3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008, USA
Telephone: 847.253.1545
Facsimile: 847.253.1443
Web Sites: *www.isaca.org*

20 September 2010

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive
Stop 8930
Gaithersburg, MD 20899

RE: Cybersecurity, Innovation and the Internet Economy

Dear Ms. Honeycutt,

The Department of Commerce Internet Policy Task Force has been charged with reviewing the cybersecurity challenges that confront the commercial sector, with an objective of ensuring that commercial enterprises and individuals can trust that their use of the Internet is safe and secure. The Internet is an engine for economic growth. It is a tool that supports education programs, civic activity and the cultural life of communities. If trust in the internet and the foundational infrastructure on which business and community services are delivered is absent, the value of the Internet will be diminished and the commercial innovation it promises cannot be achieved.

Information security professionals and information systems auditors play a vital role in ensuring trust in, and value from, information systems. Information security professionals deliver value from information systems by ensuring that the systems can be trusted. Information systems auditors provide assurance that systems can be trusted and that organization management will receive the expected value from information technology. Since the earliest days of computing, these professionals have been responsible for identifying risks, implementing and managing controls, and attesting that information is protected and systems can be trusted.

ISACA is an independent, nonprofit, international association of information security, risk management and assurance professionals (95,000 constituents in 160 countries). ISACA's members have developed, implemented, managed and assessed cybersecurity controls in commercial and critical infrastructure organizations, as well as governments, on a global basis.

ISACA contributes to the development of international security standards addressing the cybersecurity needs of organizations through a liaison relationship with the International Organization for Standardization (ISO). We have developed frameworks such as *Control Objectives for Information and related Technology* (COBIT®), which are accepted internationally and have become *de facto* standards for defining information systems controls. COBIT is utilized by a number of federal agency Inspectors General and has been successfully implemented within organizations such as the Department of Veterans Affairs and the Federal Savings and Loan Insurance Corporation. In addition, it is routinely used by leading enterprises worldwide.

ISACA provides for the continued development of its members through training and research. We also offer several distinct certifications that attest to the capabilities of assurance professionals. The Certified Information System Auditor™ (CISA®) certification, which was first offered in 1978, has been earned by almost 80,000 professionals since the program's inception. The Certified Information Security Manager® (CISM®) designation, which is specifically intended to demonstrate professional excellence in developing and managing cybersecurity programs, has been earned by more than 14,000 professionals since 2002. Both certifications are ANSI-accredited under ISO/IEC 17024:2003. Each is included in the select certifications formally approved by the US Department of Defense in its Information Assurance Technical category (DoD 8570.01-M).

As a body of professionals deeply involved with cybersecurity, and as contributors who ensure the trustworthiness of information systems, we appreciate the opportunity to contribute our views on cybersecurity, innovation and the Internet economy. We would be happy to discuss these ideas in further detail, and provide any other assistance that might be required to ensure that efforts to provide a safe and secure national cyberinfrastructure are successful and lasting.

Respectfully submitted

Richard M. Clark
Chair
ISACA Government and Regulatory Agencies Subcommittee

Attachment A

General Comments

The evolution of information systems can be characterized as a battle between those intent on compromising the security and integrity of systems and those who are charged with designing, implementing and managing the security of systems. Efforts to provide information systems that can be trusted have often lagged behind the exploits of those bent on compromising private or sensitive information or criminally exploiting systems.

The solution to the cybersecurity challenge cannot be solely technical. The Business Model for Information Security (www.isaca.org/bmis), introduced by the Marshall School of Business at the University of Southern California, and developed by ISACA, presents cybersecurity in a systemic way, whereby elements (organization, people, process and technology) are linked via dynamic interconnections (DIs) such that any change in an element or DI affects the rest of the system. The DIs (culture, human factors, architecture, enablement and support, governing, and emergence) each contribute to and influence security outcomes, resulting in systems that can be trusted or, conversely, are vulnerable to compromise and exploitation. A cybersecurity solution that does not integrate all of the components of the security system will prove to be ineffective. Reliance on technical solutions without considering the organization, its culture, the human factors inherent in the technology, and the way processes both support the technical solution and are enabled by technology will result in systems that do not achieve the desired level of protection.

Those who are intent on compromising our cybersecurity infrastructures design their attacks to look for the weakest link in the system. Those who design information and communication technologies, and who implement and manage assurance programs, need to take the same system perspective.

An organization's cybersecurity system resides within a governance structure. Within the governance structure, resources and risks are managed and value is delivered to stakeholders. Cybersecurity risks are one component of risk that management needs to consider within the context of an enterprise risk management program. Since cybersecurity is tightly intertwined with how systems are implemented, managed and used; cybersecurity risks can be defined using the definition of operational risk found in Basel II: operational risks result from inadequate or failed internal processes, people and systems, or from external events. Preventing losses from cybersecurity risk requires an understanding of business objectives, and management's attention to planning and organizing a cyberenvironment that can be trusted, acquiring and implementing technology and supporting processes necessary to meet organizational needs, delivering value by managing technology and data resources, and monitoring and evaluating the performance of the entire system of security.

COBIT Security Baseline: An Information Security Survival Kit (www.isaca.org/cobit) outlines the high-level processes that management should consider to effectively implement and control cybersecurity risks. This essential process guide outlines the baseline controls, including management planning, human resources, third-party relationships, system security, configuration management and process monitoring. These controls are within the capacity of small, medium

and large organizations, and within their technical capabilities as well, once they are understood. These controls form the baseline requirements for the availability of cybersystems, the confidentiality of private and sensitive information, the integrity of automated processes, and trust that cybersystems will deliver the value intended.

The benefit of taking a broad system view of cyberprotection and the value of a baseline of effective management procedures have been demonstrated in research studies. ISACA and several other leading commercial and not-for-profit organizations that are concerned about security and risk management, have joined together in an alliance to identify best security practices and define how these practices enhance organization performance. The IT Policy Compliance Group (www.itpolicycompliance.com) has completed several studies that demonstrate that business advantage accrues to organizations that prudently manage information systems and implement effective control structures. The September 2009 IT Policy Compliance Group report, *Guidance for Best Practices in Information Security and IT Audit*, identified the characteristics of the best-performing organizations. These organizations identify unacceptable business risks related to IT and define internal standards related to integrity, availability, and confidentiality of information and IT assets. They employ guidance found in security regulations from NIST or ISO and implement best practice frameworks such as COBIT. They conduct frequent assessments to determine the effectiveness of controls as measured against the standards they defined for integrity, availability and confidentiality. As a result, these best-performing organizations spend 55 percent less than other organizations on regulatory audits. Their exposure to loss of customer data was the lowest among companies surveyed. Customer retention was 6 percent higher than other organizations. Also higher were annual revenues (8 percent) and profits (6 percent). These admirable achievements are well within the reach of other commercial organizations. A 2010 report by the IT Policy Compliance Group, *Automation, Practice and Policy in Information Security*, reported that best-performing organizations identify critical assets and manage technical controls and configurations. These organizations understand where they are vulnerable and address these vulnerabilities. As a result, they experience the least downtime from cybersecurity events and suffer fewer incidents of data loss or theft. These reports demonstrate that, by implementing sound management practices, understanding risks and implementing effective control processes, an organization can reduce risk and, perhaps more important, innovate in ways that enhance business performance.

The Department of Commerce Internet Policy Task Force's notice of inquiry identified several areas of policy concern related to cybersecurity, including understanding the economic impact of cybercrime, building cybersecurity awareness, developing web and component security, creating effective authentication and identity management systems, engaging with others globally to effect cybersecurity, developing product assurance programs, conducting research and developing secure products, and implementing best practices. Each of these is a significant contributor to cybersecurity. However, these alone will not fill the cyberprotection gap or lead organizations to improved risk management and enhanced security performance.

Understanding the potential financial and operational consequences of cyberincidents supports management's risk management decision making. Cybersecurity awareness helps organizations, technicians and users to identify threats and implement prudent protection measures. Developing secure products through research and properly planning for the configuration and use of

technology are necessary steps in advancing cyberprotection as long as this technology placement and use are considered within the larger context of the organization, the technical architecture, the human factors that will make the technology usable or will introduce vulnerabilities, and the processes that are intended to support technology solutions. Since organizations' first use of computers, authentication and authorization have presented challenges. With the proliferation of technology and networked global systems, identity management has become even more critical. A focus on the need for best practices is essential if cybersystems are to be trusted and the value expectations of users achieved.

Specific Responses

Quantify the Economic Impact

Understanding the rate of cybersecurity victimization and the financial and operational impact these incidents have is important in policy planning for governments and organizations. The challenge in cybercrime—and all other types of crime—is collecting accurate and complete crime data. For non-cybercrimes, the federal government relies on the National Crime Information Center Uniform Crime Report to provide data relative to criminal incidents. Police agencies are required to submit crime reports to the NCIC, which enables a nationwide view of crime and investigation into specific factors related to crime.

However, even with a strict mandate, the Uniform Crime Report is not completely accurate. A similar approach for cybercrime would be difficult to implement since a mandate for all business organizations would be costly to administer. As an alternative, the National Criminal Justice Reference Service conducts various crime studies, including victimization studies. While these provide a distinct view of criminal incidents, victims may misrepresent or misclassify an incident, reducing the validity of the information. In certain critical infrastructure industry segments, anonymous reporting centers have been created to enable organizations to self-report criminal and other incidents. Information is made available to all participants, giving organizations insight into incident rates and impacts while maintaining the anonymity of the reporting organization.

Although this type of collective capability is valuable, it would be difficult to develop reporting centers for all business segments where anonymity could be ensured and participation mandated. A solution would be to use the research capabilities of the National Criminal Justice Reference Service to conduct cyberincident studies. Such an approach would leverage existing research capabilities while also providing a body of data that researchers and academics could leverage. To date, a body of empirical studies related to information security has not been developed. With the National Security Agency Information Assurance focus on creating National Centers of Academic Excellence, the number of academic programs and researchers has significantly increased. Making current and cybersecurity trend data available to this body of researchers would greatly increase the number of empirical studies that could be undertaken while also building theories that could greatly enhance the capability of government and industry to quantify and address cybersecurity issues.

Raising Awareness

Awareness is an effective means of avoiding cybersecurity incidents. Many exploits are successful because users trust identity claims or do not understand how to remain safe on the Internet. Many organizations have long recognized the importance of information security education as part of an effective protection program. This concept needs to be developed so that the general public can be made more aware of threats and protective measures and business organizations that lack dedicated and capable security staff can implement appropriate controls. While the need for cybersecurity awareness is great, the resources available to address this need are also extensive. Recently the Department of Homeland Security closed the National Cybersecurity Awareness Campaign Challenge, in which individuals and organizations competed by submitting plans for increasing cybersecurity awareness. The challenge resulted in many innovative approaches being presented. Similar campaigns should be conducted on a regular basis. Winning entries should be funded by the government, ensuring a diversity of awareness approaches targeting different audiences through different communications channels. Bringing together the resources of commercial organizations, schools, community groups and not-for-profit professional associations would provide the breadth of coverage needed to make cybersecurity awareness a national reality.

Global Engagement

The Internet has created an international environment in which individuals can communicate and share information and businesses can offer products and services. Regrettably, that same environment enables criminal elements to avoid detection and accountability for their actions. The international character of the Internet makes it necessary for all national bodies to recognize that the global cyberworld cannot be restricted by borders established within the physical world.

National standards bodies need to harmonize their work with international groups such as ISO so that standards required in one geography are consistent with those applied in others. Of particular importance are definitions and approaches related to privacy. All governments understand the importance of protecting personally identifiable information; however, definitions and approaches to privacy protection differ based on custom and law. International accords for the protection of privacy information need to be developed and agreed to by all governments to facilitate the continued evolution of global e-commerce. In addition, governments need to work together to eliminate safe havens for those who maliciously attack and compromise information systems or execute exploits against Internet users. Legal accords need to be agreed worldwide so that cybercriminals can be brought to justice.

An Incentives Framework for Evolving Cyber-Risk Options and Cybersecurity Best Practices

The challenge in cybersecurity is not that best practices need to be developed. The challenge is in communicating those best practices, demonstrating the value of implementing them, and encouraging individuals and organizations to adopt them. This represents an opportunity for ongoing research, enhanced communication and awareness, and engagement by the Small Business Administration and others who directly support commercial organizations. Just as the IT Policy Compliance Group, noted above, conducts timely research into best practices and business results, there is a need to identify best practices and quantify their beneficial impact in terms of risk reduction, business enablement and innovation. Conducting studies is not sufficient since many busy executives will not have the time to explore what current research tells them. Instead, the efforts of government agencies to promote best practices or to integrate best

practices into regulations or standards will aid adoption and use. Leveraging groups involved in promoting cybersecurity awareness will also help to ensure that the value of best practices becomes generally known.