

**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**

**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 non-nuclear 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 in-house 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.<sup>1</sup>

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

---

<sup>1</sup> Brosnan, T.M. (ed.), December 1999. "Early Warning Monitoring to Detect Hazardous Events in Water Supplies," an International Life Sciences Institute (ILSI) Risk Science Institute Workshop Report, ILSI Press, Washington, DC.

in removing biological agents and biotoxins, according to studies by the Centers for Disease Control (CDC)<sup>2</sup> and the U.S. Army Combined Arms Support Command.<sup>3</sup> 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.<sup>4</sup> 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.

---

<sup>2</sup> CDC (Centers for Disease Control and Prevention), 1999. *Critical Biological Agents for Public Health Preparedness*. CDC, Atlanta, GA.

<sup>3</sup> Burrows, W.D., and S.E. Renner, 1998. *Biological Warfare Agents as Potable Water Threats*, U.S. Army Combined Arms Support Command, Fort Lee, VA.

<sup>4</sup> Wilken, R.-D., et al., 2000. "Early Warning Systems on the Rhine and Elbe in Germany," in *Security of Public Water Supplies*, R.A. Deininger et al. (eds.), Kluwer Academic Publishers, Dordrecht (the Netherlands), London, Boston.

## Water Distribution

After being treated, the water either enters the distribution subsystem directly or enters temporary storage. Numerous reports<sup>5,6,7</sup> 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.<sup>8</sup> 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 public-supply 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

---

<sup>5</sup> Clark, R.M., and R.A. Dellinger, June 2000. “*Protecting the Nation’s Critical Infrastructure: The Vulnerability of U.S. Water Supply Systems*” in *Protecting the Nation’s Infrastructure*, v. 8, no. 2.

<sup>6</sup> DeNileon, G.P., May 2001. “*The Who, What, Why, and How of Counterterrorism Issues*” in *Journal AWWA*, American Water Works Association, Denver, CO.

<sup>7</sup> Berger, B.B., and A.H. Stevenson, 1955. “*Feasibility of Biological Warfare Against Public Water Supplies*,” in *Journal AWWA*, American Water Works Association, Denver, CO.

<sup>8</sup> Krouse, M., 2001. “*Backflow Incident Sparks Improvements*” in *OPFLOW*, 27:2:1, American Water Works Association, Denver, CO.

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.<sup>9,10</sup>

## **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 than 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 accom-

---

<sup>9</sup> Lambert, J.T., 2000. "Risk Management of SCADA Systems," at *Workshop on Protecting Our Water Supply Infrastructure*, USEPA/Department of Energy, Argonne, IL.

<sup>10</sup> Ezell, B. 1998. Risks of Cyber Attack to Supervisory Control and Data Acquisition for Water Supply, Masters Thesis, Department of Systems Engineering, University of Virginia, Charlottesville, VA.

plish 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.<sup>11</sup> Surveys of water utilities indicate their greatest concern with the SCADA systems involves disgruntled employees.<sup>12</sup>

## **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.

---

<sup>11</sup> Bass, G., et al., 1982. The Appeal of Nuclear Crimes to the Spectrum of Potential Adversaries, prepared for Sandia National Laboratories, Rand Corporation Publishers, Santa Monica, CA.

<sup>12</sup> DeNileon, G.P., May 2001. "The Who, What, Why, and How of Counterterrorism Issues" in *Journal AWWA*, American Water Works Association, Denver, CO.

## **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<sup>13</sup> 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

---

<sup>13</sup>Journal AWWA, May 2001. American Water Works Association, Denver, CO.

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.

## WITNESS DISCLOSURE INFORMATION

**Witness name:** Jeffrey J. Danneels

**Capacity in which appearing:** Representative of a non-government entity

**Name of entity being represented:** Sandia National Laboratories (GOCO)

**Position held:** Manager, Civilian Surety Programs Department

**Parent organization (managing contractor):** Lockheed Martin Corporation

**Federal contract:** Management and operating contract between Sandia Corporation and U.S. Department of Energy, DE-AC04-94AL85000. FY2002 estimated cost: \$1,580,187,000; negotiated fee: \$16,300,000.

### Curriculum vitae:

Jeffrey J. Danneels is a Department Manager within the Security Systems and Technology Center at Sandia National Laboratories, a post he has held since June 1999. He is responsible for Civilian Surety programs, which include Security of large federal dams, Architectural Surety® for buildings, security of high-voltage transmission systems, and water security. Mr. Danneels was program director for the international *Innovative Technologies for Disaster Mitigation* conference (Oct '99) in Washington, DC. This three-day Architectural Surety® conference provided a forum for experts from around the world to exchange information on mitigating the consequences of natural and man-made disasters.

Prior to this position, Mr. Danneels was the Las Vegas Operations Manager for the Yucca Mountain Project site characterization activities, which include the design and installation of experiments, numerical modeling, analyses of data, and formal reporting. His responsibilities included thermal testing, thermal-mechanical testing, convergence monitoring, and rock properties testing.

From 1994 to 1997, Mr. Danneels served as department manager for Sandia's Energy and Environment Sector Office Team. Responsibilities included developing and monitoring business metrics as well as representing Sandia's Energy and Environment business unit to sponsors and various other entities, including congressional staff, , universities, and other national laboratories and institutions.

From 1989 to 1994, Mr. Danneels served as Sandia's department manager for the Facilities Accelerated System Team, which was responsible for developing and deploying a process to rapidly install complex equipment in ultra-clean-room environments. He was the responsible manager for construction projects that include Sandia's Explosives Components Facility, Strategic Defenses Facility, and Technology Development Center. In this capacity, Mr. Danneels pioneered innovative performance-based contracts to greatly shorten the Architectural/Engineering firm selection process for line-item projects.

Mr. Danneels joined Sandia in 1985. He holds a Masters of Management from the University of New Mexico, a Masters of Science in Civil Engineering from Louisiana State University, and a Bachelor of Science in Civil Engineering from Michigan State University.

Mr. Danneels has received several significant honors for his work at Sandia, including three Sandia President's Quality Awards and, most notably, an Employee Recognition Award in 1998 for the early completion of the installation phase of the Drift Scale Test on the Yucca Mountain Project, the largest in-situ rock thermal test in the world. The success of this project was noted by the chairman of the Nuclear Regulatory Commission in a letter to the United States Congress.