SEPTEMBER 2004 / VOLUME 3, NUMBER 3

THE CIP REPORT

Corporate Governance

CIP Program Staff

John McCarthy, *Director / Principal Investigator*

Jerry Brashear, *Associate Director, National Capitol Region Project*

Emily Frye, *Associate Director, Law and Economics Programs*

Rod Nydam, *Associate Director, Private Sector Programs*

Dr. John Noftsinger, *Executive Director, JMU Institute for Infrastructure and Information Assurance*

Ken Newbold, *JMU Outreach Coordinator / JMU CIP Program Liaison*

Contact: cipp01@gmu.edu
703.993.4840

If you would like to subscribe to *The CIP Report* please click here.

This month's *CIP Report* examines the relationship between corporate governance and critical infrastructure protection. We explore the impact corporate governance has on critical infrastructure protection and homeland security.

Corporate governance has increasingly become a topic of great and timely significance. Following a period of intense international scrutiny and the discussions that ensued surrounding well-publicized corporate failures in 2001 and 2002, the many factors that contribute to the economic health of a corporation (and, ultimately, the economic security of the nation) have led to a stronger consensus on the importance of good corporate governance. Principles of accountability and responsibility, while simple, form the backbone of good practice. Security, once the domain of lower level managers, is now viewed increasingly as a CEO and board level responsibility. In a nation where over 85% of critical infrastructure is owned by the private sector, good corporate governance can benefit homeland security and our critical infrastructures.

GEORGE MASON UNIVERSITY
School of Law
CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

There have been several notable corporate governance developments in the past three years, especially with regard to financial and cyber accountability. In 2003, the Business Roundtable expanded its Corporate Governance principles to include "business risk assessment and management, business continuity, physical and cyber security, and emergency communications." Earlier this year, the April 2004 report by the National Cyber Security Partnership's Corporate Governance Task Force detailed measures that could greatly enhance critical infrastructure protection, including:

- identifying cybersecurity roles and responsibilities within corporate management structures;
- establishing risk management and quality assurance benchmarks; and,
- outlining best practices and industry metrics.

Similarly, the CISWG, sponsored by Rep. Adam Putnam's 2002 draft legislation, has produced a draft set of cybersecurity accounting metrics.

Congress and the Administration have similarly produced new laws, policies, and programs to support corporate governance and security initiatives. For example, the Sarbanes Oxley Act of 2002 has internal control provisions in Section 404 that have information security implications for the corporate world. These provisions have generated extensive debate throughout the CIP arena. Another example is the 9/11 Commission's recommendation of a national voluntary consensus standard for security preparedness that reflects corporate-wide activity for both cyber and physical systems. Secretary Ridge and the Congress support the standard, which we outline in greater detail. Regulatory and supervisory guidance prepared by the Federal Financial Institutions Examination Council, and promoted by banking supervisors, offers an excellent example of how public and private sectors are exploring appropriate corporate officer activities in a critical infrastructure setting.

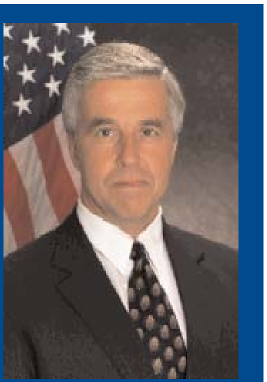
This issue further examines information security governance, information on legislative and regulatory guidelines, and public and private corporate governance initiatives provide to a comprehensive background on this important component of CIP.

Bringing Information Security to the Board

Earlier this year the National Cyber Security Partnership's Corporate Governance Task Force released "Information Security Governance: A Call to Action." The report provides an ISO 17799 standards-based information security governance (ISG) framework, along with tools and recommendations that can help guide organizations in assessing and resolving information security issues, complying with various privacy regulations, and ultimately helping improve national cyber security.

The report emphasizes that the best way to strengthen U.S. information security is to treat it as a corporate governance issue that requires the attention of Boards and CEOs. Information security is both a technical issue and a governance challenge that involves risk management, reporting and accountability. As such, it requires the active engagement of executive management and boards of directors across all industry sectors and among non-profit organizations and educational institutions. By using the ISG framework and assessment tools, organizations can integrate information security into their corporate governance programs and create a safer business community for themselves and the enterprises that interact with them.

Shannon Kellogg
Director of Corporate Government Relations
RSA Security, Inc.



"Perhaps most importantly, the [National Cyber Security] Summit served as a call to action. It represented a logical transition point from developing a national strategy to energizing the public-private partnership to implement concrete, measurable actions to improve the security of America's cyber systems...We are excited that the private sector is showing such initiative and we are committed to working together."-- **Robert Liscouski,** Assistant Secretary for Infrastructure Protection, U.S. Department of Homeland Security

The origin of this effort began in December 2003, when the U.S. Department of Homeland Security (DHS) co-hosted a National Cyber Security Summit in Santa Clara, California. The immediate outcome was the formation of the National Cyber Security Partnership (NCSP) and five NCSP task forces. Shannon Kellogg, Director of Corporate Government Relations at RSA Security Inc. explained that corporate governance was identified at the summit as a major issue that the government and private sector could work on together. Thus, the Corporate Governance Task Force was formed to create a private sector framework for organizations to improve ISG on a voluntary basis.

The recommendations that follow are designed for broad application to private sector businesses across all sectors, non-profit organizations and educational institutions:

- Organizations should adopt the information security governance framework described in the report and embed cyber security into their corporate governance process.

- Organizations should signal their commitment to information security *(Continued, Page 3)*

"The clarification of responsibilities and the quality analogy really helps when security investments are being considered - the business must decide whether the magnitude of the risk warrants the investment, it should not arbitrarily be restricted by the size of the security or IT budget. This doesn't mean they will always make the investment, but the decision is theirs to make, and the ISG process ensures they are involved in the assessment, and the decisions are made relative to the business need." -- **Mike Sullivan,** Chief Information Officer, Entrust, Inc.

"DHS has played a formative role in this effort by driving the creation of the task forces, and pushing the momentum in the private sector." -- **Dan Burton,** Vice President of Government Affairs
Entrust, Inc.

ISG Guidelines *(Cont. from Page 2)*
governance by stating on their website that they intend to use the tools developed by the Corporate Governance Task Force to assess their performance and report the results to their board of directors.

- All organizations represented on the Corporate Governance Task Force should signal their commitment to information security governance by voluntarily posting a statement on their website. In addition, TechNet, the Business Software Alliance, the Information Technology Association of America, the Chamber of Commerce and other leading trade associations and membership organizations should encourage their members to embrace information security governance and post statements on their websites. Furthermore, all National Cyber Security Summit participants should embrace information security governance and post statements on their websites, and if applicable, encourage their members to do so as well.

- The Department of Homeland Security should endorse the information security governance framework and core set of principles *(Continued, Page 4)*

The National Cyber Security Partnership (NCSP) is led by the Business Software Alliance (BSA), the Information Technology Association of America (ITAA), TechNet and the U.S. Chamber of Commerce in voluntary partnership with academics, CEOs, federal government agencies, and industry experts. Following the release of the 2003 White House National Strategy to Secure Cyberspace and the National Cyber Security Summit, the public-private partnership was established to develop shared strategies and programs to better secure and enhance America's critical information infrastructure. For more information, visit www.cyberpartnership.org.

Corporate Governance Task Force: Core Set of Principles

- CEOs should have an annual information security evaluation conducted, review the evaluation results with staff, and report on performance to the board of directors.
- Organizations should conduct periodic risk assessments of information assets as part of a risk management program.
- Organizations should implement policies and procedures based on risk assessments to secure information assets.
- Organizations should establish a security management structure to assign explicit individual roles, responsibilities, authority, and accountability.
- Organizations should develop plans and initiate actions to provide adequate information security for networks, facilities, systems and information.
- Organizations should treat information security as an integral part of the system lifecycle.
- Organizations should provide information security awareness, training and education to personnel.
- Organizations should conduct periodic testing and evaluation of the effectiveness of information security policies and procedures.
- Organizations should create and execute a plan for remedial action to address any information security deficiencies.
- Organizations should develop and implement incident response procedures.
- Organizations should establish plans, procedures and tests to provide continuity of operations.
- Organizations should use security best practices guidance, such as ISO 17799, to measure information security performance.

The **Cyber Security Industry Alliance** (CSIA), launched in February 2004 by a group of leading cyber security software, hardware and services companies, is an advocacy group dedicated to the improvement of cyber security through public policy, education and technology-focused initiatives.

Executive Director Paul Kurtz

The mission of the CSIA is to enhance cyber security through public policy initiatives, public sector partnerships, corporate outreach, academic programs, alignment behind emerging industry technology standards and public education. As the only public policy and advocacy group composed exclusively of security software, hardware and service vendors addressing key cyber security issues, the CSIA has growing influence in both the public and private sectors, and is an important voice in the CIP arena.

ISG Guidelines *(Cont. from Page 3)* outlined in the report, and encourage the private sector to make cyber security part of its corporate governance efforts.

- The Committee of Sponsoring Organizations of the Treadway Commission should revise the Internal Controls-Integrated Framework so that it explicitly addresses information security governance.

Howard Hantman, Director of Corporate Information Security at RSA Security Inc., played a key role in putting the framework together, drawing on his background as a practitioner and his experience in reporting to senior corporate management. "One of the major thrusts of this effort is to emphasize that the CIO cannot do it alone. True, it is the CIO that implements the controls, but it is the broader business that must identify information security as a function that is just as important as auditing the books. This framework identifies the specific responsibilities that senior executives and the board have as part of a governance architecture."

"This call to action is the work of many competing institutions coming together with common purpose -to develop a framework that is easy to understand and still leads to improved security; to develop a tool-set that organizations of all sizes can implement; and to deliver recommendations that will help get this done on a voluntary basis across many sectors of the economy. We have done our job and now we encourage CEOs and Boardrooms across this country to do theirs," said Art Coviello, president and CEO at RSA Security, and co-chair of the Corporate Governance Task Force.

"We cannot solve our cyber security challenges by delegating them to government officials or CIOs. The best way to strengthen US information security is to treat it as a corporate governance issue that requires the attention of Boards and CEOs," said Bill Conner, chairman, president and CEO, of Entrust, Inc., and co-chair of the Corporate Governance Task Force. "The call to action delivers the necessary framework, and the process to de-risk cyber security, corporate governance and our economy. As we implement these recommendations, we will reap the rewards of productivity growth, customer satisfaction and improved competitiveness, and gain the larger reward of enhanced homeland security."

The Cyber Security Industry Alliance, as well as TechNet, is currently engaged in outreach efforts promoting information security governance and the framework across industry, academia, and government. A full copy of the report can be downloaded at http://www.cyberpartnership.org/init-governance.html. ❖

LEGAL INSIGHTS

by Emily Frye

Cybersecurity and Corporate Governance Now: Does It Take Liability to Get Attention?

Corporate governance is an interesting animal. An amalgam of privately initiated and governmentally mandated directives, it resembles some kind of medieval beast when glimpsed from afar.

Up close, however, each appendage has a purpose. We are in the process of crafting another limb these days - although it's still hard to tell what it will look like.

The need for this new limb comes from the C-level ignorance about (or indifference to?) cybersecurity. A year ago, Adam Putnam (R-FL) circulated a draft of a bill he contemplated introducing in the House. Titled the Corporate Information Security Accountability Act (CISAA), it would have imposed information security audit reporting by all publicly traded companies. Adam Putnam, as Chair of the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census (under the umbrella of the Committee on Government Reform), had become increasingly concerned about what he perceived to be apathy toward a cybersecurity crisis on the part of corporate America.

Contemplation of a bill like CISAA set off an uproar among the private sector. Within weeks, almost every industry coalition that plays in this space was attacking the bill. On November 5, 2003, Adam Putnam convened the first meeting of a new coalition: The Corporate Information Security Working Group (CISWG). Putnam asked two questions: what's wrong with the draft of the bill? And - can you offer me a viable private-sector-led alternative to Congressional action?

Quickly, the group segmented into four teams: Best Practices, Procurement, Awareness and Education, and Liability and Incentives. Through March 2004, the teams toiled on the mundane essentials of any first-round policy process: recommendations.

Frankly, the first round of CISWG work was tedious and frustrating old ground for those of us who have worked on cybersecurity policy in recent years. The really interesting work began in May, when Bob Dix - the chief staff member running CISWG for Putnam - followed up on CISWG I with new energy to mobilize CISWG II: an even broader, more diverse group of talents to take CISWG beyond mere recommendations and into the scary realm of action.

Each team in the CISWG II has taken steps toward implementing the recommendations generated in CISWG I. Most dynamic has been the transformation of the "Best Practices" group into the "Metrics" group. Now, not only has CISWG generated a digest of best practices; it has come up with ways of measuring whether best practices have been implemented, and to what degree. Incentives and liability has matured into an analytical team that is cataloging incentives and safe harbors around cyberprotective behaviors. Awareness and Training had made October National Cybersecurity Awareness Month and Procurement has collected actual language used in existing contract templates for purposes of increasing the security of licensed software.

CISWG II is coming to a close in November - a year from the initiation of CISWG I. Whether it will go further has suddenly come into question. On September 28, 2004, Chairman Putnam announced that he had received a notable "promotion" to the House Rules Committee. While cybersecurity is near and dear to Putnam, his appointment leaves vacant the key catalytic position in the entire CISWG process. So as we go to press, the path is uncharted, the hierarchy undetermined, and the leadership ... uncertain. ❖

Board and CEO Responsibilities Outlined by Banking Regulators: FFIEC Booklets Provide Sector with Detailed IT Guidance

The Federal Financial Institutions Examination Council (FFIEC) has issued twelve IT Booklets to provide bankers with specific and helpful guidance for complying with IT regulations for financial institutions. The booklets, including Information Security and IT Operations, outline CEO and board-level responsibilities that banking examiners will consider when conducting IT audits. Senior corporate leaders, the guidance suggests, may delegate day-to-day responsibility for risk identification and assessment, physical and logical security, and use of qualified professionals. However, ultimate responsibility for "operational continuity and resilience" rests with senior officials.

The FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision. The FFIEC also develops recommendations to promote uniformity in the supervision of financial institutions. ❖

Function	CEO and Board-Level Responsibilities:
Business and IT Operations	● Effecting strong board involvement and awareness of IT activities ● Understanding risks associated with IT operations - existing and planned ● Determining risk tolerance of the institution ● Establishing and monitoring risk management policies ● Providing strategic technology planning
Information Security	The board of directors is responsible for overseeing the development, implementation, and maintenance of the institution's information security program. Oversight requires the board to provide management with guidance and receive reports on the effectiveness of management's response. The board should approve written information security policies and the information security program at least annually. The board should provide management with its expectations and requirements for: (1) Central oversight and coordination, (2) Areas of responsibility, (3) Risk measurement, (4) Monitoring and testing, (5) Reporting, and (6) Acceptable residual risk.

What the Nation's CEOs Say about Information Security

Business Roundtable is an association of chief executive officers of leading U.S. corporations with a combined workforce of more than 10 million employees in the United States. The Roundtable is committed to advocating public policies that ensure vigorous economic growth, a dynamic global economy, and the well-trained and productive U.S. workforce essential for future competitiveness. Business Roundtable believes that its potential for effectiveness is based on the fact that it draws on CEOs directly and personally, and presents government with reasoned alternatives and positive suggestions.

Following the terrorist attacks on the World Trade Center and Pentagon on September 11, 2001, Business Roundtable created a Security Task Force to address ways that the private sector could improve the security of employees, communities and companies. The Task Force is headed by FedEx Corporation's CEO, Fred Smith, and managed by Marian Hopkins, Director of Public Policy at the Business Roundtable.

The Roundtable believes that the business community has an important role in disaster response and recovery and must be a partner in a coordinated effort with federal, state and local governments. The government cannot face these challenges alone because more than 85 percent of the nation's critical infrastructure - the power grid, financial services, information services, railroads, airlines and others - is controlled by the private sector.

In May the Task Force released a report entitled, "Securing Cyberspace: Business Roundtable's Framework for the Future," which outlined the range of responsibilities for IT security. "Long-term security will follow only from shared responsibilities - whether hardening the Internet or protecting the supply chain, public and private sector must find new ways to collaborate," said Marian Hopkins. The framework includes the following principles:

Marian Hopkins
Director
Public Policy
Business Roundtable

1. Information security requires CEO attention in individual companies and as business leaders seeking collectively to promote the development of standards for secure technology.

2. Boards of directors should consider information security an essential element of corporate governance and a top priority for board review.

3. IT suppliers and end-users of these products and services have a shared responsibility for improving cyberspace security.

4. The Federal government plays an important collaborative role in information security and can assist the private sector response by sharing information about threats and vulnerabilities, helping companies overcome legal barriers and encouraging appropriate corporate actions.

(Continued, Page 10)

The Business Roundtable amended its "Principles of Corporate Governance" to include the following language:

Reviewing management's plans for business resiliency. As part of its oversight function, the Board of Directors should designate management responsibility for business resiliency. The Board should periodically review management's plans to address this issue. Business resiliency can include such items as business risk assessment and management, business continuity, physical and cyber security, and emergency communications.

The BRT's "Principles of Corporate Governance" are intended to help guide the continual advancement of corporate governance practices, and so advance the ability of U.S. public corporations to compete, create jobs and generate economic growth.

NFPA 1600 Standard: Governing Disaster, Emergency Management, and Business Continuity

The National Fire Protection Association (NFPA) and the American National Standards Institute (ANSI) have published a standard establishing a common set of criteria for disaster management, emergency management, and business continuity programs. The NFPA Disaster Management Committee is responsible for developing documents relating to preparedness, response, and recovery from disasters. In 1995, the Committee published NFPA 1600, Recommended Practice for Disaster Management. In 2000, the standard established a "total program approach" that provided a standardized basis for disaster/emergency planning and business continuity programs in private and public sectors. The 2004 standard retains the basic features of the standard published in 2000, but contains updated terminology and adds significant informational resources.

The standard requires the creation of emergency and continuity programs that include a coordinator and an advisory committee to set goals and procedures and establish performance objectives. The entity establishing the program must also conduct evaluations to assess the progress of the program. The NFPA standard identifies four main phases of emergency management that each program must incorporate: (1) Mitigation; (2) Preparedness; (3) Response; and (4) Recovery. Controlling entities must:

Conduct hazard identification and mitigation. Programs will conduct impact analysis to determine the potential damage that could be inflicted on personnel, continuity of operations, the financial condition of the entity, and public confidence in the controlling entity. The entity must subsequently develop a mitigation strategy that identifies resource capability shortfalls and includes a cost-benefit analysis. Mitigation strategies must consider such measures as:

(Continued, Page 9)

The **"Private Sector Preparedness Act of 2004"** requires DHS to develop and implement within 90 days of enactment of the legislation a comprehensive program to enhance private sector preparedness for disasters. Under the bill, the Homeland Security Secretary would develop guidance and identify best practices to assist action by the private sector in:

(1) Identifying hazards and assessing risks and impacts;
(2) Mitigating the impacts of a wide variety of hazards, including weapons of mass destruction;
(3) Managing necessary emergency preparedness and response resources;
(4) Developing mutual aid agreements;
(5) Developing and maintaining emergency preparedness and response plans, as well as associated operational procedures;
(6) Developing and maintaining communications and warning systems;
(7) Developing and conducting training and exercises to support and evaluate emergency preparedness and response plans and operational procedures;
(8) Developing and conducting training programs for security guards to implement emergency preparedness and response plans and operations procedures; and
(9) Developing procedures to respond to external requests for information from the media and the public.

In addition, the legislation would require the DHS Secretary to support development of, promulgate, and regularly update "national voluntary consensus standards" for private sector emergency preparedness.

NFPA 1600 *(Cont. from Page 8)*

- Protective systems or equipment for both cyber and physical risks;
- Establishment of hazard warning and communication procedures;
- Redundancy or duplication of critical personnel, systems, equipment, information, operations, or material.

Establish short and long-term procedures to reduce or eliminate risks. Each emergency management program must include a strategic plan, an emergency operations/response plan, a mitigation plan, a recovery plan, and a continuity plan. Continuity planning should include such elements as pre-delegation of emergency authority, standard operating procedures, and an emergency operations center. The entity will also conduct emergency exercises and evaluations and record lessons learned. The standard outlines the components of a proper Corrective Action Program that must be developed for deficiencies identified in the evaluation process.

The standard also emphasizes the importance of having a sound, flexible financial and administrative framework that complies with the program's requirements and is associated with the disaster/emergency operations. The framework must accommodate financial functions in emergency situations and the process must be documented in a written process so that data can be captured for future cost recovery. The NFPA gave the financial department a significant role in developing proper procedures, including:

- The financial department should be a member of the program committee;
- The financial department should be actively involved in identifying, prioritizing, and purchasing internal and external resources;
- The entity's financial opportunities or limitations should be identified within the strategic plan that defines the goals of the program.

Develop an incident management system that can coordinate response, continuity and recovery activities. An effective system will designate responsibility for management functions during an emergency through checklists or standard operating procedures. The standard lays out a set of response procedures that each program should incorporate that include:

- Control of access to the affected area;
- Identification and accounting for personnel engaged in activity in the incident;
- Mobilization and freezing of resources;
- Care of populations affected by emergency;
- Provision for stress management for engaged personnel and responders.

Congressman Jim Turner (D-TX) introduced a bill to enhance private sector emergency preparedness through a "community standard" for security.

Response elements of the program should also emphasize crisis communication and public information capabilities. The entity should ensure that all personnel receive information about their role in an incident and that there is a method of notifying the public about an incident and providing people with procedures to protect themselves. The NFPA recommended a central contact facility for the media, an information handling system to coordinate and clear information, and pre-scripted information bulletins as ways to disseminate information quickly and efficiently in an emergency.

Set recovery priority and time objectives. Recovery objectives are closely tied to the identification of critical functions and internal and external interdependencies. The entity must develop a recovery plan based on short- and long-term priorities, processes, vital resources, and acceptable time frames for restoration of services, facilities, programs, and infrastructure. After an incident, programs must conduct a situation analysis that includes a damage assessment and the

(Continued, Page 10)

BRT *(Cont. from Page 7)*

5. Public policy initiatives on cyber security should take a balanced and comprehensive approach that reflects the shared responsibility of end-users and IT suppliers.

6. Market solutions to cyber security are to be preferred over statutory and regulatory mandates.

7. Public disclosure of corporate information security practices should be voluntary, not mandatory.

Business Roundtable recognizes the long-term, complex challenges entailed in securing cyberspace. The Roundtable is committed to advancing the above principles and to undertaking measures that (i) inform and guide its CEOs on appropriate risk management processes and procedures for ensuring that their companies' IT systems and networks are adequately secure and the potential consequences of disruptions adequately managed; (ii) urge the marketplace to improve the overall quality and reliability of security in IT products and services; and (iii) engage and partner with leaders in the Executive Branch and Congress to develop effective, common-sense public policies that strengthen the security of cyberspace. ❖

NFPA 1600 *(Cont. from Page 9)*
identification of resources needed to support response and recovery operations.

Rep. Jim Turner (D-Texas), ranking member of the House Select Committee on Homeland Security, and other Democrats introduced in July the “Private Sector Preparedness Act of 2004,” a bill that would require the Department of Homeland Security (DHS) to issue a single, national standard for preparedness, security training, and recovery in the private sector. The bill encompasses a first-ever "community standard" for security and is underlined by NFPA 1600.

"On September 11, many companies lacked evacuation plans," Turner said in introducing the bill. "Businesses did not have the ability to identify who was working that day, or business continuity plans to resume their operations following the attacks." As 9-11 Commission Vice Chair Lee Hamilton noted, with 85 percent of the nation's critical infrastructures owned and operated by the private sector, the public sector alone could not guarantee the safety of Americans. The 9-11 Commission recommended that the private sector take specific steps to ensure preparedness for all disasters, emergencies, and acts of terrorism, and endorsed the NFPA 1600 standard. "This bill will enhance the current DHS business preparedness initiatives and will ensure the recommendations of the 9-11 Commission are put into place," Turner said. ❖

The CIP Program is directed by John A. McCarthy, a member of the faculty at George Mason University School of Law. 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 infrastructures. 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 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/archives/cipp-report-l.html.