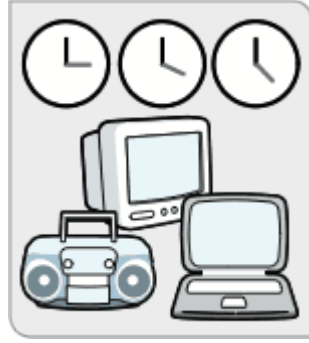
1. A biological attack is the release of germs or other biological substances. Many agents must be inhaled, enter through a cut in the skin or be eaten to make you sick. Some biological agents can cause contagious diseases, others do not.
2. A biological attack may or may not be immediately obvious. While it is possible that you will see signs of a biological attack it is perhaps more likely that local health care workers will report a pattern of unusual illness.
3. You will probably learn of the danger through an emergency radio or TV broadcast.



4. If you become aware of an unusual or suspicious release of an unknown substance nearby, it doesn't hurt to protect yourself.
5. Get away from the substance as quickly as possible.
6. Cover your mouth and nose with layers of fabric that can filter the air but still allow breathing.



7. Wash with soap and water and contact authorities.

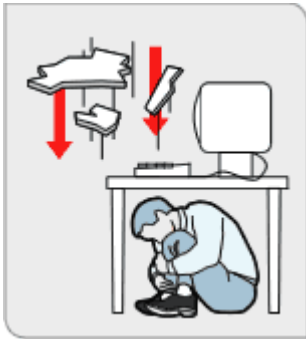


8. In the event of a biological attack, public health officials may not immediately be able to provide information on what you should do. However, you should watch TV, listen to the radio, or check the Internet for official news as it becomes available.

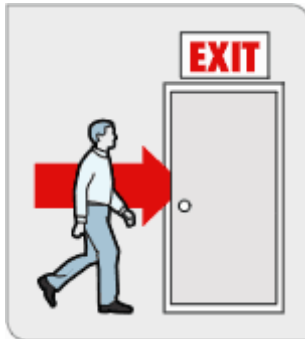


9. At the time of a declared biological emergency be suspicious, but do not automatically assume that any illness is the result of the attack. Symptoms of many common illnesses may overlap. Use common sense, practice good hygiene and cleanliness to avoid spreading germs, and seek medical advice.

## If there is an explosion...



1. Take shelter against your desk or a sturdy table.



2. Exit the building as quickly as possible.



3. Do not use elevators.



4. Check for fire and other hazards.



5. Take your emergency kit if time allows.





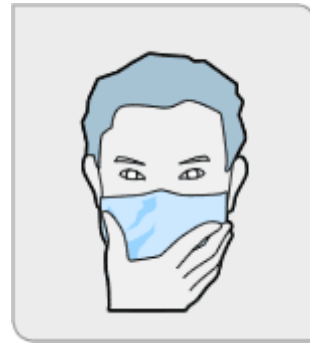
## If there is fire...



1. Exit the building as quickly as possible.



2. Crawl low in smoke.



3. Use a wet cloth to cover your nose and mouth.



4. Use the back of your hand to feel the lower, middle, and upper parts of closed doors.



5. If the door is not hot, brace yourself against the door and open it slowly.



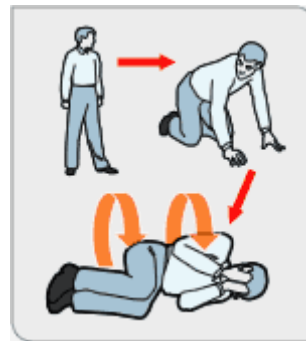
6. Do not open the door if it is hot. Look for another way out.



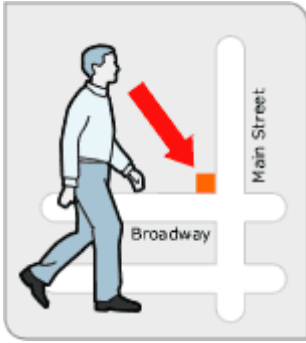
7. Use appropriate fire exits, not elevators.



8. If you catch fire, do not run!



9. Stop, Drop and Roll.



10. If you are at home, go to previously designated meeting place.



11. Account for your family members.



12. Do not go back into a burning building and carefully supervise small children.

**If there is fire...**

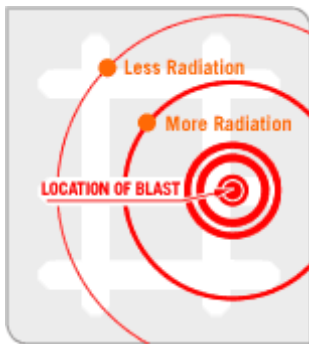


13. Call the fire department.

# Nuclear Blast



1. Take cover immediately, below ground if possible, though any shield or shelter will help protect you from the immediate effects of the blast and the pressure wave.
2. Consider if you can get out of the area;
3. Or if it would be better to go inside a building and follow your plan to "shelter-in-place".
4. In order to limit the amount of radiation you are exposed to, think about shielding, distance and time.



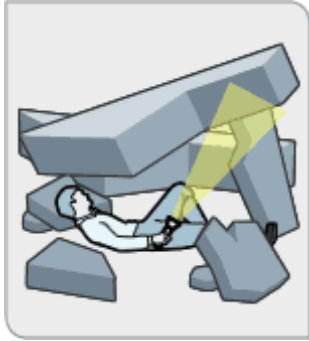
**Shielding:** If you have a thick shield between yourself and the radioactive materials more of the radiation will be absorbed, and you will be exposed to less.

**Distance:** The farther away from the blast and the fallout the lower your exposure.

**Time:** Minimize time spent exposed will also reduce your risk.



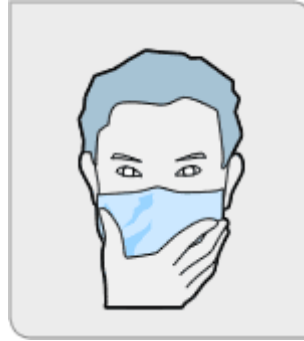
## If you are trapped in debris...



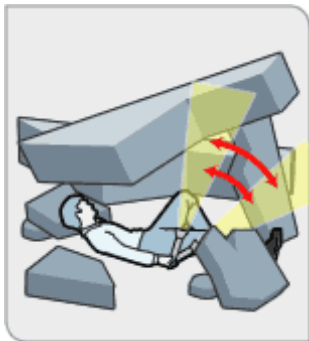
1. If possible, use a flashlight to signal your location.



2. Avoid unnecessary movement so that you don't kick up dust.



3. Cover your mouth and nose with anything you have on hand. Dense weave cotton material can create a good filter. Try to breathe through the material.



4. Tap on a pipe or wall so that rescuers can hear where you are.



5. Use a whistle if one is available. Shout only as a last resort - shouting can cause a person to inhale dangerous amounts of dust.



We welcome you to complete the assignment in Microsoft Word. You can easily find the assignment at [www.abctlc.com](http://www.abctlc.com).

Once complete, just simply fax or e-mail the answer key along with the registration page to us and allow two weeks for grading.

Once we grade it, we will e-mail a certificate of completion to you. Call us if you need any help. If you need your certificate back within 48 hours, you may be asked to pay a rush service fee of \$50.00.

You can download the assignment in Microsoft Word from TLC's website under the Assignment Page. [www.abctlc.com](http://www.abctlc.com)

You will have 90 days in order to successfully complete this assignment with a score of 70% or better.

If you need any assistance, please contact TLC's Student Services. Once you are finished, please mail, e-mail or fax your answer sheet along with your registration form.