THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION VOLUME 7 NUMBER 11

MAY 2009
WATER SECTOR

WaterISAC....2
Information Security....3
Water Security Issues....5
Water Infrastructure....7
Legal Insights....9
Cyber Conflict Perspectives....11
Cyber Workshops....15
Cyber Security Conferences....16
Save the Date....17

Contact: CIPP02@gmu.edu
703.993.4840

In this month's issue of The CIP Report, we examine the challenging issues associated with drinking water and wastewater infrastructure such as water infrastructure protection, information security, and federal legislation.

GEORGE MASON UNIVERSITY
School of Law
CENTER for INFRASTRUCTURE PROTECTION

The Water Information Sharing and Analysis Center (WaterISAC) provides information about their adaptation to the evolving all-hazards approach to security. The Water Research Foundation (WRF) discusses past and present procedures and regulations that assist water utilities with information sharing and security. The CIP Report is also pleased to include an article originally published by National Environmental Services Center (NESC) which analyzes perceived threats, security needs, and interconnections of the water systems. The Water Environment Foundation (WEF) assesses a recent report published by the American Society of Civil Engineers (ASCE) that recently rated the nation's drinking water and wastewater infrastructure.

This month, Legal Insights focuses upon terrorism and chemical security issues for water and wastewater treatment facilities such as current and emerging federal legislation. Finally, Cyber Conflict Perspectives discusses the DIMPLE (Diplomacy, Intelligence, Military, Policy, Law, Economy) standard for cyber incident management. We have also included information on recent and upcoming cyber workshops and conferences.

We hope you enjoy this issue of The CIP Report as well as find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter
Director, CIP
George Mason University, School of Law

WaterISAC: Updated, Upgraded and Still Indispensible

by John P. Sullivan, P.E.
Chief Engineer, Boston Water and Sewer Commission
Chairman, WaterISAC Board of Managers

The events of September 11, 2001 brought the threat of international terrorism to the doorstep of America's critical infrastructure. Thousands lost their lives and the attacks illuminated the need to improve information sharing between government and the private sector. Recognition of this need, combined with the acute vulnerabilities of the water sector, led to the emergence of the Water Information Sharing and Analysis Center, or "WaterISAC," as the principle mechanism for drinking water and wastewater utilities to receive threat information from government and non-governmental sources.

The passage of time since the events of that fall morning, coupled with the devastation of numerous natural disasters, sparked a maturation process within the water sector in terms of how it defines "security." The devastation wrought by hurricanes, earthquakes, forest fires and other disasters have integrated emergency planning and incident management into the context of securing critical infrastructure. Concurrently, a retooling of the tactics, techniques and procedures surrounding information sharing paralleled this new "all-hazards" approach to security.

WATERISAC

In the summer of 2008, in recognition of this shifting terrain, WaterISAC debuted a new and improved portal that sought to synthesize the needs of an all-hazards security environment with improved horizontal communication tools. The result is a unique mechanism that combines traditional features such as a team of experienced security analysts and an e-mail alert notification system with an unrivaled collection of resources that includes data about vulnerabilities, emergency response guidance, training opportunities, and research on government policies. These products are further amplified by a diverse library that contains a breadth and depth of information on issues including cybersecurity, contamination, emergency response and recovery and a variety of other topics.

This rich amalgamation of all-hazards security information is fused together with a toolbox of communication capabilities based on Web 2.0 technology. As such, WaterISAC is leading the way in cultivating cross-sector communication among a diverse community of water system managers and operators. Users can search a directory of fellow users, send private and secure email to each other, use wikis to collaborate on joint projects, and participate in online discussions. These networking tools facilitate an exchange of knowledge and experience among subscribers.

While WaterISAC is no replacement for law enforcement and emergency responders, its resources support efforts to protect against threats and respond when an incident or destructive event is suffered. Just recently, WaterISAC was intricately involved in disseminating critical mitigation procedures to defend against the threat to network systems posed by the computer worm known as "Conficker." Once they had received the information, WaterISAC subscribers utilized the secure online networking tools to communicate with one another to discuss which mitigation techniques were better suited to a water utility's specific cyber needs.

The water sector's shift to an all-hazards security posture is further

(Continued on Page 12)

Information Security within the Drinking Water Utility and Research Community

by Frank J. Blaha, Senior Project Manager
Water Research Foundation

Most drinking water infrastructure in the United States is owned by local government, making the information security requirements vastly different from those that apply to federally-held assets and information. This consideration has created difficulties in advancing the state of knowledge in the area of drinking water infrastructure security. For instance, in the 1990s, the President's Commission on Critical Infrastructure Protection (PCCIP) conducted specific studies to better understand the potential risk posed to drinking water infrastructure from a committed and determined opponent. The results of these studies would have been valuable to water utilities working on security issues; however, we can only speculate as to the value of this work since these reports were never released to the water community. Instead, under Executive Privilege, this information was extremely limited in distribution, presumably because general release of the information may have proved to be more damaging to drinking water security than helpful. Similarly, in the immediate aftermath of the September 2001 terrorist attacks, some drinking water utility members of the Water Research Foundation (the Foundation) recognized a need for the Foundation to control dissemination of potentially security-sensitive research results. Once again, it was suggested that general release of the results could be more damaging to water utilities than helpful.

These types of concerns led to two specific actions on the part of the Foundation. First, in 2003, the Foundation created information-security procedures applicable to Foundation research projects. Second, in 2005, due to a continuing need for comprehensive guidance on information security for water utilities, the Foundation initiated Project 3106, "Critical Information Policies for Water Utilities," to consider the topic in light of evolving federal and state requirements, and to provide robust guidance to water utilities in information security. The outcomes of these two efforts were similar, and both point to the importance of consistent internal policies that consider issues of information security from all perspectives.

Information-Security Procedures for the Foundation

The Foundation's information-security procedures attempt to comprehensively address information security at the Foundation, including:

1. What types of information might be security sensitive, and how such information could be recognized

2. Categorization of sensitive security information with related requirements associated with how this information can be disseminated

3. Proper marking, identification, and handling of sensitive security information

4. Ongoing and completed research projects, especially addressing the publishing or dissemination of the final project results that include security information

5. To what extent sensitive security information can be shared outside the specific drinking-water community, but specifically

(Continued on Page 4)

Information Security *(Cont. from 3)*

addressing expected partners in water security work such as law enforcement and the U.S. Environmental Protection Agency

6. The advertising of Requests for Proposals for a project expected to generate sensitive security results

7. Appropriate requirements for any researchers performing work that is likely to include sensitive security information

8. Appropriate requirements for water-community volunteers and peer reviewers associated with a project generating potentially sensitive security information

9. Control of potentially sensitive security information held at the Foundation offices

10. Communication of ongoing or completed security projects by phone, facsimile, email, and hardcopy between researchers, peer review committees, and the Foundation

11. Security considerations for Foundation staff engaged in possibly sensitive security projects

In general terms, the Foundation information-security procedures identify three levels of information for security purposes: 1) non-sensitive information; 2) sensitive security information (information that was generally useful in understanding vulnerabilities of water utilities, and could, in combination with further specifics, be used against a specific water utility); and 3) very sensitive security information (typically this is specific information relating to the vulnerabilities or situations of a specific utility). By policy, the Foundation will only include non-sensitive and sensitive security information in a final report. Final reports containing non-sensitive security information are completely unrestricted in distribution and handling. Distribution of final reports containing sensitive security information is restricted to water utilities and water-utility security partners that sign a non-disclosure agreement. This agreement alerts the recipient of the report to the special nature of the contents, and also restricts the release of that report to other parties. The sensitive security reports themselves include a marking on every page indicating that the report contains sensitive security information. As noted above, the Foundation will not publish a final report that contains very sensitive security information. This policy has allowed the Foundation to conduct a number of security-oriented projects that included access to sensitive and very sensitive security information. Water utilities have been generally satisfied with this policy.

Information Security Guidance for Water Utilities

The post-attack world was in stark contrast to the situation prior to September 2001, when most municipal water utilities were very open with both their information and access to their facilities. Indeed, before 2001, many utilities were subject to very aggressive information release laws that made almost all utility records open to the public. As information release was restricted after September 2001, decision-makers began to question how much such information would actually help a terrorist target and/or access a particular site or facility. Similarly, it was recognized that information restriction practices sometimes made it difficult for legitimate partners to obtain information to conduct valued activities for water utilities.

The final utility guidance developed through Project 3106 ultimately advised against a presumption of aggressive information restriction, and instead moved towards an approach that explicitly balances the potential risks and benefits associated with a given request for information disclosure. Most importantly, these considerations were to be part of a comprehensive information-security policy at the utility. These recommendations were made based on a review of the security literature, practices of leading water utilities, and guidance developed for analogous organizations, such as electric utilities and airport authorities. The researchers suggested that water utilities designate three levels of information sensitivity. While these three levels of information sensitivity were designated differently from the existing Foundation procedures, in essence the three levels of control are very

(Continued on Page 12)

Terrorism and Beyond: Water Systems Address Security Issues

by Caigan McKenzie, NESC Staff Writer

The U.S. Department of Homeland Security (DHS) defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on national security, national public health or safety, or any combination of those matters." The agency's 2006 National Infrastructure Protection Plan (NIPP) is a strategy that supports an all-hazards approach to protecting this critical infrastructure, with drinking water and wastewater systems identified as one of 18 sectors.

"An all-hazards approach that includes preparing for and responding to not only terrorist attacks, which include predominantly the use of explosives, intentional contamination, and cyber attacks, but also natural and man-made disasters to include pandemic planning," says John Laws, water infrastructure specialist with DHS's Office of Infrastructure Protection.

But how do small water systems' personnel perceive this all-hazards approach? "Small utilities, often staffed by few people, handle many daily challenges to supply clean and safe water services to their customers and communities," says Sandra Fallon, education and training services manager with the National Environmental Services Center (NESC). "In many cases, these immediate needs - ranging from ensuring adequate treatment and services to repairing leaks and equipment problems - take first priority. There are just so many competing priorities that must be addressed that the vulnerability assessments (VAs) and emergency response plans (ERPs) often just stay on bookshelves gathering dust."

Enterprise-Wide Security is Needed

"Water systems should determine and review security plans within the total envelope of their business continuity requirements," says Laws. "This includes their enterprise security needs such as aging infrastructure and employee retention. If your infrastructure collapses, you aren't going to be able to do business; and if you can't retain good employees, you are going to have operational problems.

"In addition to enterprise security, systems should look at physical security, cyber security, contamination, and interdependence issues specifically," continues Laws. Interdependency is when sectors rely on each other to provide products or services. Energy, for instance, needs water for steam generation control and water systems need energy to operate pumps.

"It is best that water systems determine the level of security they need through the use of one of the VA tools (currently being upgraded and automated) at the local level since no one security plan fits all systems," Laws says.

While the probability of an intentional contamination incident occurring may be low, the possibility of a threat of contamination is high. "There are hundreds of contaminants that could disrupt normal operations and cause the public to lose confidence in the water system but which would not cause illness or death," according to EPA's water security handbook.[1]

Since 9-11, there has been a push to develop real-time, online contaminant warning systems, explains Diane VanDe Hei, executive director of both the Association of Metropolitan Water Agencies and WaterISAC. "These systems are being piloted in some of the larger water systems around the country," says VanDe Hei. "Medium and smaller systems are limited in their ability to monitor chemical, biological, and

(Continued on Page 6)

[1] www.epa.gov/safewater/watersecurity/pubs/water_security_handbook_rptb.pdf.

Security Issues *(Cont. from 5)*

radiological contamination of water because of the technology's cost and availability."

System control and data acquisition systems (SCADA) are another area of concern for security breach ever since water utilities began to run them on common technology platforms such as Microsoft Windows™. "Attackers can infiltrate computers through network service ports and specialized 'backdoor' tool ports that are used for legitimate business applications," says VanDe Hei.

Resiliency is a Hot Topic

Redundancies and interconnections need to be built into the water system to ensure uninterrupted service following a point failure or local attack. "One tool everyone should be encouraged to develop is a recovery plan," says Laws. A recovery plan provides specific plans a utility must take to bring its system back into operation. One way is by developing redundancy and interoperability, which provides an alternative option for continued operations. By having duplicate components and backup generators, for example, you increase your resiliency.

"In general, resiliency embodies all the various aspects of what it takes for a utility to survive a terrorist attack, flood, storm, and other emergency situations and to recover quickly," says Laws. "If you have critical customers such as a hospital, then you need to look at what it is going to take to stay in business and deliver your product 24/7."

Perceived Threats

In interviews with water professionals about security, Fallon found that water professionals were much less concerned about terrorism than other risks.

Risk and Ranking (*most important to least important)/ % of systems facing risk (number of years until system faces risk)*

1. Aging Infrastructure/80% (4.3 to 7.1 years)
2. Lack of Planning/75% (4 years; some face it on a daily basis)
3. Retiring Operator Workforce/60.7% (6 to 7.4 years)
4. Natural Disaster/51% (6 to 7 years; some face it on an annual basis)
5. Local Vandalism/41% (3.7 years)
6. Groundwater Overpumping/19.3% (7.5 years)
7. Source Water Contamination/25% (8.8 to 9.2 years)
8. Climate Change/22.6% (20 years)
9. Terrorism/7.3% (6.9 years)

Source: "A New Look at Water Security: Protecting and Stewarding Fragile Resources." Rural Community Assistance Partnership and the National Environmental Services Center. 2007.

Resiliency also applies at the community level, explains Gerald R. Iwan, Ph.D., NESC executive director. "Communities themselves must be made and remain resilient, with water being one aspect of that resiliency. Multidisciplinary resource support to strengthen the community against all disruptions to its essential services is equally critical.

"Water systems should develop, and continually strengthen, reliable and collaborative partnerships with each other, the communities they serve, critical interdependent infrastructures, and with local response organizations, long before a critical situation develops," says Iwan. Some of these partnerships might include the public health community, local environmental agencies, broadcast and print media, nearby systems, state and federal agencies, and the community and customers they serve. In addition,

(Continued on Page 13)

Water is Key Component of Successful Infrastructure

by Anthony Reed, American Society of Civil Engineers

Drinking water and wastewater systems provide a critical public health function and are essential to life, economic development, and growth. However, each day leaking pipes lose an estimated 7 billion gallons of clean drinking water, and aging wastewater systems discharge billions of gallons of untreated wastewater into U.S. surface waters each year.

According to the American Society of Civil Engineers (ASCE),[1] which rated the nation's drinking water and wastewater infrastructure with a grade of D- in its *2009 Report Card for America's Infrastructure*,[2] hundreds of billions of dollars will be needed over the next 20 years for water and wastewater to meet the ever-increasing demand and comply with existing and future legislation.

The 1.5 million miles of pipe that comprise our nation's drinking water and wastewater infrastructure have an average lifespan of 50 to 100 years, according to the Water Environment Federation (WEF).[3] In many eastern cities (i.e. Cincinnati, Portland, Baltimore, Washington, D.C., Atlanta, etc.) some of this infrastructure is close to 200 years old. According to the General Accounting Office (GAO), 50 percent of the pipe in the nation's largest systems is near replacement age. In some cases, the infrastructure is literally falling apart.

In addition to their age, WEF notes that many drinking water and wastewater systems were originally designed for populations half their current size. Since 1950, the U.S. population has more than doubled. Much of the growth is in urban centers where it wears infrastructure down. Population growth is anticipated to continue stretching water and wastewater systems significantly beyond capacity.

Older wastewater systems are plagued by chronic overflows during major rainstorms and heavy snowmelt which brings the discharge of raw sewage into U.S. surface waters. The Environmental Protection Agency (EPA) estimated in August 2004 that the volume of combined sewer overflows discharged nationwide is 850 billion gallons per year. Sanitary sewer overflows, caused by blocked or broken pipes result in the release of as much as 10 billion gallons of raw sewage yearly.

In addition, the nation's drinking-water and wastewater systems are not highly resilient. Present capabilities to prevent failure and properly maintain or reconstitute services are inadequate. The United States has taken clean water for granted for many years and sewer and water rates have never been reflective of the true cost of service. Construction, operation and maintenance, and reconstitution of service for drinking water and wastewater infrastructure is expensive, and the monetary and societal costs incurred when this infrastructure fails are high. A GAO study showed that 29 percent of water and 41 percent of wastewater utilities were not generating enough revenue from user rates to cover the full cost of their service. As a result, maintenance is chronically on the back burner.

At the same time, investment in water infrastructure maintenance has declined dramatically. Competing needs for limited

(Continued on Page 8)

[1] Founded in 1852, the American Society of Civil Engineers represents more than 146,000 civil engineers worldwide and is America's oldest national engineering society. For more information, visit www.asce.org.

[2] For more information about the ASCE *2009 Report Card for America's Infrastructure*, go to www.infrastructurereportcard.org.

[3] Formed in 1928, the Water Environment Federation is a not-for-profit technical and educational organization with 35,000 individual members and 81 affiliated member associations representing an additional 50,000 water quality professionals throughout the world. WEF and its member associations proudly work to achieve our mission of preserving and enhancing the global water environment.

Infrastructure *(Cont. from 7)*

resources can push water and wastewater infrastructure — which is "out of sight, out of mind" — to the bottom of the priority list. With levees failing, gas pipes busting, and bridges collapsing, it becomes difficult for the public to focus on the vulnerabilities of the water infrastructure proceeding invisibly beneath us.

Not meeting the investment needs of the next 20 years risks reversing public health, environmental, and economic gains of the past three decades. According to the EPA, if the nation does not reinvest in water and wastewater infrastructure by 2016, water pollution levels may deteriorate to those observed in the 1970s. The U.S. could risk losing decades of progress in public health and environmental protection. This threatens the nation's economic well-being and quality of life.

According to ASCE's Report Card, America's drinking water systems face an annual shortfall of at least $11 billion to replace aging facilities that are near the end of their useful lives and to comply with existing and future federal water regulations. This does not account for growth in the demand for drinking water over the next 20 years. And, the EPA estimates the nation must invest $390 billion over the next 20 years to update or replace existing systems and build new ones to meet increasing demands.

Following a number of revisions, the final $787 billion economic stimulus plan included more than $7 billion for drinking water and wastewater projects, including $6 billion for the Clean Water and Drinking Water State Revolving Fund (SRF). According to ASCE president D. Wayne Klotz, P.E., D.WRE, F.ASCE, "This plan shows a historic level of leadership and concern for our nation's infrastructure." However, he also noted that, "Our crumbling infrastructure has reached crisis proportions as it jeopardizes not only our nation's prosperity, but the quality of our daily lives. The stimulus package only represents a 'down payment' on our nation's infrastructure problems."

WEF officials are encouraging local government officials to contact their state clean water or drinking water program or the SRF program managers to ensure any projects they would like to have funded are on the state's priority list. Many states have already sent letters to municipalities outlining the process or contingency plans they are developing for awarding stimulus monies. WEF is also conducting a survey to help identify implementation issues and is encouraging state officials to contact their EPA regional office for assistance with distribution of stimulus funds.

ASCE's Report Card also offers a number of solutions for the nation's drinking water and wastewater infrastructure, including:

Groundwater Replenishment System – Orange County, California

The California Department of Water Resources predicts that by 2020, the entire state will experience water shortages equal to the needs of 4 to 12 million families of four for one year. To meet growing demands and reduce reliance on water imported from northern California and the Colorado River, the Orange County Water District developed the Groundwater Replenishment (GWR) System that takes highly treated sewer water and purifies it to levels that meet state and federal drinking water standards. GWR System water will be between 35 and 75 percent cheaper than water produced by seawater desalination, and the purification process will consume about half the energy.

American Recovery and Reinvestment Act Funding – Louisville, Kentucky

The Louisville Water Company has proposed $11 million in projects that could be funded as part of the 2009 American Recovery and Reinvestment Act (P.L. 111-005). The projects would rehabilitate 75 miles of water main to extend the useful life of the system and reduce water main breaks. In addition, 9.5 miles of water main would be replaced to improve water quality, fire hydrant flow, and reduce maintenance. Together, the projects would support 101 jobs.

Downtown Water Main Project – Port Angeles, Washington

In 2008, the City of Port Angeles completed a project to replace the water mains and sidewalks in the

(Continued on Page 14)

Legal Insights

Terrorism and Chemical Security Issues for Water and Wastewater Treatment Facilities

by Brad Castleberry*

The federal government did not consider water systems as critical infrastructure until the late 1990s, and it was not until after the terrorist activities of September 11, 2001 that it developed a sense of urgency regarding security measures to safeguard the nation's water systems. To this end, Congress passed the 2002 Bioterrorism Act, a portion of which created standards for upgrading and maintaining security measures in drinking-water systems. Wastewater treatment facilities, however, were completely excluded from the Act's purview, despite the fact that wastewater infrastructure is worth more than $2 trillion.

In June 2007, the Department of Homeland Security (DHS) adopted the Chemical Facility and Anti-Terrorism Standards (CFATS) to increase security measures at the nation's chemical facilities. Currently, these regulations do not extend to water and wastewater treatment facilities, but recent Congressional attention has been directed towards bringing water and wastewater facilities into compliance with the security measures required by CFATS. This paper briefly outlines the existing regulations that govern water systems, and discusses the Congressional activities underway to close the loopholes that exempt water and wastewater treatment facilities from the stringent security regulations.

The Bioterrorism Act

One of the first changes made after 9/11 was the passage of the Public Health Security and Bioterrorism Preparedness and Response Act, or Bioterrorism Act. Signed into law on June 12, 2002, the Act established new requirements for registering the possession, use, and transfer of substances that could pose a threat to health and safety. Additionally, it improved the existing safeguards against acts of terrorism for various critical infrastructures, including drinking-water systems. Title IV of the Act, which is codified at 42 USC §300i-2, adds several provisions known as the Drinking Water Security and Safety Amendments to the Safe Drinking Water Act (SDWA). Title IV mandates that any water system serving more than 3,300 people must complete a vulnerability assessment of its facilities and then prepare an emergency response plan (ERP) that addresses the identified vulnerabilities.

The vulnerability assessment required by the Act is meant to calculate a facility's susceptibility to an intentional attack under a variety of circumstances. It also requires that those who manage a particular water system conduct a review of its pipes, constructed conveyances, and physical barriers, as well as its facilities for water collection, pretreatment, treatment, storage and distribution. The assessment includes an evaluation of all electronic and automated systems; a review of the way a facility stores and handles chemicals; and an examination of the facility's operation and maintenance.

The deadlines for submitting vulnerability assessments to the Environmental Protection Agency (EPA) depended on the size of the community serviced by the water system. Systems serving a population of more than 100,000 had only until March 2003; those systems serving between 50,000 to 100,000 had until December 2003; and water systems that served fewer than 50,000 had until June 2004 to complete their vulnerability assessments. According to reports, the EPA received 100% of the vulnerability assessments from the two largest divisions of water systems, as well as 95% of those required from the smallest water systems. A water system's

(Continued on Page 10)

Legal Insights *(Cont. from 9)*

vulnerability assessment is accessible only to select personnel with the EPA, and all such assessments are exempt from the disclosure requirements of the Freedom of Information Act. The penalty for revealing the results of a vulnerability assessment to any unauthorized person is a prison sentence of up to one year.

The Act also requires that a water system must also prepare or revise an existing ERP in response to the information gleaned from the vulnerability assessment. Under the statute, the ERP is required to be in place no later than six months after the completion of a vulnerability assessment, and it must include plans, procedures, and the identification of equipment that could be used in the event of an intentional attack on the water system. The ERP must also include an outline of the actions, procedures, and identification of equipment available to the water system that could significantly lessen the impact of an attack. Although there is no specific data on the completion of the ERPs, reports from the EPA suggest significant compliance.

To help water systems comply with Title IV, Congress appropriated funds for the critically important security enhancements identified in the submitted vulnerability assessments. The EPA was authorized to provide up to $5,000,000 per water system to upgrade security through the purchase and installation of intruder-detection equipment, fences, gates, lights, and security cameras; the rekeying of doors and locks; the improvement of computers and electronic systems; the purchase of training and guidance materials relating to security against terrorist attacks; and the security screening of employees, support service-providers, and contractors. Grants in the same amount were similarly allowed for water systems not covered by the Act, which are those that serve fewer than 3,300 people.

Chemical Facility and Anti-Terrorism Standards

CFATS requires facilities that possess certain chemicals at or above defined quantities to register with the DHS. Under its regulations, many drinking-water and wastewater facilities fall into the definition of "facility" due to their use of chlorine during the disinfection process. However, in giving DHS the power to promulgate these rules, Congress specifically provided that any of its regulations would not apply to public water systems as defined in the SDWA, or to wastewater treatment works as defined in the Federal Water Pollution Control Act (FWPCA). Also, the DHS made clear in its commentary of CFATS that drinking-water systems and water treatment facilities do not need to submit any information to the Department under the regulations. The purpose of CFATS is to reach entities not generally considered part of the chemical sector; its regulations define a facility subject to its rules as "any establishment that possesses or plans to possess, at any relevant point in time, a quantity of a chemical substance determined by the Secretary to be potentially dangerous or that meets other risk-related criteria identified by the Department." If a facility meets this definition and possesses any of the covered chemicals at the designated levels, the facility must fill out an online questionnaire called a Top-Screen. Once received, the DHS reviews the Top-Screen to determine how the facility should be regulated.

Under current regulations, the only time a water system or wastewater facility may be required to fill out a Top-Screen and then register with the DHS is if it is not fully covered by one of the above exemptions. If it is partially covered by the definitions in either the SDWA or FWPCA, the facility will have to determine if it has any of the listed chemicals at or above allowed quantities for the portion that is not covered, and then fill out a Top-Screen for the portion. If completely covered, a water system may bypass CFATS entirely.

During the past 18 months there have been indications that Congress is making an effort to close the current CFATS loopholes for water and wastewater systems. With the current CFATS regulations set to expire in October 2009, the House Homeland Security Committee (HSC) has been working on legislation that would extend the program and repeal the exception for water and wastewater facilities. Last session, HSC Chairman

(Continued on Page 13)

Cyber Conflict Perspectives

The DIMPLE Approach to International Cyber Conflict

by Eneken Tikk, M. Jur.

Given the various national approaches to cyber conflict management, one must deal with different lexicons used by lawyers, information security specialists, the media, military, etc. when addressing incidents. Not only is it difficult to understand all of these perspectives, but sometimes the terminology can cause confusion and blur the focus of the issue. What media titles "devastating cyber attacks" or "Cyber War I", would be referred to as "Computer Network Operation" or "denial-of-service attacks" by military or "SQL injections" by IT experts, depending on the type of the incident. Lawyers may have to conclude that the situation was no more than a cyber crime committed by someone "not subject to country X jurisdiction."

The variety of expressions used to describe the field of IT-related security issues may lead to misunderstanding. The term "cyber security" is currently used in the United States (US) legislation (e.g. Cyber Security Enhancement Act of 2002[1]), whereas the European Union (EU) refers to terms such as network and information security (NIS)[2], information and communication technology (ICT) security, information technology (IT) security, information security, network security, etc.

The bottom line is that managing a cyber incident requires involvement of different subject-matter experts and therefore engages different perspectives on the incident. In order to spend less time on figuring out other stakeholder's terminology, it would be easier to develop a standard understood by everyone concerned.

Professor Thomas Wingfield has proposed a tool that aims at "inter-discipline-translating" of the facts of cyber incidents. The DIMPLE standard suggests that for effective cyber incident management the events need to be described in a manner allowing experts of other relevant fields (Diplomacy, Intelligence, Military, Policy, Law, and Economy) to understand the underlying facts of each case. A uniform understanding of the details of cyber incidents would promote expert discussions in the field and avoid parallel vocabulary on the topic of common concern.

The CIP International Cyber Conflict Team, in cooperation with professor Wingfield and subject-matter experts, has decided to further develop the DIMPLE tool using the internationally accepted legal terms as the common language that will respond to input from other subject matter experts. The DIMPLE map will indicate what legal consequences are there for spreading a virus, engaging state or non-state actors in a cyber attack, attacking governmental servers versus stealing credit card information, etc. ❖

[1] Cyber Security Enhancement Act of 2002, available at: http://thomas.loc.gov/cgi-bin/bdquery/z?d107:h.r.03482: (last visited 11.11.2008).

[2] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach, COM(2001)298 final defines NIS as ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems.

WaterISAC *(Cont. from 2)*

reflected in the diverse scope of security based discussions that are taking place within the portal. Subscribers representing utilities of various types, sizes and locations have used WaterISAC as a platform to solicit information from one another on subjects ranging from using Twitter to notify customers about public health situations to available standard operating procedures for wastewater utilities in the wake of a loss of service. The volume and richness of the discussions are a testament to the diverse security issues that utility personnel deal with on a daily basis.

By providing a secure outlet for grass-roots discussions, WaterISAC is leading the way in promoting a security culture that is reflective of the needs of utility managers and operators in the field rather than cubicle-based policymakers in Washington. As the water sector continues to embrace an all-hazards approach to security, WaterISAC will simultaneously strive to expand its subscriber base and promote the importance of social networking and inter-sector communication to water and wastewater utilities around the country. ❖

Information Security *(Cont. from 4)*

similar, ranging from generally available to the public, to availability based on a "need to know," to extremely restricted and essentially not available to the public. Once the utility has specified the sensitivity of a particular item of information, the next decision is to designate an appropriate management protocol. Water utility information can be managed in many different ways, from absolute withholding to full and unrestricted disclosure.

The final report for project 3106 outlines factors that water utilities should consider when developing and implementing an overall information-security policy. This information-security policy should provide administrative, managerial, and personnel guidelines for controlling access to and protecting a utility's sensitive information and records from unauthorized dissemination, access, utilization, and tampering. It should be flexible enough to address three basic types of information access needs: (1) access to utility information by customers and the general public; (2) access to information by utility partners; and (3) access to information by regulatory agencies and oversight bodies.

There is no single policy for sensitive information management that will work for all utilities. Given its unique needs and circumstances, each utility may select from a range of options. Whatever approach a utility chooses to adopt, it is critical that the policy be designed to mesh appropriately with existing records management protocols and regulations. The report also identifies common concepts and points of overlap between sensitive information control and utility records management, and provides recommendations for the value-added linkage between these related fields of activity.

Conclusion

The safety and security of the nation's drinking water systems is a top priority. Water security is a multi-faceted concern, but protection of utility information that could be used to disrupt service, destroy critical infrastructure, or damage public confidence in the water supply is a key aspect of a comprehensive security program. Utility-specific information, such as vulnerability assessments, detailed component specifications, security plans, and security audit findings are examples of security-relevant information that must be managed appropriately at the utility level. At a more general level, such as the Foundation research projects, reports that identify general utility vulnerabilities, such as common organizational, engineering, or monitoring weaknesses, also represent security-relevant information that must be managed appropriately. ❖

Security Issues *(Cont. from 6)*

utilities should know and be familiar with the national Incident Management System (NIMS) and the Incident Command Systems (ICS) as well as their own VAs and ERPs. Personnel need to act quickly and decisively in an emergency or disaster situation. There is no time for guesswork.

Stretching Dollars

"A lot of systems are banding together — small utility with small utility and small utility with large utility — to make their systems more efficient," says VanDe Hei. Laws adds, "Utilities need to build networks within their community and with their suppliers. It's important to have a grass-roots approach to build resiliency into systems. There is very little that the federal or state governments can do outside of providing for the state or national response. All incidents start at the local level and end at the local level. So it is incumbent upon small communities to develop that resiliency in the network." ❖

This article is reprinted from On Tap, a free quarterly magazine published by the National Environmental Services Center (NESC). To learn more about services offered by the NESC visit www.nesc.wvu.edu or call toll free (800) 624-8301.

Legal Insights *(Cont. from 10)*

Bennie Thompson (D-Miss.) sponsored H.R. 5577, which proposed extending CFATS as well as giving the DHS the power to impose rules on water systems and force them to change disinfection methods. Jurisdictional issues that ultimately blocked the bill were raised when the House Energy and Commerce Committee, which oversees the EPA and drinking-water facilities, and the Transportation and Infrastructure Committee, which oversees wastewater infrastructure, both objected to the bill on grounds that it overstepped the HSC's bounds in its attempt to regulate water systems.

Most recently, there have been reports that the Energy and Commerce Committee and the HSC have teamed up to jointly author bills that would create a CFATS-type program applicable to water and wastewater systems. To date, no drafts of upcoming legislation have been released; however, any proposal associated with drinking water systems will likely include a requirement that systems periodically update the vulnerability assessments that were completed under the Bioterrorism Act; develop a site security plan that outlines responses to vulnerabilities at the facility; and review the feasibility of adopting alternate treatment technologies that could reduce the consequences of a chemical release resulting from a terrorist attack. It is anticipated that legislation would also authorize funding to help utilities carry out these activities, probably at an amount similar to the $160 million authorized under the 2002 bill.

Conclusion

The applicability of any House-generated legislation regarding wastewater facilities will remain an open question as long as the Transportation and Infrastructure Committee is not involved in the process. Some commentators speculate that there will be no resolution until a bill is created in the Senate, where the Environment and Public Works Committee has jurisdiction over both drinking-water and wastewater policy. Bottom line, the next six months should prove to be insightful for water and waster utilities wondering what their future obligations may be for security and chemical safety issues. ❖

** Brad Castleberry is a Principal at Lloyd Gosselink Rochelle &Townsend, P.C., and a member of the firm's Water Practice Group. He represents municipalities and water utilities on a variety of issues, including water rights, water supply planning, environmental permitting, and defending environmental enforcement actions. Brad is licensed to practice both law and engineering in the State of Texas. For questions or any other information regarding this article, please contact Brad at (512) 322-5856 or bcastleberry@lglawfirm.com. Brad was assisted in preparation of this article by Kathleen Oliver, who is a law student at the University of Texas School of Law.*

Infrastructure *(Cont. from 8)*

downtown area. The replacement water mains bring the city's downtown area to a service level that meets current fire flow standards, reduces seismic risks, and helps prevent water main failures due to age. The original water mains were installed in 1914. In conjunction with the water main replacement, many sidewalks were replaced with pavers that enhance the downtown appearance. Also, new conduit and wiring was installed for street and pedestrian lighting.

North City Water Reclamation Plant – San Diego, California

The City of San Diego imports approximately 90 percent of its water supply. To meet future water demands and decrease dependence on imported water, the city constructed the North City Reclamation Plant to provide reclaimed water for irrigation, landscaping, and industrial use. This state-of-the-art facility can treat up to 30 million gallons of wastewater per day, and distribute the reclaimed water to customers through 79 miles of distribution pipelines.

Pervious Paving – Marysville, Washington

The City of Marysville installed pervious paving stones instead of traditional asphalt at its Ash Avenue park-and-ride facility. Besides making the stop a much more attractive place to catch the bus, the paving stones allow stormwater to pass through and soak into the ground. The project also allowed for more parking spaces to be built because a stormwater ponder was no longer needed.

Sewer Separation Project – Washington, D.C.

About a third of the District of Columbia is served by a single pipe that carries both wastewater and stormwater runoff. During dry weather, wastewater flows to the Blue Plains treatment plant. But during rain events, both the stormwater and wastewater from the Anacosta area flow in the same pipe, which is not big enough for flows from very large storms. To prevent the combined water from backing up into homes and streets, the combined sewer system dumps the mixture into the Anacosta River. Though the untreated wastewater is diluted by stormwater, allowing this mixture to enter the river is no longer considered an acceptable solution. To improve the health of the Anacosta River, the Washington Area Sewer Authority (WASA) is working with homeowners and businesses to separate their combined pipe into two separate pipes at no charge to customers.

In addition, ASCE outlined five key solutions for improving all infrastructures in the U.S.:

- Increase federal leadership in infrastructure to address the crisis;
- Promote sustainability and resilience in infrastructure to protect the natural environment and withstand natural and man-made hazards;
- Develop federal, regional and state infrastructure plans that complement a national vision and focus on system-wide results;
- Address life-cycle costs and ongoing maintenance to meet the needs of current and future users; and
- Increase and improve infrastructure investment from all stakeholders.

Clean and safe drinking water and adequate wasterwater systems should be a national priority. Disruptions in the service provided by these critical systems can hinder disaster response and recovery efforts; expose the public to water-borne contaminants; and cause damage to roadways, structures, and other infrastructure, endangering lives and resulting in billions of dollars in losses. The question is not whether the federal government should take more responsibility for drinking water improvements, but rather how it should take more responsibility.

For more information about WEF's stimulus activities, including a complete summary of water infrastructure provisions, visit www.wef.org. ❖

CIP Hosts 2nd Cyber Conflict Workshop

CIP recently hosted the second in a series of expert workshops on cyber defense and security. Participants included U.S. and foreign representatives from academia, military, and the private sector. Building on the first workshop in 2008, this event focused on further developing military analysis into a tool for cyber incident management beyond the military arena.

The participants came up with the "Frameworks for International Cyber Security" (FICS) approach to provide a map of existing legal instruments in the field; indicate the 'gray areas' not covered effectively or sufficiently by existing legal instruments; sketch decision-making chains/trees for cyber incident management; and create models for cyber incident analysis.

This approach considers different country perspectives (e.g., DDoS attacks do not present a national security threat to the U.S.); different subject-matter approaches (military, law enforcement, intelligence, foreign policy, etc.); and different stakeholder concerns (public and private sector).

It is expected that the first FICS models will be developed on the basis of international law, which can be further elaborated at the national level, reflecting each country's respective threat assessments and national laws and governance structures.

The conclusions of these workshops will contribute to the Conference planned for September 2009 (see page 17), and will result in publications on the FICS initiative and its potential for developing legal and policy frameworks and tools for decisionmaking during cyber incidents.

.

CIP Participates in NATO Cyber Defense Workshop

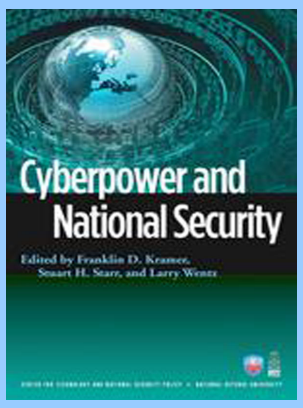
Two CIP faculty members will participate in the 11th NATO Cyber Defence Workshop from 12 to 15 of May 2009, in Athens, Greece. This event is an international forum for new ideas and approaches toward cyber defense. The workshop focuses on the analysis of incidents in international cyber defence networks and systems, identifying best practices, common challenges, and new emerging methods and possibilities for increasing collaboration. There will be three tracks: Questions for Legal Aspects of Cyber Security; Expectations from NATO CD Assistance (RRT); and Cyber Defense Exercises. The workshop is intended to promote discussion and exchange of opinions among the international collaborators, partners, authorities and governmental offices focused on the multidisciplinary responsibility of cyber incident management. A future issue of *The CIP Report* will include a review of the workshop.

New Release

Cyberpower and National Security (2009)

Featuring a chapter by CIP staff:
"Cyberpower and Critical Infrastructure Protection:
A Critical Assessment of Federal Efforts"

Available at Potomac Books



CIP Presentations at Cyber Security Conference

Two CIP faculty members spoke at the "Challenges in International Cyber Security" conference hosted by the Center for Technology and National Security Policy at the National Defense University, 29-30 April 2009.

Maeve Dion, CIP Program Manager for Education and Cyber, and Eneken Tikk, CIP Visiting Research Fellow from the NATO-accredited Cooperative Cyber Defence Centre of Excellence, presented at the conference. Eneken gave a presentation titled "Identification and Attribution: Are We Talking the Same Language?" which was part of the panel on "**Policy Challenges in Defending Against Cyber Attacks**."

Maeve spoke on the panel "**Potential Thresholds of War in Cyberspace.**" Her presentation addressed "Defining Responses to Cyber Incidents: Legal Frameworks."

The conference report, presentations, agenda, and speaker biographies will soon be available on the NDU website. The two CIP presentations are currently available on the CIP website.

The two-day conference featured keynotes from LTG Keith B. Alexander, Director, National Security Agency, and Chief, Central Security Service; General James E. Cartwright, Vice Chairman, JCS; Lt. Gen. (Ret) Harry D. Raduege, Jr., Deloitte & Touche LLP; and Mr. John Grimes, ASD (NII).

The conference marked the release of a new book, *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry Wentz. Under former-CIP Director John McCarthy, CIP staff collaborated on the chapter titled "Cyberpower and Critical Infrastructure Protection: A Critical Assessment of Federal Efforts."

Save the Date

Frameworks for International Cyber Security: A Legal and Policy Conference

September 9 - 11, 2009

Tallinn, Estonia
Organized by the Center for Infrastructure Protection and the
NATO-accredited Cooperative Cyber Defence Centre of Excellence.

Registration and agenda coming soon to www.ccdcoe.org

The Center for Infrastructure Protection works in conjunction with James Madison Univerity 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 Center is funded by a grant from the National Institute of Standards and Technology (NIST).

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