Oct. 10, 2001

Infrastructure Security

Committee Holding Hearing:

House Transportation and Infrastructure Committee - Subcommittee on Water Resources and Environment

CQ Abstract:

Water Resources and Environment Subcommittee (Chairman Duncan, R-Tenn.) of House Transportation and Infrastructure Committee held a hearing on infrastructure security.

Scheduled Witnesses:

Ronald Dick - director, National Infrastructure Protection Center, FBI; Michael Parker - assistant secretary of the Army for civil works; Glenn L. McCullough Jr. - chairman, Board of Directors, Tennessee Valley Authority; Robert Bostock - special assistant to the administrator for homeland security, Environmental Protection Agency; Beverly O'Neill - mayor, Long Beach, Calif.; Jeffrey J. Danneels - department manager, Security Systems and Technology Center, Sandia National Laboratories; John P. Sullivan Jr. - chief engineer, Boston Water and Sewer Commission and president, Association of Metropolitan Water Agencies; Patrick T. Karney - director, Metropolitan Sewer District of Greater Cincinnati, representing Association of Metropolitan Sewerage Agencies; Randy Speight - senior director, Regulatory Affairs, American Chemistry Council; Joanne Moreau - director, Office of Emergency Preparedness, East Baton Rouge Parish, La.

12102010211024

Testimony:

Jeffrey J. Danneels, department manager, Security Systems and Technology Center, Sandia National Laboratories

Statement of Jeffrey J. Danneels Department Manager, Security Systems and Technology Center Sandia National Laboratories

United States House of Representatives Committee on Transportation and Infrastructure

Subcommittee on Water Resources and the Environment "Terrorism: Are America's Water Resources and Environment at Risk?"

October 10, 2001

INTRODUCTION

Chairman Duncan and members of the subcommittee, thank you for inviting me here today to testify about "Terrorism: Are America's Water Resources and Environment at Risk?" My name is Jeffrey J. Danneels and I lead the effort at Sandia National Laboratories (Sandia) to improve the security of the water infrastructure. Sandia National Laboratories is managed and operated for the U.S. Department of Energy (DOE) by Sandia Corporation, a subsidiary of the Lockheed Martin Corporation.

Sandia is a multiprogram laboratory of DOE and one of the three National Nuclear Security Administration (NNSA) laboratories with research and development responsibility for nuclear weapons. Sandia's job is the design, development, qualification, and certification of nearly all nonnuclear subsystems of nuclear weapons. We perform substantial work in programs closely related to nuclear weapons, including intelligence, nonproliferation, and treaty verification technologies. As a multiprogram national laboratory, Sandia also performs research and development on critical infrastructure security, as well as work for other national security agencies, when our unique capabilities can make significant contributions.

I will begin my testimony with a brief overview of Sandia's capabilities that we are employing to improve the security of the water infrastructure. I will then present a systems perspective of the water system and discuss efforts underway in specific parts of the system. Finally, I will outline a comprehensive program to address both short-term and long-term security concerns.

BACKGROUND

Sandia has a rich history providing security solutions for high- consequence facilities. Sandia is the DOE's Office of Safeguards and Security lead laboratory for physical security research and development. In the past 25 years, the DOE has invested over $500 million dollars in Sandia's security program. This investment includes unique sensor-testing facilities, advanced security systems, a wealth of system-testing experience and capabilities, and a large, multidisciplinary technical base.

Sandia leads the security system engineering program for all NNSA sites and for the Department of Defense's (DoD's) Electronic Systems Command and Air Combat Command. The DOE's Office of Transportation Safeguards relies on Sandia to provide the security systems, the research and development for security improvement, and around-the-clock support for transporting special nuclear materials. The Center for Civil Force Protection (CCFP) is operated by Sandia for the Office of Science and Technology within the U.S. Department of Justice. The mission of the CCFP is to provide counterterrorism physical security advice and assistance. Sandia will soon be developing enhanced security procedures for the Interagency Working Group tasked with improving biosecurity. This effort is just getting underway.

Starting with nuclear weapons in the mid-seventies, Sandia developed performance-based methodologies to assess vulnerabilities, analyze security

systems, understand the consequences of security failures, and to provide cost-effective solutions to enhance security. We have been involved in all phases of the work, from the initial analysis through the final implementation. We have three organizations at Sandia working on national and international security programs with over 600 staff. Many of these scientists and engineers are performing research on security systems of the future.

An example of our recent research and development work is a walk- through explosives detection portal, recently licensed to a manufacturer and ready for deployment at airports around the world. The portal rapidly screens personnel for trace amounts of explosives vapor. The new preconcentrator (the device that collects the explosives) is 1000 times more sensitive, 200 times smaller, 13 times less costly, and four times faster than previously existing technology. How sensitive is it? Consider the national debt in dimes, sitting in a big pile in a warehouse. Three of the dimes are marked with a red pen. The sensitivity of the portal is similar to finding the three marked dimes in ten seconds and being able to tell which side was marked.

Sandia developed and delivers an International Training Course on Physical Protection of Nuclear Facilities and Materials for the DOE under the general auspices of the International Atomic Energy Agency (IAEA). This training course is aimed at transferring technology for preventing radiological sabotage and theft of nuclear materials. The program enables Sandia to leverage our expertise by training others to use our methodology. Since 1978, the course has been offered 15 times to over 450 personnel from 61 different countries.

Sandia has provided security solutions for nuclear power plants, DOE and DoD sites, and the Department of State and recently developed a methodology to assess and reduce the security risk at large federal dams. Sandia is a charter member of the Interagency Forum for Infrastructure Protection (IFIP), an organization formed with the focused purpose of identifying effective means to counter the security threat to our nation's high-consequence dams. With funding from the Technical Support Working Group, Sandia led the IFIP project that developed a comprehensive risk- based methodology, a training program on the methodology, and a train-the-trainer program. These materials, adapted from Sandia's unique and extensive experience with designing, developing, assessing, and enhancing physical protection systems for national security interests, have been delivered to the IFIP. IFIP members include the U.S. Army Corps of Engineers, the Bureau of Reclamation, the Tennessee Valley Authority, the Bonneville Power Administration, the Federal Bureau of Investigation (FBI), and other agencies responsible for the security of our nation's hydroelectric dams.

Sandia is presently developing a security risk methodology and training program for the water infrastructure under a project funded by the Environmental Protection Agency (EPA) and the American Water Works Association Research Foundation (AwwaRF). We have completed two water utility assessments and developed a preliminary methodology that will be refined in the coming weeks. In a parallel effort, we are developing a comprehensive training program for the water utility security risk assessment methodology.

The extensive Sandia security expertise noted above is complemented by a wide range of inhouse water expertise. This expertise, developed over the past 20 years, addresses a wide range of technical issues associated with contaminant transport, chemical interactions, risk assessment, and systems simulation for radioactive waste geologic repositories and environmental restoration sites. This water expertise provides technical support to Sandia's work in water infrastructure security.

WATER INFRASTRUCTURE AT RISK

The President's Commission on Critical Infrastructure Protection (PCCIP), established in 1996 by Executive Order 13010, probed the security of the nation's critical infrastructures. Critical infrastructures are those physical structures and information and Internet (cyber) systems essential to the minimum operations of the economy and government. The PCCIP determined the water infrastructure is highly vulnerable to a range of potential attacks.

In October of 1997, the PCCIP proposed a public/private partnership between the federal government and private industry to improve the protection of the nation's critical infrastructures. The water supply system was designated a critical infrastructure under the May 1998 Presidential Decision Directive 63, a National Security Council directive. The responsibility for the water infrastructure was assigned to the EPA.

The national water infrastructure affects every single citizen of the United States. Across the U.S., over 27 billion gallons of water are pumped on an average day. Much of the water infrastructure in our large urban areas is extremely old and is subject to both natural threats and malevolent threats, such as vandals or terrorists. An attack on the water infrastructure does not require high-tech tools, well-organized teams, or exotic chemicals. A successful attack could cause widespread panic, economic impacts, and a complete loss of public confidence not only in the affected system, but also in water supply systems throughout the country.

Security Risks to the Water Infrastructure System

Sandia employs a systems approach to solve large and complex problems, which means we strive to improve the performance of the entire system, rather than simply optimizing individual system components. The water infrastructure is comprised of many complex components that must work together as an integrated whole. To protect one component of the system and neglect the protection of others will not achieve the objective of improving the security within the water infrastructure. This systems approach provides the ability to assess critical interactions between different system components, which is frequently where failures occur.

Water Sources Upstream of Water Treatment Facilities

The first component in the water system to be assessed for security risk is the sources or supplies of water, which include reservoirs, lakes, rivers, streams, and groundwater wells. Contamination of large-volume water supplies such as reservoirs is considered difficult because significant dilution is highly likely. For example, approximately four dump truck loads of sodium cyanide mixed into a

one-million-gallon reservoir are required to yield a lethal dose to users of the system. Most storage reservoirs in large systems are between 3 million gallons on the low end and may be as high as 30 million gallons or more. As water volume decreases and the potential for dilution decreases, the risk of contamination increases. This would be the case in close proximity to water system intakes along rivers or with smaller systems with lower intake rates. The United States has 6,800 public supply drinking water intakes on rivers. Each of these intakes and the rivers that supply them can be considered vulnerable to disruption by accidental or intentional release of hazardous chemicals or biological substances.'

Many contaminating agents may be immobilized or deactivated by filtration and other treatment systems commonly employed in today's treatment plants. These processes are particularly effective in removing biological agents and biotoxins, according to studies by the Centers for Disease Control (CDC)2 and the U.S. Army Combined Arms Support Command.' While the filtration and other disinfection barriers offer a deterrent for many of the biological agents, chemicals exist that could pass through this barrier system.

To protect against the risk of contamination upstream of water intakes, early warning systems with real-time monitoring sensors are needed. Many of the components of these real-time monitoring systems are also needed in other parts of the water system. An effective early warning monitoring system would have the following attributes:

-Provides warning in sufficient time for action

-Integrates multiple sensors in a modular and expandable installation - Affordable

-Can be mass-produced

-Requires low skill and training to operate

-Covers all potential threats

-Gives minimal false positive or negative responses

-Robust, reproducible, and verifiable

-Allows remote operation

-Functions year-round

-Turns data into knowledge

-Can be installed in multiple locations

Early prototypes of these systems are being deployed in Europe and in a few locations in the U.S.4 In the event of a biological attack, there can be a significant delay time before symptoms appear, so reliance solely on the medical community would not be appropriate.

Water Treatment

For the majority of the water utilities, the next component to be assessed for risk is the water treatment facility. The water supply is pumped through either simple treatment processes for ground water or extensive treatment processes for surface water. Water treatment plants employ large quantities of chemicals that could be

used to contaminate the water or harm water utility employees and surrounding communities. However, in many treatment facilities, the chemical injection rates cannot be increased enough to pose a significant risk to the water consumer. Rather, the physical assets and the Supervisory Control and Data Acquisition (SCADA) computer systems at the water utility are a larger concern. SCADA systems allow an operator to remotely control operations and monitor system status. Many water utilities employ older, one-of-a-kind pieces of equipment, often large and expensive, that cannot be readily replaced. Security concerns were not part of the design criteria when these plants were designed and constructed. These plants are being automated rapidly, so the number of staff on-site during any given period is lower than in the past and a whole new set of vulnerabilities to cyber attack now exist.

Water Distribution

After being treated, the water either enters the distribution subsystem directly or enters temporary storage. Numerous reports 1,63 have highlighted the fact that the distribution subsystem is easily contaminated and is the most vulnerable water utility component. Accidental backflow of contaminants into the water can happen, as in the incident at the Charlotte Mecklenburg Utilities when the fire department pumped fire-fighting foam into the subsystem, demonstrating this vulnerability.' After the water leaves the plant, grab samples are collected around the distribution subsystem and sent to testing laboratories. Depending on the tests required, results are available within a few hours or up to several days after testing. Time delays associated with sampling and analysis are key drivers for the need for real-time monitoring capabilities. While intentional contamination of the water distribution subsystem has been rare in the United States, it is a potential vulnerability in the system. As noted during the discussion of the water sources upstream of water treatment facilities, early warning monitoring capabilities are needed in the distribution subsystem.

Wastewater Treatment

If the water supply, water treatment facilities, or the distribution subsystems are rendered inoperable, it is only a matter of time before the wastewater component is also inoperable. Temporary supplies of drinking water can be brought in, but the ability to treat waste, especially in metropolitan areas, is a health concern.

From the distribution subsystem, wastewater is collected and sent on to the wastewater treatment plant. This part of the system has largely been overlooked in the security efforts to date, but the wastewater component must be included as an integral part of the total system. Damage to the wastewater treatment facility not only prevents the water from being treated, but also can have significant impact on downriver water intakes. As noted previously, there are more than 6,800 publicsupply water intakes on rivers alone. The outfall of wastewater treatment plants are major "tributaries" on some rivers in the western United States: e.g., the Albuquerque wastewater treatment facility is the third largest "tributary" to the Rio Grande and becomes a significant part of the water supply for the next water utility intake downriver.

Infrastructure Interdependencies

The water infrastructure is highly interdependent with several other infrastructures. Many of the large municipal systems rely heavily on the electrical grid to move water through the system. Some water utilities have installed back-up power supplies, but many large systems do not presently have that capability. The chemical industry and the transportation system are also very important to the water utilities. Many of the water treatment chemicals are delivered by truck and some large water utilities also use railcar loads of chemicals.

All the components of the water system, except the supply, are potentially vulnerable to cyber intrusion. Dial-in and internet connections are two examples of exposure to risk. Research has shown that many water utilities are susceptible to hacking that could result in disclosure or theft of sensitive information, corruption of information, or denial of service.',"

PERFORMANCE-BASED SECURITY RISK ASSESSMENT METHODOLOGY

The key to understanding a performance-based approach is awareness that how the security system is implemented is more important that the features of the security system. Security is built from the combination of policies, procedures, people, and technology. Security policies need to be written, communicated often, and followed. In the water infrastructure, operational procedures can often be modified to help achieve the goals of the security system. People must be trained on the operation of security systems. Security system monitoring cannot be simply added as collateral responsibility to already-overloaded operators. Technology has to be employed properly to achieve the desired risk reduction. Poorly installed and poorly operating equipment can give the illusion of security while providing very little protection.

The security risk assessment methodology begins with a clear statement of the performance requirements for the security system. Based on available threat information, each utility must decide what threat or spectrum of threats they want a reasonable probability of defeating. The rest of the process then determines the ability of the system to meet those performance requirements. Critical assets are identified and the consequences of losing those assets approximated. Existing security system effectiveness is evaluated. All potential ways for the adversary to access critical assets are analyzed to ensure that no easy methods to defeat the system are left unprotected. Threat analyses are performed to understand the likelihood of various adversaries attacking the water utility. Once all the information is collected, the risk analysis is performed to determine whether the performance requirements have been met. If the performance requirements have not been met, either consequences will have to be mitigated or the effectiveness of the security system increased.

Effective security systems for water utilities contain the same elements as any effective security system: detection of adversarial action, delay of adversarial action, and response to the adversarial action.

Detection of Adversarial Action

The first required function of a security system is the discovery of adversarial action and includes sensing covert or overt actions. To discover an adversarial action, whether performed by a terrorist or any other intruder, the following events must occur:

-Sensor (equipment or personnel) reacts to an abnormal occurrence and initiates an alarm.

-Information from the sensor is reported and displayed.

-Someone assesses the information and determines the alarm to be valid or invalid.

Methods of detection include a wide range of technologies and personnel. Entry control, a means of allowing entry of authorized personnel and detecting the attempted entry of unauthorized personnel and contraband, is included in the detection function of physical protection. Entry control to various layers of the system should be designed to filter and reduce the population that has access as they approach potential targets or critical assets. Security police or other personnel also can accomplish detection. Personnel can effectively contribute to detection if they are trained in security concerns and have a means to alert the response force in the event of a problem.

An effective assessment system provides two types of information associated with detection: information about whether the alarm is a valid alarm or a nuisance alarm and details about the cause of the alarm (i.e., what, who, where, and how many). The effectiveness of the detection function is measured by the probability of sensing adversarial action and the time required for reporting and assessing the alarm.

Delay of Adversarial Action

This is the second required function of a security system. It impedes adversarial progress. Delay can be accomplished by fixed or active barriers, (e.g., doors, vaults, locks) or by sensor- activated barriers (e.g., dispensed liquids, foams). Entry control, in that it includes locks, may also be considered a delay factor in some cases. The security police force can be considered an element of delay if personnel are in fixed and well- protected positions.

Response to Adversarial Action

The third requirement of security systems comprises actions taken by utility personnel or the security force (police or law enforcement officers) to prevent adversarial success. Response consists of interrupting and stopping the event. The measure of response effectiveness is the time between receiving a communication of an adversarial action and interrupting and stopping it.

An effective security system must be able to detect the adversarial action early and delay it long enough for the response to arrive and stop the event. This approach can be applied to physical attacks upon water utilities as well as an intentional contamination. The utility must be able either to detect the contaminant before the water leaves the treatment facility or to shut down a

distribution subsystem if it is contaminated. In particular, an effective security system provides integrated detection, delay, and response.

This approach applies to outsiders, insiders, and insiders working with outsiders. In a study by the Rand Corporation, funded by Sandia, over 30 percent of the high-value crimes (not against water utilities) involved insiders, some of whom acted on their own, but most of whom were recruited by outside, professional criminals." Surveys of water utilities indicate their greatest concern with the SCADA systems involves disgruntled employees. 12

PARTNERSHIPS

In November of 2000 the EPA funded a national workshop at Sandia to begin the risk assessment methodology development for the water infrastructure. To prepare for the workshop, several Sandians reviewed the operations of a combined ground water and surface water utility to understand and to assess the effort required to adapt our methodology to the water infrastructure. We quickly determined the methodology could be adapted and used effectively by water utilities. A second major assessment, funded by AwwaRF, was completed and the adaptation of the risk assessment methodology initiated. We are now beginning to integrate cyber security assessments with the physical security assessment.

Actions Related to Water Treatment and Distribution

The water infrastructure has developed the public/private partnership called for by the PCCIP. The Water Sector Critical Infrastructure Protection Advisory Group (Advisory Group), co- chaired by Diane Vande Hei (Association of Metropolitan Water Agencies) and Brian Ramaley (Water Superintendent, Newport News), was formed in 2000. Both of the project managers (from AwwaRF and EPA) directing the work of Sandia to develop the security risk assessment methodology for water utilities are members of the Advisory Group.

AwwaRF partnered with Sandia to begin the development of the security risk assessment methodology for water utilities in the fall of 2000. The first draft copy of the methodology has been delivered to the project manager. We have also been asked by AwwaRF to develop a comprehensive training program on the methodology that will be delivered in the December 2001-January 2002 timeframe. The training course intended for utilities and their consultants is expected to expedite the assessment process by encouraging trainees to use real-world data (preferably their own water system) as examples and demonstrations of the various water infrastructure security risk assessment tools employed.

The American Water Works Association (AWWA) has been involved with Sandia since the beginning of our work. They have partnered with Sandia to deliver a security awareness course for utilities at their national workshop.

The Association of Metropolitan Water Agencies (AMWA) has also been involved with Sandia from the beginning of this effort. Not only are they providing leadership to the Advisory Group, but also they are proposing legislation to enlarge and accelerate the program to improve security for the water infrastructure.

Actions Related to Water Sources

Recently, Sandia has been discussing the possibility of developing and deploying early-warning systems for river monitoring with the United States Geological Survey (USGS). The USGS has a long history of scientific research, field testing, and application of river-monitoring technologies. The USGS also maintains a national field network of monitoring stations and data acquisition and transmission networks for monitoring river conditions. While individual water utilities are responsible for the quality of the water once it enters their facility, an early warning monitoring capability upstream of the raw water intake would enhance the ability to thwart chemical and biological contaminants.

PLAN FOR IMPROVING THE SECURITY OF THE WATER INFRASTRUCTURE

Sandia is now working on multiple fronts to refine the generic security risk assessment methodology and to perform system-wide assessments at critical locations. This effort is being lead by the EPA in cooperation with the respective water utilities. Sandia is reassigning security staff to quickly respond to a request to ramp up the program.

The efforts to improve the security of the water infrastructure must be matched by security improvements in other critical infrastructures, those that the water infrastructure relies upon, to ensure a coordinated, balanced approach that enhances national infrastructure security. The protection of the electric power grid, the transportation system, and the chemical industry are critical to the success of the overall program.

Assessments and Security Improvement

As noted previously, EPA funded a national workshop at Sandia in November 2000 to begin development of the risk assessment methodology. Participants at that workshop, including the EPA, the FBI, the CDC, industry associations, and several major water utilities, developed a methodology framework that has subsequently been tested and refined through risk assessments of the water systems of two U.S. cities. These assessment tools are being further tested on additional larger municipal systems and will soon be available to other water utilities.

In the near term, a three-day awareness course will be made available by AWWA so that individual utilities can immediately begin their own assessments using the structured methodology. Sandia can assist the EPA in conducting assessments in 10 high- priority municipal systems in the coming months. Simultaneously, we will be conducting training for additional assessment teams that will be able to assess a large number of additional facilities. All utilities can receive the awareness course so that they can begin the process with no delay.

An accelerated program would allow the assessment of multiple sites, providing valuable information on common vulnerabilities and cost-effective solutions to those vulnerabilities.

Information Sharing

AMWA has been awarded a grant from the EPA to develop and operate an Information and Analysis Center (ISAC) for the water infrastructure. This unprecedented activity for the water infrastructure will allow information to be captured, catalogued, and shared with the membership. No water utility wants to share information that could potentially damage their reputation, cause a loss of confidence, or result in some form of litigation, so all information collected by or for the ISAC should be anonymous, but authenticated. In other words, the information should be verified as reliable, but the source should not be identifiable.

An important set of information to be captured in the ISAC and shared with utilities could be termed "best practices" or "lessons learned." As water utilities embark on improving their security systems, many potential vulnerabilities - as well as novel fixes - will be discovered. Sharing those vulnerabilities and improvements will reduce the cost and expedite the security enhancements for other water utilities. This information should be contained in the ISAC and be readily available to the membership on a need-to-know basis.

Education and Training

A quick method to improve water security is to provide awareness training. An awareness video will be supplied to its members by the AWWA. AWWA is also planning to deliver an awareness course by the middle of November 2001. The goal of the awareness program is to educate the utilities on the importance of protecting their infrastructure and the beginning steps on how to accomplish this protection.

As mentioned above, AwwaRF is partnering with Sandia to develop the next phase, with a commitment to start training water utilities and their consultants in December of 2001. This three- day course will allow the trainees to make significant progress on the assessment of their own facilities.

Several long-term activities are required to make security an integral part of the water utility of the future. Security workshops, similar to the one held in Washington, DC at the last AWWA national workshop, should be offered at each subsequent national event. Educational programs for the public should be developed to stress the importance of the water infrastructure and to enlist their support in protecting it. Finally, we need to reach out to the American Society of Civil Engineers and other professional societies to make security an integral part of the design for all retrofits, upgrades, and new water utility designs. Considering security requirements during the conceptual design phase of new facilities can accomplish the security goals of the system for pennies on the dollar of what it would cost to install later.

Part of the security improvement program involves the development of emergency operation plans. Waiting for the occurrence of an event is too late. Plans for physical, cyber, and contamination attacks should be documented, disseminated, and trained. Relationships should be established with emergency operations personnel and other available resources; training together is strongly recommended. The May 2001 issue of AWWA's Water Journal" contains several

excellent recommendations on available resources and partnerships that should be established.

Research and Development

Research and development projects are needed in several areas to enhance the security of the water sector. Further development of security risk assessment methodologies, enhanced security systems specifically designed for water utilities, operational research into inherent security designs, fail-safe measures, real-time sensing of water quality, and advanced treatment methods are all areas requiring investment.

The assessment tools being developed can be further improved, streamlined, and parts of the methodology computerized. The goal is to reduce the cost and time required for performing assessments as much as possible, while providing a thorough, comprehensive methodology. Water utility facilities are not normally designed to be high-security areas, so research into technologies that would reduce the cost of security implementation would be beneficial. More active systems may need to be developed to assist in the response function.

As mentioned earlier, if operational changes can be made that increase security, they are more palatable to the utility because such changes reduce the life-cycle costs for the security system. Research into alternate methods of redundancy - e.g., dual systems - could result in significant increases in security.

Sandia and the DOE's Chemical/Biological Nonproliferation Program have invested over $11 million to design and prototype handheld chemistry laboratories. The work draws upon Sandia's expertise in microsystem technology to miniaturize laboratory chemical analysis. This effort has resulted in the development of two hand- portable systems capable of rapid and sensitive analysis of chemical constituents and impurities - one for gases and the other for liquids. The focus to date of the liquid analysis system has been biowarfare agents such as biotoxins. Experiments with the prototype liquid analysis system have demonstrated complete analysis of toxins in less than 4 minutes. Sandia conducted tests with the Edgewood Chemical and Biological Center in Maryland to test the handheld chemical analysis system in the laboratory. The microChemLab unit successfully collected, separated, and detected trace levels of various nerve agents and blister agents. The gas phase analysis takes only 2 minutes and is capable of portable operation. With an investment in research and development, real-time sensing systems to monitor water quality could be made available.

Bacteria are in the size range of 0.1 micrometers and larger while viruses are 45 nanometers and larger. The process of nanofiltration effectively removes any particle larger than 1 nanometer, which includes both viruses and bacteria. Nanofiltration is slightly less robust than reverse osmosis, but it is also less costly to operate. Research into advanced treatment methods like nanofiltration may eliminate the hazard posed by many of the potential biological contaminants. Both utility-size and point-of-use nanofiltration systems can be produced.

CONCLUSIONS

The public/private partnership initiated last year between the EPA, AwwaRF, and Sandia is a good model to collectively put the right programs in place to do the right things, as we all seek to better protect the water infrastructure. The efforts underway, such as the development of the risk assessment methodology for water utilities, will require refinements to provide a solid foundation for improving security. Train-the-trainer programs to increase the number of qualified assessment individuals available to the water utilities are important. While the methodology is being refined, it's also important that highly qualified individuals assess water utilities using the current methodology and make recommendations at a number of critical facilities around the country.

The public/private partnership model developed for the water supply and distribution subsystems should be extended to the source water and wastewater communities. Early in this testimony I mentioned that we have to look at the entire system and these two areas should move forward in concert with the water supply and distribution subsystems.

Throughout the water infrastructure, but especially in the source water and distribution subsystems, early warning monitoring capabilities have to be developed and installed. We must know what's in the water and have time to react before it's consumed. Advanced treatment processes in both the treatment facilities and point-of-use applications could render many of the contaminants harmless.

We may need to rethink the way we treat and deliver water. Distributed treatment systems or other measures not employed today may be needed. The water delivery methods of the future may be radically different from those employed today. Our collective goal is to make the water infrastructure an unattractive target of terrorism.

Ronald L. Dick, director, National Infrastructure Protection Center, Federal Bureau of Investigation

Statement for the Record of

Ronald L. Dick, Deputy Assistant Director, Counter Terrorism Division, and Director, National Infrastructure Protection Center, Federal Bureau of Investigation

Before the House Committee on Transportation and Infrastructure

Subcommittee on Water Resources and Environment

October 10, 2001

Mr. Chairman, Congressman DeFazio, and members of the committee, thank you for inviting me here today to testify on the topic, "Terrorism: Are America's Water Resources and Environment at Risk?" Holding this hearing demonstrates your individual commitments to improving the security of our critical infrastructures and this committee's leadership on this issue in Congress. Our work here is vitally important because the stakes involved are enormous. The September I I attacks on the World Trade Center, Pentagon and Pennsylvania have demonstrated how a significant disruption to the transportation industry or

any other critical infrastructure will certainly have a cascading effect on others. My testimony today will address our role in protecting the Nation's infrastructures, our progress relating to water infrastructure issues, and the need for continued trust and cooperation.

The FBI and America's Water Resource Infrastructure

Federal Government Role

With the signing of an executive order, the new Office of Homeland Security will be responsible for coordinating a wide variety of federal, state and local security activities to combat terrorism. In the event of a terrorist incident, the FBI is the lead federal agency for crisis management and Federal Emergency Management Administration (FEMA) is the lead for consequence management of the incident. Both agencies are tasked with the coordination of overall federal support to the affected state and local jurisdictions. During a terrorist event involving a water/wastewater facility, the Environmental Protection Agency (EPA), the lead federal agency for the water sector, will support either the FBI or FEMA in response to the incident. The FBI also maintains close coordination with EPA in order to facilitate response planning for terrorist incidents at facilities under the purview of EPA. The National Infrastructure Protection Center (NIPC)/FBI will continue to provide the water sector with timely, substantive, and actionable information on specific threats to their sector.

Threat Environment

Based upon available intelligence and investigative information, there are no specific credible threats to major water ways or distribution networks at this time. Due to the vital importance of water to all life forms, however, the FBI considers all threats to attack the water supply as serious threats.

The FBI coordinates a robust and well exercised threat assessment process in order to assess the credibility of communicated threats involving chemical, biological and radiological/nuclear materials, including any directed against the water infrastructure. This credibility process utilizes specialized, technical, internal FBI assets as well as technical experts from a number of other Federal agencies, including, but not limited to: Department of Defense (DoD), Department of Energy (DOE), Health and Human Services (HHS), the EPA and FEMA. Communicated threats are normally assessed from three viewpoints: operational practicality, technical feasibility, and the behavioral resolve of the individual(s) communicating the threat. A threat assessment may be conducted via conference call, and a preliminary assessment will be made within one hour of receipt of the threat at FBI Headquarters.

Depending on the circumstances, a threat assessment conference call involving a , specific water/wastewater facility threat may include facility management/security personnel as well. Upon assessment of the threat as credible, the FBI will make appropriate notifications to other Federal agencies, as appropriate, to initiate deployment, if necessary, of assets to address the threat. The onscene commander (OSC) will also receive information on a recommended course of action to address the situation

Each FBI Field Office has a Weapons of Mass Destruction (WMD) Coordinator whose primary function is to coordinate the assessment of and response to incidents involving the use or threatened use of chemical, biological, and radiological/nuclear materials. Each WMD Coordinator is tasked with establishing appropriate liaison with regional, state and local emergency response personnel as well as with critical facilities within each Field Office's jurisdiction in order to facilitate notification and response to WMD incidents. As a result of recent events, each FBI Field Office has been instructed to reach out to critical facilities to re-establish liaison contacts and ensure prompt notification and appropriate response.

With regard to contamination by biological agents, the Nation's water supply may seem to be a logical target for a terrorist attack. In reality, targeting the water supply may prove difficult. In order to be successful, a terrorist would have to have large amounts of agent, and some knowledge of the water supply network and access to critical locations within the network. It is important to stress however, that the FBI has no general or specific threat information of a planned attack on the Nation's water supply. To summarize the most important points:

1. The contamination of a water supply with a biological agent that causes illness or death of victims is possible, but not probable.

2. Contamination of a water reservoir with a biological agent would likely not produce a large risk to public health because of the dilution effect, filtration and disinfection of the water.

3. A successful attack would require knowledge of, and access to, critical nodes of the water supply network.

4. A successful attack would likely involve either disruption of the water treatment process (e.g., destruction of plumbing or release of disinfectants) or post-treatment contamination near the target.

In order to prevent contamination of a water supply, local water works or utilities should maintain a secure perimeter around the source (if possible) and the treatment facility. In addition, security should be maintained around critical nodes such as tunnels, pumping facilities, storage facilities, and the network of water mains and subsidiary pipes should be enhanced.

Biological agents can cause disease through ingestion, but are not as deadly as they would be if they were inhaled. Microorganisms vary in their stability in water. Most bacteria and viruses are inactivated by the chlorination process at water treatment facilities.

Most of the water supply threats received in the last several years involve the threatened release of a biological organism or toxin into a reservoir. In order for this to be successful (i.e., to cause illness or death), a terrorist would have to overcome the dilution provided by the large volume of water in the reservoir. For some organisms that require high doses to cause illness, producing enough organisms can become a formidable task.

Contamination of a water storage tower requires less material to cause disease, but would affect only a small area. Enhanced physical security of critical nodes in the network (such as water storage towers) and maintenance and monitoring of adequate chlorine levels would reduce this risk.

With regard to cyber-manipulation, there are growing numbers of water supply systems that use Supervisory Control And Data Acquisition (SCADA) systems, the digital controls for pumps and treatment facilities. There are vulnerabilities in this system that could lead to water supply problems.In addition, more water system operators are being given access to the Internet via the SCADA systems local area network (LAN). As a result, water systems are more likely to encounter denial of service attacks, viruses, and other malicious programs, which could severely disrupt the operation of these systems. However, most of the systems also have the capability to run the treatment plant without using these digital systems, if needed to protect public health.

Affecting a city-sized population by a hazardous industrial chemical attack on a drinking water supply is not credible. A hazardous industrial chemical attack on a post-purification drinking water storage facility in a small municipality or a building-specific target is likely to be more credible but difficult to carry out with out site-specific knowledge and access. To summarize the key facts:

1. The amount of hazardous industrial chemical needed to contaminate the drinking water supply of a city-sized population center is enormous ("truck loads").

2. Quality control procedures in place at water treatment facilities involve monitoring, filtration and treatment of the water before it enters the distribution infrastructure.

3. Only 1 to 2% of the total water consumption is used for drinking and preparation of food.

4. Contaminated sources can be isolated from the distribution infrastructure. Furthermore dilution, evaporation, and chemical and biological degradation will also lessen the impact of a pre- treatment assault.

Dependence on Other Key Infrastructures

There is a great deal of interdependency between water and other infrastructures, the most important being the electric power sector. If power is interrupted or withdrawn, it affects the entire water system. To a lesser degree, telecommunications service outages or system degradations could affect remote control access to pivotal systems, and a disruption to the nation's transportation infrastructure could delay the delivery of needed chemicals for water purification.

Security Planning and Coordination Efforts

The FBI continues to provide leadership in its Presidentially- mandated mission to anticipate, prevent, respond to, and resolve any terrorist incident. At the national level, the FBI coordinates with its Federal agency partners in various aspects of counter terrorism planning. A number of initiatives have been underway within the last several years at the federal level in order to increase domestic

preparedness for a terrorist incident, particularly one involving WMD. These initiatives have included training and equipping state and local "first responders", i.e., fire, police, emergency medical services personnel who would be the first to arrive on the scene of a WMD incident. While not specifically designed for water infrastructure facilities, these types of initiatives only serve to improve the coordination of any type of WMD response. Water infrastructure facilities should contact their local FBI field office in order to discuss planning issues and to implement procedures to ensure effective integration of national-level response assets, should an incident occur at a facility.

Every state has its own Emergency Response Plan (ERP) that coordinates entities to respond to emergencies. These entities have routine practice drills and utilize simulated scenarios in training. Within each agency, there are emergency response teams that deal with chemical contamination, spills, etc. All of these efforts are coordinated closely with FEMA. The largest of the local utilities have ERPs and the smaller ones are beginning to create them as well. These ERPs deal most specifically with power outages and loss of service. There is also a robust informal network between the agencies.

Each FBI field office has a WMD Incident Contingency Plan (WMDICP) which is prepared by the WMD coordinator. These plans were designed to quickly identify field office, as well as state, local and regional Federal assets that can be called upon by the field office to assist in the response to any type of WMD event.In formulation of these plans, field offices have been instructed to identify critical facilities as well as appropriate security contacts at these facilities. While individual field office WMDICPs may not include facilities such as water/wastewater facilities, they would include regional assets (EPA and FEMA regional offices, state and local public health labs, etc.) which would greatly assist in the response to incidents at such facilities. Local facilities should also be strongly encouraged to reach out to their local FBI field offices for further coordination and security planning assistance.

Threat Notification

At this time, the water sector is at heightened alert, which means companies have taken additional security measures such as increasing security patrols of physical facilities and regular checks of gates and locks. All large systems have ERP's in place and are well connected with state emergency response personnel. Plans vary from system to system; however, they all deal with such matters as evacuation, closing the water supply to affected areas, providing public notice, and providing bottled water and other uncontaminated alternatives. The Association of Metropolitan Water Agencies (AMWA) also provides NIPC's warnings to the Association of Metropolitan Sewer Agencies (AMSA) which then notifies its constituency.

The NIPC/FBI currently disseminates warning messages to AMWA, the prospective water sector Information Sharing and Analysis Center (ISAC), in order to notify the water sector as early as possible, of threats to facilities, systems and networks. The timeliness and actionable content of NIPC/FBI warning messages will be measurably enhanced when the NIPC and the water sector

establish a comprehensive, two-way information-sharing program. The NIPC and AMWA, in fact, are currently drafting standard operating procedures for such an information-sharing effort. The NIPCAMWA information sharing program sets up, among other things, mechanisms for sending water company incident reports to the NIPC/FBI and for more expeditiously issuing substantive warning messages and threat assessments to the water sector.

In response to a threat, the FBI, as lead federal agency, coordinates the United States Government's response. The response begins with a threat assessment coordinated by the Weapons of Mass Destruction Operations Unit (WMDOU). This is initiated when the FBI receives notification of an incident or threat. WMDOU immediately notifies subject matter experts and federal agencies with relevant authorities to conduct a real-time assessment and determine the, credibility of the threat. Based on the credibility and scope of the threat, WMDOU will coordinate an appropriate and tailored response by federal assets and the owners and operators of the facility to meet the requirements of the on-scene responders, and will oversee the investigation to its successful conclusion.

The FBI currently manages a number of programs in order to enhance real-time information sharing, intelligence gathering, and provide timely dissemination of threat warnings:

1. The NIPC's Watch and Warning Unit provides strategic analysis and warnings.

2. The NIPC's InfraGard program gathers information from InfraGard members, creates a report, and disseminates it to other members.

3. The NIPC's Key Asset Initiative has identified over 5,700 entities vital to our national security. 404 of those are water supply and treatment companies.

4. The FBI Domestic Terrorism/Counter Terrorism Planning Section works to enhance operational cooperation and information sharing within the U.S. Intelligence and law enforcement Community (USIC). Representatives from 20 federal agencies participate in the Center. Detailees work their daily shifts side by side with FBI special agents and analysts.

5. The FBI currently heads Joint Terrorism Task Forces (JTTFs) in 35 field offices across the United States. JTTFs integrate the resources of federal, state and local agencies in combating terrorism at the state, local, and regional level. The JTTFs represent a valuable resource for information regarding the local threat environment.

6. The FBI manages the National Threat Warning System (NTWS) to ensure that vital information regarding terrorism reaches those in the U.S. counter terrorism and law enforcement communities. Alert, advisory or assessment messages are transmitted. Currently over 34 federal agencies involved in the U.S. government's counter terrorism effort receive information via secure teletype using this system. The messages are also transmitted to all FBI Field Offices and Foreign Liaison Posts. If the threat information requires nationwide dissemination to all federal, state and local law enforcement agencies, the FBI transmits messages via the National Law Enforcement Telecommunications System (NLETS), which reaches over 18,000 agencies.

7. The FBI disseminates appropriate threat warnings to over 40,000 companies in the private sector via the unclassified Awareness of National Security Issues and Response (ANSIR) Program.

National Infrastructure Protection Center (NIPCI

The mission of the NIPC is to provide "a national focal point for gathering information on threats to the infrastructures" and to provide "the principal means of facilitating and coordinating the Federal Government's response to an incident, mitigating attacks, investigating threats and monitoring reconstitution efforts." Current guidelines defines critical infrastructures to include "those physical and cyber-based systems essential to the minimum operations of the economy and government," to include, without limitation, "telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private." The NIPC is the only organization in the federal government with such a comprehensive national infrastructure protection mission. The NIPC gathers together under one roof representatives from, among others, the law enforcement, intelligence, and defense communities, who collectively provide a unique analytical, deterrence, and response perspective to threat and incident information obtained from investigation, intelligence collection, foreign liaison, and private sector cooperation. This perspective ensures that no single "community" addresses threats to critical infrastructures in a vacuum; rather, all information is examined from a multi- discipline perspective for potential impact as a security, defense, counterintelligence, terrorism or law enforcement matter, and an appropriate response is developed and implemented.

While developing our infrastructure protection capabilities, the NIPC has held firm to two basic tenets that grew from extensive study by the President's Commission on Critical Infrastructure Protection. First, the government can only respond effectively to threats by focusing on protecting assets against attack while simultaneously identifying and responding to those who nonetheless would attempt or succeed in launching those attacks. And second, the government can only help protect this nation's most critical infrastructures by building and promoting a coalition of trust, one ... amongst all government agencies, two ... between the government and the private sector, three ... amongst the different business interests within the private sector itself, and four ... in concert with the greater international community. Therefore, the NIPC has focused on developing its capacity to warn, investigate, respond to, and build partnerships, all at the same time. As our techniques continue to mature and our trusted partnerships gel, we will continue to witness ever-better results.

NIPC Watch Center and Multi-Agency Staffing

The NIPC's Watch Center operates around the clock and communicates daily with the DoD and its Joint Task Force for Computer Network Operations (JTF-CNO). The Watch Center is also connected to the watch centers of several of our close allies. U.S. Army Major General Dave Bryan, Commander of the JTF-CNO, recently remarked that, "The NIPC and JTF-CNO have established an outstanding working relationship. We have become interdependent, with each realizing that neither can totally achieve its mission without the other." I couldn't agree more.

The NIPC's ability to fulfill the expectations and needs of its Department of Defense component is achieved by the interagency structure of the Center, which includes the NIPC's Deputy Director Rear Admiral James Plehal, USNR, and the NIPC's Executive Director, Steven Kaplan, a Supervisory Special Agent from the Air Force Office of Special Investigations.The staffing of these positions indicates the FBI's desire for broad, high-level, multi-agency ownership of the NIPC and our collective commitment to achieve meaningful and effective coordination across the law enforcement, intelligence, defense, and other critical government operations communities.

Within the Center, the NIPC has full-time representatives from a dozen federal government agencies, led in number by the FBI and the Department of Defense, as well as from three foreign partners: the United Kingdom, Canada, and Australia. We are partners with the General Services Administration's Federal Computer Incident Response Capability (FedCIRC), in order to further secure our government technology systems and services. We also team up regularly with the EPA, CIA, and NSA to work on matters of common concern.

Cooperative Relationships Among Federal Agencies

The placement of the NIPC under the jurisdiction of the FBI endows the Center with both the authorities and the ability to combine law enforcement information flowing into the NIPC from the FBI field offices with other information streams derived from open, confidential, and classified sources. This capability is unique in the federal government for reasons of privacy and civil rights.

The NIPC has established effective information sharing and cooperative investigative relationships across the U.S. Government.A written protocol was signed with the Department of Transportation's (DOT) Federal Aviation Administration (FAA) which will reinforce how information is shared between FAA and NIPC and how that information will be communicated. This protocol documents a long-standing informal process of information sharing between NIPC and FAA. Informal arrangements have already been established with the Federal Communications Commission, Department of Transportation's (DOT) National Response Center, DOT Office of Pipeline Safety, Department of Energy's Office of Emergency Management, and others, which allow the NIPC to receive detailed sector-specific incident reports in a timely manner. Formal information sharing procedures should soon be completed with several other agencies, including the National Coordinating Center for Telecommunications and the FEMA's National Fire Administration.

The NIPC functions in a task force-like way, coordinating investigations in a multitude of jurisdictions, both domestically and internationally. This is essential due to the transnational nature of cyber intrusions and other critical infrastructure threats.

Interagency Coordination Cell

To instill further cooperation and establish an essential process to resolve conflicts among investigative agencies, the NIPC asserted a leadership role by farming an Interagency Coordination Cell (IACC) at the Center. The IACC meets

on a monthly basis and includes representation from U.S. Secret Service, NASA, U.S. Postal Service, Department of Defense Criminal Investigative Organizations, U.S. Customs, Departments of Energy, State and Education, Social Security Administration, Treasury Inspector General for Tax Administration and the CIA. The cell works to resolve conflicts regarding investigative and operational matters among agencies and assists agencies in combining resources on matters of common interest. The NIPC anticipates that this cell will expand to include all investigative agencies and inspectors general in the federal government having cyber or other critical infrastructure responsibilities. As we noted in various Congressional hearings, including a Senate hearing last week, the IACC has led to the formation of several task forces and prevented intrusions and compromises of U.S. Government systems. The IACC was instrumental in coordinating the augmentation of the PENTTBOM investigation in the aftermath of the September 11 attacks.

Warnings and Advisories

The NIPC sends out infrastructure information to address cyber or infrastructure events with possible significant impact. These are distributed to partners in the private and public sectors. A number of recent advisories sent out by the NIPC (see, for example, Advisory 01-022, titled "Mass Mailing Worm W32.Nimda.A@mm") serve to demonstrate the continued collaboration between the NIPC and its partner, FedCIRC. The NIPC serves as a member of FedCIRC's Senior Advisory Council and has daily contact with that entity as well as a number of others including NSA and DoD's Joint Task Force - Computer Network Operations (JTF-CNO). On issues of national concern, the recent incidents involving the Leaves, Code Red and Nimda worms are good examples of the NIPC's success in working with the National Security Council and our partner agencies to disseminate information and coordinate strategic efforts in a timely and effective manner.

InfraGard Initiative

Over the past three years, the FBI cultivated a number of initiatives that have developed into increased capabilities, all of which are being actively used to mitigate the terrorist threat and to prepare our response to the events of September 11th. The NIPC has developed InfraGard into the largest government/private sector joint partnership for infrastructure protection in the world. We have taken it from its humble roots of a few dozen members in just two states to its current membership of over 2,000 partners, 31of which are associated with aspects of the nation's water infrastructure. It is the most extensive government-private sector partnership for infrastructure protection in the world, and it is a service we provide to InfraGard members free of charge. InfraGard expands direct contacts with the private sector infrastructure owners and operators and shares information about cyber intrusions and other critical infrastructure vulnerabilities through the formation of local InfraGard chapters within the jurisdiction of each of the 56 FBI Field Offices and several of their Resident Agencies (subdivisions of the larger field offices).

A key element of the InfraGard initiative is the confidentiality of reporting by members. The reporting entities edit out the identifying information about themselves on the notices that are sent to other members of the InfraGard network. This process is called sanitization and it protects the information provided by the victim of a cyber attack. Much of the information provided by the private sector is proprietary and is treated as such. InfraGard provides its membership the capability to write an encrypted sanitized report for dissemination to other members. This measure helps to build a trusted relationship with the private sector and at the same time encourages other private sector companies to report cyber attacks to law enforcement.

Key Asset Initiative

Since 1998, the NIPC has been developing the FBI's Key Asset Initiative, identifying over 5,700 entities vital to our national security, including our economic well-being.The information is maintained in a database to support the broader effort to protect the critical infrastructures against both physical and cyber threats. This initiative benefits national security planning efforts by providing a better understanding of the location, importance, contact information and crisis management for critical infrastructure assets across the country. We have worked with the DoD, EPA, and the Critical Infrastructure Assurance Office (CIAO) in this regard. Following the September 11, 2001, events and at the request of the National Security Council, the NIPC has leveraged the Key Asset Initiative to undertake an all- agency effort to prepare a comprehensive, centralized database of critical infrastructure assets in the United States.

Information Sharing and Analysis Centers

Our multi-agency team works with current and soon to be established Information ISAC's, which represent the critical infrastructures identified in PDD-63, including those that represent the water, financial services, electric power, telecommunications, and information technology sectors. Since September 1 lt', we have provided threat assessments on an ongoing basis for ISAC representatives from those sectors. We are also connected with the18,000 police departments and Sheriffs offices that bravely serve our nation daily and in times of crisis. This past March, the NIPC and the Emergency Law Enforcement Services Sector Forum completed the nation's Emergency Law Enforcement Sector Plan together with a "Guide for State and Local Law Enforcement Agencies." This significant achievement represents the nation's first and only completed sector plan and is being used as a model by the other critical infrastructure sectors. Taken together, the Plan and the Guide provide our emergency law enforcement first responders with procedures that are immediately useful to enhance the security of their data and communications systems.

Strategic Analysis

We have established four strategic directions for our capability growth through 2005: prediction, prevention, detection, and mitigation. None of these are new concepts, but NIPC has renewed its focus on each of them in order to strengthen our strategic analysis capabilities.NIPC has worked to further strengthen its

longstanding efforts in the early detection and mitigation of cyber attacks. These strategic directions will be significantly advanced by our intensified cooperation with federal agencies and the private sector. Our most ambitious strategic directions, prediction and prevention, are intended to forestall attacks before they occur. We are seeking ways to forecast or predict hostile capabilities in much the same way that the military forecasts weapons threats. The goal here is to forecast these threats with sufficient warning to prevent them.A key to success in these areas will be strengthened cooperation with intelligence collectors and the application of sophisticated new analytic tools to better learn from day-to-day trends. The strategy of prevention is reminiscent -of traditional community policing programs but with our infrastructure partners and key system vendors.

As we work on these strategic directions, we will have many opportunities to stretch our capabilities. With respect to all of these, the NIPC is committed to continuous improvement through a sustained process of documenting "lessons learned" from significant events. The NIPC also remains committed to achieving all of its objectives while upholding the fundamental Constitutional rights of our citizens.

The NIPC is also enhancing its strategic analysis capability through the "data warehousing and data mining" project. This will allow the NIPC to retrieve incident data originating from multiple sources. Data warehousing includes the ability to conduct real-time all-source analysis and report generation.

Improving Information Sharing

The NIPC actively exchanges information with private sector companies, the ISACs; members of the InfraGard Initiative, and the public as part of the NIPC's outreach and information sharing activities. Through NIPC's aggressive outreach efforts, we receive incident reports from the private sector. The NIPC has proven that it can properly safeguard their information and disseminate warning messages and useful information in return. Private sector reporting of infrastructure incidents is partially responsible for the issuance of more warnings each year.

Over the past two years the NIPC and the North American Electric Reliability Council (NERC)-the ISAC for the electric power sector- have established an indications, analysis and warning program (IAW) program, which makes possible the timely exchange of information valued by both the NIPC and the electric power sector. This relationship is possible because of a commitment both on the part of NERC and the NIPC to build cooperative relations. Since the September 11 attacks, NIPC and NERC have held daily conference calls. The close NERC-NIPC relationship is no accident, but the result of two interrelated sets of actions. First, as Eugene Gorzelnik, Director of Communications for the NERC, stated in his prepared statement at the May 22, 2001 hearing before the Senate Judiciary Committee's Subcommittee on Technology and Terrorism:

[The NERC Board of Trustees in the late 1980s resolved that each electric utility should develop a close working relationship with its local Federal Bureau of Investigation (FBI) office, if it did not already have such a relationship. The

Board also said the NERC staff should establish and maintain a working relationship with the FBI at the national level.

Second, the NIPC and NERC worked for over two years on building the successful partnership that now exists. It took dedicated individuals in both organizations to make it happen. The same type of relationship is now building with the Water Resources Sector and the Association of Metropolitan.. Water Agencies (AMWA). It is this success and dedication to achieving results that the NIPC is working to emulate with the other ISACs.

The NIPC also continues to meet regularly with current and prospective ISACs from other sectors, particularly the financial services (FS-ISAC), information technology, water supply, and telecommunications (NCC-ISAC) sectors, to develop and implement more formal information sharing arrangements, drawing largely on the model developed with the electric power sector. In the past, information exchanges with these ISACs have consisted of a one- way flow of NIPC warning messages and products being provided to the ISACs. However, in recent months the NIPC has received greater participation from sector companies as they become increasingly aware that reporting to the NIPC enhances the value and timeliness of NIPC warning products disseminated to their sector. Productive discussions held more recently with the FS- ISAC and IT-ISAC, in particular, should significantly advance a two-way information exchange with the financial services industry. The NIPC is currently working with the FS-ISAC, NCC- ISAC and prospective ISACs to develop and test secure communication mechanisms, which will facilitate the sharing of high-threshold, near real-time incident information. In March 2001, we were commended by the FS-ISAC for our advisory on e- commerce vulnerabilities (NIPC Advisory 01-003). According to the FS-ISAC, that advisory, coupled with the NIPC press conference on March 8, 2001, stopped over 1600 attempted exploitations by hackers the day immediately following the press conference.

Training

Over the past three years, NIPC has provided training for more than 2,500 participants from federal, state, local and foreign law enforcement and security agencies. The NIPC's training program complements training offered by the FBI's Training Division as well as training offered by the DoD and the National Cyber Crime Training Partnership. Trained investigators are essential to our successfully combating computer intrusions.

Conclusion:

The FBI and NIPC provide a national focal point for gathering information on threats to the infrastructures, and the principal means of facilitating and coordinating the Federal Government's response to an incident. The FBI and NIPC have been staffed with personnel from across a broad spectrum of federal agencies, and undertaken several initiatives to include the private sector as a principal partner in infrastructure protection. The Water Supply Infrastructure is used by all Americans every day, and we will continue our efforts to improve trust and increase cooperation with the water sector and all our public and private

partners. We will continually improve in the coming years in order to master the perpetually evolving challenges involved with infrastructure protection and information assurance. Thank you for inviting me here today, and I welcome any questions you have.

Marianne Horinko, assistant administrator, Office of Solid Waste and Emergency Response, U.S. Environmental Protection Agency

WRITTEN STATEMENT OF

MARIANNE HORINKO ASSISTANT ADMINISTRATOR OFFICE OF SOLID WASTE AND EMERGENCY RESPONSE U.S. ENVIRONMENTAL PROTECTION AGENCY

BEFORE THE SUBCOMMITTEE ON WATER RESOURCES AND ENVIRONMENT OF THE COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE

OCTOBER 10, 2001

Thank you for the opportunity to discuss the Environmental Protection Agency's (EPA) role in domestic terrorism preparedness and, more specifically, the Agency's role in protection of the nation's water resources. I am the Assistant Administrator for Solid Waste and Emergency Response. Also with me here today are Diane Regas from EPA's Office of Water and Jim Makris from EPA's Office of Solid Waste and Emergency Response.

The tragic events of September 11, 2001, have justifiably raised concern over our vulnerability to terrorist attack. As a nation, we are scrutinizing our efforts to prepare for and to prevent terrorist events. Realizing that we must always remain vigilant to new threats and must always be ready to respond, the Agency welcomes the opportunity this hearing offers to examine these issues. A brief overview of the Agency's role and actions as part of the response effort to the attacks of September 11, 2001, may be a useful starting point.

Before the second plane had struck the World Trade Center in Manhattan the morning of September 11, 2001, EPA headquarters had already begun coordination with our Region 2 office to address the crash of the first plane. Ten minutes later, our EPA headquarters had linked all of our east coast regional offices to begin coordination and support of the New York response effort. EPA's Emergency Response Program was present on site in New York, Virginia, and Pennsylvania within hours of the four plane crashes.

Throughout the response effort, EPA has worked in coordination with our federal partners to monitor and protect human health and the environment from potential hazards associated with the three crash sites. At both the World Trade Center and the Pentagon, EPA provided monitoring for various air contaminants. In addition, at the World TradeEenter, EPA assisted in debris removal, and cleanup of dust and debris from the streets using HEPA vacuum trucks. EPA has found no evidence of a general threat to public health, but onsite rescue and recovery crews should take appropriate precautions to protect themselves. EPA's and OSHA's monitoring has provided key data to help guide those crews in making appropriate

decisions about how to protect themselves. We have also provided rescue workers and others onsite with protective gear and health and safety recommendations for the difficult conditions on site, and set up washing stations for response workers at Ground Zero and vehicles and heavy equipment departing the Zone to be washed down prior to departure. Signs informing rescuers of the need to wear protective gear are posted throughout the washing stations.

Regarding water concerns associated with the crash site in Manhattan, EPA collected and tested drinking water at distribution points. Following several days of heavy rain in New York, EPA collected water samples from storm sewers and surface runoff to determine if potential contamination from the World Trade Center site was entering the Hudson or East rivers. EPA has also collected water samples from the 131 Street Pump Station, which transfers wastewater from lower Manhattan to the Newton Creek Wastewater Treatment Plant in Brooklyn. As a precaution the Newton Creek plant is segregating the sewage flows from lower Manhattan and will not use the sludge from these flows for beneficial use.

Background/Authorities

EPA has led the National Response System (NRS) for over 30 years. The NRS is the system by which our local, state and federal responders address hazardous material ,and oil spill emergencies. These contaminants can include chemical, biological, and radioactive materials that also could be components of weapons of mass destruction (WMD). The Agency's basis for its emergency response program is outlined under the National Oil and Hazardous Substances Pollution Contingency Plan (NCP - 40 CFR Part 300). The NRS was originally authorized under the Clean Water Act and supplemented by the authorities of the Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA or Superfund), and is codified in the NCP. The National Response Team (NRT), established by the NCP, consists of 16 Federal agencies with responsibilities, interests, and expertise in various aspects of emergency response to pollution incidents. The EPA serves as chair and the Coast Guard serves as vice chair of the NRT.

Additionally, by direction of the President, EPA has a significant role in counter terrorism activities. EPA is assigned the task of assisting the FBI during crisis management in threat assessments and determining the type of hazards associated with releases or potential releases of materials in a terrorist incident. EPA, as the lead agency for Hazardous Materials Response under Emergency Support Function (ESF) 10 of the Federal Response Plan, is also assigned to assist the Federal Emergency Management Agency during consequence management with environmental monitoring, decontamination, and long-term site cleanup. The EPA also has a role in enhancing the nation's capabilities to respond to terrorists events.EPA is also the lead agency for critical infrastructure protection for the Water Supply Sector. In the Nunn-LugarDomenici legislation, EPA was identified as one of the six key federal agencies for assisting in the WMD training program for the nation's first responders.

Protection of America's Drinking Water

The Agency's efforts are not limited to emergency response actions. Indeed, we have been focusing significant effort on emergency preparedness with particular attention to the nation's drinking water supplies. The drinking water industry in the United States comprises over 168,000 public water systems that range in size from very large - - those serving over 100,000 people - - to very small - - those serving between 25 - 500 people. The responsibility for protecting our nation's drinking water is a shared responsibility among the Federal, State and local governments with drinking water utilities. For terrorist and other seditious acts, a formal public/private partnership was established in 1998 in response to the requirements of a Presidential Decision Directive. This partnership includes such Federal agencies as the CDC (Centers for Disease Control and Prevention), DOD (Department of Defense), DOE (Department of Energy), FBI (Federal Bureau of Investigation), FEMA (Federal Emergency Management Agency) and such water-related organizations as the Association of Metropolitan 4

Water Agencies, and the American Water Works Association. In November of 1998, a preliminary plan on National Infrastructure Assurance: Water Supply Sector was drafted. Some of the activities described in the plan have been under development for the past 2%Z years and are in or near the implementation stage. Others are being designed expeditiously and will be in place in 2002. On the whole this plan has served as an effective blue print for EPA and its partners to develop a comprehensive approach to protecting the nation's drinking water supplies.

Activities in five principal areas are underway:

the development of tools to assess vulnerabilities of drinking water utilities to terrorist acts.

the identification of actions to minimize such vulnerabilities.

the revision and enhancement of existing emergency operations plans to take into account special needs that might be necessary following terrorist acts.

the establishment of a secure, web-based information center on drinking water alerts, threats, and/or actual incidents that will be accessible to all drinking water utilities. research on biological and chemical contaminants that are considered weapons of mass destruction.

Some specific projects related to each of these activities include:

-The Sandia National Laboratory of the Department of Energy in partnership with the American Water Works Association Research Foundation is developing a "tool kit" to assist drinking water systems in conducting vulnerability assessments and identifying remedial action. This resource will be available in early November 2001. As an interim measure, EPA has disseminated a fact sheet that outlines measures utilities can take immediately to protect their drinking water supplies. This document should now be in the hands of every state drinking water program manager who, in turn, will send it to a public water systems in his/her state. The Agency has also sent out an advisory to the law enforcement community through the National Law Enforcement Telecommunications System asking local police to include critical drinking water assets on regular patrols.;

As this "tool kit" is being developed, the American Water Works Association Research Foundation is concurrently drafting training materials that will provide step-by-step guidance to drinking water utilities on conducting vulnerability assessments, identifying remedial actions and strengthening their emergency operation plans. Formal training sessions will begin as soon as the "tool kit" is ready and will be directed initially to over 300 of the largest drinking water utilities, which each serve 100,000 or more consumers. Again, we expect that these training sessions will begin next month. Training others to conduct vulnerability assessments will be an integral component of this effort. Consequently, the Agency envisions that a significant cadre of professionals will be available by the end of 2001 to assist systems of all sizes, and especially small systems, in doing these vulnerability assessments.. ,

The American Water Works Association Research Foundation is currently developing an 6 emergency operations checklist to be included in the training materials that will be ready in November. In addition, FEMA is assessing existing emergency operations manuals for drinking water systems and will develop a "model" manual for systems to follow. The Agency's anticipated schedule for the distribution of this document is mid-2002.

The Association of Metropolitan Water Agencies has received funds to develop an Information Sharing and Analysis Center (ISAC). This secure, web-based, "virtual center" will provide utilities, State and local emergency response agencies, .State drinking water agencies, and EPA with alerts and notices of threats as well as provide for incident reporting by utilities. The FBI will be a principal participant in ensuring the security of this information. We are optimistic that this center will be operational in late 2002.

Research is being conducted by the Department of Defense on specific "river spill" and "pipeline" models to determine the fate and transport of contaminants within a source water watershed and drinking water system. In addition, the University of North Carolina at Greensboro has been given funds to develop biodetectors for contaminants. While research is not normally a short-term endeavor, these projects are being conducted on an accelerated schedule and data will be available in mid-2002. Ongoing research to better understand potential biological and chemical contaminants, their fate and transport within drinking water (from source water to distribution); ways to counteract such contaminants through water treatment, and related health effects of public exposure to such contaminants is provided to EPA by CDC, DOD, and the US Army Aberdeen Proving Grounds.

All these activities and projects will bolster the existing methods for responding to emergency situations, including terrorist acts. Currently, a drinking water utility would activate its existing emergency response plan with local law enforcement (including the FBI) and its state emergency officials. If needed, these provide for shutting down the system, notifying the public of any emergency steps they might need to take (e.g., boiling water) and providing alternate sources of water. EPA's extensive network of expert emergency response ;personnel can be dispatched to the scene immediately to support local communities. They have considerable

experience and expertise in working with local, state, and federal emergency officials and are prepared to provide support for monitoring, clean up, and expert advice on contaminants, just as we have in NYC and the Pentagon.

Recognizing the need to ensure appropriate coordination of these many activities, EPA has established a Water Protection Task Force that will not only keep an eye on these drinking waterrelated projects but will also guide efforts on longer-term drinking water infrastructure protection as well as wastewater treatment infrastructure protection.

EPA's Counter-Terrorism Activities

As EPA continues to strengthen its counter-terrorism (CT) program by building on the existing NRS for hazardous materials (hazmat) prevention, preparedness, and response, the Agency is involved in a variety of activities with federal, state, and local officials that include: responding to terrorism threats; pre-deploying for special events; planning, coordination, and outreach; and training and exercises. EPA was asked to chair the Security and Safety of U.S. Facilities Group of the National Security Council's Policy Coordinating Committee for Counter-terrorism and National Preparedness.

In the regions, the Agency's first responders are the On-Scene Coordinators (or OSCs). The OSCs have been actively involved with local, state, and federal authorities in preparing for and responding to threats of terrorism. EPA's OSCs, located throughout the United States, have broad response authority and a proven record of success in responding rapidly to emergency situations.

Our expertise in performing off-site monitoring, extent of contamination surveys, working with health officials to establish safe cleanup levels, conducting protective cleanup actions, and communicating technical information/data to impacted citizens is essential for a successful Federal response to an act of terrorism that involves a release of chemical, biological, or radioactive material. EPA brings unique capabilities and experience to the response process.

EPA has a mandate and a history of working closely with State Emergency Response

Commissions (SERCs) and Local Emergency Planning Committees (LEPCs) to develop emergency response plans for hazardous materials releases. We are expanding this work with SERCs and LEPCs to encourage them to incorporate terrorism response issues into their existing emergency response plans. We have worked closely with other federal agencies to develop interagency response plans for terrorist incidents including the U.S. Government Interagency Domestic Terrorism Concept of Operations Plan (CONPLAN), the Terrorism Incident Annex to the Federal Response Plan, the Department of Defense CONPLAN 0500, and the Administration's Five-Year Interagency Counter-terrorism and Technology Crime Plan.

EPA's National Enforcement Investigations Center (NEIC) conducts the forensic evidence collection on nonmilitary industrial chemicals in the event of an eco-terrorism event. NEIC trains state, local, and federal personnel in this type of work and are active members of the multiagency task force in the counter-

terrorism effort. EPA's Criminal Investigation division typically investigates such incidents jointly with the FBI, after the immediate response actions are completed.

EPA is currently providing supplemental hazardous materials training to its OSCs to ensure their health and safety when responding t& a terrorist incident, particularly one involving WMD. EPA's basic and advanced hazardous materials training has also been provided to some of the National Guard WMD Civil Support Teams and to other federal, state, and local emergency responders. We have been an integral part of the Nunn-Lugar- Domenici Domestic Preparedness Program and its predecessor under DOJ providing terrorism response training to local emergency responders. To test its readiness and coordination with other agencies, we have participated in several terrorism exercises, most recently the TOPOFF Exercise in May 2000 and the Wasatch Rings Exercise in April 2001 (in preparation for the 2002 Olympics). We have also participated in the ITRAP interagency series of exercises for senior department and agency policy and counter terrorism coordination officials.

Conclusion

Finally, Mr. Chairman, I would like to emphasize that the Administrator, Governor Whitman, has made very clear to the entire Agency that there is no higher priority than ensuring that EPA's mission - protecting the environment and the public health - extends to homeland security. The expertise and experience the Agency has developed over 31 years is certainly a tremendous asset to the work that Governor Ridge will be doing and to the work you will be doing. We intend to use that asset to the fullest.

Clearly, the Administrator believes very strongly that EPA's efforts to help secure the safety and integrity of America's water supply and infrastructure must be undertaken with great speed, energy, and attention. Deadlines that were established before September 11t' for such action are no longer appropriate. We don't have any time to waste in completing this work and we intend to devote the resources necessary to make certain it is done as quickly as possible.

I know if the Administrator were here she would tell you that we welcome the opportunity to work with you, your colleagues in the Congress, and with Governor Ridge and the Office of Homeland Security, to meet the expectation every American shares - that the federal government is hard at work meeting the concerns of the American people and the demands that the events of September 11 have placed before us.

Thank you.

Patrick T. Karney, director, Metropolitan Sewer District of Greater Cincinnati, Ohio

TESTIMONY OF THE ASSOCIATION OFMETROPOLITAN SEWERAGE AGENCIES (AMSA)

October 10, 2001

on TERRORISM: ARE AMERICA'S WATER RESOURCES AND ENVRIONMENT A T RISK?

Presented by PATRICK T. KARNEY, P.E, DEE Director Metropolitan Sewer District of Greater Cincinnati Cincinnati, Ohio

Submitted to The SUBCOMMITTEE ON WATER RESOURCES AND ENVIRONMENT HOUSE COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE U.S. HOUSE OF REPRESENTATIVES

Introduction

Good morning Chairman Duncan, Representative DeFazio and members of the Subcommittee, my name is Pat Karney. I am Director of the Metropolitan Sewer District (MSD) of Greater Cincinnati and serve as a member of the Association of Metropolitan Sewerage Agencies (AMSA) Wastewater Infrastructure Security Task Force. MSD employs 650 environmental professionals who serve 800,000 users in Hamilton County. AMSA represents the interests' of more than 260 publicly owned treatment works (POTWs). AMSA's members treat 18 billion gallons of wastewater every day and provide service to the majority of the United States' sewered population.

On behalf of AMSA and the Metropolitan Sewer District of Greater Cincinnati, thank you for your support of the wastewater community by calling today's hearing and inviting us to testify on infrastructure security.

To answer the question posed by the title of this hearing-yes, America's wastewater utilities, water resources and the environment are at risk from future terrorist attacks. The events of the past month have revealed how little our industry knows about the unique risks posed by terrorist threats and how we can better prepare ourselves for an uncertain future. MSD has been reviewing and strengthening the effectiveness of its security procedures over the past two years. We now realize that we will have to plan for the unimaginable if we are to fully protect the city's citizens, MSD employees and our public assets from a broader, and more serious, array of risks. Perhaps most disturbing to the majority of public wastewater utility managers is the scarcity of resources to assist us in conducting vulnerability assessments and the rarity of security expertise in the wastewater infrastructure sector.

Mr. Chairman, I will begin my testimony with a review of how Cincinnati conducted readiness exercises prior to September 11, followed by a brief look at our response since the terrorist attack on our country. I will close my remarks with an overview of what AMSA is doing to assist the wastewater treatment industry to prepare for the future.

Review of MSD Preparedness

Cincinnati officials felt they were well prepared for an emergency following the completion of two annual exercises focused on weapons of mass destruction, which was funded, in part, by the federal government. Our first responders spent several days in training and in practice drills during each week's program. To conclude the week, city department heads along with hospital, military, law

enforcement (local, state and the FBI), FEMA (state and federal), and associated volunteer organization personnel participated in a daylong tabletop scenario. The first year we participated in the exercise revealed a lack of coordination between agencies and, in many cases, a complete ignorance as to which agencies participate in preparedness, response and recovery from disasters. Most of the deficiencies were addressed through personal interaction between the participants before the session ended. The second year helped to focus us on enhancing our communications and coordination of efforts.

The last of these annual events was a full-scale mock chemical attack, sniper and bombplanting exercise conducted at MSD's Mill Creek Water Reclamation Facility. Fire, police, SWAT, and medical first responders all were involved. The day included the set-up of a National Guard decontamination tent, and treatment of exposed "victims".

Cincinnati has long maintained its own Emergency Operations Center (EOC) in the city. This center is wired for multiple phone and computer communications lines, and is equipped with emergency power backup in the event of a sustained power outage. The city manager activates the EOC in the event of an imminent emergency situation or in response to an incident such as the 1997 flooding of the Ohio River.

MSD historically has played a major role in chemical spill response and investigation, whether accidental or intentional in origin. This role has increased MSD's visibility and the frequency of communications with emergency and law enforcement personnel. I am proud of the respect given to us by local fire, police, and HAZMAT agencies, as well as by state and federal law enforcement officials. In addition to the recognition that MSD receives as an organization, two of the District's Division of Industrial Waste supervisors received award citations from Ohio's 25th Annual Inland Spills Conference this past month. MSD has gained valuable experience in prevention, investigation, and cleanup through its participation in these successful joint operations.

MSD's recently-formed Security Task Force has included the following incidents on a list of major security threats: violence in the workplace, civil unrest, service interruption to associated utilities and infrastructure, vandalism, theft, irate customers, weather related emergencies and terrorist attacks.Aside from physical plant damage, these threats can cause a disruption of operations and service at the water reclamation facilities, pump stations, service garages and with the underground collection system. Cyber interference could affect MSD's computers, management information, and customer service systems. The loss of electricity or natural gas supplies would adversely impact our service delivery. The Task Force also discussed the use of the physical facilities and collection system for negative purposes. On September 10, we were reasonably comfortable with the level of our knowledge and secure in our readiness and response capabilities.

MSD's Response Since September 11

As with all City of Cincinnati government departments, MSD went into an immediate "lock down" condition before noon on September 11`". We doubled

security personnel at all staffed facilities throughout the County. All persons passing through our gates were questioned and had to state the purpose for their presence at the facility. This information was recorded. These heightened security conditions remain in effect today.

We also have changed our procedures for the swipe-card locks on all exterior-building doors. They no longer are turned off during the workday but remain in an active mode. Perimeter security has been tightened, with some "hardening" of access points now in effect. We immediately reviewed all process controls and chemical feed systems to ensure their safety and eliminate any possible risks, including the removal of some chemicals from various MSD sites.

An advisory was issued to all MSD environmental professionals regarding our heightened state of awareness, and requested their cooperation during this time of shifting procedures and other changes. MSD employees have accepted these changes readily and have made a few of their own by decorating every one of our facilities with numerous small American flags and red, white and blue decorations. We have changed the way we conduct our business, and will continually add new security and process measures as we gain the knowledge to identify additional risks and weaknesses. MSD's preparedness has provided Cincinnati with more experience perhaps, than other wastewater utilities, but we still have a lot to learn.

AMSA Prepares to Help POTWs

Nationwide AMSA members comply with federal, state and local regulations that require the development of safety, health and emergency preparedness plans in response to chemical spills, natural disasters and other emergencies. Now, however, wastewater utilities need to perform comprehensive vulnerability assessments and prepare emergency response and recovery plans in response to potential terrorist activities. As you know, the water supply sector was included as critical infrastructure under the May 1998 Presidential Decision Directive 63. Our colleagues in the drinking water sector have been engaged since then in a variety of information sharing and risk identification programs to help ensure the safety of the public drinking water supply. Until about a month ago, wastewater treatment plants and collection systems were viewed merely as a subcategory of water supply, and received little attention as security threats were assessed. Today, law enforcement agencies, the U.S. Environmental Protection Agency (EPA), and others clearly consider wastewater treatment plants and collection systems as possible targets for terrorist activities.

Immediately following the events of September 11, AMSA's Board of Directors took decisive action to support wastewater utilities nationwide as they strengthened their systems against terrorist threats. An AMSA Wastewater Infrastructure Security Task Force was formed; funds were allocated to immediately begin exploration of publicly owned treatment works (POTW) security needs and to identify tools and initiatives to support enhanced security; the Association established itself as a link between the FBI and its members for the distribution of advisories; and, Managing & Protecting Water Infrastructure Assets was identified as the theme for AMSA's February 2002 conference.

Our efforts have also included outreach to the U.S. EPA, the Federal Emergency Management Agency, the U.S. Army Corps of Engineers, and the National Infrastructure Protection Center in an effort to pinpoint programs or experts in the area of wastewater infrastructure security.

In the short-term we plan to develop a wastewater utility "checklist," directing attention to key areas of concern and vulnerability. We have also identified the need for an industry specific, asset-focused, risk-based, self-assessment tool with the goal of fully protecting the assets of the nation's wastewater utilities. Once vulnerabilities are assessed, our efforts and resources must be expeditiously focused on upgrading and enhancing wastewater infrastructure security - as well as ensuring continuity of service.

Such essential undertakings to ensure the security of our nation's aging infrastructure will clearly require federal support.

As the sole representative of public wastewater treatment agencies, AMSA is uniquely qualified to gather information, communicate with the industry, and develop the necessary materials, programs and initiatives to support POTWs across the country. AMSA and its members will need your help to secure our future and protect not only our infrastructure assets, but also public safety, public health and our environment.

Mr. Chairman, AMSA looks forward to working with you and the Subcommittee to address this important need. Thank you for this opportunity to testify today. I will be happy to answer any questions.

Glenn L. McCullough, Jr., chairman, Tennessee Valley Authority

Testimony of

Glenn L. McCullough, Jr. Chairman Tennessee Valley Authority

Before the House Transportation and Infrastructure

Subcommittee on Water Resources and Environment

October 10, 2001

Good morning, Mr. Chairman and members of the Subcommittee. I am honored to be here, and I am pleased to give you an update on how TVA ensures the safety of our employees, our facilities, and the people of the Tennessee Valley, particularly at this time. We appreciate your leadership as our Nation unites to recover from the recent attacks and to protect our citizens from future threats.

We at TVA are particularly mindful of the need to protect TVA facilities in the seven-state region we serve. For many years, we have had extensive security measures in place throughout TVA's operations. These measures range from police patrols at our recreation areas to armed security officers at our nuclear facilities. We anticipate emergency situations that could arise, and we conduct emergency drills to ensure we can respond quickly and effectively. Strong security measures are part of our daily operations and our commitment to protect our employees, our facilities and the public is among TVA's highest priorities.

Now, in light of the attacks on America on September 11, our security measures are more stringent than ever. Heightened security measures are in force in our office buildings, at our dams and power plants, and throughout the TVA system. The value of our emergency plans and emergency drills has never been demonstrated more clearly, and we are continuing to further strengthen our overall security program.

In nearly seven decades of service to the Tennessee Valley, the employees of TVA have risen to many challenges. Like our fellow citizens across the United States, the 13,388 employees of TVA will use their talents, hard work and creativity to meet this challenge, as well.

Background on TVA

TVA exists to serve the public good, and our vision is that TVA will achieve excellence in business performance and public service for the good of the people of the Tennessee Valley. TVA was established by Congress in 1933, primarily to provide flood control, navigation, and electric power in the Tennessee Valley's seven state region. TVA's facilities in the Southeastern United States range from dams with navigation locks to large power plants and an extensive transmission system. TVA is not only the nation's largest producer of public power, but it also serves as a regional economic development agency and the steward of the Tennessee River basin. TVA improves the quality of life in the Tennessee Valley through integrated management of the Tennessee River system and environmental stewardship; meets customers' needs with affordable, reliable electric power; and supports sustainable economic development in the region. The TVA power system is 100 percent self-financed through its power revenues.

The Tennessee River is the fifth largest river system in the United States. It stretches 652 miles from Knoxville, Tennessee, to Paducah, Kentucky, where it flows into the Ohio River and ultimately the Mississippi. It encompasses more than 11,000 miles of shoreline, 49 dams and 14 locks. About 34,000 loaded barges travel the Tennessee River each year - the equivalent of 2 million trucks traveling our Nation's highways. Prior to the creation of TVA, the Tennessee River flooded on a regular basis, causing millions of dollars of damage per year.

TVA employees are on the job around the clock, every day, providing wholesale power to 158 local municipal and cooperative power distributors through a network of transmission lines in the seven state region. TVA also sells power directly to 62 large industrial and federal customers. Ultimately, TVA supplies electricity for 8.3 million people over a power service area covering 80,000 square miles. This area includes Tennessee and parts of Mississippi, Alabama, Georgia, North Carolina, Virginia, and Kentucky.

TVA Infrastructure

The TVA power system includes hydro facilities, coal-fired power plants, nuclear power plants, power transmission facilities and some other, smaller power generating units.

TVA has 49 dams with 14 locks on the Tennessee River and its tributaries, including 33 wholly or partially earthen dams. Of the 49 dams, 29 produce hydro-

electric power, and 11 of those rank among the Nation's lowest-cost producers of hydro-electric power. Last year, these plants produced about 6 percent of TVA's total electrical generation.

TVA's 11 coal-fired power plants produce more than 60 percent of TVA's annual power generation. In fiscal year 2000, TVA's power generation from these plants reached 95.3 million megawatt-hours, the most generation since 1996 and the third-highest generation on record for TVA's coal plants.

TVA's three nuclear plants are located in East Tennessee and North Alabama, and these plants produce about a third of TVA's power generation - almost 47 billion kilowatt-hours of electricity last year.In fiscal year 2000, the plants set a generation record for the fifth consecutive year and increased their output for the eighth consecutive year. For the past three years, TVA's nuclear units have been ranked among the top 25 performers in the United States. In 1999, they were ranked among the top 50 worldwide during 1999 by Nucleonics Week, a national nuclear industry publication.

TVA electricity is delivered to power distributors and other customers by way of 17,000 miles of transmission lines. The TVA system is one of the largest single-owned transmission systems in the United States. It includes 240,000 right-of way acres with 850 individual delivery and interchange points.

TVA also operates four combustion turbine plants for peaking capacity and one pumped-storage facility to help provide affordable, reliable power even when power demands are greatest.

In the integrated management of the Tennessee River system, TVA balances the demands on the river system in order to protect the region's natural resources and support sustainable development. In addition to navigation, flood control, and electric power production, the Tennessee River system provides for water quality protection, public land conservation, and outdoor recreation. About 4 million Valley residents depend on the Tennessee River system for their water supply. TVA serves as a steward of the river, its 41,000 square-mile watershed, and the Valley's natural resources.

Overview of TVA Emergency Management/Planning

The TVA Act authorizes the TVA Board of Directors to provide for the safety and security of TVA's employees, property, and facilities and to enforce federal, state, and local laws on TVA property. We take that responsibility very seriously. Our actions include anticipating emergency conditions, and we have emergency plans in place for our critical functions and major operations. These operations include our fossil, hydro, and nuclear plants, and our transmission system.

When the attacks on America occurred on September 11, the TVA Police and TVA employees throughout the agency immediately implemented our emergency plans. They activated all our major Emergency Operations Centers, including centers in Knoxville and Chattanooga, Tennessee. Our System Operations Center was placed on "full alert" status, and we activated our back-up System Operations Center to ensure that the Tennessee Valley's power supply would not be interrupted.

We dispatched uniformed TVA Police officers to protect critical TVA facilities 24 hours a day, seven days a week. We were in contact with the state emergency management agencies and the U.S. Department of Energy. Additionally, we took several other specific actions, including the following:

-TVA employees did walk-down inspections at our 500 kV substations near major cities and critical communications locations.

-Helicopters normally used to inspect and maintain transmission lines were fueled and placed on standby.

-All maintenance work on critical equipment and lines was suspended, and all maintenance at substations was suspended.

-Fort Campbell notified us that troops had been placed at the substation that supplies power to that military installation.

-We implemented rigorous access control requirements for anyone entering TVA offices and facilities, posted officers at all critical TVA facilities, and implemented stringent controls on the delivery of materials and supplies to our loading docks.

We stationed TVA Police boats on the river immediately adjacent to the emergency cooling-water pumping stations at our nuclear plants.

-Visitor tours at the hydro sites were discontinued, and access was closed at some recreational facilities.

-Power supply and transmission alerts were declared.

Most of these security measures are still in force. Exceptions include the easing of some of our more stringent requirements on deliveries to our facilities and the easing of access requirements at some recreational facilities. We have also placed our emergency operations centers on standby.

Employees throughout TVA support our emergency efforts, and a key role is played by the TVA Police and its 192 sworn officers. Amendments to the TVA Act that were enacted in 1994 authorized TVA to appoint federally commissioned police officers to carry firearms, execute warrants and conduct investigations. The TVA Police is accredited through the Commission on Accreditation for Law Enforcement Agencies.

Actions Since September 11

I am proud of the way the men and women of TVA responded to the terrible events of September 11, and we continue to be vigilant. We are working to further strengthen our ability to protect people and property.

Since September 11, we have identified the need for a more comprehensive, overarching plan to better integrate all of the agency's emergency plans and Emergency Operations Centers. Currently, our business units have plans in place for responding to emergencies within their own areas and for meeting statutory and regulatory requirements. Our major business units also have their own Emergency Operations Centers. Additionally, we have a radiological emergency

plan, environmental response plan, dam safety emergency plan, and transmission emergency plan.

The comprehensive plan we develop will help us do a better job of coordinating these efforts. It will address improved communication, the activation and deactivation of all Emergency Operation Centers, and the sharing of information and other resources throughout TVA. It will also address what we must do to provide security on an ongoing basis and in emergency conditions.

One component of this comprehensive plan will be our efforts to ensure that we have continuity of TVA operations in an emergency. In 1999, TVA began developing a comprehensive "Continuity of Operations" capability. This capability ensures that essential agency functions continue when normal operations are disrupted. We are working to widen our efforts in this area to include more TVA organizations, such as all our major office complexes and power plants, to ensure our ability to operate in an emergency.

Our comprehensive plan will also address how we work with other agencies at all levels of government. In working with the National Guard, for example, we want to ensure that we have fast, direct methods for getting approval for National Guard staffing at critical TVA facilities, if needed. I am pleased to let you know that the Governors of three states and TVA are working together to meet this need.

Nuclear Security

At our nuclear power plants, we have taken additional security measures since the events of September 11, and we will maintain this level of security for as long as necessary. Each nuclear plant has a security plan that meets federal regulations and is approved by the Nuclear Regulatory Commission. The plan for each site is designed specifically for that plant and takes into account the local terrain, general plant layout, and location of vital equipment.

TVA's Nuclear Security staff contracts with Pinkerton Government Services to provide armed security for each TVA nuclear facility, and these security officers are well-trained and highly skilled. In keeping with federal regulations and industry standards, these employees must complete a background investigation, pass psychological and medical evaluations, and pass rigorous security training. Pinkerton Government Services and Burns Security have provided experienced and highly skilled security officers for TVA's nuclear plants for more than three years. These employees are highly motivated and have demonstrated their ability to implement security measures at our plants.

Since September 11, our Nuclear Security staff has worked closely with the TVA Police, local law enforcement agencies, the FBI, and state emergency and law enforcement agencies. Each TVA nuclear site meets stringent standards set by the Nuclear Regulatory Commission, and each has the capabilities necessary to protect our employees, equipment and the public in the event of a threat.

Water Quality

As I mentioned, TVA serves as steward of the Tennessee River system. TVA began a year round water-quality monitoring program 10 years ago. At 60 sites throughout the watershed, TVA monitors for a number of substances, including PCBs, metals, naturally occurring chemicals that indicate some kind of pollution, chlorophyll, algae, and sediment quality, among other things. Water samples are analyzed, and fish samples are analyzed for chemicals that accumulate in the fish.

We also have in place emergency response measures we use to contain and clean up any accidental - or deliberate - spill of hazardous materials into the water. These measures include the fact that, because TVA has operational jurisdiction over all the dams in the system, TVA does, when necessary, impound water to contain a pollutant between two dams. Our emergency procedures ensure that we respond quickly and that we work in close partnership with state and local agencies to address problems.

Conclusion

The attacks of September 11 raise a new level of concern, coupled with action, for all of us. I am proud of the speed and skill with which TVA employees acted to ensure that our facilities were safe as we saw danger and destruction elsewhere. I am proud of the way TVA employees are taking action to ensure that our emergency measures are made even stronger so that our facilities continue to be safe. And I am proud of the way TVA is working with federal authorities, the National Guard, the Valley Governors, state agencies, and others in the power industry to plan our actions and share information so that all of us are more secure from future threats. Thank you for this opportunity to share TVA's actions with you and I commend the leadership that each of you and your colleagues in Congress have provided to ensure that freedom prevails over fear, and you can count on TVA's full cooperation as we continue forward together.

Joanne Moreau, director, Office of Emergency Preparedness, East Baton Rouge Parish, La.

U.S. House of Representatives Committee on Transportation and Infrastructure The Subcommittee on Water Resources and Environment hearing on "Terrorism: Are America's Water Resources and Environment at Risk?

As presented by

Ms. JoAnne H. Moreau, CEM Director East Baton Rouge Parish Office of Emergency Preparedness and East Baton Rouge Parish Local Emergency Planning Committee

October 10, 2001

Good morning, and thank you for the opportunity to address this distinguished committee and many guests regarding the important and immediate issues facing local jurisdictions across the nation following the tragedies of September 11th.It is truly an honor to be asked to speak on behalf of the Local Emergency Planning Committee in my community, the City and Parish of East Baton Rouge - and its responders, public officials and citizens.It is our collective belief, from personal and frequent experience, that all government begins and ends at the local level.

Regardless of the origin or nature of harmful events, local governments have the initial and most intimate responsibility, authority and accountability for all events affecting the safety of American citizens from prevention, preparedness, response and mitigation to recovery, when all others have returned to where they came from, and we alone remain to contend with the lasting consequences. And so we are sincerely appreciative of the overtures from Congress and our federal partners to support our efforts back home, and in these exigent times, we welcome and accept your assistance more than ever.

I would like to share with you today the status of my communities' domestic preparedness efforts prior to September 11, 2001; what transpired in the days following; where we ultimately wish to be; and, finally, I would like to make some recommendations with respect to how Congress and federal agencies can further prevention, preparedness and response capabilities for local and state governments, and then, of course, answer any questions you may have.

To begin, although no one community or government entity can prepare completely for every conceivable circumstance, I am pleased to tell this committee that our community has for years promoted partnering programs between government and business and industry stake-holders and resourceproviders which have established effective measures and processes to confront all potential hazards, including threats and acts of terrorist violence. Many of these emergency response capabilities grew out of chemical disaster planning under the auspices of SARA Title III and the affiliated role of our Local Emergency Planning Committee, known as the LEPC. From 1986 forward the LEPC directed the collaboration of emergency managers; police, fire, public works and emergency medical providers; mutual aid systems, which include business and industry representatives; and public and elected officials. Incidentally, I want to relate to you that our LEPC embraced EPA's Risk Management Program as yet another opportunity to focus on chemical release prevention and response, and together with our industry partners we conducted the public information roll-out procedures necessary for implementation of the plan. This initiative, as is so often the case, with catastrophic events, was not respectful of jurisdictional boundaries, and we helped to create and participated in a multi- parish RMP task force along the industrial corridor of the lower Mississippi River. Representatives from both industry and government worked together to provide the community with accurate and timely information. This task force fostered collaborating and information exchange and helped both government and industry work together to identify the source and solutions to some worst- case scenarios. It gave us an opportunity to talk together candidly and promoted future dialogue, while respecting jurisdictional boundaries.

May I inject here with emphasis that we strongly supported the EPA and FBI controls which prevented our industries' worst-case scenarios and related off-site consequence information from being posted on the Internet. In fact, I wish to suggest that perhaps public access to the most sensitive Tier II data collected under the federal Emergency Preparedness and Community Right-to-Know Act should be revisited, with a view toward striking a balance between public

privilege and security of key industrial assets. It has been my personal experience that the only requests for this type of information has not been from within the community, but rather from agencies or persons with the intent to use the information for some type of professional financial gain.

In Baton Rouge, we quickly recognized the collective efficiency and responsiveness of the LEPC through its diverse members and their organizations, and began to apply those talents and practical resources toward a unified approach to natural disasters, human-caused catastrophes, school violence and even marine transportation safety and highway traffic incident management initiatives. While the LEPC by legal definition and requirement serves to address a community's chemical preparedness, we as community planners would be remiss if we did not take advantage of the collective knowledge and adopt an "all- hazards" approach. Additionally, I cannot stress enough the usefulness of such a team in the identification and development of programs that provide for the improvement of emergency response.

Following the bombing of the Murrah Building in Oklahoma City, our community placed this template squarely over the potential threats poised against us by both domestic and transnational terrorists.Beginning in 1996 with our own personnel and resources, and then through partnering with others, we developed terrorism awareness training forums for our first responders, followed by those for public officials, and next for business and industry interests. The solid foundations and demonstrated successes of the LEPC gave rise to the creation in 1997 of a Weapons of Mass Destruction Coordinating Council which identified and implemented additional forums for joint training, and secured enhancements for communications systems in order to link together first responders from all tiers of government and fields of service, as well as industry firefighters and hazardous materials responders.

With a forward view toward the potential for terrorist deployment of chemical and biological weapons of mass destruction, the Council formed a healthcare alliance network within the LEPC to promote partnering and better communications among local hospitals, physicians and other healthcare providers. We established a special healthcare subcommittee, chaired by a former emergency room physician and now parish coroner, Dr. Louis Cataldie, for the express purpose of advancing hospital capability assessments, procedures for local administration of the National Pharmaceutical Stockpile, and ultimately were successful in the development of a portable morgue unit that has statewide deployment capabilities for an incident resulting in mass fatalities.

The East Baton Rouge LEPC recognized that public health information and support needed within our community and it's responders were often difficult to obtain.Information, communications, medical surveillance and laboratory testing issues that arise are now critical at local, state and national levels. We welcome the participation of public health representatives, however, this area remains a weak link in our community. Baton Rouge however, under the direction of Dr. Cataldie addressed those issues head on and identified alternate sources of information and data collection. With assistance and funding from the Department

of Justice, we developed a medical training schedule and have implemented an on-going educational program resulting in over 130 physicians and nurses participating.

The Healthcare Committee continues to set goals and implement a community medical information system responsible for addressing distribution of pertinent medical information within all sectors of government and industry. Additionally, we have taken the lead and are developing a statewide Metropolitan Medical Response Task Force that will assist less organized LEPC's and jurisdictions.

As an initiative of the State Emergency Response Commission, the facilitation and sharing of information and resources statewide will assist our community should we too be left to deal with a tragedy like that which affected our country on September 11th. In Louisiana, four major metropolitan areas have been identified under the Nunn-LugarDomenici Program and using the LEPC/SERC model we are working "not to reinvent the wheel", but rather, to "use the wheel, and advance our state forward."

As our momentum grew in the arena of counter-terrorism preparedness, we could not wait to be contacted by others, although we soon were, but instead we reached out to those who could best assist our efforts as we addressed our public safety and response concerns. I'm pleased to report to you that our resources have recently been further augmented by our community's inclusion in the federal Metropolitan Medical Response System initiative. Furthermore, FBI HQ in Washington informed our community that our recruitment, three years ago, of an FBI Special Agent to serve on our LEPC was a first in the country. Our LEPC and SERC sponsored various and frequent training forums, drills, exercises and strategy development meetings. Representatives for these forums included bringing to Baton Rouge experts from EPA, FEMA, DOJ, the Center for Domestic Preparedness at Fort McClellan, the NDPO, the CDC, ATSDR, the Louisiana National Guard 62"d Civil Support Team, the Business Executives for National Security, the United States Coast Guard and the National Domestic Preparedness Consortium.

As the scope of our programs expanded and our reputation for innovation and pro-activity broadened, we began to be approached by other agencies and organizations who wished to contribute to our initiatives and to reciprocally benefit their own.Our community was recruited by the National Domestic Preparedness Office for membership on their State and Local Advisory Committee. The Texas A&M University System invited us to serve on the Advisory Group for the George Bush School of Leadership Development in Emergency Response. The Department of Justice, Office of Justice Programs in conjunction with Texas A&M piloted through the communities of Baton Rouge and Cedar Rapids, Iowa the threat and risk assessment component and grants instrument process for the nationwide Domestic Preparedness Equipment Grant Program.The National Guard Bureau requested our guidance for design of their counter-terrorism initiatives; FEMA asked that we test their terrorism exercise module.Our Mayor-President and members of our emergency response

community traveled to FBI Headquarters at Quantico to produce a counter-terrorism preparedness and partnering video, which was distributed nationally.The

National Chemical Educational Foundation recognized our involvement of young students and senior citizens, in both training and operational elements of our emergency preparedness system through a national award for best practices. The Environmental Protection Agency created a Local Emergency Planning Committee bulletin that promoted our development of a Health Alert Network.

May I pause here for a moment to say, that although immensely proud of my community's accomplishments, I am not boasting, but rather presenting to you our credentials as a progressive and model community. I am in hopes that we may be viewed as a beneficial resource in support of other jurisdictions, and that we may demonstrate good stewardship of the assistance that we have received from others, in anticipation of gaining even more.

I am pleased to point out that we in Baton Rouge have, in fact, derived direct advantage from two congressionally-mandated federal programs: the Nunn-Lugar-Domenici bill, and the Metropolitan Medical Response System initiative.The merit of these two programs for our first responders and medical community cannot be overstated, for this we are grateful. The direct lines of communication with federal agencies responsible for program delivery and oversight have allowed our community the opportunity to advance such programs and not have unnecessary impediments which so often result from additional layers of government and program interpretation.Having embraced these programs, are thankful we did.

Now, please permit me to draw a time-line delineating our efforts since the horrific terrorist attacks of September 11th. First, we experienced validation for our existing systems through execution of crucial communications and operations at critically heightened levels of alertness and readiness. These pre-positioned mechanisms facilitated necessary and efficient collaboration among our local and state law enforcement authorities, especially in significant cooperation with airport security police, as well as university police departments with respect to large public assemblies for sporting events. These established systems further augmented key asset identification and related security intensification for petro-chemical and nuclear sites, as well as transportation infrastructure and public utilities, including energy and drinking water providers.I should point out, as well, that numerous, timely and informative advisories were posted both to government employees and the public regarding relevant current events and official precautions and actions by means, respectively, of internal communications and news media relations.

The direct link of the many agencies from both public and private sectors responsible for continuity of government and critical infrastructure support were never more valuable and clearly more critical than during the terrorist attacks of September 11th .Without the prior training and solid foundations established, our community may have been gravely affected by the occurrences of that tragic day. However, thankfully, our community leaders' dedication and commitment to public safety, and trust, served as the basis for public calm. Under the direction of

our mayor, our community and its leaders worked tireless to ensure public information was delivered in a timely manner. Particular attention was given to information exchange.

Finally, where we, as a community, would like to be with respect to counter-terrorism preparedness, sentiments which I genuinely believe are shared by our friends and colleagues in other communities across the nation, may I express to you the following observations and recommendations.

First, perhaps what is most desperately needed at the local jurisdiction level is immediate access to training, equipment and information, absent prolonged studies and protracted, layered processes.Personal protective equipment and similar emergency operations tools should be made immediately available to all of our first responders, so that our personnel will not have to attempt to breathe fresh air through their hats, as we observed New York Police Department personnel having to do on September 11th. Assignment of counter-terrorism equipment and training should be made to localities based on direct input from the communities themselves, following rapid evaluations of risks, vulnerabilities and need. In recent years, for example, the federal government has poured millions of dollars in training funds into the fire services of some communities to the point of saturation, to the exclusion of other emergency services groups in those very communities whose needs remain unaddressed. As a coordinating agency responsible for all public safety/service agencies, we should not limit ourselves to fire and police, but rather broaden our response to all agencies, including public works who play such an important role in overall response and recovery.

Secondly, it is essential that federal assets and resources be committed for planning, modeling and practical implementation for an adequate public health response to WMD events. While the Metropolitan Medical Response System and certain elements from the U.S. DHH and OPH which are contained in the DOJ Domestic Preparedness Equipment Grant Program have made their way to some communities, they have been delivered in a sealed package manner that does not easily lend the program to effective integration with state and local agencies and practitioners responsible for administration. Face-to-face communications among medical professionals from every tier of government and pre-event establishment of clear and workable protocols are essential to the successful maintenance of the public's health in times of imminent or actual threat. However, this cannot be accomplished without a clear understanding of the roles which both sectors, medical and response, play in the pre and post incident phases of any emergency. Public health must be come to the table before an incident to develop the same relationships, same networks and similar training as that of the first responders. Without shared knowledge of each system, we will continue to face these issues repeatedly. Lines of communications must clearly be opened and a dialogue must be maintained with room for expansion and future growth to address deficiencies.

Third, it is imperative to strip away some of the long-standing, irrational impediments to the meaningful sharing of intelligence information possessed by federal law enforcement and national security agencies.While I have personally observed some loosening of restrictions in our community, the best sources of

intelligence and investigative data seem still to reside with CNN and the FOX News Network. It is paramount to public safety and citizens' peace of mind that federal intelligence information be exchanged with local and state law enforcement in order to facilitate prevention and preparation before tragic consequences occur in our communities. While I certainly appreciate that some sensitive information may not be relevant to every community, and that certain matters must be safeguarded in the interest of national security, you must believe me when I tell you that following the terrorist attacks against United States citizens on American soil, the term "top secret" no longer evokes the passive acceptance and reverence it once did in our community.As much federal attention and energy must be applied to preventing terrorist acts in our community as has been committed to response and recovery in the aftermath. This will require up close and personal contact with those in authority in our hometowns.

Fourth, and finally, I am greatly encouraged by President Bush's creation of the Office of Homeland Security, and I wish to strongly urge advice to Congress and the federal agencies that will assist its duties.This office must be protected from the pitfalls that have doomed similar initiatives to failure in recent times.Most apparent should be the fate of the National

Domestic Preparedness Office, whose "one-stop shopping" blueprint represented a remarkably comprehensive and workable plan, only to fall victim to turf battles, financial war and petty, destructive jealousies at the federal level. It is vital that the President's vision does not become diluted by beltway contracts and the selfish agendas of public and private enterprises. It is critical that the mission of this Office be carried out effectively with the joint and full support of all available federal resources, while retaining the autonomy necessary for success. The President's inclusion of a crucial interface with local and state agencies must be integral in its organization, and exercised to full advantage. The body of federal knowledge, experience and assets and their value to national security are self-evident; but so should be the fact that when it comes to homeland security, the experts are, after all, "back home".

This concludes my remarks. Thank you again for the great privilege to meet with you today, and please be assured that my services and the resources of the City and Parish of East Baton Rouge are yours to command.

Beverly O'Neill, mayor, City of Long Beach, California

TESTIMONY

BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES COMMITTEE ON TRANSPORTATION AND INFRASTRUCUTURE, SUBCOMMITTEE ON WATER RESOURCES AND ENVIRONMENT HONORABLE JOHN J. DUNCAN CHAIRMAN

BY BEVERLY O'NEILL, MAYOR CITY OF LONG BEACH, CALIFORNIA

ON TERRORISM: ARE AMERICA'S WATER RESOURCES AND ENVIRONMENT AT RISK?

OCTOBER 10, 2001

Mr. Chairman and Members, thank you for the opportunity to testify.

In addition to being a Mayor of a large City, my involvement with the California League of Cities and the United States Conference of Mayors may provide a special perspective to this Subcommittee.

I am pleased to present to you today, my City's security concerns that are under the jurisdiction of this distinguished Subcommittee.

City-Wide Security

The City of Long Beach has in place, in coordination with the State of California, an emergency response plan and a hazardous material response plan, which comply with the Standardized Emergency Management System.

In 1998, Long Beach was selected under the Nunn-LugarDominici Terrorism Protection Act as one of the largest cities in the Nation, to focus on anti-terrorist training and equipping for local responders. We carried out, therefore, a Department of Defense Grant Program.

Since then, Long Beach was awarded a second, Department of Health and Human Services, anti-terrorism grant, geared to responding to a chemical and biological event.

Lastly, the Department of Justice also provided the City with a demonstration grant to purchase equipment required in dealing with a terrorist event.

Mr. Chairman, this Federal investment in Long Beach is not misplaced. Since we host America's largest Port, Boeing Company C- 17 aircraft production, as well as other aerospace industry such as Gulfstream Aerospace Corporation, we are an example of a city that has a major responsibility to provide for secure infrastructure.

However, to fully benefit from the three Federal antiterrorism grants mentioned, we find ourselves in the position of having insufficient resources to sustain the programs in the out years.

Seaport Security

The Port of Long Beach, a Department of my City, along with the neighboring Port of Los Angeles, comprise the largest seaport complex in the United States and the third largest in the world. Astonishingly, that complex now handles over 1/3 of all US cargo.

Several aspects of Port of Long Beach operations are under the jurisdiction of this Subcommittee and represent significant National security relevance; the focus of this hearing.

1. On September 11, the Port Security Taskforce was promptly activated. It coordinates National, State and local vessel security and disaster response functions.

2. As a National Port Readiness port, to assure defense related cargo throughput, the Port of Long Beach stands ready to serve emerging deployment demands.

3. The Port's general infrastructure improvement needs now take on new National security importance. We need a new bridge over a strategic Federal waterway. The I-710 Federal Highway needs reconstruction to continue carrying 35% of America's trade cargo.

4. Senator Holling's port security legislation is indeed welcome, but we are concerned that unfunded mandates would require ports to perform Federal functions without accompanying Federal appropriations.

5. The Port's proposed Intelligent Transportation System appropriations request, now before the Conferees, is meant to efficiently schedule truck travel over limited Interstate roadways. This new innovative system also serves as an efficient port security monitoring system that we now need. Thankfully it is ready to build.

Water Resources Security

Now, Mr. Chairman, about how Long Beach is protecting its water supply and also assuring its delivery, especially under emergency circumstances.

Accompanying me here today is Kevin Wattier, General Manager of the Long Beach Water Department. Mr. Wattier has overseen operations at five of our Nation's largest water treatment facilities.

The Long Beach Water Department has built and operates the Nation's largest groundwater treatment facility. We deliver an uninterrupted supply of quality water to our citizens and industry through a reservoir system of thirtythree fully enclosed tanks containing over 110 million gallons of water, 900 miles of pipeline, over 18,000 gate control valves and more than 6,000 fire hydrants. We have operated these facilities in a manner that is efficient and environmentally responsible.

Nonetheless, since September 11, we have taken a critical look at protecting our water supply and the way in which it is delivered throughout the City.

For example, we limited access to treatment and supply facilities. We eliminated information on filtration and water treatment supplied to the public through the Internet and other publications. We also intensified water sample testing for all twenty-six of the Department's wells.

While we made significant investments in new water infrastructure, due to the events of September 11, we must now balance the need to replace old infrastructure with the immediate need for security related infrastructure improvements. our security upgrades to facilities include new cameras, intrusion alarms, and perimeter maintenance. We are evaluating increases in security related staffing levels. We are assessing new water quality monitoring systems that give the earliest possible warning of water contamination events.

Fortunately, for some time now, by capitalizing on emerging technology, the Long Beach Water Department found solutions not only to meet current need, but also to fully anticipate future water security infrastructure requirements.

We completed the third year of a 20-year program to replace and reline the City's entire old unlined cast iron pipe, at a cost of $10 million per year. We are reaping the benefits of this program, as water main breaks have decreased by over 50 percent, and water quality, fire flow and water pressure are significantly improved. These actions certainly support our needed water source protection and water delivery priorities.

It is no wonder then that the gap between available funding and the costs incurred for infrastructure improvements is widening. It is evident that this funding gap will increase due to added demand occasioned by new National antiterrorism priorities. Certainly, municipal water utilities like Long Beach need Federal assistance.

Environmental Security

The City also finds that its attention to environmental security is now more compelling than ever.

The City hosts the Los Cerritos Wetlands. It is located immediately adjacent to our downtown and is, therefore, subject to degradation pressures; if not to the threat of terrorism.

We are working with the Corps of Engineers and other local and Federal agencies to enhance and protect these wetlands.

Interestingly, the Los Cerritos wetlands could have future relevance to new Long Beach water supply initiatives such as a new generation of desalinization.

FY2002 Appropriations will enable those wetlands initiatives as well as continue Federal Water Reclamation programs that have been underway for three years to protect the City's ground water supply.

Conclusion

In conclusion Mr. Chairman and Members, Congressional consideration of new security-related, critical infrastructure funding would be extremely appropriate at this time.

However, Mr. Chairman, if you would ask what immediate federal assistance Long Beach needs to help enable the foregoing security measures, I would urge, first that the Appropriations' Conferees accept Congressman Horn's and Senator Feinstein's request for $7.2 Million to fund the Advanced Transportation Information Management System. That system provides dramatically heightened port security, now especially necessary.

Secondly, in the spirit of demonstrating how to improve National infrastructure security, I would recommend that a fourth Federal anti-terrorism grant be made available to the City to be used specifically to prove-out water and environmental infrastructure security measures of significance to America.

I respectfully thank the Committee for this opportunity to appear.

Mike Parker, assistant secretary for civil works, U.S. Army

COMPLETE STATEMENT OF

MR. MIKE PARKER ASSISTANT SECRETARY OF THE ARMY (CIVIL WORKS)

FOR THE HEARING BEFORE THE SUBCOMMITTEE ON WATER RESOURCES AND ENVIRONMENT COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE

UNITED STATES HOUSE OF REPRESENTATIVES ON TERRORISM: ARE AMERICA'S WATER RESOURCES AND ENVIRONMENT AT RISK

MR. CHAIRMAN AND MEMBERS OF THE SUBCOMMITTEE:

INTRODUCTION

I am Mike Parker, for the last couple of weeks, the Assistant Secretary of the Army for Civil Works. I appreciate the opportunity to speak to you today, and I feel very much at home, having been in this room many times and seeing friendly faces with whom I previously had the honor to serve as a Member of this body.

Thank you for the opportunity to provide information on the Army Corps of Engineers activities to address the issues resulting from the events of September 11, 2001. First, allow me to say how proud I am to be associated with the Corps of Engineers, its record, and the manner in which it has begun to move out to protect the large part of America's water infrastructure that is our responsibility. I want to assure you that the Corps will prove itself worthy of the trust which that responsibility conveys.

Within two hours of the terrorist attacks on the World Trade Center, Corps employees were at ground zero lending assistance. Thousands of New York City residents were evacuated on Corps civil works vessels from lower Manhatten. We provided expert structural assessments, emergency power to get the stock market up and running and oversight for the removal of what will likely exceed 1 million tons of debris. Within hours of the attack on the Pentagon, Corps structural engineers were on site providing expert advice. We are presently conducting a comprehensive force protection analysis to make the rebuilt Pentagon safer from terrorist intervention in the future. We continue to support local and military leaders with every asset the Corps can muster.

In conjunction with its military construction mission, the Corps has developed indepth anti-terrorism/force protection (AT/FP) expertise. The Corps serves as the DoD lead for "Public Works" under the Critical Infrastructure Program established under PDD 63. The Corps laboratories and technology transfer centers were instrumental in the development of the DoD AT/FP standards now used by all Services in MILCON, major repair and other programs. These standards and the underlying technologies are being widely used by the State Department in their embassy program.

For example, we have world-class AT/FP applications engineers at our Protective Design and Electronic Security Centers who are supported by the best available research assets within the Engineer Research and Development Centers six laboratory network. Expertise available there (to the Corps and others) includes, among other things: Survivability and Protective Structures, Sustainment

Engineering, Battlespace Environment, Military and Civil Infrastructure, and Environmental Quality. We have hundreds of employees trained by them, and experience born of work on the Khobar Towers, Murrah Federal Building, World Trade Center, the Pentagon, and other sites; some well-known; others not-so-well-known. The Corps Centers and labs are supported by some of the leading AT/FP engineering and construction firms through effective contracting vehicles.

We are in the process of leveraging the expertise gained in the Corps military mission areas to protect the Corps critical water resources infrastructure from terrorist activities. Fortunately, we are not starting from scratch. Over the past few years the Corps has been working diligently with other agencies, including Bureau of Reclamation, Department of Energy, Tennessee Valley Authority, Environmental Protection Agency, and the Federal Bureau of Investigation to develop a comprehensive security assessment process to identify risks to critical facilities such as locks, dams and hydropower facilities. As the security assessments are completed we will apply the Corps (and others) AT/FP expertise site by critical site to mitigate security risks uncovered.

Today, temporary protection measures are in place, including restricted public access, increased standoff distances to critical structures, increased patrol activities, contracted additional guard support, increased coordination with local law enforcement, and establishment of early warning telephone procedures.

A civil works infrastructure management team has been established at headquarters and the field, and the Corps has begun the task of assessing the need for more specific, effective protective measures. The centerpiece of this effort is the risk assessment and protection of dams methodology called RAM-D developed by the Interagency Forum on Infrastructure Protection from the efforts early mentioned. I have with me a copy of the training material and workbooks that teams will be using over the next several months to complete this comprehensive civil works security assessment.

By using this Risk Assessment Methodology for Dams, security risks to dams and other Corps infrastructure can be assessed quickly, in a structured, systematic manner, even though the structures to be assessed have been built at different times to meet specific set of criteria and sited in unique environments. The Corps of Engineers has already put in place a plan to conduct these assessments on our critical dams and other infrastructure, and to cooperate with other agencies on still more dams. We will also cooperate on other types of structures, as requested. The lack of standardizing tools may make for a slower process, but the assessment should be no less accurate.

We are also actively involved with the Nation's leading engineering and construction industry associations, professional societies and standards writing organizations to improve the security and survivability of public and private buildings throughout the country.

The subject of this Hearing has been posed in the form of a question: "Terrorism: Are America's Water Resources and Environment at Risk?", and the answer can only be a reluctant, sobering, "Yes". Risk is everywhere, and impossible to

eliminate, entirely. However, there are many forms of risk, many ways to minimize and manage it. The Corps of Engineers has already begun the process of protecting the resources entrusted to it, and the people who work and visit there. I am proud of the Corps and confident of its ability to achieve and maintain the results demanded by the American people and their representatives in this August body.

CONCLUSION

The President, Secretary of Defense Rumsfeld, Secretary of the Army White and I are committed to providing the leadership and resources for the Army Corps of Engineers to carrying out its vital military and civil works missions in these difficult times. Mr. Chairman that concludes my statement and I would be pleased to address any questions that you or the committee may have.

Randy G. Speight, Jr., director, Chemical Emergency Transportation Center, American Chemistry Council

STATEMENT OF

RANDY G. SPEIGHT, JR. DIRECTOR CHEMICAL TRANSPORTATION EMERGENCY CENTER

on behalf of the AMERICAN CHEMISTRY COUNCIL before the HOUSE TRANSPORTATION AND INFRASTRUCTURE COMMITTEE SUBCOMMITTEE ON WATER RESOURCES AND THE ENVIRONMENT

OCTOBER 10, 2001

Mr. Chairman, Members of the Subcommittee, my name in Randy Speight. I am Director, Chemical Emergency Transportation Center, for the American Chemistry Council. The American Chemistry Council represents the leading companies engaged in the business of chemistry. Council members apply the science of chemistry to make innovate products and services that make people's lives better, healthier and safer. The Council is committed to improved environmental, health and safety performance through Responsible Care, common sense advocacy designed to address major public policy issues, and health and environmental research and product testing.

I am pleased to testify at today's hearing on critical infrastructure protection. In particular, you have asked me to address those provisions of the Superfund Amendments and Reauthorization Act that deal with emergency reporting, preparedness and response (SARA Title III).

The chemical industry is a critical-and indispensable-part of our nation's infrastructure. It is a $460-billion-a-year enterprise in the United States, the largest of its kind in the world. The industry makes thousands of products that make people's lives better, safer and healthier-from medicines to medical equipment, from the space-age materials used by the military in stealth aircraft, in aviation fuel, for night vision equipment and in satellite communications systems, to ensuring that the water we drink is clean and safe.

The industry employs more than one million men and women in the United States-in jobs that on average pay more than 25 percent above similar manufacturing jobs. The industry is creative and innovative-accounting for one in every seven patents awarded each year in the United States and, at $31 billion a year, it is the largest private-sector spender in research and development.

The industry also is an important contributor to the nation's economic security: Every other manufacturing sector-from automobiles to housing to agriculture to computers to airlines to telecommunications-depends in some way on the products of chemistry for their survival and growth. What's more, many non-manufacturing sectors also depend on the industry: The business of chemistry contributes $21.5 billion a year in revenues to the railroad, trucking companies, barge operators, and other logistics suppliers.

And the industry is the nation's largest exporter: products of chemistry are responsible for 1 of every 10 U.S. export dollars.

The chemical industry is committed not only to making products that improve people's health and standard of living, but also to ensuring the safety of our employees, customers and the people who live in plant communities and who benefit daily from our products. Our attention to safety-which has made us one of the safest manufacturing industries in the nation-extends to the security of individual manufacturing facilities. During the last decade-and especially for the last five years-our industry has paid increasing attention-and devoted increasing resources-to improving security. A number of things have contributed to our increased attention to security-and to taking steps to keep our products from being misused. These have included:

The threat of cyber terrorism.

Economic espionage against our companies.

Attempts to keep our products from being used to make illegal drugs

Attempts by terrorists to misuse our products

Our successful work with the Drug Enforcement Administration on illicit drug manufacture and with the State Department on the treaty to ban chemical weapons has contributed significantly to our increased attention to security matters.

A few years ago, we began working with the Environmental Protection Agency on developing and implementing the federal Risk Management Program. The RMP, as it is known, was created by the 1990 Amendments to the Clean Air Act. Among other things, it requires our industry and others to report publicly what we are doing to prevent accidents. The American Chemistry Council supported this program.

When we began getting ready for this important program, questions arose about whether any of the information gathered as a part of the RMP could be used by terrorists to target any of the facilities-in our industry and others-that are obligated to report under the program. The answer we received from federal law enforcement and national security experts at the FBI, CIA, NSC and Secret

Service was that terrorists potentially could use some of it, especially if it were made easily-and anonymously- available via the Internet.

Based on the recommendations of these agencies, Congress approved legislation preventing some of the RMP data-the off-site consequence analysis information- from being posted on the Internet. We continue to have concerns, however, that this information is still available in reading rooms in every state. In addition, other federal agencies have publicly available databases which may have potentially sensitive information. In light of the events of September 11, we believe that all agencies should review their public databases and remove any sensitive information, at least on a temporary basis.

Since the attacks of September 11, the chemical industry has taken a number of steps to strengthen security at our facilities. Examples of these include:

-Tightening access to facilities. This includes tighter monitoring of deliveries of materials and allowing only employee vehicles on site.

Recommending to federal law enforcement officials that they examine all licenses of all drivers of hazardous materials.

Demanding the highest standards from our shippers and carriers. For example: some companies have ordered that second drivers be added to shipments; that no truck shipments can be left unattended; and that no stops can be made between the plant and delivery; that carriers be required to conduct background security checks on their employees.

Communicating with local emergency officials and briefing them on our security efforts. We have a long and close relationship with local emergency officials - police and fire departments.

Communicating and coordinating with local emergency officials to keep up to date on their plans.

Increasing surveillance and the number of security guards at plant sites.

Conducting our own background checks.

Cooperating with the CIA in an effort to understand how our products could be used as weapons and determining how to respond.

Using our existing risk assessment tools for national security purposes.

Permitting cleaning crews to work only during business hours.

Communicating with federal officials, including the FBI to discuss ways to further improve security of our facilities.

Could anyone have been adequately prepared for the events of September 11? Every sector of our government and every industry now realize we all need to do more.

In addition to the security measures mentioned above, we have taken the following actions:

We have urged President Bush to proceed with plans to conduct a comprehensive security assessment of the chemical industry. Our industry believes it will benefit

from a comprehensive assessment conducted by appropriate federal law enforcement, national security and safety experts. While we are taking aggressive steps to make our operations more secure, we recognize that we cannot achieve this objective by ourselves. It is vitally important to forge a long-term partnership with the government to create a robust intelligence and information-sharing system between government agencies and chemical industry experts.

We hope a comprehensive assessment conducted by law enforcement and national security agencies will also help in establishing a formal information-sharing process between these organizations and our industry. Planning and actions by our industry must be based, in large measure, on what law enforcement and national security agencies tell us about threats of terrorist attacks. As we move forward, we must be assured of sustained and clear communications with these agencies. The assessment, we believe, can help achieve this objective.

We are also calling upon Congress to enact H.R. 2435, sponsored by Representatives Davis and Moran of Virginia, and S. 1456, sponsored by Senators Bennett of Utah and Kyl of Arizona. The bills will improve the ability of companies to share vulnerability data within our own membership, with other industry sectors, and with the federal government.

In addition, we are petitioning the government to officially designate our industry as a critical part of the nation's infrastructure under the Partnership for Critical Infrastructurean industry-government partnership devoted to improving security in critical sectors of the government and private industry. Among other things, the designation will provide additional effective opportunities to work with key elements of the Executive Branch in strengthening security, including the Department of Justice, Department of Defense and the Department of Commerce.

As noted earlier, within days after the attacks, we urged federal law enforcement agencies to conduct a review of all hazardous materials licenses-as a precaution. We have also urged EPA Administrator Whitman to evaluate the integrity of the system that makes the off-site consequence analysis data available. That system, of course, was developed before the September 11 attacks. Just as our industry has revisited existing security policies and actions-and revised them where necessary-we believe EPA should also revisit-and temporarily revise-its policies on the availability of this data. We believe the Agency should temporarily prevent access to this data while it conducts the evaluation, which we believe should be done with the assistance of federal law enforcement and national security agencies and the new Office of Homeland Security.

Finally, we are developing a set of management guidelines for our members as they take additional steps to strengthen security at their facilities and in the transportation of hazardous materials. The guidelines will be ready at the end of the month.

You have asked me to address The Emergency Planning and Community Right-to-Know Act of 1986 (also known as EPCRA, or SARA Title III). EPCRA requires each state to have a State Emergency Planning Committee (SERC). SERCs are then subdivided into Local Emergency Planning Committees.

Members of LEPCs include fire fighters, local public health officials, representatives from local government and the media, community groups and industry representatives. LEPCs engage in a collaborative effort for planning and responding to emergencies involving chemicals. The American Chemistry Council supported the 1986 legislation that created the LEPCs, and the industry has been actively involved in the national LEPC network. To be sure, many LEPCs would exist in name only if it were not for the involvement of our industry and its participation and support.

Emergency Response Mutual Aid Programs attest to the high level of preparedness and response within our industry. Manufacturers of products that pose a very high risk if spilled or involved in an accident have developed mutual aid agreement to provide immediate assistance in the event of an emergency. These producers have agreed that in the event of an incident involving those products, the closest capable response team will assist until the shipper or manufacturer of the product involved is able to get to the scene.

Additionally, our industry works closely with other allied trade associations to provide assistance as well. Associations such as the Chlorine Institute, the Compressed Gas Association, and others have established response programs to ensure that emergency responders at the scene of emergencies involving these products have immediate access to the needed information and expertise. There are approximately 17 of these mutual aid groups. All of these groups are activated through CHEMTREC, the American Chemistry Council's Chemical Emergency Transportation Center.

Another key element in the emergency response network are the carriers and transporters. These include trucking companies, railroads, barge and shipping lines, cargo air carriers, forwarders, terminals and others that are involved in transportation and distribution of hazardous materials. When incidents occur in transportation, they are a key resource for information and assistance because of the container vessels and vehicles that may be involved. Their expertise is often critical to successful mitigation of the emergencies involving hazardous materials.

Since September 11, much attention has been paid by the government and the nation's media to the security of our nation's transportation system-including that part of it used to ship hazardous materials. It is worth noting that these materials are critical to our nation's economy-and to the health and well-being of our people. Chlorine, for example, is used to make the water we drink safe as well as dozens of other products. Many medicines are chlorine based. Chlorine is also used to manufacture medical equipment and protective clothing. It's also used to make certain lightweight metals, such as titanium and magnesium, used in modern aircraft.

Of course, people want to know what our industry-and other industries-are doing to make sure these products are being transported safely and, importantly, what programs are in place to respond to an accidental release.

As the co-leader of the American Chemistry Council's Distribution Team, I would like to use our industry's TRANSCAER program (which stands for Transportation

Community Awareness Emergency Response) as an excellent example of one of the more important things we do to protect the public. TRANSCAER is an example of how our industry and the national network of Local Emergency Planning Committees work-and plantogether.

TRANSCAER is one of many voluntary safety programs conducted by our industry that is largely unseen by the public, but the kind of program people expect of us. TRANSCAER is a national effort- and involves not only the chemical industry, but also transportation organizations and local emergency response services. It is designed to assist communities that have major transportation routes within their jurisdictions respond to a transportation incident involving hazardous materials. Through TRANSCAER, the industry assists in planning, preparing, assessing, testing and revising a community's HAZMAT emergency response plan. Among other things, TRANSCAER is used to:

-Establish on-going relationships between industry, transportation companies and LEPCs.

Review existing emergency response plans (which are required by SARA).

Assist LEPCs in establishing a transportation advisory group to review and update emergency response plans to ensure they include a plan to handle transportation emergencies.

Assist LEPCs in implementing transportation flow studies

Assist LEPCs in revising response plans.

Review community emergency response resource and training needs.

Test response plans-and assess their effectiveness.

Another example of our industry's actions in this area is CHEMTREC. As The New York Times noted recently, CHEMTREC is a "Round-the-Clock Guard for Chemical Threats."[September 29, 2001] CHEMTREC is an acronym for Chemical Transportation Emergency Center. It is a 24hour emergency communications center and has operated as a public service of the American Chemistry Council since 1971. It provides local emergency respondersfirefighters, emergency medical personnel and law enforcement officials) with round-the clock resources for information and assistance for spills, leaks, fires, exposures and other emergencies involving chemicals and hazardous materials. CHEMTREC produced information to emergency service workers who responded to the attacks at both the World Trade Center and the Pentagon.

From an international perspective, the American Chemistry Council, through CHEMTREC, has working relationships with hazardous materials/chemical emergency centers in countries all over the world to allow information exchange and to provide information and assistance for products that may have originated outside the U.S.

In addition to its public service role, CHEMTREC also provides a service to shippers of hazardous materials-who are required by U.S. Department of Transportation regulations to have a 24-hour emergency telephone number for

shipments of regulated hazardous materials. CHEMTREC has four components: prevention, preparedness, emergency response and recovery.

Prevention. CHEMTREC works with local emergency response agencies and hazardous material shippers to assist in the prevention of incidents involving chemicals primarily through outreach and awareness of applicable regulations and safety procedures related to the transportation of hazardous materials.

Through improved understanding of the causes of incidents that have occurred through the review of their company's incident reports from CHEMTREC, shippers are able to better identify those factors that may be contributing factors to incidents. This information can help identify processes and procedures that may help in preventing incidents from occurring.

Preparedness. Preventing emergencies from occurring is everyone's top priority. In the unfortunate event that an emergency incident should occur, the key to effective mitigation is being prepared and trained to handle an incident quickly and effectively. The safety of the public and the emergency responders is of highest concern. Effective preparedness includes making sure that emergency responders have the necessary training and resources to handle incidents that are likely to occur in their communities. CHEMTREC provides outreach programs, materials and participates in exercises and drills to better prepare emergency responders to handle hazardous materials emergencies. Through the sponsorship of comprehensive hazardous materials emergency response training workshops and seminars, emergency responders from local communities as well as industry are able to learn new response skills and techniques. Additionally, by local emergency responders and industry working together through joint training and exercises, the management of actual incidents is greatly improved.

Emergency response. When an incident occurs, CHEMTREC provides immediate information and assistance. CHEMTREC maintains an extensive database of product and chemical information and has 24- hour contacts with thousands of product shippers and manufacturers that are able to provide additional technical information should it be necessary. CHEMTREC also is able to provide assistance to physicians who need information to treat victims that may have had an exposure during a chemical emergency.

In addition to the emergency information and contacts through CHEMTREC, the Council and its member companies have formed several mutual aid networks that are able to provide on scene assistance from the closest capable expert, regardless of the manufacturer of the chemical involved.

In the event of an incident involving chemical-biological materials, CHEMTREC has a working relationship with the Department of Defense Chemical Biological Defense Command and the National Response Center to ensure that information and assistance is available quickly to emergency response personnel. CHEMTREC maintains technical information and material safety data sheets on most of the known chemical agents-and provides a link to the National Response Center, which is the key link to the appropriate federal agencies for incidents involving weapons of mass destruction or chemical and biological materials.

Recovery. Hazardous materials emergencies often require site clean up and remediation. CHEMTREC also maintains a network of emergency response contractors and industrial hazardous materials teams that shippers can access for on-scene response.

Another industry initiative is our Responsible Care program. It is a condition of membership in the Council. Through Responsible Care, ACC member companies have made a public commitment to improve our industry's overall environmental and safety and health performance. The Council's Responsible Care initiative requires companies to Continually improve their health, safety and environmental performance Listen and respond to public concerns

Assist each other to achieve optimum performance, and Report their goals and progress to the public.

As part of Responsible Care, American Chemistry Council members and our partner companies are required to improve the dialogue between chemical plant facilities and their local communities. This is accomplished through a Community Advisory Panel (CAP). A CAP consists of a group of individuals who live near or around a chemical facility who meet regularly with plant management to discuss issues of mutual interest. Members include representatives of environmental groups, civic leaders, business leaders, homemakers, hourly workers, and other community representatives such as clergy, health care providers, emergency responders and educators.

There is another element of SARA whose importance in this crisis might be overlooked. That is Section 313, Toxic Chemical Release Inventory (TRI) reporting. Under this provision, companies in our industry and other in other industries report to the public on their emissions to air, land and water of more than 600 chemical products. Since 1988 the chemical industry has reduced emissions by 58% while boosting production by 18%. Since enactment of Section 313, the members of the American Chemistry Council have engaged in an ongoing dialogue with plant communities about these emissions-and steps we are taking to reduce them. Frequently, this dialogue includes discussions about plant security. Since September 11, a number of questions have been asked of our industry about what we're doing to strengthen security at our facilities. Many of these questions have come from state and local governments and, of course, from the people who live in plant communities. We are responding to those inquiries providing relevant information about our steps to improve safety and security.

Mr. Chairman and members of the Subcommittee, I hope I have provided you with useful information about the many ways in which the chemical industry reaches out to LEPCs and other plant neighbors in collaborative efforts to prevent and respond to plant or transportation emergencies of all kinds. We are continually improving our capacity to meet the new safety and security challenges which our nation faces in this time of crisis.

John P. Sullivan, Jr., chief engineer, Boston Water and Sewer Commission

October 10, 2001

Testimony

before the Subcommittee on Water Resources and Environment Committee on Transportation and Infrastructure U.S. House of Representatives on Terrorism: Are America's Water Resources and Environment at Risk?

by John P. Sullivan, Jr. Chief Engineer Boston Water and Sewer Commission on behalf of the Association of Metropolitan Water Agencies

Good morning, Chairman Duncan, Congressman DeFazio and members of the subcommittee. Thank you for hosting this important hearing.

My name is John Sullivan, the Chief Engineer of the Boston Water and Sewer Commission (BWSC) and President of the Association of Metropolitan Water Agencies (AMWA). AMWA is a nonprofit organization representing the nation's largest publicly owned water agencies that serve more than 100,000 people. These large systems provide drinking water to approximately 160 million people.

BWSC provides retail water and sewer services to residents and businesses in the city of Boston and is the largest of the 46 communities served by the water treatment and transmission system operated by the Massachusetts Water Resources Authority (MWRA). MWRA provides 230 million gallons a day of drinking water to 2.2 million people in the greater Boston area and beyond. BWSC works in partnership with MWRA to ensure that top quality drinking water is delivered uninterrupted to Boston customers.

In my testimony today, I would like to discuss our local water system security activities in addition to the activities AMWA has undertaken to enhance security of the nation's water supply systems.

National Activities

Since September 11, the nation's drinking water utilities have been on a heightened state of alert to protect against the potential disruption of water service and biological and chemical contamination of drinking water supplies. Fortunately, before September 11, the water supply community was already at work with the U.S. Environmental Protection Agency (EPA), the Federal Bureau of Investigation (FBI) and other federal agencies to develop methods and tools to protect water system facilities and consumers. This unique partnership was established in response to Presidential Decision Directive (PDD) 63 where EPA was identified as the lead federal agency for water supply and AMWA subsequently appointed as the water sectors liaison on infrastructure security.

To coordinate efforts among the various national associations, AMWA established a Critical Infrastructure Protection (CIP) Advisory Group. The EPA, FBI and the Department of Energy provide liaisons to the Advisory Group to ensure that we coordinate our efforts with the appropriate federal entities as well.

Several drinking water organizations and EPA are currently sponsoring various research and development projects addressing water system security issues. These projects include tools for assessing vulnerabilities, preparations for response and recovery in the event of an attack, understanding the impact of potential

biological and chemical agents, and training of water system personnel on security issues.

Specific projects include the following:

AMWA received a grant in late September 2001 from EPA to develop a Water Information Sharing and Analysis Center (ISAC). The Water ISAC will be a web-based tool providing threat alerts and potential vulnerabilities to water and wastewater systems. The system will also provide a mechanism for systems to report incidents for analysis. At this time, an analysis is being conducted of possible design criteria for the Water ISAC.

-The American Water Work Association Research Foundation (AWWARF) is in the last stages of developing a vulnerability assessment tool for water systems. This tool will allow water systems to conduct a risk-based, self-assessment of the physical vulnerabilities to water facilities including source water and intake, treatment plants, and the distribution system. The final project will be published in November 2001. AWWARF is also preparing a training workshop to train water systems on how to use the tool.

-EPA has begun a project to evaluate water systems emergency operation plans for the purpose of developing a guide for water systems. This guide would identify important elements, common areas, and possible best practices and provide template or boilerplate suggestions.

Association of Metropolitan Water Agencies

-EPA is also sponsoring a project to develop two contaminant transport models. One mode looks at the transportation of contaminants in rivers and streams (RiverSpill) and the second model addresses transport within water treatment plants and distribution systems (PipelineNet).

-EPA has also started a project to develop a cyber vulnerability assessment tool. This tool would allow water systems to conduct a risk-based, self-assessment of cyber vulnerabilities at water facilities including process controls, SCADA, and vulnerabilities through Internet access.

-In addition, EPA is compiling from available sources, potential chemical agents that could be used to intentionally contaminate water systems. The report is intended to help water systems understand the nature and impacts of chemical contaminants.

-CDC is developing a list of potential biological agents that could potentially be used to contaminate water systems. The report will address information on the nature of the biological agent, impacts on water systems, and human health effects.

The American Water Works Association (AWWA) is also developing training to provide an overview of water systems security issues. The course will be conducted at a number of locations.

Local Security Related Activities

On the local level, MWRA is primarily responsible for safeguarding the delivery of water to customer communities and for developing contingency plans to deal with emergency and catastrophic events that may interrupt or otherwise threaten the water supply. What follows is a brief summary of the design and operation of the regional and community water system.

The massive Quabbin Reservoir contains 412 billion gallons of raw water and is so large that water resides in the reservoir for years before reaching the transmission system. The reservoir is 17 miles long and 3 miles wide in spots. The Wachusett Reservoir contains 65 billion gallons and is 8.5 miles long by 1 mile wide. Water generally takes months to cross the Wachusett before heading to treatment and tunnels leading to metro Boston.

MWRA performs daily water testing and physical measurements before and after treatment. On a 24-7 basis, MWRA staff constantly watches water chemistry on computer screens linked to real-time testing devices. Alarms are set to notify operators when certain parameters move outside of specified ranges. All treatment chemicals are tested for purity before delivery. MWRA currently uses chlorine to disinfect the drinking water. Chlorine is an effective tool against a range of bacteria, viruses and chemicals, and MWRA can quickly change the chlorine dose if needed. Given the enormous size of the reservoirs, testing and monitoring, and treatment, experts believe it is quite impractical to successfully contaminate such a large water system.

Almost the entire MWRA system is located underground in tunnels, covered storage tanks and pipelines. Access is extremely limited. MWRA has redundant tunnels and pipes, as well as backup water supplies, and regularly trains staff on emergency response actions. MWRA closely watches water chemistry in the metro Boston area distribution network while communities' conduct weekly testing.

Prior to the profound events of September 11, MWRA was well on its way to implementing a $1.7 billion water system renovation and improvement program, including the construction of a new ozone treatment plant in Marlborough, an 18-mile long deep rock tunnel for transmission, and several covered underground storage tanks totaling 230 million gallons located throughout the service area. Major renovations to aging pipelines through community streets are also underway. All of these infrastructure improvements will include enhancements that will provide further protection of the regional water system.

Before September 11, MWRA had been carrying out clearly articulated, written strategies in its Business Plan related to emergency readiness and responsiveness and system security. Over 250 staff have been trained on the Incident Command System Standard (ICS) principles of unified command structure and resource management. Staff have identified critical facilities and events and have developed emergency response plans for key facilities. An Emergency Operations Center was in place and activated for managing significant events. Communications protocols and directories have been developed, monitoring and response protocols are in place for several significant scenarios, and simulations have been conducted. Last year, a panel of national and international experts

advised MWRA on a risk assessment approach. A security consultant prepared a report recommending additional security enhancements.

The unprecedented events of September 11 obviously brought a sense of urgency, as the term "worst case scenario" took on new meaning for the water industry. MWRA's Executive Director appointed a Task Force on Security and Emergency Preparedness and charged it with a 30-day timetable to reassess MWRA's current efforts and to develop immediate, short- and long-term recommendations in response to recent events. State Police, complemented by the National Guard, patrol key facilities and sites.

The events of September 11 have caused utilities to review their emergency preparedness plans, step up discussions with state and federal agencies, and communicate with their customers. Many things have been discussed at the congressional level that would enhance watersheds and water supply. These discussions need to continue with enactment of legislation that will help better protect our nation's infrastructures.

Next Steps

In terms of congressional action to help address system vulnerabilities,we urge you to support the following:

Physical Vulnerability Assessments for Water Systems - It is essential that vulnerability assessments be conducted for the nation's largest water supply systems. Once the assessments are completed, water suppliers can implement their recommendations, adding to the security of the nation's water supplies. AMWA is requesting that Congress appropriate $100 million for the nation's water systems so that these assessments can be largely completed next year.

Emergency Response Plan Enhancement/Development - Currently, all large water systems and many smaller water systems have emergency response or operation plans in place. These plans were developed to address mainly natural disasters, such as floods and earthquakes, and accidental events, such as hazardous waste spills. Typically, these plans don't specifically address intentional acts of terrorism, although aspects of the current plans would be invoked for all types of emergencies. AMWA is requesting that Congress appropriate $55 million for emergency response plan enhancement and development.

D Authorization of Research & Development into Understanding Threats Against Water and Wastewater Systems and Methods and Technologies to Prevent and Respond to Attacks - A substantial investment is needed for water infrastructure security R&D to address potential vulnerabilities at our nation's water systems. Research is needed to address three fundamental areas of vulnerabilities for water and wastewater systems: physical vulnerabilities including disruption of flow and contamination by chemical, biological, or radiological agents; "cyber" vulnerabilities including process control equipment, Supervisory Control and Data Acquisitions (SCADA) systems, and other information systems; and vulnerabilities associated with interdependencies with other critical infrastructure sectors such as energy, telecommunications, transportation, and emergency services. Specific areas of research needed include: vulnerability assessment

tools; technologies and processes for protecting physical assets and information and process control systems; training, education, and awareness programs; information sharing tools; demonstration projects; real-time monitoring and detection systems; and response and recovery plans.

We are asking Congress to authorize funding for water infrastructure research and development and to immediately appropriate funds for this purpose.

D Infrastructure Funding - Infrastructure funding assistance is critical. Infrastructure rehabilitation helps national security by providing better treatment, better storage, better transmission, and better distribution. In the economic stimulus package we are asking Congress to provide $5 billion for water and wastewater infrastructure to both improve our infrastructures but to also create many new jobs.

Members of the subcommittee, thank you for the opportunity to testify today. I would be happy to answer any questions you may have.