The CIP Report

VOLUME 1, ISSUE 3 SEPTEMBER 2002

Water Issue

What's Inside

CIP Project Staff

John A. McCarthy
Executive Director

Kevin "Kip" Thomas
Research Associate Professor/
Working Groups Project Manager

Meredith Gilchrest
CIP Law and Policy Research
Archivist/ Outreach Program
Manager

Rebecca Luria
Project Administrator/
Executive Assistant

George Baker
Interim Director
Institute for Infrastructure and
Information Assurance

Ken Newbold
JMU Outreach Coordinator/
JMU CIP Project Liaison

Contact: cipp01@gmu.edu
703-993-4840

President Bush Names JMU's President Rose To Advisory Group

September 23, 2002

HARRISONBURG - James Madison University President Linwood H. Rose has been appointed by President George W. Bush to a 24-member National Infrastructure Advisory Committee (NIAC).

Rose, president of JMU since 1998, is the only college president named to the committee.

Established by President Bush's Executive Order 13231, NIAC will make recommendations regarding the security of the cyber and information systems of the United States' national security and economic critical infrastructures. The committee will also examine ways that partnerships between the public and private sectors can be enhanced to improve cyber security, the White House said.

"Needless to say, I am extremely honored and pleased to be the only college president appointed to a national advisory committee by the president of the United States," Rose said. "I

(Continued, Page 5)

THE TECH CENTER
National Center for Technology & Law
CRITICAL INFRASTRUCTURE PROTECTION PROJECT

WaterISAC: Taking Water Security To The Next Level

America's drinking water and wastewater utilities were addressing security long before September 11. Large public systems already had protective systems in place to deter sabotage of their facilities and water sources. In the changed world following the attacks, however, these systems are taking on new initiatives to protect their infrastructure and resources. The Water Information Sharing and Analysis Center (WaterISAC) is an important new tool for their anti-terrorist arsenals.

The WaterISAC will use a secure web-based environment to provide early warning of potential physical, contamination and cyber threats. Its array of

(Continued, Page 6)

Water Supply CIP: Five Years After the Commission Report

Irwin M. Pikus, Ph.D., J.D.
Former Commissioner, President's Commission on Critical Infrastructure Protection
Visiting Professor, Systems Engineering, University of Virginia

The October 1997 report of the President's Commission on Critical Infrastructure Protection (PCCIP) recommended a comprehensive program of security collaboration between government and the owners and operators of the nation's critical infrastructures. The PCCIP called for raising awareness, assessing threats and vulnerabilities, analyzing and managing risks, and ensuring adequate resources – human and fiscal. It recommended that the President assign lead responsibility to various agencies; EPA for the water supply sector.

At that time, the security concerns of most water utilities in the United States were limited to minor vandalism. Physical security around water system elements was minimal. SCADA systems were just beginning to be implemented and cyber security was a secondary concern. Water quality was measured against criteria mandated by EPA and State authorities with no thought for the more sophisticated chemical, biological or nuclear contaminants in a terrorist's arsenal.

The past five years have seen a major turn-around. Led by industry groups - Association of Metropolitan Water Agencies (AMWA), American Water Works Association (AWWA) - the water supply industry has made remarkable progress. It has elevated security to highest priority. Recent revelations of Al Qaeda's interest in US water supplies and dams demonstrate the urgency of these efforts. Nearly every water supply company is now aware of its major vulnerabilities and undertaken significant mitigation efforts. Of course, there is still much to do.

Vulnerability assessment gained early attention. With support from EPA and the AWWA-Research Foundation, Sandia National Laboratories has developed a powerful methodology for assessing water system vulnerabilities called Risk Assessment Methodology - Water (RAM-W). This methodology follows seven stages:

1) characterizing the site;
2) identifying critical assets and failure modes;
3) determining consequences of failures;
4) defining threats;
5) evaluating effectiveness of protective measures;
6) estimating risks; and
7) designing risk mitigation measures and tradeoffs.

Sandia has now trained a number of private firms who perform assessments for utilities or train the utilities to do their own. A few leading firms begin with the general philosophy of RAM-W but employ methodology tuned specifically to the utility's needs.

In June the President signed the Public Health Security and Bioterrorism Response Act 2002. Title IV of the Act deals with the safety of drinking water supply and authorizes EPA financial assistance to water utilities in conducting vulnerability assessments. It establishes a timetable for community water systems serving more than 3300 people to conduct assessments and submit them to EPA. Each such system must also develop emergency response plans coordinated with local emergency planning activities. EPA has awarded grants to about 430 of the nation's largest drinking water systems (providing water to more than 100,000 customers) and waste-water utilities (treating more than 15 million gallons/day). These systems serve over 50 percent of the population.

PCCIP recommended establishing information sharing and analysis centers (ISACs). After considering the approach taken by existing ISACs, the water community, under AMWA's

(Continued, Page 3)

Bioterrorism Preparedness Bill has Implications for Water Sector

The President signed into law the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 in an effort to prevent and detect bioterrorist attacks, to strengthen communications between healthcare providers and public health officials, to expedite medical treatments across the country, and to develop better medicine for the future.

Title Four of the act addresses drinking water security and safety. It requires every community water system serving more than 3,300 people to conduct a vulnerability assessment and to prepare or update emergency response plans within six months. The vulnerability assessments must be submitted to the Environmental Protection Agency (EPA) but will be exempt from disclosure under FOIA. The legislation authorized $160 million in financial assistance for FY 2002 to go toward vulnerability assessments, emergency response plans, basic security enhancements of critical importance, and immediate and urgent security needs.

The act requires the EPA to review methods to prevent, detect, and respond to the intentional introduction of chemical, biological, and radiological contaminants into water systems, and to review methods of preventing water supply disruption.

The EPA has received supplemental appropriations for FY 2002 to support counter terrorism activities, and is working with numerous partners in its efforts to secure the nation's water infrastructure. In cooperation with these partners, the EPA's Water Protection Task Force has a number of activities underway, including:

- Direct grant assistance to large drinking water facilities (regularly serving more than 100,000 people) for up to $115,000 to develop vulnerability assessments, emergency response/operating plans, and security enhancement plans and designs;
- Support for the development of tools, training, and technical assistance for small and medium drinking water and wastewater utilities;
- Promotion of information sharing and research to improve treatment and detection of water supply contamination.

Water Supply CIP: Five Years After *(continued from Page 2)* leadership and a grant from EPA, is in the process of establishing its own ISAC. It is being configured as an internet-based, highly secure system to accomplish three ends:

- disseminate early warnings;
- facilitate sharing information about security incidents; and
- promote detailed incident analysis by experts.

The ISAC, expected to be operational this Fall, will be a membership organization with fees tied to utility size.

The PCCIP identified contamination as one of the most serious threats to the nation's water supply. It called for further R&D to better understand this vulnerability and to develop technological approaches to monitoring and water handling in order to mitigate this threat. The R&D effort in counter-contamination technology is still in its infancy. Nevertheless, most water utilities now are aware of the problem and that there is no "quick fix."

To summarize, the water utility community, with EPA's support and the leadership of industry associations, has grasped the significance of their security problems and has embarked on a long term, high priority effort to manage them. If current rates of progress continue, this infrastructure may well serve as a model of government-industry partnership for infrastructure security.

The Water Infrastructure in Canada and the United States: The Need for Cross-Border Information Sharing Mechanisms

Katie Tolan
EWA Canada- ktolan@ewa-canada.com

There is a growing need for Canada and the U.S. to establish a collaborative relationship for sharing information related to threats to our critical infrastructures. Our two countries share the longest border in the world; 1.3 billion U.S. dollars worth of goods and services cross the border every day; 200 million border crossings take place annually; the telecommunications infrastructure and electrical power grids are interconnected; and cross-border interdependencies exist in all critical infrastructures. Threats to critical infrastructures in one country could impact the national security and economic well being of the other.

Canada and the United States: Sharing Water and Power

The water infrastructure in Canada is used in agriculture, manufacturing processes, power generation, mining, and human consumption. As in the U.S., three attributes are crucial to water supply users. There must be water on demand; it must be delivered at sufficient pressure; and it must be safe for use. Disruption could affect regional power grids, the production of food and manufactured goods, the security of various facilities, the delivery of emergency services, and public health.

Disruptions to the Canadian water infrastructure would be felt in the U.S. Over 300 lakes and rivers either cross or straddle the Canadian-U.S. border and water from these lakes and rivers generate power that is used by the two countries. Canada and the U.S. have a history of cooperation on water-related issues that stretches back to the 1909 signing of the *Boundary Waters Treaty*. This Treaty established mechanisms for power sharing that still exist between Canada and the U.S. today.

Other treaties including *The Niagara Water Diversion Treaty* of 1950 and the *The Columbia River Treaty* of 1961 have had a significant impact on establishing protocols for water diversion, sharing power, constructing major dams, and economic development in Canada and the U.S. Resulting interdependencies have created shared threats. One emerging threat, highlighted in June 2002, is the concern, expressed by U.S. analysts, that perpetrators could use cyber tools to take command of the floodgates in a dam or substations handling 300,000 volts of electric power. If such a scenario happened this would create threats to human life, economic viability, and the delivery of emergency services. These consequences could be felt in Canada and the U.S.

The Need for Cross-Border Collaboration

The need to share cross-border threat data was captured in the "Blue Cascades" Report published in July 2002. Participants responded to scenarios in which the region's electric power was disrupted, causing region wide power outages, disruptions of the region's telecommunications and natural gas distribution, as well as threats to a major water system. Findings include:

- *U.S. and Canadian cooperation was limited in law enforcement, response and recovery and information sharing;*
- *There is no common, continent wide alert system with threat levels that have a corresponding set of actions required;*
- *There is no mechanism for cross-border sharing of U.S. and Canadian threat information or a common color-coded terrorist alert system.*

Many interdependencies exist between Canada and the U.S. in the water infrastructure. Disruptions could be felt equally in both countries. Establishing mechanisms for early warning is an effective way to mitigate threats. This could be partially fulfilled through the development of information sharing protocols between Canada and the U.S. on threat information to the water infrastructure.

Press Release: Rose to Advisory Committee *(continued from page 1)* am most grateful to have the opportunity to serve on a committee with some of the nation's most important business, industrial and political leaders."

Rose credited his appointment to work that is taking place on the JMU campus on information security.

"This appointment is a direct result of the tremendous job that James Madison University and its outstanding faculty members are doing in the field of cyber security," Rose said. "JMU has quickly emerged as a national leader in information security and it pleases me to realize that the efforts of our faculty are being recognized in this manner."

With the development of its College of Integrated Science and Technology, JMU has quickly become a national leader in the field of technology. JMU is one of 36 universities in the nation recognized by the National Security Agency as Centers of Academic Excellence in Information Assurance Education.

Partnered with George Mason University, JMU is carrying out a $6.5 million project to help address the legal, technical and policy issues involved in protecting the United States' vital computer systems from cyber-attack.

JMU offers the nation's first distance-learning-based master of science degree in computer science with a concentration in information security and a master of business administration degree with a concentration in information security. JMU also is home to the Commonwealth Information Security Center, established in July 2001.

Members of the advisory committee appointed by President Bush represent major sectors of the economy — banking and finance, transportation, energy, information technology and manufacturing. The council also includes representatives from academia, state and local government and law enforcement. The council will work closely with the President's National Security and Telecommunications Advisory Committee, the White House said.

Richard K. Davidson will serve as chairman of the National Infrastructure Advisory Board. He is currently the chairman, president and CEO of Union Pacific Corp.

In addition to Rose, other members are:

- Alfred R. Berkeley III, vice chairman, NASDAQ Stockmarket Inc.
- Martin G. McGuinn, chairman and CEO, Mellon Financial Corp.
- Richard M. Kovacevich, chairman and CEO, Wells Fargo.
- L. George Martinez, chairman, Sterling Bank and Sterling Bancshares Inc.
- Charles O. Holliday, Jr., chairman and CEO, DuPont Co.
- Margaret Grayson, president and CEO, V-ONE Corp.
- John W. Thompson, chairman and CEO, Symantec Corp.
- Thomas E. Noonan, chairman, president and CEO, Internet Security Systems, Inc.
- George H. Conrades, chairman and CEO, Akamai Technologies.
- Craig R. Barrett, CEO, Intel Corp.
- Enrique Hernandez, Jr., president and CEO, Inter-Con Security Systems Inc.
- Maynard G. Webb, COO, e-Bay
- Erle Nye, chairman and CEO, TXU Corp.
- Marilyn Ware, chairman, American Waterworks Co.
- Archie W. Dunham, Chairman, ConocoPhillips.
- Donald John Carty, chairman and CEO, American Airlines.
- Thomas H. Weidemeyer, COO, UPS.
- William F. Owens, governor of Colorado.
- Jorge Santini, mayor of San Juan, Puerto Rico.
- Raymond W. Kelly, police commissioner, City of New York.
- Gilbert G. Gallegos, chief of police, Albuquerque, N. M.
- Karen Katen, president, Pfizer Global Pharmaceuticals and executive vice president, Pfizer Inc.

WaterISAC *(continued from page 1)*
information and tools will assist utilities in identifying and assessing threats, in taking measures to mitigate those threats and in analyzing incident reports. The WaterISAC will also serve as an important link between the water community and federal government agencies and ultimately will encompass collaborative tools for utilities, law enforcement officials and emergency responders to effectively and efficiently share information in a secure environment. December 2002 is the target date for the official roll out of the WaterISAC.

Water Utilities Are Critical Infrastructure

Water utilities must protect their critical facilities from terrorist and other threats because safe drinking water is fundamental to the nation's health and economic prosperity. In 1998, Presidential Decision Directive 63 (PDD-63) designated the water sector as one of eight critical infrastructure sectors because an attack on any one of them could significantly harm the health and economic well-being of U.S. communities. PDD-63 and President George W. Bush's 2001 Executive Order 13231 (EO 13231), which reasserted the earlier directive, both made establishment of ISACs a key national security objective.

Already water utilities are conducting vulnerability assessments of their systems, performing upgrades to enhance security and improving emergency response planning. The 2002 bioterrorism act requires the nearly 9,000 water utilities that serve more than 3,300 people to conduct vulnerability assessments to identify weaknesses and potential threats. Even before September 2001, however, some larger water utilities had begun to assess their systems' vulnerabilities using a tool developed in 1999 by Sandia National Laboratories.

As part of the new focus on security initiatives, water systems are encouraged to develop contacts and relationships with their local law enforcement and local FBI office. In addition, many communities have Local Emergency Planning Committees (LEPC). The role of the WaterISAC is to supplement and enhance these efforts for water systems, providing up-to-date intelligence and analysis that can be used to continuously improve and renew their emergency plans.

Much More Than A Clearinghouse

The WaterISAC will be much more than a security clearinghouse. While it gathers and distributes information on threats to the water industry, it will take the additional steps of analyzing the credibility of the information and identifying trends. This extremely sensitive and valuable information will be distributed to subscribing water systems through encrypted email and a secure portal, making the WaterISAC the one place where all sensitive security-related information is available to U.S. drinking water and wastewater utilities.

For the first time, water systems will have a forum for the secure exchange of sensitive information and intelligence. When fully realized, the WaterISAC will provide a secure meeting ground for the drinking water and wastewater community -- a convenient, efficient and low-cost source of reliable
security information.

Beyond these immediate objectives, the WaterISAC will also be designed to offer a repository for security-related plans and documents, a focal point for online training and education on security topics, a place where utility managers can share information, counsel and advice in a secure setting, a contact point for links and resources beyond the world of water utilities and a security library tailored to the needs of utilities

Secure Handling Of Sensitive Information

Analysts for the WaterISAC have top secret clearance and will operate in a secure environment. The computer servers for the WaterISAC portal reside in the cleared facility and are protected by security barriers and monitored by Information Technology (IT) security experts. Communications from the WaterISAC to subscribing utilities will be conducted through encrypted email.

A number of different sources will be used to gather information for the WaterISAC, including government (local, state, federal and law enforcement), classified sources (intelligence community), publicly available information (Internet, newspapers), the water community (utilities, water associations and research foundations), and private entities (think tanks, etc.). WaterISAC analysts will gather information from these sources and then assess, sanitize and disseminate it, enabling water utilities to make better-informed security decisions.

Within the WaterISAC's analytical organization, a lead analyst will be in charge of a specific threat. Depending on the information, contamination, physical, and/or cyber analysts would be brought in to review the raw data. Subject-matter experts will be on call and brought in on an as-needed basis. In conducting analysis for the WaterISAC, analysts will look for patterns and trends in seemingly unrelated events and will seek associations that may link several events together.

User Friendly Web Interface

The web interface for the WaterISAC is designed to be user friendly, with a homepage that provides sensitive security information in an easy-to-find format. Other elements of the WaterISAC web site will include:

- Resource library – Database of contaminants
- Access incident reporting analysis
- Repository for vulnerability assessment tools and research
- Collaboration via chat rooms and forums in a secure environment
- Incident reporting with identification of trends across industry or region
- Utility profiles
- Key web site links
- Online help

WaterISAC Governance

The Association of Metropolitan Water Agencies (AMWA) is developing the WaterISAC with funding assistance from the U.S. Environmental Protection Agency. AMWA has contracted with a team of contractors headed by Westin Engineering, Inc. and including HDR, EWA Information and Infrastructure Technologies and Candle Corporation. The WaterISAC development relies on an advisory panel of water utility mangers for recommendations and advice. In addition, AMWA has established a non-profit organization (WaterISAC Corporation) which will be governed by a board of utility managers appointed by the following organizations:

- American Water Works Association
- Association of Metropolitan Sewerage Agencies
- Association of Metropolitan Water Agencies
- Awwa Research Foundation
- National Association of Water Companies
- National Rural Water Association
- Water Environment Federation
- Water Environment Research Foundation

Subscriptions To The WaterISAC

The WaterISAC is open to all U.S. drinking water and wastewater systems. The information on the WaterISAC is specifically geared to drinking water and wastewater utility executives, mangers, operators and security officers. Because of the sensitive nature of the information, subscribers will be asked to agree to set standards of security and confidentiality of information.

Law's Role in Efficient Public-Private Cooperation for Critical Infrastructure Protection

Professor Amitai Aviram-aaviram@gmu.edu

A much-cited joke tells of two people who turned to their Rabbi to resolve a conflict between them. One pleaded his case to the Rabbi, who replied, "You are right". "But Rabbi," protested the other and asserted his claim, to which the Rabbi's response was "you are right as well". "You're not solving the dispute by declaring they're both right," intervened the Rabbi's wife. The Rabbi gave this some consideration and finally replied: "you, too, are right".

Assigning responsibility for protecting critical infrastructure – not only in the water sector, which this issue of The CIP Report addresses in depth, but in all types of critical infrastructure – may be similar. Those who urge for a government-sponsored solution point to the need for coordination in implementing security measures, since one poorly-protected link jeopardizes the entire network. They also note that some private parties may have independent agendas that are not entirely aligned with implementing the best security solution. They are right.

Others, advocating for privately developed solutions, argue that many minds are more likely to reach an innovative solution than a single one. By unleashing numerous separate teams to independently devise solutions, and by letting the market identify the successful solutions, better results can be achieved faster. They too are right.

Admitting that both claims have merit is of little use. But identifying the relative advantages of the public and private sectors and suggesting how the two sectors can interface most efficiently (or advising what currently prevents this efficient interface) can award us with the best of both worlds. Law, and in particular a branch of legal scholarship known as 'private ordering', examines precisely these issues. Private ordering assesses the social benefits and relative advantages of private regulation regimes. Contemporary scholarship in this field examines the unique abilities possessed by networks – institutions that benefit their members more as the number of members and their participation increase. An exchange, such as eBay or the Chicago Board of Trade, is an example of a network: as the number of people trading through the exchange increase, so do the benefits to each of them, since more buyers, sellers, and items to trade are available.

Networks have advantages over government in some aspects of mitigating harmful behavior. For example, the threat of being excluded from some networks may be more effective than that of being fined by government; the ability to track illegal activity done over a network is greater than the same activity done in a dark alley. Networks are particularly powerful when the benefits from transacting through them are so great that it is not practical to do business otherwise. In such cases, exclusion from the network, or intercepting activity conducted on the network, operates like a law of physics, that cannot be broken and needs no enforcement, rather than a "legal" law, that can be violated and therefore is meaningful only if violations are detected and punished. In certain high-reliability organizations, where the stakes are too great to allow harmful activity to occur and be punished later, these "laws of physics" may be the only viable option.

It is true that powerful private networks can do harm as well as good. Some laws (in particular, antitrust) are concerned with curbing that power. Legal research can guide these laws to ensure that such necessary precautions do not overextend to limit networks' ability to efficiently police security.

Additional information on the WaterISAC can be found online at www.waterisac.org.

The WaterISAC will provide –

- Alerts of potential and actual physical or cyber attacks.
- Access to information from the FBI, EPA, CDC, intelligence agencies and other federal agencies.
- A database of chemical, biological and radiological agents.
- Information on physical vulnerabilities and security solutions.
- Notification of cyber vulnerabilities and technical fixes.
- Research, reports and other information.
- A secure mechanism to report security incidents.
- Access to vulnerability assessment tools and resources.
- Emergency preparedness and response resources.
- An electronic bulletin board and other forums on security topics.
- Summaries of open-source security information.
- Information on security products and services.

James Madison News Updates

James Madison University is taking the lead in designing and implementing a novel diagnostic system, intended to provide more realistic insights into the dynamics of failures in complex networked systems.

Research is directed toward determining the most critical failure points and the most cost-effective protection upgrades for a given system. Fundamental is the development of a Network Security Risk Assessment Model, extending conventional Probabilistic Risk Assessment into the time domain.

This model will compute the evolution of overall mission failure probability over time by evaluating initial probabilities of adverse events, onset times of their effects, and system recovery times. Computation will quantify the overall network functional survivability over time and would evaluate the cost of network downtime, lost data, and the liabilities associated with network malfunction.

Such a model should prove helpful in evaluating the seriousness of anticipated system failure modes. It would also be useful for postmortems of actual breakdowns by providing a framework for comparing the effectiveness of alternative countermeasure approaches and upgrade options.

+++++++

James Madison University personnel arranged and hosted a first meeting between representatives of Virginia state agencies and infrastructure resource persons within the Federal government. Hosted at JMU's Chantilly office on September 6, the session brought together state government staffers and officials from two Federal agencies slated to become part of the Department of Homeland Security.

Representative of the Virginia Department of Technology Planning and Department of Information Technology shared plans and concerns arising from the ongoing "Secure Virginia Initiative" for infrastructure assurance.

Insights from the Federal Computer Incident Response Center (FedCIRC) and the Critical Infrastructure Assurance Office (CIAO) were seen as directly applicable to Virginia government needs. Both short-term and long-term activities were identified for partnering efforts.

George Baker, Interim Director of the Institute for Infrastructure and Information Assurance at JMU, provided an overview of the work being done under both the (Federal) CIPP and (state) CTRF grants.

Given the highly positive nature of this first meeting, all participants agreed to continuing and expanding information and resource exchanges in future sessions.

Water and Critical Infrastructure: Links to Organizations and Resources

Organizations

Advisory Committee on Water Information - http://water.usgs.gov/wicp/
American Water Works Association – http://www.awwa.org
American Water Works Research Foundation – http://www.awwarf.com
American Water Resources Association - http://www.awra.org/
Association of Metropolitan Sewage Agencies – http://www.amsa-cleanwater.org
Association of Metropolitan Water Agencies-http://www.amwa.net
National Association of Water Companies – http://www.nawc.org/
National Rural Water Association – http://www.nrwa.org
Water Environment Federation – http://www.wef.org
Water Environment Research Foundation – http://www.werf.org
WaterISAC – http://www.waterisac.org
EPA Infrastructure Security - http://www.epa.gov/safewater/security/index.html
US Army Corps of Engineers – http://www.usace.army.mil

Legal, Policy, and Security Resources

EPA Water Laws and Policies - http://www.epa.gov/water/laws.html
Water & State FOIA Laws - http://www.amwa.net/isac/StateFOIA.pdf
Safe Drinking Water Act - http://www.amwa.net/features/sdwa/sdwa1996/s1.html
National Association of Regulatory Utility Commissioners – http://www.naruc.org
Water Sector Cyber Strategy – http://www.pcis.org (link to Water Systems)
Secure Cyberspace (Federal Government) - http://www.whitehouse.gov/pcipb/
The National Strategy for Homeland Security – http://whitehouse.gov/homeland/book/index.html
Drinking and Wastewater Financing: http://www.epa.gov/owm/cwfinance/index.htm
National Water Infrastructure Protection Center – http://www.nipc.gov
Federal Emergency Management Agency -http://www.fema.gov/rrr/waterf.shtm

The CIP Report is published by LegalNet Works, Inc. on behalf of the CIP Project. Formed in 1996, LegalNet Works Incorporated focuses on the development of information security laws and regulations with an emphasis on liability, risk management, national security, regulatory compliance, and privacy. LegalNet consults both government and industry officials on legal and policy reform in these complex areas (http://www.legalnet.com). For further information, please contact info@legalnet.com.

If you would like to be added to the distribution list for *The CIP Report,* please send an e-mail to cipp01@gmu.edu.