THE CIP REPORT

CRITICAL INFRASTRUCTURE PROTECTION PROGRAM VOLUME 6 NUMBER 4

OCTOBER 2007

WATER SECTOR

This month's edition of *The CIP Report* is focused on the Water Sector. The Water Sector, which includes drinking water and waste water assets, provides 84% of the U.S. population with potable water, includes 160,000 public drinking water utilities and more than 16,000 waste water utilities, and is under the guidance of the Safe Drinking Water Act and the Clean Water Act. This vital sector, working with the Environmental Protection Agency (EPA), its Sector Specific Agency, released its Sector-Specific Plan in May of 2007.

We are pleased to feature an interview with Ben Grumbles, the Assistant Administrator for Water at the EPA on security risks faced by the Water Sector and EPA efforts to reduce this risk. In addition to this interview, we have excerpted key pieces of the Water Sector-Specific Plan to provide background into the Water Sector's profile and goals, highlighted the Water Information Sharing and Analysis Center's (WaterISAC) security and preparedness services, as well as overviewed the EPA's Environfacts Data Warehouse, which contains data on drinking water, wastewater, hazardous waste, toxic releases, air emissions, radiation, land clean-up, and other issues of environmental interest. We also included information on cybersecurity training for the Water Sector, and a recent tabletop exercise on energy-water interdependencies. In addition to these pieces, we have included some CIP Program research into ownership of the Water Sector infrastructure, as well as a mapping and visualization project that will provide tools showing how sectors organize, assess risks, and identify owners/operators, interdependencies, partners, and authorities.

The CIP Program is also pleased to announce the release of the Pandemic Monograph, which is highlighted in this issue and now available on the CIP Program website. In addition to information on this newly released monograph, we also include an invitation to a forthcoming event co-hosted with St. Mary's Center for Terrorism Law at the National Press Club in Washington, D.C. on November 15-16, 2007.

As always, we thank you for your continued support of the CIP Program.

Interview with
Benjamin H. Grumbles, Assistant Administrator for Water U.S. Environmental Protection Agency
May 2007

Q: What security risks do water and wastewater utilities—the water sector—face?

A: We categorize the various risks that the water sector faces into vulnerabilities, consequences, or the threat of an attack. Drinking water utilities can be vulnerable to a variety of attacks through physical assault, intentional contamination, and cyber intrusion. As for consequences, an attack, or in some instances even the threat of an attack, could seriously jeopardize the public health, economic vitality, and the general functioning of a community. Determining contamination threats to the water sector remains a challenge. However, the Environmental Protection Agency (EPA) is continuing to work with the U.S. Department of Homeland Security (DHS) and others within the intelligence community to analyze these threats. In addition to terrorist threats, our office also considers the value of an all-hazards approach to preparedness. Hurricanes Katrina's and Rita's devastation speaks directly to the need for improved response capabilities that can be used for both terrorist incidents and natural disasters. This helps encourage utilities to take action in this area—a water or wastewater utility may not consider terrorism to be a likely threat, but the very real need to prepare for hurricanes, earthquakes, or power outages may resonate strongly with that utility.

Q: How is EPA reducing risk to the water sector?

A: The approach to water security has been evolving, starting with risk identification and moving towards risk reduction. The Bioterrorism Act of 2002 mandated that large utilities conduct vulnerability assessments and certify the updating of emergency response plans. Utilities have largely complied with the Act's requirements, and many within the sector have begun to reduce their risks. The progression to risk reduction occurs as we are moving past statutory requirements towards a voluntary basis for improving security. If a utility's water security program ends with the preparation of a vulnerability assessment, then it has reduced its risk only to a modest degree. We must encourage utilities to take the next critical step—adopting security measures that will reduce high risks identified by a vulnerability assessment. Therefore, our programs must appeal to all utilities, regardless of any given utility's perception of the security threat to its operations.

A robust security program will enable utilities to prepare for an array of serious events, not only for terrorism. This distinction is critical; otherwise, security programs will be viewed as competing for limited resources with other equally important demands, such as addressing aging infrastructure or ensuring regulatory compliance. At EPA,

Benjamin H. Grumbles was confirmed by the United States Senate on November 20, 2004, as Assistant Administrator for Water at the U.S. Environmental Protection Agency. Prior to that Ben served as Deputy Assistant Administrator for Water and Acting Associate Administrator for Congressional and Intergovernmental Relations.

Before coming to EPA in 2002, Mr. Grumbles was Deputy Chief of Staff and Environmental Counsel for the Committee on Science in the U.S. House of Representatives. He also served for over 15 years in various capacities on the House Transportation and Infrastructure Committee, including Senior Counsel for the Water Resources and Environment Subcommittee. From 1993 to 2004, he was an adjunct professor of law at the George Washington University Law School.

(Continued on Page 3)

Grumbles Interview *(Cont. from 2)*

we are working with our partner organizations in the water sector to identify multiple benefits to show how security programs can complement, instead of compete with, other priorities. These partner organizations include water and wastewater industry associations, state drinking water programs, and laboratory associations.

Q: What are EPA's challenges to reducing risk to the water sector?

A: The Bioterrorism Act's mandate to utilities to prepare vulnerability assessments was a one-time only requirement. Also, the law did not apply to utilities serving fewer than 3,300 people and to wastewater utilities of any size. There are no other requirements for water and wastewater utilities to improve security or reduce risk. It is important for all utilities, regardless of size, to participate in the nation's efforts to protect its critical infrastructure. Many utilities have undertaken risk assessments voluntarily, a clear signal of their commitment to fully serving their communities.

Some drinking water systems that completed their vulnerability assessments have predictably asked, "we have identified our weaknesses, now what do we do?" While completing a vulnerability assessment is an important step, an awareness of threats, vulnerabilities, and consequences has not always translated into preparedness. One of the challenges we face, therefore, is not only raising awareness within the sector, but defining what it means to be prepared, so as to transform awareness into action. Along the same lines, water sector representatives have expressed the need for clear expectations as to what constitutes an effective security program so that they can justify and obtain the resources needed to improve security and preparedness.

Another challenge for utilities is navigating the multi-organizational system that has emerged over the last several years to enhance preparedness and response. This includes a rigorously structured incident management system for improving the response to incidents at local, state, and federal levels. But with new acronyms to learn, and with new organizations emerging, the uninformed water utility can easily find itself on the outside of such structures. This could be problematic should some significant incident occur.

One more challenge involves the shared responsibility among utilities, responders, associations, public health agencies, the government, and others in improving security and preparedness. In general, without help from its partners, no organization acting alone can achieve the desired outcome of reducing risk. Indeed, partnerships are absolutely a key factor to success--not only due to the size and diversity of the sector, but also due to the voluntary nature of the effort.

Q: Is EPA working toward an overall strategy for improving water security?

A: Yes - one of our current priorities has been working in close collaboration with the Water Sector Coordinating Council to develop the water Sector Specific Plan. DHS convened these Sector Councils, which for our sector represents drinking water and wastewater utilities and their associations, in part to serve as focal points of input to the federal government's homeland security efforts. The final sector plan will establish specific sector goals and objectives that will guide our collective efforts in implementing the strategy of the National Infrastructure Protection Plan (NIPP).
To gauge our success at improving water security, we are developing national aggregate measures, which are required by the NIPP, to assess the water sector's progress. This task involves many challenging issues, which we are addressing with utilities and other key stakeholders.

Q: What is EPA's approach to working with the water sector?

A: Partnerships are critical to our mission, so EPA and other federal agencies are using the Federal government NIPP "Partnership Model" to ensure the federal government coordinates with federal, state, and local government entities as well as with private/public sector partners. Our goal is to ensure critical infrastructure owners and operators be prepared to prevent, detect, respond to, and recover from man-made and naturally occurring incidents. The NIPP Partnership Model led to the creation of Sector and Government Coordinating Councils. DHS convened these Sector Councils, which for our sector represent drinking water and wastewater utilities and their associations, to serve as focal points for input to the federal

(Continued on Page 17)

Water Sector-Specific Plan (SSP) Excerpts

Below are select excerpts from the Water SSP. The full SSP is publicly available at http://www.dhs.gov/nipp.

Executive Summary

The drinking water and wastewater sector (Water Sector) is vulnerable to a variety of attacks, including contamination with deadly agents and physical and cyber attacks. If these attacks were to occur, the result could be large numbers of illnesses or casualties or denial of service that would also affect public health and economic vitality. Critical services such as firefighting and health care (hospitals), and other dependent and interdependent sectors such as energy, transportation, and food and agriculture, would suffer negative impacts from a denial of Water Sector service. In collaboration with the entire sector, a broad-based strategy to address security needs is being implemented. This work includes providing support to utilities by preparing vulnerability assessment and emergency response tools, providing technical and financial assistance, and exchanging information. (p. 1)

Sector Profile and Goals

For decades, owner/operators of Water Sector assets have developed and improved plans to respond to manmade and natural disasters. Recently, either voluntarily or by legislative mandate, utilities have conducted risk assessments. Based on the findings of those assessments, owner/operators have created or updated emergency response plans (ERPs) and implemented security enhancements.

EPA's Water Sector Security Mission is to provide national leadership in developing and promoting security programs that enhance the sector's ability to prevent, detect, respond to, and recover from terrorist attacks, other intentional acts, natural disasters, and other hazards (the all-hazards approach). (p. 13)

Because almost all drinking water and most wastewater programs are delegated to the States, EPA must work with them to ensure implementation of programmatic and security-related initiatives. In addition to Federal programmatic responsibilities, States also have their own initiatives and priorities. The State programs maintain inventories of drinking water and wastewater facilities, regularly inspect these utilities, provide technical assistance, maintain laboratory and operator certification programs, and monitor compliance by reviewing analytical results. States review and approve plans and specifications for new and expanded drinking water and wastewater facilities, and take enforcement actions as needed.

The Water Sector GCC enables interagency and cross-jurisdictional coordination. It is composed of representatives from various levels of government-Federal, State, territorial, tribal, and local. The GCC was formed in January 2005 and meets as needed. Members include representatives of EPA, DHS (FEMA), DoD (USACE), DOI (BuRec), FERC, DOS, HHS (CDC and the Office of Public Health Emergency Preparedness), USDA, ASDWA, and ASIWPCA. The Water Sector's GCC coordinates strategies, activities, policies, and communication across government entities. The WSCC and GCC work together to coordinate sector CIP activities. (p. 31)

The academic and research center communities play important roles in enabling national CI/KR protection and implementation of the NIPP, including:

- Supporting research, development, testing, evaluation, and deployment of CIP technologies;
- Analyzing, developing, and sharing best practices related to CIP efforts;
- Preparing or disseminating guidelines, courses, and descriptions of best practices for physical and cyber security;
- Developing and providing suitable security risk analysis and risk management courses for CIP professionals; and
- Conducting research to identify new technologies and analytical methods that can be applied by security partners to support CIP efforts. (p. 31)

(Continued on Page 5)

Water SSP *(Cont. from 4)*

Vision Statement for the Water Sector

The Water Sector's Security Vision is a secure and resilient drinking water and wastewater infrastructure that provides clean and safe water as an integral part of daily life. This Vision assures the economic vitality of and public confidence in the Nation's drinking water and wastewater through a layered defense of effective preparedness and security practices in the sector.

Water Sector Overarching Strategic Goals and Supporting Objectives

Goal 1: Sustain protection of public health and the environment.

- **Objective 1:** Encourage integration of security concepts into daily business operations at utilities to foster a security culture.
- **Objective 2:** Evaluate and develop security-related surveillance, monitoring, warning, and response capabilities to recognize risks introduced into Water Sector systems that affect public health and economic viability.
- **Objective 3:** Develop a nationwide laboratory network for water quality security that integrates Federal and State laboratory resources and uses standardized diagnostic protocols and procedures, or develop a supporting laboratory network capable of analyzing security threats to water quality.

Goal 2: Recognize and reduce risks in the Water Sector.

- **Objective 1:** Improve identification of vulnerabilities based on knowledge and best available information, with the intent of increasing the sector's overall security posture.
- **Objective 2:** Improve identification of potential threats through sector partners' (water utilities; national associations; and Federal, State, and local governments) knowledge base and communications with the intent of increasing overall sector security posture.
- **Objective 3:** Identify and refine public health and economic impact consequences of manmade or natural incidents to improve utility risk assessments and enhance the sector's overall security posture.

Goal 3: Maintain a resilient infrastructure.

- **Objective 1:** Emphasize continuity of drinking water and wastewater services as it pertains to utility emergency preparedness, response, and recovery planning.
- **Objective 2:** Explore and expand implementation of mutual aid agreements/compacts in the Water Sector. The sector has significantly enhanced its resilience through agreements among utilities and States; increasing the number and scope of these will further enhance resiliency.
- **Objective 3:** Identify and implement key response and recovery strategies. Response and recovery from an incident in the sector will be crucial to maintaining public health and confidence.
- **Objective 4:** Increase understanding of how the sector is interdependent with other critical infrastructure sectors. Sectors such as Public Health and Emergency Services are largely dependent on the Water Sector for their continuity of operations, while the Water Sector is dependent on sectors such as Chemical and Electricity for continuity of its operations.

Goal 4: Increase communication, outreach, and public confidence.

- **Objective 1:** Communicate with the public about the level of security and resilience in the Water Sector and provide outreach to ensure the public's ability to be prepared and respond to a natural disaster or manmade incident.
- **Objective 2:** Enhance communication and coordination among utilities and Federal, State, and local officials and agencies to provide information about threats.
- **Objective 3:** Improve relationships among all Water Sector

(Continued on Page 14)

WaterISAC: Security and Preparedness for the Water Sector

WaterISAC, the Water Information Sharing and Analysis Center (www.WaterISAC.org), is a highly secure online subscription service that gathers sensitive information and intelligence from numerous sources and then quickly assesses and disseminates it to subscribing drinking water and wastewater utilities through a secure portal.

A repository for water security data, WaterISAC serves as a resource for education on water security topics, a contact point for resources beyond the world of utilities, and a secure library tailored to the needs of the water sector. WaterISAC centralizes the security resources that water personnel rely on, making it easier and faster to find the information they need to keep their utilities safe and secure.

WaterISAC offers its subscribers unique access to information, intelligence, data, and resources in one convenient, secure portal. Rather than simply reposting various alerts and bulletins, WaterISAC analysts gather, assess, and then quickly disseminate critical information with detailed analysis that specifically shows how certain threats could impact water utilities.

Whether a water system is in jeopardy due to a terrorist threat or inoperable due to a natural disaster, utility managers can obtain from WaterISAC the best information to develop defenses or to address consequences. When time is critical and lives are at stake, circumstances may not wait for a call from a state primacy agency, City Hall, or even law enforcement agencies. WaterISAC provides an immediate source for the essential tools that drinking water and wastewater utilities require in these extraordinary circumstances.

WaterISAC's goal is to communicate information to utilities as close to real-time as possible. The Department of Homeland Security (DHS) and the U.S. Environmental Protection Agency (EPA) are the primary sources of federal security threat notifications for the water sector, and both rely on a variety of official and unofficial networks to disseminate this information. And, while the information delivered through these channels may eventually reach local water utility management, DHS and EPA know that the most direct route to water systems is via the water sector itself. This is why the water sector established WaterISAC.

Federal agencies have many clients for their security information, but WaterISAC has only one client: the water utility community. Analysts at WaterISAC sort through a mountain of data from a myriad of sources and share with utilities online and via e-mail only what is relevant to water security. WaterISAC also offers a free, basic service that disseminates notifications from EPA and DHS that focus on water security.

Communication is equally critical in the event of natural disasters, and WaterISAC can provide the most useful information to address preparedness, response, and recovery – with speed and accuracy that can literally save lives. Software developed for anti-terror assessments can be used to inventory infrastructure vulnerabilities from natural threats as well. Lessons learned from events like the August 2003 blackout provide a wealth of information on interdependencies and recovery. If a natural disaster results in a contamination event, there are a host of resources on microbial and chemical contaminants and how to deal with them.

WaterISAC tracks not only physical incidents and trends, but also cyber issues that may impact the water sector's ability to carry out normal operations. Supervisory Control and Data Acquisition (SCADA) systems are often used in the water industry,
(Continued on Page 7)

WaterISAC *(Cont. from 6)*

and manual backup systems may or may not be in place. It is essential that water utility managers be informed of threats to cyber systems as soon as they are known. WaterISAC rapidly communicates threat information that may affect SCADA systems as well as threats to utility business systems.

WaterISAC takes every precaution to ensure the portal remains secure from any unauthorized access. The online operation is hosted inside a government-designated "top secret" security clearance facility. The system is further protected by state-of-the-art cyber security provisions that are constantly monitoring for unauthorized login attempts or breaches of the system.

Incidents are reported directly through the secure portal. Allowing subscribers to report incidents facilitates a nationwide forum for sharing information and raises the awareness of the entire sector. While water utilities may learn of threats against them from federal or state sources, the utilities themselves are often the first to learn of a security incident, either due to monitoring or even through direct communication from a terrorist. In such cases, the ability to quickly reach the proper authorities is essential. WaterISAC maintains updated contact information for the FBI, EPA's emergency operations center, state homeland security agencies, and other authorities.

Training is a vital element in a sound security plan, and

(Continued on Page 14)

WaterISAC Services for the Water Sector

Rapid Alert Notification – 24/7

WaterISAC works around the clock with federal government, intelligence, as well as public health and environmental agencies to gather, analyze, and electronically disseminate potential or actual threats to the nation's water sector.

Enhanced Security

With access to white papers and highly classified intelligence, WaterISAC is among the first resources in the nation to receive early warnings of physical, contamination, and even cyber threats. During an emergency, WaterISAC subscribers can then take quick action to reduce or even prevent damage or injuries.

Expert Water Sector Analysis

Raw information about security threats distributed directly by law enforcement and government agencies often fails to provide comprehensive details that explain how such threats impact drinking water or wastewater systems. WaterISAC analysts have government security clearances and are experts in intelligence collection and assessment, providing detailed and often unique intelligence that clearly identifies trends and explains how threats may impact the water sector. WaterISAC analysts even provide subscribers with suggested mitigating security actions.

Secure Information Exchange

Through a secure online portal, WaterISAC has created a nationwide network of drinking water and wastewater utilities that have a forum for sharing and discussing sensitive information and intelligence. Reporting incidents and reviewing posted threats and hazards is one way that water utilities can collectively raise awareness, keeping utility managers and engineers better prepared.

Comprehensive Resources

Information on various contaminants, threats, and hazards comes from a wide range of sources. However, WaterISAC subscribers have access to an extensive and centralized database of chemical, biological, and radiological contaminants, and related information. Plus, reference tables help utility managers and chemists quickly find the information needed to address threats. WaterISAC also helps utilities complete and continually improve their vulnerability assessments as well as their emergency preparedness and response plans. Reducing your utility's vulnerabilities and increasing your utility's preparedness can mean less disruption of service when a disaster strikes.

More information is available at www.WaterISAC.org.

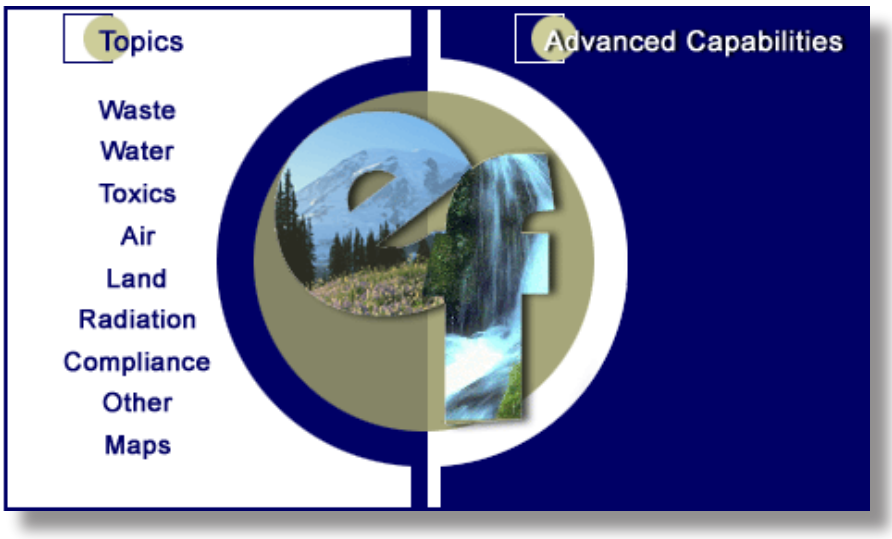
Infrastructure Information Available Through Environmental Protection Agency Resources

The vast number of useful resources available on EPA's website lends significantly to expanded knowledge of the Water Sector. The general infrastructure information offered in its public databases is invaluable as entities such as the CIP Program study the composition of the nation's Critical Infrastructure/ Key Resources (CI/KR) sectors. An overview of these EPA resources, particularly the Permit Compliance System (PCS), is found below.

EPA's Envirofacts Data Warehouse, contains data on drinking water, wastewater, hazardous waste, toxic releases, air emissions, radiation, land clean-up, and other issues of environmental interest. With regard to water, wastewater facility information housed in PCS complements data available in the Safe Drinking Water Information System (SDWIS) and the National Drinking Water Contaminant Occurrence Database (NCOD). Envirofacts also offers data on drinking water microbial and disinfection byproducts through its Information Collection Rule (ICR).

For over two decades, PCS has "served as the official national information system used for management of the [National Pollutant Discharge Elimination System (NPDES)] program," which regulates facilities in accordance with the Clean Water Act. Specifically, as noted on PCS's website, it "provides information on companies which have been issued permits to discharge waste water into rivers." Its website allows the public to query PCS databases for information ranging from facility names and geographic locations (addresses as well as longitude and latitude coordinates) to standard industrial classifications to permit types and permit dates of issuance and expiration. As an added environmental consideration, data on types of chemicals used at various facilities are available. PCS also houses information on related laws and regulations.

Information found through a PCS customized query was essential in the development of meaningful statistics for the wastewater subsector as part of the CIP Program's Sector Mapping Project. The customized query function allowed researchers to easily gather information on facility names, EPA Region assignment, and, most importantly, types of ownership. Moreover, data included in the PCS's databases is comparatively up-to-date, and a current transition of data to EPA's Integrated Compliance Information System for NPDES (ICIS-NPDES) will further enhance access to such information in a consistent format that better meets the needs of the NPDES program and database users. Notably, Enforcement & Compliance History Online (ECHO) offers data drawn from both PCS and ICIS-NPDES and allows users to explicitly select one source or the other as information continues to transfer to the new system.



Pertinent water data may also be found in additional EPA resources such as Clean Watersheds Needs Survey (CWNS) databases and the Federal Registry System, but recent data may not be as readily available in the public domain or address as broad wastewater categories as PCS. Beyond traditional databases, EPA's *EnviroMapper* allows for interactive, geographic mapping of facilities listed in the many elements of the Envirofacts Data Warehouse. ❖

Cybersecurity Training for Water Infrastructure – WISE Up!

By Christine Pommerening

Everyone interested in cyber security for utilities has probably seen the video released on September 26, 2007 by now – a diesel-electric generator stalling and going up in smoke after a simulated hacker attack exploits a programming vulnerability in its control system. For the water security community, the case of an insider using SCADA system knowledge to cause a pump station failure in Australia in 2000 was equally disturbing. But while such dependence of physical assets on cyber systems is widely known, it is still little understood, especially on the plant operator level. Given that the design of most SCADA systems and PCS components are beyond the control of owners and operators – what can be expected of the average utility's personnel to protect the water infrastructure from cyber attacks? To answer this question, a look at the training materials and security guidances for water and wastewater utilities is instructive.

Within the widely-distributed Water Infrastructure Security Enhancements (WISE) curriculum for wastewater/stormwater utilities, cyber security is addressed within the "Management" module (Operations and Design being the other two, plus an introductory module.) The management responsibilities include considerations of policies, risk assessment, cyber security, communications, and training. The section focuses on threats, methods, and consequences from cyber intruders, and the operational practices to defend against them. Intruders are categorized as outside hackers, outside attackers, and inside attackers. Methods addressed are hacking via the Internet or the SCADA network modem, interception of radio transmission, and unauthorized insider access. Consequences listed range from physical process malfunctions to data manipulation to identity theft. The policies and procedures recommended are:

- Post security policies in control room,
- Require system logon, pass words, and specify user privileges based on responsibility level,
- Create an audit trail for changes,
- Reset all passwords away from default,
- Back up information on a daily basis,
- Control access to cabinets and rooms, and
- Restrict access to cyber systems.

The training then specifies 22 operational practices, such as disconnecting unnecessary connections, including numbers and letters in passwords, and restricting sensitive data to appropriate personnel. Finally, it is suggested to perform a cyber vulnerability analysis that estimates the dependence on SCADA, the capability to operate in manual mode, connectivity and remote access profiles, and password policies. Looking at this training module alone, the cyber security approach on both management and operational levels does not seem very sophisticated. Yet time and again, empirical evidence suggests that it is the violation of such basic rules as having strong passwords or making sure a laptop is not taken off the premises that causes the most serious breaches in cyber security.

The true strength of the WISE approach is not so much the technical detail (the cyber security session makes up far less than 10% of the overall training) but the embeddedness of cyber security in a larger process. WISE is a cooperative effort between the American Water Works Association (AWWA), the Water Environment Federation (WEF), the American Society of Civil Engineers (ASCE), with the findings of the EPA, who devised the training program's approach to enhance security in their respective areas of water infrastructure. In phase one, three interim voluntary security guidance documents were developed and completed in December 2004. Phase two consisted of the preparation of training materials that were released in July 2005. They were designed as one-day courses in which the seven sections of the guidances were combined into four modules: Introduction, Managing for Reduced Risk and Cybersecurity, Operational Considerations and Emergency Response, and Design Considerations for Reducing Risk and Electric and Electronic Security Devices. In phase three, an ANSI-accredited standards process was used to publish two "Guidelines for the Physical Security" for water and wastewater/stormwater utilities,

(Continued on Page 14)

Exercising for Improved Preparedness and Response

In order to help gauge preparedness and simulate response, sectors regularly conduct exercises, often via workshops and tabletops. Stakeholders in the Water Sector, for example, conducted a tabletop exercise on energy-water interdependencies from April 24-25, 2007. As noted on the exercise's dedicated website (http://www.seenergywater.govtools.us/), the Southeast Energy-Water Interdependence Exercise, named Black Water, was held with the following objectives in mind:

- Increase participant understanding of the interdependencies between the energy sector and the water supply and waste water management systems,
- Identify in a scenario setting, the potential secondary impacts associated with disturbances in those water services,
- Assess current communication procedures and interaction between the electricity and water sectors,
- Identify opportunities for increased collaboration between the electricity and water sectors to identify measures for reducing impacts of electricity outages and facilitating effective response, and
- Educate participants about energy assurance planning, including the use of State Energy Assurance Guidelines, to test state plans' legal and regulatory energy emergency response authorities and approaches and identify differences and potential problems.

Attendees were given a scenario "that reflect[ed] sectoral, geographic, and jurisdictional interdependencies inherent in the region's energy and water infrastructure." Held in Decatur, Georgia, Black Water's geographic focus centered on the Southeast region of the United States, with many participants hailing from metropolitan Atlanta area utilities. Active participation in Black Water aided stakeholders in assessing state and local emergency planning, improving broader understanding of interdependencies between electric and water infrastructures, and enhancing decision-making in emergent situations.

In addition to information garnered during exercise discussion, attendees received various supporting information. Black Water's website offers links to some of this information, including EPA's Water Security and "14 Features of Active and Effective Security" webpages, the American

(Continued on Page 15)

14 Features of Active and Effective Security

Organizational

- Explicit commitment to security (#1)
- Promote security awareness (#2)
- Defined security roles and employee expectations (#5)

Operational

- Vulnerability Assessment (VA) up-to-date (#3)
- Security resources and implementation priorities (#4)
- Contamination detection (#7)
- Threat-level based protocols (#10)
- Emergency Response Plan (ERP) tested and up-to-date (#11)
- Utility-specific measures and self assessment (#14)

Infrastructure

- Intrusion detection and access control (#6)
- Information protection and continuity (#8)
- Design and construction standards (#9)

External

- Communications (#12)
- Partnerships (#13)

Source: EPA, http://cfpub.epa.gov/safewater/watersecurity/14features.cfm

Visualizing Critical Infrastructure Sectors

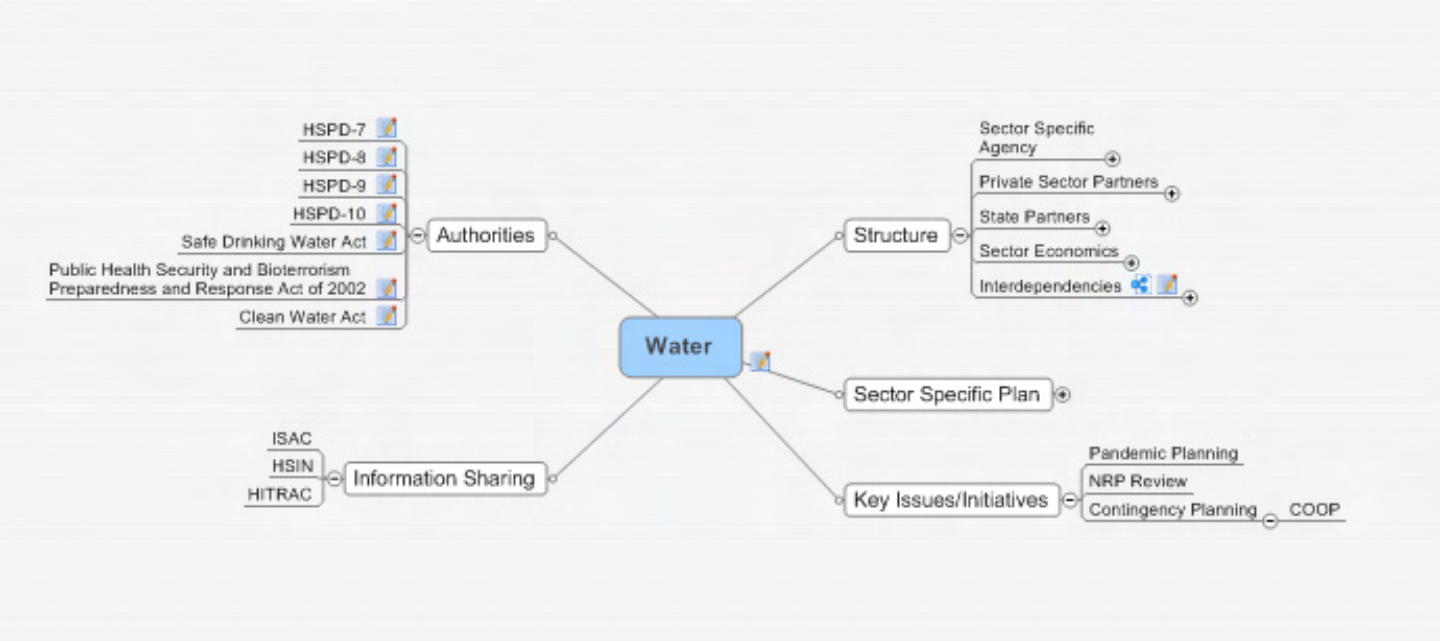
By James Creel

Given the extensive scope and diversity of critical infrastructures in the United States, it is difficult to capture the many aspects of each sector, let alone compare sectors along common dimensions. In particular, there is no central repository for this information, and little visualization of entities and relations beyond long texts and tables. The data, however, could potentially be much more informative if combined in a logical map.

As a result, the CIP Program has sought a better and more interactive way to visualize the critical infrastructure and key resource (CI/KR) sectors. Using Mindjet Manager software, its researchers are creating sector maps. These maps are, in essence, snapshots of each of the 17 CI/KR sectors as defined by the U.S. Department of Homeland Security (DHS).

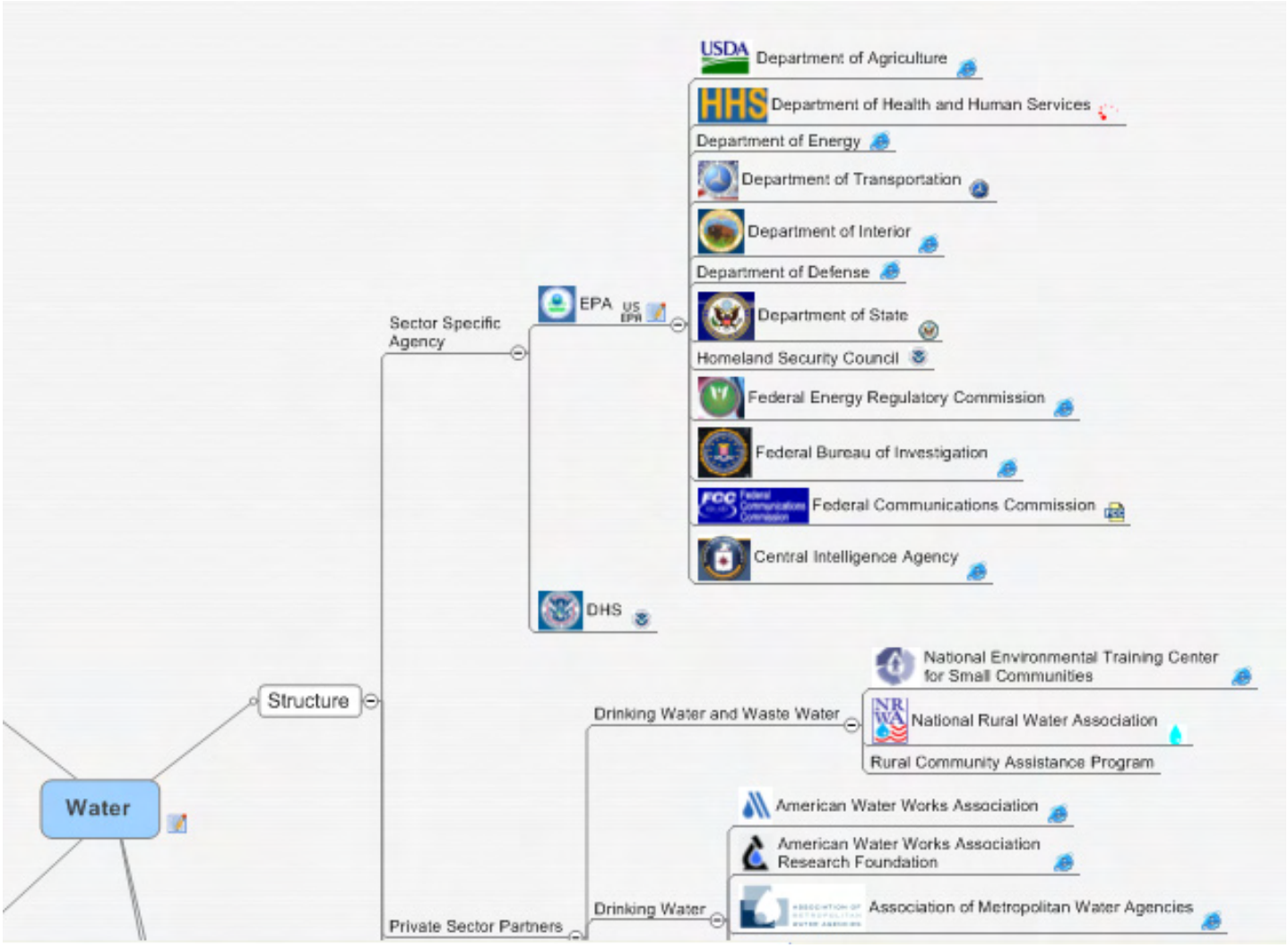
Mindjet allows the user to visually organize and manage information. Through the CIP Program's Sector Mapping Project, the sector maps offer a blueprint of how each sector is structured, how it assesses risks, etc. Each map identifies assets, owner/operators, interdependencies, Federal, State, and local partners, and authorities. Sector economics and statistics are also included in each map.

In clearly organizing information and visualizing the many facets of each sector, these maps can serve as valuable tools for industry experts at both the public and private level. The majority of sector information is disparate and available through countless sources. The Sector Mapping Project allows those with an interest in sector attributes to view this information at a single glance. In addition to this descriptive dimension, the analytical value lies in identifying missing data categories, visualizing commonalities and differences between sectors, and better understanding sector interdependencies on physical, functional, and governmental levels.



(Continued on Page 12)

Visualization *(Cont. from 11)*



Each map has the format of a flow-chart or organizational chart that allows the user to select particular topics of each sector and either collapse or expand the available information.

For instance, expanding a particular branch of the map allows the user to view more information such as notes fields, hyperlinks to other Mindjet maps and websites, and attachments to various reference materials and government documents.

Each Sector-Specific Plan (SSP) that has been made available to the public will be used in creating sector maps with the Mindjet software. Information collected from sector organization websites, operated by both public and private entities, has yielded much information as well. Using public sources, CIP Program researchers will continue to compile relevant information that helps further define the structure and components of each sector.

The Banking and Finance, Nuclear, Oil and Natural Gas, and Water Sector snapshots are nearing completion. As each sector map is completed, it will be available for download on the CIP Program's Sector Mapping Project webpage, located at: http://cipp.gmu.edu/research/SectorMappingProject.php. ❖

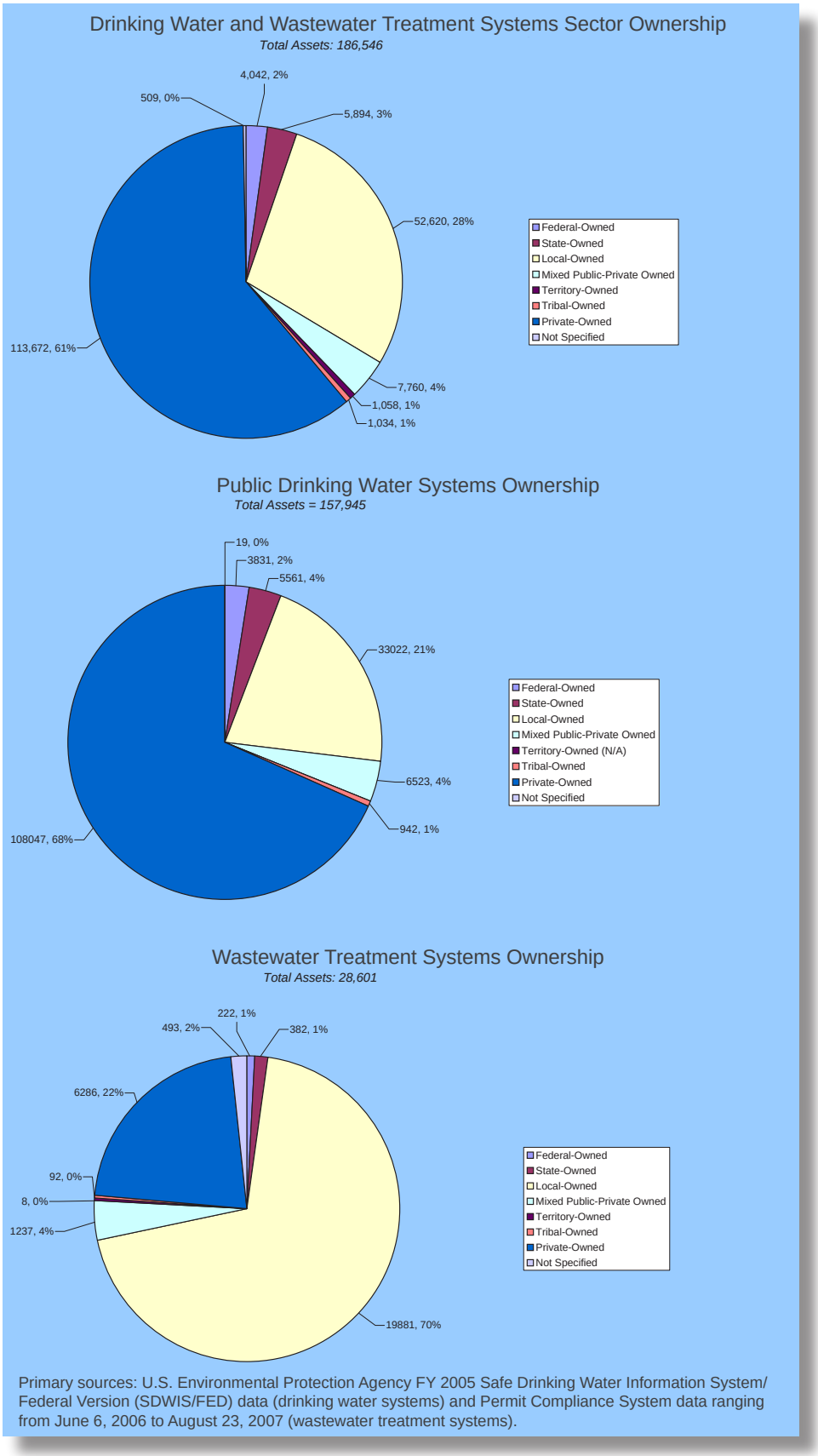
Ownership of Water Sector Infrastructure

While it is a commonly-accepted assertion that approximately 85% of critical infrastructure is owned and/or operated by the private sector, the specific percentage of type of ownership may vary between the 17 critical infrastructure and key resource (CI/KR) sectors. For instance, one would naturally assume that the ownership of infrastructure within the Government Facilities Sector favors the public sector and that ownership of assets within the Commercial Facilities Sector is predominantly private. To better understand select sectors and their components, CIP Program researchers have analyzed the ownership of various infrastructures as part of the Sector Mapping Project.

Taking a closer look at infrastructure within the Drinking Water and Wastewater Treatment Systems Sector (Water Sector), researchers identified type of ownership for over 185,000 drinking water and wastewater treatment systems using numerous data sources and cross-tabbing of information. Types of ownership include: Federal, State, Territorial, local, tribal, private sector, and mixed public-private sector. The ownership of a small number of systems was categorized as "not specified," meaning that the original data source labeled it as such and that researchers could not ascertain ownership type beyond a reasonable doubt.

As expected for the Water Sector, the majority of assets were either

(Continued on Page 15)



Primary sources: U.S. Environmental Protection Agency FY 2005 Safe Drinking Water Information System/ Federal Version (SDWIS/FED) data (drinking water systems) and Permit Compliance System data ranging from June 6, 2006 to August 23, 2007 (wastewater treatment systems).

Water SSP *(Cont. from 5)*
security partners through a strong public-private partnership characterized by trusted relationships. (pp. 34-35)

Managing and Coordinating SSA Responsibilities

EPA's responsibility as the SSA for the Water Sector involves: (1) collaborating with all relevant Federal departments and agencies, State and local governments, and the private sector; (2) conducting or facilitating vulnerability assessments of the sector; and (3) encouraging risk management strategies to protect against and mitigate the effects of all-hazards attacks against CI/KR. This includes collaborating with sector security partners and supporting sector-coordinating mechanisms to: (1) identify, prioritize, and coordinate protection of CI/KR; and (2) facilitate sharing of information and physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices. (pp. 94-95) ❖

WaterISAC *(Cont. from 7)*
WaterISAC's knowledge base holds a variety of training aids. The library includes a wide range of practical guidance on such topics as utility perimeter security, bomb threat disaster planning, chlorine safety, elevated water storage tank security, securing your distribution system, design of source-water monitoring systems, and using contaminant information in evaluating water contamination.

In its commitment to reaching the entire water sector, WaterISAC developed two tiers of service to meet the needs of the water utilities as well as local law enforcement, municipalities, and other local offices that are also connected to the water sector. WaterISAC Pro is designed exclusively for drinking water and wastewater utility systems, with benefits that address the unique security needs of water systems. The Pro service is provided at a nominal fee. WaterISAC Basic is a free service designed for local law enforcement, municipal departments, and other offices that want to remain connected to the water sector but do not have the same security needs as the water systems themselves.

Today, WaterISAC proudly serves thousands of drinking water and wastewater systems nationwide. WaterISAC is overseen by a Board of Managers comprised of drinking water and wastewater utility executives and is administered by the Association of Metropolitan Water Agencies. ❖

WaterISAC Information Sharing & Analysis Center

WISE *(Cont. from 9)*
respectively, in December 2006.

This process alone deserves special attention, and commendation, since this is the first instance for one of the 17 CI/KR that government and industry efforts tied into an existing standards development process to provide guidance and training for CIP. As such, these guidance and training modules can be integrated into the curricula of certification providers such as ASIS International's Certified Protection Professional (CPP) and Physical Security Professional (PSP), as well as into college degree programs. The long-term improvement of the security stance within any given sector is less dependent on physical or cyber upgrades, but rather on the awareness, education, and training of owners and operators. ❖

Preparedness *(Cont. from 10)*

Water Works Association's (AWWA) Water Infrastructure Security Enhancement (WISE) webpage, and a publication entitled *Utilities Helping Utilities: An Action Plan for Mutual Aid and Assistance Networks for Water and Wastewater Utilities* drafted by representatives of AWWA and the California Utilities Emergency Association. These supporting documents and webpages offer a wealth of information for those with a vested interest in water security issues and emergency preparedness.

To further assist stakeholders in testing their preparedness and response, numerous training mechanisms have been developed by both Federal agencies and private sector associations. Specifically with regard to Water Sector tabletop exercises, the EPA released the *Emergency Response Tabletop Exercises for Drinking Water and Wastewater Systems* CD in January 2005, available for order at http://cfpub.epa.gov/safewater/watersecurity/trainingcd.cfm. A list of training courses and workshops is also available on EPA's Water Security webpage. More generally, the U.S. Department of Homeland Security's Homeland Security Exercise and Evaluation Program (HSEEP) provides standard policy and guidance for exercise development, execution, and evaluation. This standardized information, related templates, and lessons learned and best practices are available at https://hseep.dhs.gov. ❖

Ownership *(Cont. from 13)*

locally or privately-owned. Researchers found that approximately 61% of the Water Sector is owned by the private sector and 28% is owned by local governments. The remaining percentage is split between mixed public-private entities (4%), State governments (3%), Federal government (2%), U.S. Territories (1%), and tribal entities (1%). Specifically, according to FY 2005 data, an estimated 68% of the Nation's public drinking water systems are owned by the private sector and 21% by local governments. Conversely, 76% of the U.S. population is served by locally-owned systems and 19% by privately-owned drinking water systems. Municipalities and regional entities account for the ownership of 70% of the wastewater treatment systems included in recently updated EPA databases (June 2006 – August 2007); the private sector owns 22% of wastewater treatment systems.

Of note, the above figures do not represent drinking water and wastewater treatment service for the entire U.S. population. The May 2007 Water Sector-Specific Plan (SSP) states that public drinking water systems supply water to an estimated 84% of the population. The balance of the population drinks water from private wells, springs, and the like; EPA does not regulate drinking water wells that service fewer than 25 people. Wastewater treatment system figures represent roughly 75% of the U.S. population; almost 25% of the population is serviced through unsewered systems, such as septic tanks. Additionally, EPA data sources may not fully reflect infrastructure owned by tribal entities due to varying reporting requirements.

Importantly, there is no single authoritative or all-purpose source for the types of data under comprehensive analysis by CIP Program researchers. For example, data that have been collected by regulatory agencies are useful for their purposes, but may have limitations for economic analysis, and vice versa. Disparate data also exists in the public domain that can hinder researchers from conducting the types of thorough analysis a Federal agency with extensive resources may produce. To elaborate, due to the nature of some information and measures in place to protect sensitive data, publicly available databases do not necessarily express all relevant information. That being said, however, the results of CIP Program infrastructure ownership analysis closely mirrors those illustrated in figures in the Water SSP when broken down by population served rather than number of assets. ❖

Monograph on Vaccine Prioritization During an Influenza Pandemic

The threat of an influenza pandemic is a very important issue. The United States government has spent millions of dollars preparing for this possible and potentially devastating threat. Due to the uncertainty of when an influenza pandemic may actually occur, preparation and response plans are the best tools to minimize the effects of a pandemic. In 2005, the Health and Human Services created a Pandemic Influenza Plan which provides detailed tasks for government agencies to utilize when creating their influenza response plan. The plan addresses several challenges the threat of an influenza pandemic creates. For example, while the government is aggressively working to increase the number of stockpiled vaccines, if a pandemic were to occur, there may not be enough of readily available vaccines to vaccinate the entire US population. Thus, the plan provides recommendations for vaccine prioritization plans.

The Critical Infrastructure Protection Program invited several leading experts to discuss various aspects about vaccine prioritization. We compiled the essays into a monograph and the monograph is now posted on our website at http://cipp.gmu.edu/research/PandemicMonograph.php.

The first essay, written by Dr. Colleen Hardy of the CIP Program, summarizes the Health and Human Services recommendations concerning vaccine prioritization during an influenza pandemic. Dr. Hardy also reviews the National Infrastructure Advisory Council's (NIAC) Working Group on Pandemics' report, which identifies a list of vital goods and services that must be maintained to ensure national security during an influenza pandemic.

The second essay, submitted by Dr. Peter Leitner of the Higgins Counterterrorism Research Center, explores several issues surrounding vaccinating first responders. Dr. Leitner examines the challenge that first responders may not report to work until they have ensured their family's safety and well-being.

Michelle Milgrim, the Assistant Director of Patient Care Services for Fairfax County's Health Department, submitted an essay on Fairfax County's response to an influenza pandemic. Ms. Milgrim's essay demonstrates the decisions that must be made to respond to an influenza pandemic.

The final essay, submitted by Dr. Ezekiel J. Emanuel and Dr. Alan Wertheimer of the Department of Bioethics at the Clinical Center at the National Institute of Health, addresses ethical dilemmas that surround vaccine prioritization. They compare different approaches and provide disadvantages and advantages of each approach.

Vaccine prioritization is one of many challenges an influenza pandemic creates. The essays demonstrate and explain the numerous difficulties that encompass this monumental challenge. The CIP Program would like to thank the authors for their time and dedication and for addressing this important topic.

Grumbles Interview *(Cont. from 3)*

government's homeland security efforts.

Through these types of partnerships, states have assisted EPA and DHS with security-related matters, including the review of DHS's Joint Strategic Sector Assessment (which is an unclassified analysis of threat in the water sector) and providing of information to DHS to populate its National Asset Database.

As we continue to move forward in this collaborative environment, other matters, and projects will require the assistance and perspective of state representatives. DHS is in the process of establishing a State, Local, and Tribal Government Coordinating Council to ensure that these entities' perspectives and knowledge are properly captured as we move forward in implementing programs that better protect the nation's critical infrastructure.

One of the challenges we face is .... defining what it means to be prepared, so as to transform awareness into action.

Q: What are some of these water security programs?

A: EPA is concurrently pursuing multiple program initiatives to help the water sector improve security and reduce risk. One of these efforts involves defining and disseminating best security practices, or what we call "active and effective security programs." In 2005, the National Drinking Water Advisory Council (NDWAC) recommended 14 features that constitute an effective security program. We recently conducted a pilot case study to identify best security practices and information gaps in Washington State with Seattle/King County utilities and agencies within the community that these utilities actively coordinate with. These utilities and state and local agencies—including health departments—represent what we believe is a very effective approach to reducing risk and improving detection and response times. Our goal was to document current active and effective security and emergency practices related to the community's water and wastewater systems. Results will help other communities to implement an active and effective security and emergency preparedness program.

EPA is also undertaking a consequence analysis project to analyze the human health and economic consequences of hypothetical events impacting the water sector. This is important because results will be used to better assist water utilities in protecting critical infrastructure and key resources. As indicated in the NIPP, critical infrastructure areas need to conduct risk assessments to identify and better manage the highest risk vulnerabilities. This project will analyze the human health and economic impacts of various terrorist scenarios for the water sector.

Q: How is EPA assisting the water sector in preparedness and response?

A: During the last 4 years, we have provided key tools, such as a CD-ROM emergency response exercises, and nationwide training to upwards of 10,000 utilities. This year, we are focusing our training on the Incident Command System to promote the integration of water utilities into the emergency response structure. This includes EPA's role under the National Response Plan (NRP). The NRP establishes a comprehensive all-hazards approach to enhance the ability of the United States to manage domestic incidents, and is currently being revised. In this revision, EPA's role will be better defined, with regard to supporting water infrastructure in the event of a national incident.

We are also working in partnership with the American Water Works Association (AWWA) to promote intra-state Mutual Aid Agreements among utilities. These agreements will expedite the rapid deployment of emergency support, including equipment and personnel, to restore critical operations as quickly as possible. In addition, these agreements commonly produce Water and Wastewater Agency Response Networks (WARNs). Mutual aid and assistance agreements allow utilities to share personnel and resources after an emergency and also resolve key issues such as liability, workers' compensation, and reimbursement. Through a grant to AWWA, five mutual aid workshops covering 21 states occurred in 2006. An additional five workshops covering the remaining 29 states will occur in 2007. Currently, four

(Continued on Page 18)

Grumbles Interview *(Cont. from 17)*

states have established WARNs, and many other states are in the process of establishing WARNs. Subsequent efforts at EPA will focus on promoting inter-state Mutual Aid Agreements.

EPA has also developed a tool for utilities to assist with planning and responding to water contamination events, specifically. The Water Contaminant Information Tool (WCIT) is a secure, on-line database that provides immediate, critical information that a responder needs to know about the fate, transport, and health effects of chemical, biological, and radiological contaminants of concern for water security. As a planning tool, WCIT supports vulnerability assessments, emergency response plans, and site-specific response guidelines. As a response tool, WCIT provides contaminant data to help responders (including utilities) make appropriate response decisions.

In the aftermath of a contamination incident, decontamination becomes an urgent issue to both water and wastewater treatment plants. To address water sector decontamination issues and challenges, EPA began working closely with its partners and stakeholders to develop a decontamination strategy. The strategy will respond to the water sector's need for information, tools, and resources enabling the timely recovery and "return to service" of utility operations from "all-hazards" contamination incidents. The strategy will also help EPA meet requirements under Homeland Security Presidential Directive 10 (HSPD 10), which charges us with developing strategies, guidelines, and plans for decontamination in collaboration with DHS and our other federal partners.

Q: What is EPA doing to respond to the previous directive, Homeland Security Presidential Directive 9?

A: EPA will continue our projects, known as the Water Security initiative and Water Laboratory Alliance (WLA). The Water Security initiative and WLA were developed in response to Homeland Security Presidential Directive 9 (HSPD 9) and charges EPA with both developing surveillance and monitoring systems to provide early detection of water contamination and to develop nationwide laboratory networks to support monitoring and response. The Water Security initiative involves the design, deployment, and testing of comprehensive "contamination warning systems at pilot utilities." The WLA will provide the drinking water sector a nationwide network of laboratories for support during contamination events for analysis of contaminants for which routine water laboratories generally will not have capabilities.

Q: What is EPA's approach for the Water Security initiative?

A: This approach combines five monitoring strategies to provide timely detection of a wide range of contaminants that could pose a threat to public health. These components include: 1) continuous monitoring of water quality parameters in the water distribution system; 2) periodic sampling and laboratory analysis of high-priority contaminants; 3) monitoring public health indicators of contamination, such as emergency medical services and 911 calls; 4) monitoring for unusual consumer complaints about drinking water; and 5) enhanced physical security monitoring (e.g., alarms and cameras) at critical drinking water facilities. The overall goal of the Water Security initiative is to design and demonstrate an approach for detecting possible contamination in drinking water systems through a pilot program, which is well underway, and will be fully deployed this summer. Additional pilots at other water utilities will begin later this year. After the Water Security initiative concept for monitoring and surveillance has been proven through these pilots, we want drinking water utilities of all sizes and characteristics across the country to adopt and implement this approach for an effective contamination warning system.

Q: How will the Water Laboratory Alliance work to help the water sector?

A: The WLA will provide drinking water utilities with an integrated nationwide network of laboratories with analytical capabilities and capacity to address non-routine chemical, biological, and radiological contaminants, including chemical and biological warfare agents. These contaminants pose threats to our water supplies, but it is not cost effective for every water utility to upgrade its capabilities to address all of them.

The WLA is being developed based on existing networks such as the Centers for Disease Control and Prevention (CDC) Laboratory Response Network (LRN). We are leveraging existing laboratory

(Continued on Page 19)

Grumbles Interview *(Cont. from 18)*
network capability, capacity, and infrastructure to fill gaps in national laboratory preparedness for drinking water analyses. Laboratory infrastructure that is being leveraged from other networks includes analytical methods, membership criteria, and critical materials, such as laboratory reagents. While the WLA will focus solely on drinking water, it will also be an integral part of EPA's new Environmental Laboratory Response Network (eLRN), which focuses on analyses of all environmental matrices.

Q: What can the public do to participate in water security efforts?

A: Concerned citizens can help protect their water resources by joining together with law enforcement, neighborhood watch groups, drinking water and wastewater system personnel, and local public health and safety officials to promote public awareness and education in areas relevant to water security. Our Water Security website can give you more information at www.epa.gov/watersecurity. ❖

Legal Conference on State Open Government Law and Practice in a Post-9/11 World

Thursday & Friday, November 15-16, 2007
The National Press Club, Washington, D.C.

The CIP Program will be participating in a major national legal and policy conference slated for November 15-16, 2007, at the National Press Club in Washington, D.C. The conference will feature approximately 30 legal and policy subject matter experts, who will comment on the non-release provisions to open government laws enacted by various states since the September 11, 2001 terrorist attacks. The event will include the release of a new book detailing changes in State public information laws, and as a point of comparison, the book will also contain similar legislation from four other nations plagued by international terrorism -- Israel, Colombia, France and the United Kingdom.

The conference is made possible by the Center for Terrorism Law, at St. Mary's University School of Law in San Antonio. The conference is supported by a 2006 Congressionally-directed Homeland Defense and Civil Support Threat Information Collection grant, administered by the Air Force Research Laboratory. The Center for Terrorism Law is a non-profit, non-partisan academic research center dedicated to examining legal issues associated with terrorism and the War on Terror. A vital partner in this endeavor is the Reporters Committee for the Freedom of the Press (RCFP). RCFP accepts no money from the federal grant or the Center for Terrorism Law for its participation.

Conference panelists will comment on the following categories of concern:

Critical Infrastructure
Public Health
First Response
Cyber Security
Political Structure
Terror Investigations

For more information contact Ms. Ema Garcia at emaisabel36@yahoo.com
Center for Terrorism Law: http://www.stmarytx.edu/ctl/

The CIP Program works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems and economic processes supporting the nation's critical infrastructure. The CIP Program is funded by a grant from The National Institute of Standards and Technology (NIST).

The CIP Report is published by Zeichner Risk Analytics, LLC (ZRA) on behalf of the CIP Program. ZRA is the leading provider of risk and security governance knowledge for senior business and government professionals. ZRA's vision is to be a consistent and reliable source of strategic and operational intelligence to support core business processes, functions, and assurance goals.

If you would like to be added to the distribution list for The CIP Report, please click on this link: http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1