Congressman Harold Ford, Jr.

THE MID-SOUTH ANTI-TERRORISM SUMMIT

Monday, October 15, 2001

9:30 a.m.

Shelby County Commission Chambers

160 N. Main Street

Table of Contents

HAROLD E. FORD, JR.
9TH DISTRICT, TENNESSEE

COMMITTEES:
EDUCATION
AND THE WORKFORCE
SUBCOMMITTEES:
EDUCATION REFORM
EMPLOYER-EMPLOYEE RELATIONS

FINANCIAL SERVICES
SUBCOMMITTEES:
CAPITAL MARKETS, INSURANCE, AND
GOVERNMENT-SPONSORED ENTERPRISES
FINANCIAL INSTITUTIONS AND
CONSUMER CREDIT

Congress of the United States
House of Representatives
Washington, DC 20515–4209

OFFICES:
325 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
TEL.: (202) 225–3265
FAX: (202) 225–5663

167 NORTH MAIN, SUITE 369
MEMPHIS, TN 38103
TEL.: (901) 544–4131
FAX: (901) 544–4329

WEBSITE:
www.house.gov/ford

October 15, 2001

Dear Participant:

Thank you for attending and participating in this important meeting.

In an introduction to a book examining the failure to anticipate the attack against Pearl Harbor, the distinguished academic Thomas Schelling observed that "the results at Pearl Harbor were sudden, concentrated and dramatic. The failure, however, was cumulative, widespread and rather drearily familiar. This is why surprise, when it happens to a government, cannot be described just in terms of started people. Whether at Pearl Harbor or the Berlin Wall, surprise is everything involved in a government's failure to anticipate effectively."

Now is not the time to place blame for the diabolical and coordinated events of September 11, 2001. Rather, in the spirit of Schelling's words, we can and must prepare ourselves to anticipate and respond to future terrorist acts. In doing so, even if one life is saved, the effort will be worthwhile. Terrorists, as the investigation of the attacks on New York and Washington have uncovered, operate in the shadows and are worldwide in scope, so the effort to detect and prevent future acts of terror is all the more challenging. But there are things we can do at home to protect our citizens.

President Bush and Government Sundquist made a good start by assigning cabinet level officials to head federal and state departments of homeland security. Here at home, the Memphis-Shelby County emergency Management Agency, hospital emergency response officials, law enforcement and our elected officials have undertaken the task of protecting our citizens.

Today's discussion will focus on opening the lines of communication between the critical players, answering questions, and assessing the needs of both the government and the private sector. By assembling the key leaders, we can take appropriate steps to empower local experts and allay the concerns of our citizens. Moreover, an open forum allows our leaders and citizens alike join in this effort with confidence.

I hope this summit is useful and I stand ready to work with you as we meet this new challenge.

Sincerely,

HAROLD FORD, JR.
Member of Congress

Congressman Harold Ford, Jr

Memphis-Shelby County Anti- Terrorism Summit

Monday, October 15, 2001

Shelby County Commission Chambers

Agenda:

8:30 - 9:00
Continental Breakfast

9:00 - 9:10
Welcome
Congressman Harold Ford, Jr.

9:10 - 9:30
Panel I - Overview of Local Planning

Mr. Phil Thomas, Agent in Charge, Federal Bureau of Investigation
Mr. Tim Viertel, Special Agent in Charge, U.S. Secret Service
Mr. Don Wright, Chief Deputy, Office of Shelby County Sheriff
Mr. Joe Lowery, Memphis-Shelby County Emergency Mgmt. Agency
Mr. Michael Lambert, Memphis Fire Department Emergency Response Coordinator
Col. John Mogen, Deputy Director, Tennessee Office of Homeland Security

9:30 - 10:00
Questions and Identification of Priorities

10:00 - 10:20

Panel II - Protecting our Transportation and Infrastructure Systems

Lt. Commander Mike Lopez, United States Coast Guard
Commander Bob O'Brien, United States Coast Guard, Marine Safety Office
Director Walter Crews, Memphis Police Department
Mr. Don McCrory, Executive Director, Memphis-Shelby County Port Commission
Mr. Tommy Jackson, Security and Facilities Manager, Memphis Light Gas & Water
Mr. Charlie Todd, Tennessee Valley Authority
Mr. Larry Cox, President, Memphis-Shelby County Airport Authority

10:20 - 10:40
Questions and Identification of Priorities

10:40 - 11:00

Panel III - Meeting the Public Health Challenge

Ms. Yvonne Madlock, Director, Shelby County Health Department
Dr. Bruce Steinhauer, President Regional Medical Center at Memphis
Mr. Michael Buckler, Safety Officer, Baptist Memorial Hospital
Dr. Joe Holly, Baptist East Hospital
Ms. Pam Harris, Methodist Healthcare
Mr. Charlie Franklin, UT Bowld Hospital
Ms. Linda Montarano, Delta Medical Center

11:00 - 11:30
Questions and Identification of Priorities

11:30
Wrap up and Call to Action
Congressman Harold Ford, Jr.

Bioterrorism briefings & FAQs from Centers for Disease Control, Chemical and Biological Weapons Nonproliferation Project and Center for Civilian Biological Weapons Non-proliferation Project.

Frequently Asked Questions
Bioterrorism Concerns after September 11

Since the terrorist attacks of September 11, public concern regarding a potential biological attack has heightened. The Johns Hopkins Center for Civilian Biodefense Studies received a steady stream of phone calls from the general public seeking more information about bioterrorism and ways to protect themselves. In response, the Center prepared the following "Frequently Asked Questions" (FAQ) fact sheet. Individuals may also want to contact their local health department and physician for additional information.

Should I buy a gas mask?

No. A mask would only protect you if you were wearing it at the exact moment a bioterrorist attack occurred. Unfortunately, a release of a biological agent is most likely to be done "covertly," that is, without anyone knowing it. That means you would not know ahead of time to put on your mask. To wear a mask continuously or "just in case" a bioterrorist attack occurs, is impractical, if not impossible.

To work effectively, masks must be specially fitted to the wearer, and wearers must be trained in their use. This is usually done for the military and for workers in industries and laboratories who face routine exposure to chemicals and germs on the job. Gas masks purchased at an Army surplus store or off the internet carry no guarantees that they will work. In fact, one national chain of surplus stores provides the following statement: *"(X) has been selling gas masks as a novelty item since 1948. We have never been able to warrant their effectiveness and we cannot do so at this time...We do not know what each type of gas mask we sell might or might not be effective against...We do not know the age of each gas mask..."*

In brief, no guarantees whatsoever are provided. More serious is the fact that the masks can be dangerous. There are reports of accidental suffocation when people have worn masks incorrectly, as happened to some Israeli civilians during the Persian Gulf War.

return to top

Should I have my own supply of antibiotics?

There are a number of different germs a bioterrorist might use to carry out an attack. Many antibiotics are effective for a variety of diseases, but there is no antibiotic that is effective against all diseases. Thus, no single pill can protect against all types of biological weapon attacks. Keeping a supply of antibiotics on hand poses other problems because the antibiotics have a limited "shelf life" before they lose their strength.

There is currently no justification for taking antibiotics. Also, it should be known that antibiotics can cause side effects. They should only be taken with medical supervision.

return to top

Is it safe for me to drink water from the tap?

It would be extremely difficult for a bioterrorist to contaminate our drinking water supplies to cause widespread illness. There are two reasons. First of all, huge amounts of water are pumped daily from our reservoirs, most of which is used for industrial and other purposes; very little is actually consumed. Thus, anything deliberately put into the water supply would be greatly diluted. Secondly, water treatment facilities routinely filter the water supply and add chlorine in order to kill harmful germs.

return to top

What is smallpox?

Smallpox is a disease caused by the *Variola* virus. Historically, 1 out of 3 people who contracted the disease died. The disease can spread from person to person. Transmission usually occurs only after the patient develops a fever and rash. Although there is no treatment for the disease, a vaccine against smallpox provides excellent protection and serves to stop the spread of the disease. While many vaccines must be given weeks or months before a person is exposed to infection, smallpox vaccine is different. It protects a person even when given 2 to 3 days after exposure to the disease and may prevent a fatal outcome even when given as late as 4 to 5 days after exposure.

Smallpox was stamped out globally by 1980 and vaccination stopped everywhere in the world. However, the Centers for Disease Control and Prevention (CDC) maintain an emergency supply of smallpox vaccine. Currently there are 12-15 million doses in storage, and a program to produce more vaccine began a year ago. For more information on smallpox, click here.

return to top

If smallpox is a potential threat to the U.S., why shouldn't we all get vaccinated?

The vaccine may cause serious side effects. In 1972, the U.S. decided to stop routinely vaccinating its citizens because many people were experiencing side effects, while they had almost no risk of getting smallpox. By 1972, the disease was present only in a few countries of Asia and Africa. Today, health authorities would only recommend vaccination if there was clear evidence that the disease had resurfaced and those in the U.S. were at risk of acquiring infection.

Many people over age 30 have a vaccination scar. Vaccination consists of introducing the virus into the top layers of the skin. Over the following few days, a blister forms at the site of vaccination (usually the upper arm). The arm is sore, and there is fever. Very rarely, some people get a vaccine-related infection of the brain (about 1 case per 300,000 vaccinations); one fourth of these cases are fatal. Other potential negative effects of the vaccine are a severe skin reaction, spread of the vaccine virus (known as *Vaccinia*) to other parts of the body, and spread of the *Vaccinia* virus to other people.

return to top

If I was vaccinated against smallpox before 1980, am I still protected?

Probably not. Vaccination has been shown to wear off in most people after 10 years but may last longer if the person has been successfully vaccinated on multiple occasions. If health authorities determine that you have been exposed to smallpox or are at risk of infection, they would recommend that you be re-vaccinated immediately.

return to top

What is anthrax?

Anthrax is a disease caused by bacteria called *Bacillus anthracis*. The form of the disease that health authorities are concerned that a bioterrorist attack might produce is inhalational anthrax. Inhalational anthrax occurs when a person breathes in anthrax spores. As early as a day or two after exposure or as late as seven weeks afterward, the spores begin to grow rapidly and the victim develops fever, has difficulty breathing and feels miserable. Death typically occurs within a few days after these symptoms if the person doesn't receive medical treatment. It is believed that antibiotics can stop the disease if they are taken at the time the anthrax spores begin to grow or very soon thereafter.

In the event of a bioterrorist attack, health authorities would conduct a rapid investigation, determine the place and time of the release, and identify individuals who need antibiotics. The federal government has stockpiled antibiotics for large-scale distribution in the event of a bioterrorist attack. For more information on anthrax, click here.

return to top

Is anthrax contagious?

No. Anthrax is not contagious. It does not spread from person to person. Healthy people who come into contact with persons sick with anthrax cannot acquire the disease.

return to top

What is the National Pharmaceutical Stockpile (NPS)?

The NPS is a large reserve of antibiotics, chemical antidotes and other medical supplies set aside for emergencies. The CDC reports that it has the capacity to move these stockpiled materials to affected areas in the U.S. within 12 hours of notification. There are a number of different stockpiles, strategically located around the country. In addition to the medical supplies already set aside, the federal government has made agreements with drug manufacturers to make large amounts of additional emergency medicine. For more information on the NPS, go to http://www.cdc.gov/nceh/nps/default.htm.

return to top

What can I do to protect myself and my family?

Unfortunately, there is presently little that individuals can do in advance to protect themselves from a bioterrorist attack. However, there is much that government agencies, health care institutions and public health departments can and should be doing to improve the capacity to protect the public following a bioterrorist attack. Medical institutions and public health agencies, in particular, have not received adequate attention and resources to cope with disasters like bioterrorism. For more information, click here.

You can express your concern regarding adequate protections against the potential threat of bioterrorism to your local leaders. In each area, local health departments have an important responsibility for helping protect your community against outbreaks of infectious disease, whether they occur in nature or because of a malicious terrorist act. They can assist you with additional bioterrorism-related concerns that are pertinent to your own community.

return to top

What if my fear about bioterrorism is having a serious impact on my family and work life?

Given the attacks upon civilians that took place on September 11, it is reasonable for citizens to feel anxious about their personal safety. Should your fear get to the point that it stops you from doing the things you would normally do in a day, it might be helpful to talk with someone. Your health care provider can make a referral if you do not already have someone in mind. In the wake of the attack on New York City, we have learned how helpful it has been to many New Yorkers to speak with a counselor or to go to a mental health center.

return to top

Anthrax

Frequently Asked Questions

What is anthrax?

Anthrax is an acute infectious disease caused by the spore-forming bacterium *Bacillus anthracis*. Anthrax most commonly occurs in wild and domestic lower vertebrates (cattle, sheep, goats, camels, antelopes, and other herbivores), but it can also occur in humans when they are exposed to infected animals or tissue from infected animals.

▲Top

Why has anthrax become a current issue?

Because anthrax is considered to be a potential agent for use in biological warfare, the Department of Defense (DoD) has begun mandatory vaccination of all active duty military personnel who might be involved in conflict.

How common is anthrax and who can get it?

Anthrax is most common in agricultural regions where it occurs in animals. These include South and Central America, Southern and Eastern Europe, Asia, Africa, the Caribbean, and the Middle East. When anthrax affects humans, it is usually due to an occupational exposure to infected animals or their products. Workers who are exposed to dead animals and animal products from other countries where anthrax is more common may become infected with *B. anthracis* (industrial anthrax). Anthrax in wild livestock has occurred in the United States.

▲Top

How is anthrax transmitted?

Anthrax infection can occur in three forms: cutaneous (skin), inhalation, and gastrointestinal. *B. anthracis* spores can live in the soil for many years, and humans can become infected with anthrax by handling products from infected animals or by inhaling anthrax spores from contaminated animal products. Anthrax can also be spread by eating undercooked meat from infected animals. It is rare to find infected animals in the United States.

▲Top

What are the symptoms of anthrax?

Symptoms of disease vary depending on how the disease was contracted, but symptoms usually occur within 7 days.

Cutaneous: Most (about 95%) anthrax infections occur when the bacterium enters a cut or abrasion on the skin, such as when handling contaminated wool, hides, leather or hair products (especially goat hair) of infected animals. Skin infection begins as a raised itchy bump that resembles an insect bite but within 1-2 days develops into a vesicle and then a painless ulcer, usually 1-3 cm in diameter, with a characteristic black necrotic (dying) area in the center. Lymph glands in the adjacent area may swell. About 20% of untreated cases of cutaneous anthrax will result in death. Deaths are rare with appropriate antimicrobial therapy.

Inhalation: Initial symptoms may resemble a common cold. After several days, the symptoms may progress to severe breathing problems and shock. Inhalation anthrax is usually fatal.

Intestinal: The intestinal disease form of anthrax may follow the consumption of contaminated meat and is characterized by an acute inflammation of the intestinal tract. Initial signs of nausea, loss of appetite, vomiting, fever are followed by abdominal pain, vomiting of blood, and severe diarrhea. Intestinal anthrax results in death in 25% to 60% of cases.

▲Top

Where is anthrax usually found?

Anthrax can be found globally. It is more common in developing countries or countries

without veterinary public health programs. Certain regions of the world (South and Central America, Southern and Eastern Europe, Asia, Africa, the Caribbean, and the Middle East) report more anthrax in animals than others.

Can anthrax be spread from person-to-person?

Direct person-to-person spread of anthrax is extremely unlikely to occur. Communicability is not a concern in managing or visiting with patients with inhalational anthrax.

▲Top

Is there a way to prevent infection?

In countries where anthrax is common and vaccination levels of animal herds are low, humans should avoid contact with livestock and animal products and avoid eating meat that has not been properly slaughtered and cooked. Also, an anthrax vaccine has been licensed for use in humans. The vaccine is reported to be 93% effective in protecting against anthrax.

What is the anthrax vaccine?

The anthrax vaccine is manufactured and distributed by BioPort, Corporation, Lansing, Michigan. The vaccine is a cell-free filtrate vaccine, which means it contains no dead or live bacteria in the preparation. The final product contains no more than 2.4 mg of aluminum hydroxide as adjuvant. Anthrax vaccines intended for animals should not be used in humans.

▲Top

Who should get vaccinated against anthrax?

The Advisory Committee on Immunization Practices has recommend anthrax vaccination for the following groups:

- Persons who work directly with the organism in the laboratory
- Persons who work with imported animal hides or furs in areas where standards are insufficient to prevent exposure to anthrax spores.
- Persons who handle potentially infected animal products in high-incidence areas. (Incidence is low in the United States, but veterinarians who travel to work in other countries where incidence is higher should consider being vaccinated.)
- Military personnel deployed to areas with high risk for exposure to the organism (as when it is used as a biological warfare weapon).

  The anthrax Vaccine Immunization Program in the U.S. Army Surgeon General's Office can be reached at 1-877-GETVACC (1-877-438-8222). http://www.anthrax.osd.mil

  Pregnant women should be vaccinated only if absolutely necessary.

▲Top

What is the protocol for anthrax vaccination?

The immunization consists of three subcutaneous injections given 2 weeks apart followed by three additional subcutaneous injections given at 6, 12, and 18 months. Annual booster injections of the vaccine are recommended thereafter.

Are there adverse reactions to the anthrax vaccine?

Mild local reactions occur in 30% of recipients and consist of slight tenderness and redness at the injection site. Severe local reactions are infrequent and consist of extensive swelling of the forearm in addition to the local reaction. Systemic reactions occur in fewer than 0.2% of recipients.

▲Top

How is anthrax diagnosed?

Anthrax is diagnosed by isolating *B. anthracis* from the blood, skin lesions, or respiratory secretions or by measuring specific antibodies in the blood of persons with suspected cases.

Is there a treatment for anthrax?

Doctors can prescribe effective antibiotics. To be effective, treatment should be initiated early. If left untreated, the disease can be fatal.

▲Top

Where can I get more information about the recent Department of Defense decision to require men and women in the Armed Services to be vaccinated against anthrax?

The Department of Defense recommends that servicemen and women contact their chain of command on questions about the vaccine and its distribution. The anthrax Vaccine Immunization Program in the U.S. Army Surgeon General's Office can be reached at 1-877-GETVACC (1-877-438-8222). http://www.anthrax.osd.mil

▲Top

Disease Listing | General Information | Technical Information | Additional Information

Accessibility | Privacy Policy Notice | FOIA

CDC Home | Search | Health Topics A-Z

This page last reviewed October 1, 2001

Centers for Disease Control and Prevention
National Center for Infectious Diseases
Division of Bacterial and Mycotic Diseases

THE HENRY L. STIMSON CENTER

Chemical and Biological Weapons Nonproliferation Project

Frequently Asked Questions: Personal Protection & Chemical or Biological Terrorism

Since the September 11th attacks on the World Trade Center and the Pentagon, the Stimson Center's Chemical and Biological Weapons Nonproliferation Project has received numerous inquiries from citizens and the media about how individuals could protect themselves in the event of a chemical or biological disaster. Such questions are understandable given concerns about subsequent attacks on US soil, so the project's director, Amy E. Smithson, Ph.D., answers below the most frequently asked questions. Her answers are based on extensive interviews with hazardous materials firefighters, physicians, public health officials, chemical and biological weapons experts, and others who have lengthy experience with chemical and biological defense precautions and who have dealt first-hand with chemical accidents and disease outbreaks. She wishes to underscore, however, that she is not a physician. A separate FAQ page titled *"Likelihood Terrorists Can Acquire & Use Chemical or Biological Weapons"* provides perspective on this highly unlikely possibility.

What are the signs that a poison gas attack (or a chemical accident) might be taking place?

One of the many unsettling characteristics of chemical agents is that some of them cannot be seen or smelled. Citizens can protect themselves by observing the following rule of thumb: If a single person is on the ground, choking or seizing, it is likely this individual is having a heart attack or some sort of seizure. However, if

several people are down, coughing, vomiting, or seizing, they could be reacting to the presence of a toxic substance. Evacuate the area immediately and dial 911, making sure to tell the dispatcher that a hazardous gas may be present.

- **Indoors:** If indoors, exit the building as rapidly as possible. Once outside, if you believe that you may have been exposed to the toxic substance, discarding your modesty and shedding your clothes could save your life. Taking off your outer clothing can remove roughly 80 percent of the contamination hazard. Look for a nearby fountain, pool, or other source of water so that you can quickly and thoroughly rinse any skin that may have been exposed (e.g., jump in the pool). Studies show that water alone is an effective decontaminant. Rescuers will arrive within minutes, and firefighters will hook up hoses and spray everyone to decontaminate them. Try to remain calm. Rescuers will triage everyone so that they can give medical attention to the most seriously affected individuals first. Even if you are showing no symptoms of exposure (e.g., eye problems), paramedics and physicians on scene will want to give you a check-up and advise you about follow-up care. Police officers will also want to speak with you about what you may have observed that could help them catch the individual(s) responsible.

- **Outdoors:** Birds and other small animals would very quickly be overcome by a poison gas, so if birds are dropping from the sky, that is another warning sign of toxic trouble. The most important thing to do is to get a physical barrier between you and the toxic cloud. Get indoors quickly--preferably into a building but even being inside a car will help. Shut all windows and doors and turn off the air conditioner. Try to plug any air drafts (e.g., under doors). This technique is known as sheltering in place. Call 911 and notify authorities that a hazardous gas may be present. If that is indeed the case, the wind will carry the toxic hazard away within a relatively short period of time. Stay indoors, and turn on the television and/or radio for news and announcements. Authorities will notify you when it is safe to go outside. If you are at home, put your clothes in a plastic bag and take a shower, which will help remove any contamination that might have occurred before you were able to get indoors.

What are the signs of a biological attack?

By now, the media has repeatedly broadcast that biological agents can be dispersed from commercial sprayers, such as crop dusters. Often omitted from these reports is the fact that, among other complications, commercial equipment would have to be modified for such an attack strategy to have a chance of success.

Still, crop dusters are out of place over cities, and the FBI has already placed restrictions about where they can fly. Were I to see one over a metropolitan area, I would immediately go indoors, shut all windows and doors, turn off the air conditioner, and notify authorities. The same would hold true for any other unusual spraying activities. For instance, a person tending a rooftop garden would not raise my suspicions, but an individual deliberately spraying a substance from a rooftop, or a truck dispersing a misty substance through side vents, would.

Keep in mind that occasionally local authorities employ helicopters and other means to spray approved pesticides to control mosquitoes and other pests. Officially sanctioned spraying activities are announced well in advance, repeatedly. A call to local authorities can confirm whether any spraying that you might observe would fall into that category.

What can citizens do to protect themselves from a possible biological disaster?

Frankly, it may not be apparent that a biological agent has been dispersed until people begin falling ill several days later. For most biological agents, the initial symptoms would resemble a flu-like malaise. Across the nation, local, state, and federal authorities are putting capabilities in place to improve the ability to detect abnormal public health problems rapidly---to distinguish between multiple cases of the flu or a possible biological agent attack.

As the normal cold and flu season rolls around in the next few months, please do not jump to the conclusion that you have been infected with a biowarfare agent if you begin to feel achy or have the sniffles. In fact, people catch colds throughout the year. You are more likely to get hit by lightning than to be the victim of a bioterrorist attack.

If, however, you hear reports that a biological agent may have just been released, stay indoors or get indoors right away, shut all windows and doors, and turn off the air conditioning system. The most worrisome method of biological agent dissemination is aerosol dispersal. For a biowarfare aerosol to make you ill, microscopic particles must find their way into your lungs. Therefore, putting a physical barrier in between you and a possible aerosol cloud is a key self-protection step.

Of course, a gas mask can provide respiratory protection. Alternately, a surgical mask or one of the respiratory protection masks recommended for various construction and laboratory tasks would help to screen out particulate matter that might be in the air, but these do not provide ironclad respiratory protection.. To protect your airway, masks need to be fitted snugly over the mouth and nose.

The Army Handbook on Medical Management of Biological Casualties recommends that medical personnel attending patients infected with most biowarfare agents employ what is known as "standard precautions." This term essentially means wearing a surgical mask and gloves. Standard precautions are effective against anthrax, brucellosis, Q fever, tularemia, viral encephalitis, botulinum toxin, and Staphylococcal enterotoxin b.

Should citizens stockpile antibiotics?

NO. Keeping a stockpile of antibiotics is, in short, a bad idea. While antibiotics would be used to treat individuals who might fall ill during a disease outbreak, the use of these medications should always be done at the direction of a physician. People who self-medicate themselves or their children could very well do more harm than good because adverse side effects may occur. Moreover, overuse of

antibiotics, as well as their misuse (to treat illnesses such as colds), is harmful as it reduces the ability of these drugs to work in serious health emergencies.

The US government keeps a cache of antibiotics and other medical supplies that can arrive in an area in which an outbreak has occurred within 12 hours.

What precautions can citizens take with their water supply?

Poisoning of a city's water supply is much more easily said than done. However, citizens can protect themselves by boiling their drinking water, which will kill any microorganisms that may have survived the municipal filtration systems. Another option is to use a personal water filtration system.

Where should citizens turn for instructions in the event of a chemical or biological disaster?

The electronic and print media can be very useful sources of information, especially when events are developing at a rapid pace. However, reporters can occasionally pass along faulty or inaccurate information. Local, state, and national public health, public safety, and emergency management officials would be the most reliable sources of information. As soon as the circumstances are understood, these officials will call press conferences to convey accurate information and instructions to the public. Subsequent press conferences will be called as frequently as possible to update the public about the steps that local, state, and federal government organizations are taking to address the situation and what individuals can do to help themselves and their fellow citizens. In a genuine disaster, the Emergency Broadcast System would also probably be employed to give instructions to citizens.

Should citizens buy gas masks?

The chances that terrorists will turn to poisonous substances instead of conventional bombs are very, very remote. Various news reports have noted that citizens are opting to purchase protective masks as a way to defend against chemical or biological terrorism. There are several important factors to bear in mind when considering this option.

In order for a mask to protect you against a *chemical* weapons attack, you would need to carry the mask with you at all times---24 hours a day, 7 days a week---and be prepared to put it on immediately if chemical emergency was suspected. To guard against a *biological* attack, you would need not only to carry the mask but also wear it at all times, since the presence of biological agents is not obvious without advanced sensors.

Gas masks capable of effectively protecting people from either chemical or biological agents are not a "one size fits all" purchase. At this point there are many different sizes and brands of masks available on the open market. It is critically important to make sure that the mask fits you properly---a loose gas mask defeats the purpose. Reputable dealers would be able to provide instructions not only on finding the right mask fit, but also on how to put it on, how to maintain it, and how

to take care of the filters the mask uses as a barrier against microscopic particles.

All that being said, if you would feel more comfortable purchasing a gas mask, by all means, go ahead. Steer clear of Internet auctions and classifieds. Make sure that the seller can answer your questions about fit and upkeep. For the record, I personally do not carry a gas mask with me. I take the subway to and from work daily, and I continue to go to meetings and other events in large buildings.

Note also that the only nation that has issued gas masks to all of its citizens in recent history is the state of Israel during the Gulf War. During the Gulf War, more Israelis died attempting to put on their gas masks than from Scud missile attacks.

 The Chemical and Biological Weapons Nonproliferation Project

| Home | About Us | What's New | Search | Publications | Projects |

Airport Security - Congressional Research Service

Airport Security

Robert S. Kirk

Issue Definition

The September 11, 2001, hijacking of four airliners from three different airports and the enormous loss of life that resulted from terrorist attacks using those aircraft as weapons has focused concerns in Congress about airport security in the United States. The interest is not new. In recent years, Congress has held hearings, ordered studies, appropriated funds, and passed airport security legislation. The overarching issue is the degree of federal involvement needed both to make commercial air travel safer and to restore the public's confidence in the security of our nation's airway and airports. (See page on Aviation Security Technology in this briefing book.)

Current Situation

The FAA responded to the terrorist attacks by grounding all commercial aircraft and ordering stepped-up security measures at airports, including: requiring a thorough search and security check of all airplanes and airports before passengers are allowed to board; forbidding curbside check-in (now restored at many airports); discontinuing off-airport check-in; declaring boarding areas off limits to all but ticket-carrying passengers; closer monitoring of vehicles near airport terminals; and imposing a total ban on knives, including plastic knives typically used in fast food restaurants (regulations had allowed knives under four inches, such as the knives reportedly used in the September 11 hijacking). At this writing, all major U.S. airports have reopened after meeting the more stringent new FAA security requirements.

Policy Analysis

Airport security antiterrorist efforts are generally directed toward preventing penetration by terrorists who pose as passengers, infiltrate as employees, or slip into restricted zones at an airport to plant explosives or hijack an aircraft. To counter these efforts, airlines screen passengers and baggage. Airports and airlines require employee background checks. They have also tightened secure area access requirements. During the past two years, however, General Accounting Office (GAO) and Department of Transportation (DOT) Inspector General (IG) investigations have criticized security measures at major airports. In its report, *Long-Standing Problems Impair Airport Screeners' Performance (GAO/RCED-00-75; June 28, 2000),* GAO found that screeners' performance in detecting dangerous objects was not satisfactory. It blamed rapid employee turnover (mostly because of low wages), insufficient training, and inadequate monitoring of screeners. The DOT IG's March 23, 2001, *Aviation Security* memorandum to the FAA administrator stated that baggage screeners were screening fewer bags per day than the recently installed explosive detection systems could screen per hour. The IG also found that airport operators and airlines frequently were not complying with the background check requirements for employees with access to secure areas of their airports. IG personnel were also able to access secure areas without being challenged 68% of the time. The IG argued that employees must be held accountable for compliance with airport access control requirements. The IG found that, while the FAA had made significant progress in

deploying existing advanced security technologies, it had failed to integrate the various security assets into a seamless security system.

Airport Security Improvement Act of 2000 (P.L. 106-528). The Act included a number of changes that would implement some of the GAO and IG recommendations. By November 22, 2002, the FAA and Federal Bureau of Investigation (FBI) are to expand the electronic fingerprint transmission pilot project (for criminal history background checks of prospective employees) to an industry-wide program. Any airport, airline, or screening company may, however, opt out of the electronic fingerprint program if they feel the program would not be cost effective. Screener training standards were expanded. Improvement standards and sanctions were also set forth for secure area access control. The final rule for the implementing regulations of this Act has not been published.

Airport Security Regulations: Final Rule, Airport Security and Airport Operator Security; Final Rule (Federal Register v. 66, July 17, 2001). These rules are an update of 14 CFR parts 107, 108, 139. They reflect the security mandates of the Federal Aviation Reauthorization Act of 1996 (P.L. 104-264) and are also an implementation of some of the recommendations of the White House Commission on Aviation Safety and Security, chaired by then-Vice President Gore. The notice to revise parts 107 and 108 was published August 1, 1997. The effective date of the final rules is November 14, 2001--over four years after the first notice.

Options and Implications for U.S. Policy

This history of less-than-satisfactory investigative reports on airport security and long delays in implementation of regulatory improvements, combined with the impact of the September 11 attack, have led to a near consensus for an increased federal role in airport security. However, there are significant differences of opinion on the appropriate form and depth of federal involvement.

Federalizing Airport Security Operations and Employees . For most proponents, federalizing airport security simply means making airport security a federal law enforcement and national security function. Federal agents would be hired to screen passengers and baggage and, in some proposals, would also patrol the secure and public areas of airports. FAA estimates that this would require 28,000 full time equivalent employees at a cost of roughly $1.8 billion. This federalizing option has the advantage of conceptual simplicity, and, according to proponents, is the best way to restore public confidence in U.S. airport security. Critics warn that this option will create a bureaucracy that could become as ineffective as the current system and at a much higher cost.

Not-For-Profit Organization. Another option would be to establish a not-for-profit corporation that would provide security services under FAA oversight. Proponents of this option argue that this would avoid expanding the federal bureaucracy and would also be more likely to be managed efficiently. Critics argue that, after the September 11 attacks, the public expects a stronger federal involvement. They also assert that there is no guarantee that a not-for-profit entity will be any better managed than a federal agency.

Strengthening and Enforcing the Regulation of Airport Security. Under this option (which most closely matches the Bush Administration's proposal) the federal presence and oversight would increase, but private companies would continue to provide front-line security employees. They would, however, work under stricter background checks, training, and

federal supervision. This is seen as less expensive and would also give federal security managers more freedom to hire and fire based on merit and performance than they could if employees were protected by U.S. civil service law. Opponents of this solution generally argue that profit-driven contract airport security services have performed poorly over many years and it is doubtful that they will ever achieve the level of security that could be provided by using federal agents.

Role of Congress/Legislation

Funding Airport Security. Congress responded quickly to the September 11 attacks by passing the 2001 Emergency Supplemental Appropriations Act for Recovery and Response to Terrorist Attacks on the United States (P.L. 107-38). The Act provides $40 billion to pay the costs of a variety of responses, including "providing increased transportation security." The Administration has set aside $3 billion for aviation security from this source.

Legislative Action. At this writing, the only bill that has seen legislative action, on the floor of either chamber, is the Aviation Security Act of 2001, S. 1447, introduced by Senator Hollings. After multiple amendments, the Senate passed the bill by a 100-0 vote on October 11, 2001. The bill would federalize aviation security. S. 1447 shifts the authority for the law enforcement aspects of aviation security from the Department of Transportation (DOT) to the Department of Justice (DOJ). Front-line screening of passengers and baggage would be carried out by federal DOJ employees. The bill also shifts the Federal Air Marshal Program to DOJ and allows DOJ the option of placing marshals on all flights. The costs of the program would be supported by charging the airlines $2.50 per boarding passenger. Leadership in the House has expressed opposition to hiring federal employees in the place of contractor personnel for the screening of passengers and baggage.

CRS Products

CRS Report RL31151(pdf). *Aviation Security: Screening Passengers and Baggage.*

CRS Report RL31150(pdf). *Selected Aviation Security Legislation in the Aftermath of the September 11 Attack.*

CRS Contact: Robert Kirk 7-7769.

Page last updated October 12, 2001.

Return to CRS Briefing Books. | Return to CRS Terrorism Briefing Book.

Electric utility infrastructure protection
Congressional Research Service

Electric Utility Infrastructure

Amy Abel and Mark Holt

Issue Definition

The electric utility industry operates as a integrated system of generation, transmission, and distribution facilities. Each of these components has vulnerabilities to attacks. These include physical attacks, as well as attacks on computer systems, or cyber attacks. Physical attacks could include destruction of transmission towers and substations, control centers, powerplants, or fuel delivery systems. Cyber attacks could include attempts to interrupt power plant and transmission system operations. The current electric power system in the United States consists of over 9,200 electric generating units connected to over 300,000 miles of transmission lines. 154,503 miles of transmission lines are rated at 230 kilovolts or higher. In addition, there are approximately 150 control centers that control the flow of electricity through the system under normal operating conditions.

The Current Situation

In 1996, the President's Commission on Critical Infrastructure Protection was created to address concerns relating to the vulnerability of critical national infrastructures. In response to the Commission's report, President Clinton signed Presidential Decision Directive 63 (PDD - 63) that outlines a series of actions designed to defend critical infrastructures from various threats. Based on the directive, the Office of Critical Infrastructure Protection in the Department of Energy (DOE) is the lead agency for the energy industry to coordinate responses to energy emergencies, but it has limited authority in the infrastructure assurance area. The North American Electric Reliability Council (NERC) has assumed coordination responsibilities for the private electric utility sector. As sector coordinator, NERC functions include assessing sector vulnerabilities and developing a plan to reduce system vulnerabilities; proposing a system for identifying and averting attacks; and developing a plan to alert, contain, and deflect an attack in progress and then to reconstitute minimum essential capabilities in the aftermath of the attack. (See NERC document: An Approach to Action for the Electricity Sector, at [ftp://www.nerc.com/pub/sys/all_updl/cip/ApproachforAction_June2001.pdf]).

The President's Commission on Critical Infrastructure Protection issued a report in October 1997 that described electric power vulnerabilities. The Commission report stated that:

> Of particular concern are the bulk power grid (consisting of generating stations, transmission lines with voltages of 100 kV or higher, plus 150 control centers and associated substations) and the distribution portion of those electric power systems where interruption could lead to a major metropolitan outage....

Most significant physical vulnerabilities appear to be related to substations, although certain generation facilities and transmission lines are also inviting targets. There is general agreement that, since the industry designs its systems for stability during single and some double failures, a coordinated attack on multiple targets would be necessary to cause a significant disruption of service. Furthermore, such an attack would need to hit multiple targets simultaneously or in

rapid sequence.

Because of the complexity of the grid, attackers would have difficulty replicating cascading outages such as the two Western power outages of July and August 1996.

Generation. Technological innovations in the past 20 years have changed the nature of new electric generating units. Beginning in the 1980s, gas-fired combined cycle technology began replacing large central station powerplants for capacity additions. More recently, generating technologies that are not reliant on the transmission grid, generally called distributed generation (DG), have emerged. Total installed capacity in 1999, not including backup power, was 845,168 megawatts. The Gas Technology Institute (GTI) estimates that, in 1998, installed DG capacity was 28,000 megawatts (Mw), of which 18,000 represents backup power applications. GTI estimates that installed DG capacity will increase to 75,000 Mw by 2015.

However, the majority of electric generating units still depend on the transmission and distribution system to deliver electricity to their ultimate consumers. Under most circumstances, destruction of one powerplant would not result in degradation of service. In normal operations, it is fairly common for a powerplant to unexpectedly go off-line for a variety of reasons. However, in situations where systems are operating with very little reserve margin, strategically and simultaneously eliminating the ability of several powerplants to generate electricity could result in widespread blackouts.

Nuclear Power Plant Security. At the recommendation of the Nuclear Regulatory Commission (NRC), all U.S. nuclear power plants went to the highest level of security following the September 11 terrorist attacks. Details of nuclear plant security measures are classified, but they generally involve multiple perimeter controls, internal controls on personnel movement through key reactor buildings, and armed security forces. The terrorist attacks have also prompted NRC to review the adequacy of its nuclear plant security requirements.

NRC requires nuclear plants to conduct "force on force" exercises every eight years to test the ability of their security systems to repel terrorist attacks. These tests, conducted under the Operational Safeguards Response Evaluation (OSRE) program, may be replaced by the industry-initiated Safeguards Performance Assessment (SPA) program, which is scheduled to soon begin a one-year pilot period. The industry SPA program involves more frequent tests than OSRE-every three years-but concerns have been raised about the adequacy of the SPA tests and of NRC's oversight.

Nuclear plant security systems are aimed primarily at preventing intruders from damaging crucial reactor safety systems or gaining access to a plant's reactor control room. If reactor cooling systems were destroyed or otherwise disabled, a reactor's highly radioactive nuclear fuel could overheat and escape into the atmosphere. Even after a reactor's nuclear chain reaction is halted through the insertion of control rods, the reactor core must be actively cooled to prevent radioactive decay heat from causing a catastrophic meltdown, as nearly occurred at the Three Mile Island plant in 1979.

The methods used in the recent attacks on the Pentagon and the World Trade Center have raised concerns about the potential effects of airliner crashes at nuclear power plants. Nuclear reactors are surrounded by thick containment structures made of pre-stressed concrete and steel. However, the containment structures are designed to prevent the release of radioactive materials during a core-melt accident, rather than to protect the reactor from airplanes and

other airborne projectiles. If an airplane penetrated the reactor containment and damaged the reactor core cooling systems, either through direct impact or by a resulting fire, a meltdown could occur.

At the International Atomic Energy Agency (IAEA) general conference that convened September 17, a number of conflicting statements were issued about the ability of reactor containments to protect against airplane crashes. Nuclear reactors in the United States and around the world use a wide variety of containment designs, some of which are likely to be more resistant to airplane crashes than others, although none are believed to be invulnerable. IAEA spokesman David Kyd was quoted in news reports as saying about nuclear power plants, "If you postulate the risk of a jumbo jet full of fuel, it's clear their design wasn't conceived to withstand such an impact." NRC released a fact sheet at http://www.nrc.gov/OPA/gmo/tip/fssecurity.html September 21, 2001, stating that the agency's regulations "did not specifically contemplate attacks by aircraft such as Boeing 757s and 767s and nuclear power plants were not designed to withstand such crashes. Detailed engineering analyses of a large airliner crash have not yet been performed."

The Nuclear Control Institute and the Committee to Bridge the Gap issued a statement September 25, 2001, criticizing NRC security requirements as inadequate in light of the recent terrorist attacks. Among the groups' recommendations were that National Guard troops equipped with anti-aircraft weapons be deployed at nuclear power plants and that new background investigations be carried out on all nuclear plant workers to ensure that no terrorists had penetrated the workforce.

An NRC fact sheet (http://www.nrc.gov/OPA/gmo/tip/fssecurity.html) on current nuclear power plant security requirements notes that physical barriers, security procedures, and a well-trained security force must be fully integrated to provide adequate plant security. Specific nuclear reactor security regulations are found at 10 CFR Part 73.

Transmission. The components of the electric transmission and distribution system include switchyards, transmission lines, substations, and distribution lines. The switchyard receives electricity from the generating plant and transforms the electricity to be compatible with the transmission lines. Transmission lines are sets of conductors insulated from each other and the towers that support them. Conductors are generally wires or cables suitable for carrying an electric current. Substations receive electricity from high-voltage transmission lines and reduce the voltage for use on the distribution system. The distribution lines carry electricity to the ultimate consumers.

Widespread electric outages could result from a coordinated attack on the transmission infrastructure. Simultaneously demolishing high-voltage transmission towers in geographically select areas, or more simply shooting out insulators on many transmission towers across a dispersed geographic region, could result in widespread outages by eliminating built-in transmission redundancies. Destruction of substations would cause a more localized power outage. However, because few redundancies exist in the distribution system, substation sabotage could create longer-term blackouts than attacks on the bulk power system.

Control Centers and Cyber Security. Because electricity cannot be economically stored in large quantities, control of the flow of power from generation to the customer on a real-time basis is essential. In the United States, there are about 150 control centers that manage the flow of energy in the nation's bulk power supply system (generation and transmission). The power system control centers provide remote monitoring and control of all the major power system

elements, including powerplants and transmission lines, within a particular control area. Control center dispatchers monitor and control all of the generation and transmission facilities within their system in order to control the flow of electricity within the system and the interconnections to adjacent control areas.

Actual control is carried out by supervisory control and data acquisition (SCADA) systems whose job is to execute schedules to facilitate electricity purchases, and to ensure that power levels and voltages are within acceptable limits. These SCADA systems are linked to the control centers and, therefore, to outside telecommunications systems. Moreover, the growth of deregulated electricity markets has resulted in the expansion of electronic networks over which electricity is bought and sold. As a result, the electric utility industry is becoming increasingly vulnerable to attacks on computer systems. Such attacks could result in widespread disruption of the nation's electricity supply. Any disruption, however, while serious, could probably be accommodated in a reasonable amount of time. Much of the planning that went into ways to deal with potential Y2K problems would likely serve to address attacks on the computer systems controlling computer operations. Nevertheless, any disruption could cause substantial economic and public safety problems, and additional efforts appear to be required to enhance system security.

Control centers are also vulnerable to physical damage and intrusion. Loss of the control center does not halt the flow of electricity, but makes control of the power system virtually impossible. If a control center is damaged, manual controls must be employed or, where backup control centers are available, they must be manned and placed in service.

Policy Analysis

The interdependency of the electric utility sector with other industries underscores the importance of a reliable system. For example, power outages affect virtually every mode of transportation, and, conversely, the electric system infrastructure depends strongly on the fuel delivery and storage infrastructure and on the transportation infrastructure (see Surface Transportation). There are three ways to address potential attacks on the electric sector and limit the impact of such attacks: (1) prevent damage; (2) limit consequences, and (3) speed recovery. Several policy questions emerge from these approaches.

United States has been moving to a more competitive electric power industry, both in the wholesale and retail sectors. Market transparency has been a goal in the shift towards a competitive market. As a result, more operating information is publicly available. It is very easy to obtain real-time information on the Web that includes which powerplants are operating, power demands, power supplies, and prices. A saboteur could use this information to plan physical and cyber attacks on critical electric utility industry infrastructure. To prevent potential attacks, one issue is whether operating information should be available to the public.

NERC's recent report ([ftp://www.nerc.com/pub/sys/all_updl/cip/ApproachforAction_June2001.pdf]) details an approach for utilities to deal with threats to the reliability of electricity and to recover quickly from any attack. However, utility compliance with any of the proposals is voluntary. If critical infrastructure protection standards (both improving physical security and preventing cyber attacks) are included as a role for proposed Electric Reliability Organizations(EROs), compliance would be enforceable. Current legislation that would mandate utility participation in an ERO with Federal Energy Regulatory Commission (FERC) enforcement jurisdiction include H.R. 312, H.R. 2814, S. 172, S. 388, and S. 597. If compliance with NERC proposals

becomes mandatory, one issue for Congress is whether utilities would need financial assistance from the federal government to pay for implementation.

Redundancy in the system, both from generation reserves and alternative transmission paths and systems, is one way to recover from and prevent outages. In addition, utilities routinely loan equipment and crews to help restore other utilities' power after an emergency.

However, utilities generally maintain spare parts inventories only as needed to permit maintenance and replace failed components. Stockpiling of critical equipment has been identified as one method to speed recovery from an attack. The Defense Production Act permits the government to requisition equipment needed in case of a threat to the national security. However, there is no general power to intervene in a major economic emergency that has no national security or defense implications. (See, Office of Technology Assessment, *Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage,* OTA-E-453, June 1990.) At issue is whether a more coordinated stockpiling of critical parts is necessary and whether legislation may be needed to amend existing law to mandate participation by private utilities.

For nuclear power plant security, the high degree of planning and organization demonstrated in the attacks on the Pentagon and World Trade Center may prompt NRC to reexamine its assumptions about potential terrorist attacks on nuclear power plants. Such a review could consider the likely consequences of a direct airliner crash on a nuclear power plant, whether crucial plant cooling systems could be adequately protected from such an attack, and whether the NRC should require reactors to be retrofitted with such protections.

Role of Congress/Legislation

A bill to tighten security at commercial nuclear power plants was approved by the House Energy and Commerce Committee October 3, 2001. The amended Committee Print, which has yet to be introduced, would give arrest authority to reactor security personnel, provide criminal penalties for sabotage, and require NRC to revise its reactor security regulations to account for increased threats. In particular, the revised NRC regulations would have to consider the terrorist attacks on the World Trade Center and the Pentagon, the potential for attacks by multiple teams of at least 20 intruders, the use of modern explosive devices and other powerful weaponry, attacks by plant employees, long-duration fires, and other severe threats. All shipments of highly radioactive spent nuclear fuel would require armed escorts "capable of repelling attacks by a large number of attackers working as several coordinated teams and using sophisticated techniques and equipment."

CRS Products

CRS Briefing Book: Electric Utility Restructuring.

CRS Issue Brief IB10006. *Electricity: The Road Toward Restructuring.*

CRS Briefing Book: Terrorism. Nuclear Power Plant Emergency Response, by Mark Holt.

CRS Contact: Amy Abel (7-7239)

Page last updated October 9, 2001.

Water supply infrastructure protection
Congressional Research Service

Water Supply Infrastructure

Claudia Copeland and Betsy Cody

Issue Definition

The nation's water supply and water quality infrastructure have long been recognized as being potentially vulnerable to terrorist attacks of various types, including physical disruption, bioterrorism/chemical contamination, and cyber attack. Interest in such problems has increased since the September 11, 2001 attacks on the World Trade Center and the Pentagon. Damage or destruction to these systems by terrorist attack could disrupt the delivery of vital human services, threatening public health and the environment, or possibly causing loss of life.

Current Situation

Water infrastructure systems include surface and ground water sources of untreated water for municipal, industrial, agricultural, and consumer needs; dams, reservoirs, aqueducts, and pipes that contain and transport raw water; treatment facilities that remove contaminants; finished water reservoirs; systems that distribute water to users; and wastewater collection and treatment facilities. Across the country, these systems comprise more than 75,000 dams and reservoirs, thousands of miles of pipes and aqueducts, 55,000 community drinking water facilities, and about 16,000 publicly owned wastewater treatment facilities. Ownership and management are both public and private; the federal government has responsibility for hundreds of dams and diversion structures, but the vast majority of the nation's water infrastructure is either privately owned or owned by non-federal units of government.

The federal government has built hundreds of water projects over the years, primarily dams and reservoirs for irrigation development and flood control, with municipal and industrial water use as an incidental, self-financed, project purpose. Because of the size and scope of many of these facilities, they are critically entwined with the nation's overall water supply, transportation, and electricity infrastructure. The largest federal water resource facilities were built and are managed by the Bureau of Reclamation (Bureau) of the Department of the Interior and the U.S. Army Corps of Engineers (Corps) of the Department of Defense. Bureau reservoirs, particularly those along the Colorado River, supply water to millions of people via Bureau and non-Bureau aqueducts. The Corps supplies water to thousands of cities, towns, and industries from lakes and reservoirs throughout the country.

A fairly small number of drinking water and wastewater utilities (about 15% of these systems) provide water services to more than 75% of the U.S. population. Arguably, these large systems, located primarily in urban areas, have the greatest vulnerability to terrorist attacks, while the large number of small systems that each serve fewer than 10,000 persons are less likely to be perceived as key targets by terrorists. However, smaller systems and utilities also tend to be less protected and, thus, are more vulnerable to attack, whether by vandals or terrorists.

Threats resulting in physical destruction to any of these systems could include disruption of operating or distribution system components, power or telecommunications systems,

electronic control systems, and actual damage to reservoirs and pumping stations. A loss of flow and pressure would cause problems for water customers and also would drastically hinder firefighting efforts. Bioterrorism or chemical threats could deliver massive contamination by small amounts of microbiological agents or toxic chemicals and could endanger the public health of thousands. (See the Chemical/Biological Terrorist Threat section of this briefing book.) Characteristics that are relevant to an agent's potential as a biological weapon include its stability in a drinking water system, virulence, culturability in the quantity required, and resistance to detection. Cyber attacks on computer operations can affect an entire infrastructure network, and hacking in water utility systems could result in theft or corruption of information or denial of service.

Federal dam operators went on "high-alert" after the September 11 terrorist attacks. The Bureau closed its visitor facilities at Grand Coulee, Hoover, and Glen Canyon dams. Because of their size, any breach could endanger lives and property downstream. Consequently, security threats are under constant review, and coordination efforts with both the National Guard and local law enforcement officials are ongoing. The Corps closed all its facilities to visitors after September 11, although locks and dams remained operational.

Utility operators also have been under heightened security conditions since September 11. Most utilities (especially in urban areas) have emergency preparedness plans addressing issues such as redundancy of operations, public notification, and coordination with state and local law enforcement and emergency response officials. However, many of these were developed to respond to natural disasters, domestic threats, such as vandalism, and, in some cases, cyber attacks. Thus, it is unclear whether existing plans and coordination mechanisms incorporate sufficient procedures to address serious terrorist threats. Utility officials are reluctant to disclose these plans, since doing so might alert terrorists to vulnerabilities.

Policy Analysis

Water supply was one of eight critical infrastructure systems identified in President Clinton's 1998 Presidential Decision Directive 63 (PDD-63) as part of a coordinated national effort to achieve the capability to protect the nation's critical infrastructure from intentional acts that would diminish them. (See the Critical Information Infrastructure section of this briefing book.) In the water supply sector, these efforts are focused primarily on the 330 large community water supply systems which each serve more than 100,000 persons. The Environmental Protection Agency (EPA) was identified as the lead federal agency. In 2000, EPA established a partnership with the American Metropolitan Water Association (AMWA) and American Water Works Association (AWWA) to undertake jointly measures to safeguard water supplies from terrorist acts. AWWA's Research Foundation has contracted for development of a physical vulnerability assessment tool for water systems. EPA received a $2.3 million appropriation in FY2001 and requested $1.8 million for FY2002 to support efforts which include developing a cyber vulnerability assessment tool and evaluating water system emergency operation plans. An Information Sharing and Analysis Center (ISAC) supported by an EPA grant has been established under AMWA's leadership to allow for dissemination of alerts about threats to water supply and wastewater systems. Information may include threats or vulnerabilities that have been detected and viable resolutions. It is expected to be operating in about six months.

Some federal research is underway in areas such as detection and treatment of chemical agents and evaluating threats from biological or chemical agents introduced into a water system. However, in the January 2001 report of the President's Commission on Critical Infrastructure

Protection, ongoing water sector research was characterized as a small effort that leaves a number of gaps and shortfalls. This report stated that gaps exist in four major areas.

- Threat/vulnerability risk assessments,
- Identification and characterization of biological and chemical agents,
- Establishing a center of excellence to support communities in conducting vulnerability and risk assessment, and
- Application of information assurance techniques to computerized systems used for operational data and control operations.

Less attention has been focused on protecting wastewater treatment facilities than drinking water systems, perhaps because destruction of these plants probably represents more of an environmental threat (i.e., by release of untreated sewage into the environment) than direct threats to life or public health and welfare. Vulnerabilities do exist, however. For example, destruction of chemical containers at wastewater or drinking water treatment plants could result in environmental release of toxic chemical agents, such as chlorine gas.

Federal officials have been reassessing federal infrastructure vulnerabilities for several years. The Bureau's "site security" program is aimed at ensuring protection of its 358 high- and significant-hazard dams and facilities and 58 hydroelectric plants. For FY2002, the Bush Administration requested $1.755 million for Bureau site security and $4 million for the Corps' national emergency preparedness program to assist civil governments in responding to all regional/national emergencies, including acts of terrorism, as well as assuring continuity of Corps operations.

Options and Implications for U.S. Policy

Policymakers may consider a number of options in this area, including enhanced physical security, communication and coordination, and research. A key question is whether protective measures should be focused on the largest systems and facilities, where risks to the public are greatest, or on all, since small facilities may be more vulnerable. A related question is responsibility for additional steps, because the federal government has direct control over only a limited portion of the water supply sector, while the majority are not federal. One possible option (especially for federal facilities such as dams and reservoirs maintained by the Bureau and the Corps) could be to restrict visitor access, including at adjacent recreational facilities, which could raise objections from the public. Another option is review of existing preparedness plans to ensure that they adequately address newer security concerns.

Policymakers also may examine measures to improve coordination and exchange of information on vulnerabilities, risks, threats, and responses. A number of research needs could be addressed, including tools for vulnerability and risk analysis, identification and response to biological/chemical agents, monitoring of current water supplies, and development of information technology. Finally, the costs of additional protections and how to pay for them are of interest, and policymakers may consider needed resources and how to direct them at public and private sector priorities.

Role of Congress/Legislation

Thus far, Congress has addressed issues of security concerning the nation's water infrastructure by appropriating funds to support existing programs of EPA, the federal water resource agencies, and others. Congressional oversight is anticipated, as well as legislation that could address the options discussed above and additional proposals which are likely to emerge. For example, legislation authorizing the Bureau to contract with local law enforcement officials and take other measures to protect dams and related facilities has been introduced (H.R. 2925/S. 1480). The House Committee on Resources ordered H.R. 2925 to be reported, amended, by unanimous consent on October 3.

CRS Products

CRS Report RS21026(pdf). *Terrorism and Security Issues Facing the Water Infrastructure Sector.*

CRS Contacts: Claudia Copeland (7-7227); Betsy Cody (7-7229)

Page last updated October 5, 2001.

Return to CRS Briefing Books. | Return to CRS Terrorism Briefing Book.

Food safety and agriculture protection
Congressional Research Service

Food Safety and Agriculture

Alex Segarra and Jean M. Rawson

Issue Definition

The terrorist attacks of September 11 have heightened security concerns about both the safety of our national food supply and the physical and biological integrity of the U.S. agricultural system. Recent outbreaks of foot-and-mouth disease (FMD) in the United Kingdom and findings of "mad cow" disease in Europe illustrate how even small disease outbreaks can have a severe economic effect, mainly by threatening consumer confidence, depressing agricultural production and disrupting trade (See CRS Report RS20890(pdf) and CRS Report RS20839(pdf)). These recent experiences also indicate that, should these or other agents be deliberately introduced into the United States, the cost of containment, eradication, and market loss could reach into the tens of billions of dollars. Now, the finding of two cases of deadly anthrax in Florida raises concerns about the physical security of pathogen culture collections held by the U.S. Department of Agriculture for research purposes.

Similarly, strong concerns exist about the potential for deliberate introduction of foodborne pathogens or toxic agents into the food chain. Widely publicized outbreaks of foodborne illness, such as *E. coli* O157:H7 in hamburger and *Salmonella* in poultry and eggs, or the presence of pesticides in California watermelons, remain fresh in the minds of many consumers because they have been responsible for loss of life, and have caused costly disruptions in food markets. There are also concerns about the disruption in food supplies if there are attacks against key transportation infrastructure installations, such as river locks, bridges or ports and their effect on agriculture. (See the Surface Transportation section of this electronic briefing book.)

Current Situation

While the national food supply and the physical integrity of the agricultural system in the United States were not directly affected by the September 11 attacks, there were ripple effects. Commodity markets in New York and Chicago closed for two days. As markets reopened, a short-lived spike in prices was observed in grains market futures, and some countries seemed to delay trading while seeking a better understanding of the new market conditions. (Slight increases in commodity prices also accompanied the 1993 attack on the World Trade Center, according to analysts). Other disruptions were caused by the shutdown of air traffic, which delayed shipments and deliveries and caused some losses of perishable products, and prevented such airborne production practices as crop dusting and cotton plant defoliation in preparation for harvesting. The Secretary of Agriculture has said that there was no impact on U.S. farm exports. A more precise estimate of the overall economic impact on U.S. agriculture of the September 11 attacks is not yet available.

Policy Analysis

U.S. programs to protect agricultural production and assure food safety are designed to deal

primarily with accidental, low probability events occurring within the parameters of a free and open market. A number of agencies of the Department of Agriculture (USDA) are charged with responsibilities in these areas. The Animal and Plant Health Inspection Service (APHIS) is responsible for protecting against the entry of foreign plant pests and animal diseases. The Food Safety and Inspection Service (FSIS) inspects the slaughter and processing of beef, veal, lamb, pork, goats, horses, and poultry, and is responsible for the safety of eggs used in liquid egg products and as an ingredient in processed foods. The Agricultural Research Service, USDA's in-house research agency, is responsible for supporting the regulatory missions of APHIS and FSIS with scientific information, and operates animal disease bio-containment laboratories in Plum Island, N.Y., and Ames, IA. These USDA agencies have significant connections with the Food and Drug Administration (FDA), which is responsible for the safety of all other foods besides meat and poultry, and the Environmental Protection Agency (EPA), which regulates pesticides used on foods.

Foreign Pests and Animal Diseases. APHIS, in cooperation with other state and federal agencies, is charged to protect against *accidental* introductions of plant pests and animal diseases through inspection of craft, cargo, and passengers at U.S. ports of entry. APHIS is also responsible for establishing quarantines, controlling the interstate commerce of regulated articles, and directing and coordinating eradication efforts with state and federal agencies inside areas of quarantine. While APHIS has, in the past, successfully kept out or intercepted many foreign pests and diseases flowing through commercial and trade channels, some concerns have been raised about its ability to respond to deliberate, and perhaps domestically initiated, introductions of disease agents or pests. These concerns were heightened recently by a report by the USDA's Office of the Inspector General (OIG) http://www.usda.gov/oig/auditrpt/50601-3-Ch.pdf stating that deficiencies in APHIS-FSIS coordination of meat cargo inspection procedures could increase the possibility of the introduction of foot-and-mouth and "mad cow" diseases.

In the aftermath of September 11, according to APHIS officials, the agency is increasing the inspection staff at U.S. ports of entry by 350 and is adding 20 veterinarians to imported and domestic disease surveillance and control programs. APHIS also is stepping up the agency's smuggling interdiction activities and making $1.5 million in grants available to states specifically to help them plan their response to potential foreign animal disease outbreaks.

Anthrax. The discovery of anthrax in Florida on October 4, 2001, raises concerns about its further use in possible bioterrorism attacks. One person has died and another has been exposed as a result of this incident. Anthrax, formerly known as 'woolsorters disease,' is caused by a soil bacteria associated with animal agriculture worldwide called *Bacillus anthracis*. In the United States, anthrax infections occur in domestic and wild animals and are most commonly reported in the Great Plains states from Texas to North Dakota. Anthrax also infects humans where the disease exhibits three forms: cutaneous, gastrointestinal, and the more deadly pulmonary or inhalation type.

Hundreds of cutaneous anthrax cases were reported in humans during the 20th century in the United States, but only 18 cases of inhalation anthrax were reported (roughly 5% of the cases), the most recent one occurring in 1976. The Florida victims are the first inhalation anthrax cases detected since 1976. Only one gastrointestinal case has been reported in the United States, found in Minnesota in July 2000. The last confirmed case of human anthrax reported in the United States before the Florida incident was a cutaneous case reported in Texas in July 2001. Historically, better farm and slaughter sanitation practices, as well as active state and federal disease surveillance programs, have reduced incidence of human anthrax from

approximately 130 cases annually in the early 1900s to zero cases between 1993 and 2000.

In the light of the events of September 11, USDA is increasing its efforts to secure Agricultural Research Service (ARS) pathogen culture collections used in disease diagnostic and treatment research. According to USDA officials, laboratory security has been increased at several facilities involved in research of animal pathogens such as foot-and-mouth disease and anthrax. Concerns about a lack of adequate physical and biological security and about deteriorating facilities have been raised since 1992, when an internal USDA review pointed at serious infrastructure problems. Earmarks for improvements of sensitive facilities totaled $16 million in FY2001.

Food Safety. FSIS inspects most meat, poultry, and processed egg products sold for human consumption, and is responsible for certifying that foreign meat and poultry plants that export to the United States are operating under an inspection system that is equivalent to the U.S. system. FSIS has 8,000 inspectors located at roughly 6,500 meat and poultry slaughtering and processing plants. In contrast, the Food and Drug Administration (FDA, an agency of the Department of Health and Human Services) responsible for the safety of all other domestic and imported foods, has 800 inspectors covering roughly 53,000 food establishments and U.S. ports of entry. It largely relies on food companies' self-interest in producing safe products. FDA inspects about 1% of all imported foods annually. Consumer groups and some policymakers have voiced concern over the discrepancies between FSIS and FDA inspection coverage for more than 20 years, and legislation has been introduced (but not passed) in nearly every recent Congress to reform food safety authorities and procedures to eliminate gaps in coverage. Recent events are likely to raise this as an important long-term policy issue. Meanwhile, each agency is making an effort to coordinate food safety enhancements in the aftermath of the terrorist attack.

Initial information from FSIS indicates that the agency is educating its inspection force to heighten awareness of pre- and post-mortem factors that could signal unusual problems. More specific information is available from FDA, whose activities are likely to be useful to FSIS as well. According to an FDA official, the agency is focusing its efforts on prevention and response. In the first category, FDA reportedly is contracting with a private firm to identify vulnerabilities in the farm-to-table food chain and is working with state and local food safety agencies to strengthen their existing food safety inspection programs. In the response category, according to the FDA official, the agency seeks to (1) improve its laboratories' abilities to diagnose infectious or toxic agents and rapidly share information; (2) improve its ability to detect counterfeit brand-name food labels on tampered products; (3) improve traceback mechanisms for bulk ingredients as well as for water and milk; and (4) determine how best to regulate the safety of food products while they are being transported.

Options and Implications for U.S. Policy

The current food safety and agricultural protection systems are not designed specifically to cope with terrorist actions, but observers generally assert that they could be strengthened or reconfigured to serve more defensive purposes. Contingency plans already exist at the federal and state levels to deal with limited outbreaks of foodborne or foreign animal/plant diseases in the United States. Most plans contain elements for the participation of multiple agencies, and in some cases cooperation from foreign governments, but there has been persistent criticism of poor coordination among agencies and insufficient government inspection and surveillance capabilities.

Role of Congress/Legislation

Responsibility for ensuring the safety of our national food supply, and for protecting the physical and biological integrity of the U.S. agricultural system remains scattered among dozens of federal, state and local agencies. Although the objective of achieving emergency coordination has been high in the agenda for many years, critics argue that the system still is far from seamless. Experience with foot and mouth and "mad cow" diseases in Europe has increased Congressional oversight actions designed to improve coordination and communications between agencies in tackling these or similar emergencies.

In July 2001, Congress passed the Animal Disease Risk Assessment, Prevention and Control Act of 2001 (P.L. 107-9), which requires USDA to develop a strategic action report on ways to coordinate and prevent animal and plant diseases from entering the United States. In addition, two bills have been introduced in the 107th Congress to strengthen criminal penalties for agroterrorism under the Racketeer Influenced and Corrupt Organizations (RICO)Act (H.R.2060), and to protect and promote the public safety and interstate commerce from certain violent, threatening, obstructive, and destructive conduct that is intended to injure, intimidate, or interfere with plant or animal enterprises (H.R. 2795).

CRS Contacts: Alex Segarra (7-9664), Jean Rawson (7-7283), and Donna Vogt (7-7285)

Page last updated October 10, 2001.

Return to CRS Briefing Books. | Return to CRS Terrorism Briefing Book.

Surface transportation systems protection
Congressional Research Service

Surface Transportation Systems

D. Randy Peterman, John Frittelli, and Paul Rothberg

Issue Definition

To those whose goals include killing or injuring people and disrupting life in a community, surface transportation systems, such as transit operations, railroads and yards, seaports, bridges and tunnels, and vehicles transporting hazardous materials, offer a tempting target. The events of September 11 show that threats are posed not only to passengers, but also by the use of vehicles as weapons. Depending upon the type of incident, thousands of people could be placed in danger. Also, because of the essential role that surface transportation systems play in the movement of goods as well as people, terrorist actions could threaten our economic well-being and national security. As these risks are considered, questions are being asked, such as: What efforts are underway or could be taken to reduce these vulnerabilities? In particular: What is the Department of Transportation (DOT) doing to reduce these risks? What other options might be considered?

Vulnerabilities and Current Responses

About one-third of terrorist attacks around the world reportedly target transportation. The majority of these attacks, and the cause of the greatest number of casualties, are against public transportation. This may be due to the comparative ease of access to public transportation facilities compared with the security measures taken in aviation. Securing public transportation from attack is difficult. Transit's effectiveness depends, in part, on passengers having easy access to it, and, in part, on operating over many routes on fixed schedules with frequent stops. Screening passengers ranges from impossible (for buses, which pick up people from makeshift stops along the road) to difficult (for fixed-rail systems, which pick up passengers from many stations with multiple points of street access).

Similarly, hundreds of thousands of miles of rail, highway, and oil and gas pipeline networks make these systems impossible to safeguard. Rail and highways (trucks) daily carry thousands of shipments of hazardous materials, which would pose an array of safety risks if these materials were released during transportation. Poisonous and flammable gases are two examples of materials that are of particular concern. Bridges and tunnels also are major points of vulnerability to attacks that might both take lives and disrupt these transportation networks.

Seaports are also vulnerable. Seaports are typically located in large urban areas; however, because of the efficient flow of intermodal cargo by rail and truck to the nation's interior, inland cities are also vulnerable components of the seaport system. Competition between ports means that moving large amounts of cargo rapidly and efficiently takes precedent over security matters. Reportedly, only 1-2% of sea containers arriving at the nation's seaports are inspected.

To address these vulnerabilities, numerous federal efforts are underway. DOT has asked the domestic transportation industry to remain at a heightened state of alert and to implement security measures commensurate with this level of security; the Federal Bureau of

Investigation has warned that representatives at industrial facilities, particularly those that manufacture, distribute, or transport or store hazardous materials, should be especially vigilant. DOT's Office of Intelligence and Security monitors threats to transportation. Senior managers of the Federal Highway Administration are meeting with state DOT officials to analyze vulnerable points in the highway infrastructure and what actions should be taken to reduce these risks. DOT's Research and Special Programs Administration (RSPA) conducts the "Transportation Infrastructure Assurance" research program, which is intended to assess possible countermeasures to security threats of the physical and information infrastructure of the transportation system. The FY2001 appropriation for this effort is $1 million, as is the FY2002 request. During the current fiscal year, RSPA is sponsoring studies to assess the interdependencies of critical operating elements of the transportation system, examining the dependencies of transportation systems on information and communication systems, and defining the transportation requirements of emergency teams that might respond to incidents involving weapons of mass destruction. The Federal Transit Administration has an Office of Safety and Security, which provides free security audits to help transit systems develop security plans and also publishes security-related materials. The Office of Pipeline Safety is concerned about the vulnerability of oil and gas pipelines to different types of releases, including those caused by sabotage. Monitoring systems and emergency response systems are integral components of pipeline safety.

Because of the difficulty of protecting transportation systems from attack, the focus of federal policy has been to improve the response to attacks. Several federal agencies, including the DOT, the Environmental Protection Agency, and the Federal Emergency Management Agency, provide assistance to strengthen state and local efforts in the areas of planning and training. Such efforts are also useful as preparation for accidents and natural disasters, as well as crime prevention.

Policy Options and Implications

A variety of different options, each with its own set of costs and benefits, could be employed to reduce vulnerabilities from terrorists attacks to surface transportation systems. At the simplest level, trash cans can be removed from subway stations to eliminate a potential hiding place for bombs (as London has done, resulting in a trash-filled subway system), and packages left unattended in public areas can be examined for weapons. Various technologies, e.g., video cameras, sensors, and tracking devices, can reduce the likelihood, but not prevent, terrorist attacks; these can raise issues of privacy as well as cost and effectiveness. Increased public awareness is another component of a systematic approach.

Terrorism is a low-probability, high-consequence event, making the need for extensive precautions uncertain; since most precautions are also expensive, this uncertainty usually results in minimal precautions being taken. Moreover, it is not clear what precautions can be taken that would be truly effective. Every conceivable precaution could potentially be defeated, and precautions that make one mode less vulnerable may simply shift the threat to more vulnerable targets.

Role of Congress/Legislation

Prior to September 11, bills had been introduced in the 107th Congress to address the security of surface transportation systems. H.R. 525, The Preparedness Against Domestic Terrorism Act of 2001, would, among other things, create a President's Council on Domestic Terrorism Preparedness charged with developing a Domestic Terrorism Preparedness Plan and

implementation strategy, including an assessment of the risks to transportation infrastructure and passengers and evaluation of the means of protecting them. The bill would provide $9 million in FY2002 to carry out its purposes. This bill may be affected by the President's creation of a new White House Office of Homeland Security, to be headed by Pennsylvania Governor Tom Ridge, to coordinate the federal government's strategy against terrorism. For its part, the House of Representatives has created a Select Subcommittee on Terrorism and Homeland Defense.

The Senate recommended $40 million for seaport security in the Department of Justice FY2002 Appropriations bill (S. 1215). The funds are directed towards enhancing the physical security of ports as well as new equipment for law enforcement agencies. This appears to be in response to a fall 2000 *Report of the Interagency Commission on Crime and Security in U.S. Seaports*, which found that the state of security in U.S. seaports generally ranges from poor to fair (although, in a few cases, it is good). S. 1214, The Port and Maritime Security Act of 2001, also addresses some of the inadequacies of seaport security identified by the report; it was reported by the Senate Commerce Committee on August 2, 2001. The bill authorizes $68 million for the U.S. Customs Service to purchase new x-ray screening equipment for cargo containers and $80 million for DOT to provide loan guarantees and grants to local port authorities for improved security infrastructure. The bill also sets baseline standards for port security measures and formalizes procedures for conducting vulnerability assessments. Port authorities, maritime unions, freight forwarders and custom house brokers have criticized this legislation for potentially adding costs and delays to operations.

Given the importance of emergency response, Congress has been interested in reviewing the DOT-administered Emergency Preparedness Grants Program, which provides funds, improved training, and technical assistance to enhance planning and emergency response to releases of hazardous materials. (In general, many of the same responders that would deal with a hazmat spill would also be involved in responding to terrorist attacks.) For FY2002, DOT is requesting the authority to award $5.0 million for planning grants and $7.8 million for training grants. As Congress considers the reauthorization of federal hazardous materials law, 49 U.S.C 5101 et. seq., it might be worthwhile to consider the funding base for this program and whether additional funds are needed. Many in industry, which now finances this grant program, would be reluctant to bear the sole burden of paying for increased grants.

CRS Contact: Transit - D. Randy Peterman (7-3267); Railroads and Seaports - John Frittelli, (7-7033); Highways and Pipelines - Paul Rothberg (7-7012)

Page last updated September 24, 2001.

Return to CRS Briefing Books. | Return to CRS Terrorism Briefing Book.

Chemical/Biological Terrorist Threat

Steve Bowman

Issue Definition

A number of factors have combined to make the possible terrorist use of chemical or biological weapons (CBW) in the United States a focus of attention. The Aum Shin Rikyo nerve agent attack in the Tokyo subway demonstrated the feasibility of terrorist use. The World Trade Center and Pentagon attacks have brought mass casualty terrorism to U.S. territory. And, though neither of the U.S. attacks involved chemical or biological weapons, many worry that these could be "the next step." Though there is no debate about the vulnerability of civilian populations to this type of attack, there is controversy about the likelihood of it occurring, and what can be done to deter and prepare.

Current Situation

It is necessary to distinguish between chemical and biological weapons. Chemical weapons are toxic or lethal chemicals used to disable or kill. There are several types: nerve agents disrupt the body's nervous system; choking agents inhibit respiration, blood agents reduce the oxygen in the blood; and vesicants create large blisters on any tissue they contact. They can be effective either through inhalation or, in some cases, contact with the skin. Effects are immediate, or in the case of vesicants, within hours. The Organization for the Prohibition of Chemical Weapons, which oversees the implementation of the Chemical Weapons Convention, provides extensive information on the characteristics of chemical weapons.

Biological agents are live organisms (e.g. bacteria, viruses) that cause fatal diseases such as anthrax, or that produce fatal toxins in the body such as botulinum. Biological agents, because of the minute amounts needed to infect and the possibility of contagion, are generally considered capable of creating far greater casualties than chemical agents. Those contaminated may show no symptoms for several days, and initial symptoms of many diseases are simply "flu-like", providing no distinctive characteristics, and thus making detection and treatment more difficult. Though generally the threat to humans is most often considered, chemical and biological weapons can be used against agriculture and livestock. The federal Center for Disease Control and Prevention has an extensive database on bioterrorism agents.

The U.S. intelligence community has not publically assessed any terrorist group as currently possessing chemical or biological weapons. However, the Director of the CIA has testified before the Senate Foreign Relations Committee that Osama bin Laden's associates are attempting to acquire these weapons and/or the capability to produce them. In addition, some nations that have been designated by the State Department as state sponsors of terrorism either have or are developing CBW capabilities. These include Iran, Iraq, Libya, North Korea, and Syria. The Oklahoma City bombing, although it did not employ CBW, demonstrated clearly that mass casualty terrorism may also be of domestic origin, and consequently the threat of CBW terrorism by domestic groups or individuals cannot be ruled out. However, no domestic CBW threat assessment has been undertaken. One reason for this is that while the intelligence community may collect intelligence freely abroad, there are significant legal constraints on the

collection of domestic intelligence.

Policy Analysis

There has been no terrorist use of chemical weapons since the Tokyo attack, and no terrorist use of biological weapons in modern times. This has led to the question of what factors have deterred or inhibited their use. A variety of factors have been suggested.

Chemical and biological weapons remain significantly more difficult to obtain or manufacture than conventional explosives. Characterizations of CBW as "relatively easy to produce" are generally made in comparison to nuclear weapons, not conventional weapons. The components of the Oklahoma City bomb were openly purchased and combined in a short period of time, and easily transported, constructed, and detonated by two men with limited resources. The Aum shin Rikyo, with trained scientists, laboratories and very large financial resources, after several years of work with both chemical and biological agents were able to mount only a relatively unsophisticated nerve agent attack that actually killed only 12 people, including at least one of the terrorists.

Chemical and biological weapons do not destroy infrastructure, and for many terrorists, physical destruction of a target (e.g the Murrah Federal Building) is an important symbolic element of the attack. CBW also have the disadvantages of being extremely dangerous to handle and transport. Given the extreme care with which they must be handled, the first potential casualties could be the terrorists themselves, even before an attack is attempted. CBW must be disseminated efficiently to effect mass casualties. Chemical agents are difficult to disperse efficiently, particularly in open air settings. Consequently, even though lethal in small doses, relatively large amounts (gallons) are needed to effect mass casualties. Biological agents require significantly smaller amounts (pounds), but still require efficient delivery methods, though with contagious agents (e.g. smallpox) this difficulty is greatly reduced. Explosive devices are generally unsuitable for effective CBW delivery because an explosion can burn or kill a significant portion of the agent.

Supply-side legal restrictions on the transfer and possession of certain chemical and biological agents may also have had a deterrent effect. Current federal law provides a range of prohibitions on CBW agents. Finally, a specific moral or psychological aversion to these weapons may have had a constraining effect.

There are strong concerns, however, that all these possible constraints on CBW terrorist use are rapidly eroding. Aum Shin Rikyo demonstrated that an independent terrorist group, without the resources of state sponsorship, can produce and employ these weapons. This indicates that technological barriers are not insurmountable. The number of nation states that are believed to have CBW programs, and to also sponsor terrorist activity, could also increase the probability of their use. The notoriety of CBW may also serve to encourage interest, as evidenced by the large increase in CBW hoaxes that have been reported in the media.

Some have argued that the use of chemical weapons in the Iran-Iraq War in the 1980's indicates that, for at least some, any moral taboo against these weapons has been erased, and that their use against a sufficiently hated enemy would be approved of by those sympathetic to the terrorists' movement. The strong psychological impact of CBW, and the immediate, intense, and large-scale attention their use engenders, could also be attractive to some terrorists.

Role of Congress/Legislation

Regardless of the probability assessment of their use, chemical and biological weapons carry such a strong psychological impact, and present the possibility of such large-scale casualties and disruption, that once the possibility of their use is raised, serious consideration must be given to deterrence, detection, protection, and remediation. For the last few years, the federal government has significantly increased its investment in CBW-defense related efforts, within both existing military programs and newly instituted programs to better protect the civilian population. According to the Office of Management and Budget, the FY2002 federal budget request under congressional consideration contains over $1.7 billion spread among 15 federal agencies and departments for primarily CBW-related programs. These programs are focused primarily on improved detection, protection, and decontamination equipment; medical training and diagnostic facilities; and improved pharmaceuticals and vaccines.

The General Accounting Office (GAO) has repeatedly emphasized the need for a "validated comprehensive threat assessment" which includes both foreign and domestic threats, and judges the CBW agents mostly likely to be used. Without this benchmark, GAO maintains, it is impossible to determine whether funds are being used wisely. GAO has also noted that no national standard for an acceptable level of preparedness has been established. Both of these issues could be addressed through congressional direction to the Executive Branch or establishment of a special commission.

Possible legislative vehicles include 1) H.R. 525, which seeks to create a President's Council on Domestic Terrorism Preparedness, and delineates its responsibilities and; or H.R. 1158, which seeks to create a homeland security agency, with extensive responsibilities over terrorism related programs. However, the President's recent announcement that he is creating a cabinet-level Office of Homeland Security may lead Congress to defer action on these bills for the immediate future.

CRS Products

CRS Report RL31059(pdf). *Biological Weapons: A Primer.*

CRS Issue Brief IB94029. *The Chemical Weapons Convention.* (updated regularly)

CRS Contact: Steve Bowman (7-7613)

Page last updated September 24, 2001.

Return to CRS Briefing Books. | Return to CRS Terrorism Briefing Book.

Emergency readiness kits and information
Emergency Management Agency

About the EMA

What is the LEPC?

Emergency Readiness Kits and Information

Planning for your Home and Family

Weather Survival Information

Earthquake Planning and Preparedness

Links

EMA HOME

EMERGENCY READINESS KITS and INFORMATION

An Emergency can occur at any time and anywhere. When it does you may not have much time to react. A highway spill of hazardous materials could mean instant evacuation. A winter storm could confine your family at home. An earthquake, flood or tornado could isolate you from basic services - gas, water, telephone, electricity - for days.

Your family will cope best by preparing for an emergency before it happens. One way to prepare is to assemble an **Emergency Readiness Kit**. Once an emergency event has occurred you will not have time to shop or search for supplies. If you gather your supplies and equipment in advance your family can endure an evacuation or in place sheltering.

Water

One or two gallons per person per day. Two quarts for drinking and two quarts for food preparation and sanitation.

In your home you can use the water stored in your hot water heater to supplement your supply as necessary.

Food

Ready to eat - canned meats, fruits, & vegetables
Canned juices - milk, soup
High Energy Foods - peanut butter, jelly, crackers, granola bars & trail mix
Specialty foods for - infants, elderly, persons on special diets
Comfort/stress foods - such as instant coffee, hard candy, sweetened cereals, lollipops and tea bags.

First Aid Kit

Your Emergency First Aid Kit Should Include:

- Adhesive bandages in assorted sizes (band aids)
- Triangular bandages (3)
- Moistened towelettes
- Petroleum jelly
- Latex gloves (2 pr.)
- Pain relief tablets such as aspirin or Tylenol (adult & child strength.
- Sterile gauze pad
- Roller bandages (3" wide)
- Antiseptic
- Assorted safety pins
- Sunscreen
- Antacids
- Adhesive tape (1" wide)
- Scissors, tweezers, needle
- Thermometer
- Assorted soaps
- Anti-diarrhea medication
- Laxatives

Specialty Items

Baby

-Formula/Powdered -Milk
-Bottles
-Diapers
-Ointment/Medicines

Adult

-Prescription medication
-Extra eye glasses or contacts
-Denture needs, etc

Misc

-Books, cards, games
-Important documents & telephone numbers

Tools & Supplies

- Paper plates, cups and plastic utensils
- Battery operated radio with extra batteries
- Flashlight with extra batteries
- Small amount of cash and/or traveler checks
- Non-electric can opener
- Utility Knife
- Small fire extinguisher (with ABC rating)
- Plastic storage containers
- Needle and thread
- Map of local area
- Pliers
- Hammer
- Adjustable wrench
- Duct tape
- Electricians tape
- Masking tape
- Matches in waterproof container
- Aluminum foil
- Plastic storage wrap
- Paper and pencils
- Plastic sheeting

Clothing & Bedding

- Sturdy shoes or boots
- Hat/gloves
- Rain gear
- Blankets/Sleeping bag
- Thermal underwear
- Sunglasses

Emergency Readiness Car Kit

- Battery Powered Radio w/extra batteries
- Blanket(s)
- Adjustable Wrench, Pliers & Hammer
- First Aid Kit w/manual
- Sturdy shoes/long Trousers
- Flashlight w/extra batteries
- Booster cables
- Fire Extinguisher w/ABC rating
- Bottled water/Nonperishable food
- Road flares/Help Sign