STATEMENT

OF

CATHERINE A. ALLEN
CHAIRMAN AND CEO, THE SANTA FE GROUP

BEFORE THE

UNITED STATES CONGRESS
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON INFORMATION POLICY,
CENSUS AND NATIONAL ARCHIVES
US HOUSE OF REPRESENTATIVES

HEARING ON
CYBERSECURITY: A REVIEW OF PUBLIC AND PRIVATE SECTOR EFFORTS TO SECURE OUR NATION'S INTERNET INFRASTRUCTURE

OCTOBER 23, 2007

**TESTIMONY OF CATHERINE A. ALLEN**
**CHAIRMAN AND CEO, THE SANTA FE GROUP**

**Introduction**

Thank you, Chairman Clay, and Members of the Subcommittee and Committee for the opportunity to submit testimony before you today on private and public sector efforts to secure our nation's Internet infrastructure.

My testimony today will address three points:

- The importance of resiliency and security of the Internet
- Important steps the private sector is taking to prevent and respond to Internet disruptions and security threats
- Recommendations for the public sector on ways to improve resiliency of the Internet and coordinate recovery, if disrupted

I am Catherine Allen, Chairman and CEO of The Santa Fe Group, a strategic consulting firm specializing in risk management, fraud prevention, business continuity, payments risk and information security, based in Santa Fe, New Mexico. Earlier this year I retired as the Founding CEO of BITS, a CEO-driven nonprofit financial services industry consortium of 100 of the largest financial institutions in the U.S. BITS is a division of The Financial Services Roundtable.

BITS' mission is to serve the financial services industry's needs at the interface between commerce, technology and financial services. BITS members hold about $9 trillion of the nation's total managed financial assets of about $18 trillion. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect. BITS works with government organizations including the U.S. Department of Homeland Security, U.S. Department of the Treasury, federal financial regulators, Federal Reserve, technology associations, and major third-party service providers to achieve its mission.

The Santa Fe Group is a strategic partner and preferred provider to BITS. The Santa Fe Group has worked with BITS since I was recruited to lead BITS ten years ago. Many Santa Fe Group staff members are former BITS employees. The Santa Fe Group has managed a number of projects for

BITS related to safety and soundness of financial infrastructures. Today we manage the Financial Institution Shared Assessments Program, an industry-led effort that helps ensure security and efficiency in the third-party service provider security assessment process through rigorous standards and safeguards that are being adopted by financial institutions and their service providers. The Santa Fe Group also created the Santa Fe Group Vendor Council, a service provider-led group that takes a leadership role in the financial services industry to discuss issues of security and reliability. This group works with financial institutions and publishes best practices for ensuring the reliability of the systems upon which financial institutions rely, including the Internet. The Santa Fe Group's core capability is risk management consulting for financial institutions on such issues as fraud reduction, safety and security, and payments systems.

I speak today as a subject matter expert, rather than on behalf of BITS or the financial services industry. But because of my past responsibilities at BITS, I will be mentioning some of the work the industry, through BITS, has accomplished in the business continuity and security areas.

Like you, Chairman Clay, I too am originally from Missouri. I grew up in northeast Missouri in a rural area 100 miles from St. Louis. Access to the Internet has brought a multitude of opportunities to my hometown that weren't there in my childhood. Resiliency of the Internet is as critical to economic growth, banking, communications, education and farming in that town as it is to national security. The Internet offers rural Americans access to global opportunities. I now live in New Mexico, another state that is largely made up of ranches, Indian reservations, small towns and rural areas. It too has benefited from global access the Internet provides, from selling art and Navajo rugs to Europeans online, to supporting our national laboratories at Sandia and Los Alamos, to providing the basis for development of the film, alternative energy and aeronautics industries in our state.

A resilient and secure Internet infrastructure that serves as our economic and communications backbone is critically important to economic growth and competitiveness.

**Importance of Resiliency and Security**

Our nation's competitiveness, economic vibrancy and physical security relies on the security, reliability, recoverability, continuity and availability of information infrastructures and systems, most importantly, the Internet. The information technology, telecommunications and power industries play the most critical roles because they are the underpinnings of the Internet. If there are security threats caused by malware, hacking or denial of service based on vulnerabilities in software, hardware or other components, there are likely to be disruptions. The telecommunications, power and IT industries are interdependent. A disruption in one means a disruption in another.

In the industry where I have spent most of my career — financial services — continuity of services is not only a regulatory requirement, it is essential in managing our reputational, operational and financial risks. Customer trust in the security and continuity of financial transactions is vital to the stability of the industry and the strength of the nation's economy.

The financial sector is both a target for cyber criminals, as organized crime shifts from drugs to fraud and identity theft to maximize revenues, as well as terrorists, who use the Internet for money laundering, communications, and financing. With 9/11, the industry has also become a symbolic target.

The threats to resiliency and security of the Internet include:

- Exponential growth of purposeful, targeted criminal activity, especially by organized criminals.
- Online crimes like phishing, which targets the financial services industry in 9 of 10 instances, are thriving. At any given time, fraudulent websites mimic hundreds of brands.
- Hundreds of software vulnerabilities are discovered each month in various applications, from browser plug-ins to critical business software.
- Even commonly used firewalls and anti-virus solutions from the worlds largest vendors are affected by severe vulnerabilities.

What is important for the Subcommittee to consider is how pervasive the Internet is today, for all types of businesses, for all types and ages of users and for all geographic regions in the world. Cell phones with Internet access can be found in any developing country or at the base of Canyon

de Chelly. Blackberries are used for Internet access from Bejing to Bowling Green, Missouri. Farmers access the Internet to check commodities futures markets and grandmothers download pictures of their grandbabies across the globe.

Major Internet disruptions would not only undermine global commerce and financial transactions, it would disrupt the way we live our lives every day, across the world.

**Private-Sector Efforts**

The financial services industry has done a great deal to strengthen business continuity planning and to coordinate prior to and during times of crisis. Financial institutions have business continuity plans which they constantly update, refine and test. This is a regulatory requirement and part of our risk management process. Financial institutions are driven to understand and manage IT-related risks because of several factors:

- Reputational risk if systems fail and customer information and transactions are compromised
- Financial risk if electronic payments and transactions systems are breached and fraud occurs
- Regulatory compliance risks if appropriate policies and procedures are not followed

Most financial institutions — and all that are deemed mission-critical to the U.S. economy — are required by our regulators to have recovery operations in place and back-up in a very narrow timeframe if disruptions occur. All are required to have back-up facilities and to be able to transition systems in near real time. If the Internet is down because of vulnerabilities in IT, telecommunications or power, we cannot meet our regulatory requirements.

I want to highlight some examples of the financial services industry's leadership in mitigating some of the risks it faces, because these examples can be models for all critical infrastructure industries.

Members of the financial services industry are sharing information, analyzing threats, creating best practices, and urging the software and technology industries to do more to provide more secure products and services. The financial services industry has established the Financial

Services Information Sharing and Analysis Center (FS-ISAC) and the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) to share information on threats and to coordinate and collaborate with government agencies. The FS-ISAC and the FSSCC continue to work with the U.S. Department of Treasury and DHS to promote information sharing and best practices within the sector and across other critical infrastructure sectors such as telecommunications and energy. Most of BITS' work over the past decade has been shared with and adopted by the FS-ISAC and FSSCC as well as being made public and free to the industry.

For many years BITS and others in the financial services industry have urged major software providers to develop more secure software and to accept greater accountability for the software they market and service. This has been part of a larger effort by members of the user community that rely on technology provided by the information technology industry—private-sector companies, universities, and government agencies—to demand greater *accountability* for the security of information technology products and services.

- The *BITS Consumer Confidence Toolkit: Data Security and Financial Services* provides an overview of industry efforts to address data security challenges. BITS is currently working on projects to address key management challenges with encryption technologies and the security of wireless technologies.
- In 2004, BITS hosted a Software Security CEO Summit to bring leaders from the financial services and information technology communities together. We outlined the impact that software vulnerabilities have on the financial services industry, proposed business requirements for software companies, and offered procurement language for financial institutions to use. Following the Summit, we initiated joint work plans with major software providers and developed a best practices guide for patching and testing software.
- In 1999, BITS created the BITS Product Certification Program (BPCP) which provides product testing by unbiased and professional facilities against baseline security criteria established by the financial services industry. A product certification, the *BITS Tested Mark*, is awarded to those products that meet the defined criteria. An option is available for technology providers to meet the product certification requirements via the internationally recognized Common Criteria certification schema. BITS has urged DHS to support efforts to enhance product certification programs, including the Common

Criteria program run by the National Security Agency (NSA) and National Institutes of Technology and Standards (NIST).

- Financial institutions have extensive expertise in educating customers about securing their computers and avoiding the lure of fraudsters. However, financial institutions also know that this is an ongoing challenge. In 2005, The Roundtable's Board of Directors approved the *Voluntary Guidelines for Consumer Confidence in Online Financial Services* and *Critical Success Factors for Security and Awareness Programs of Financial Institution Employee.*
- BITS has been focusing on making email more secure and reliable. Email is a necessary and important means of communication with customers, business partners, and service providers. In April 2007, BITS released the *BITS Email Security Toolkit: Protocols and Recommendations for Reducing the Risk.* The toolkit recommends email technology protocols for financial services, Internet service providers, and other business partners. BITS would encourage government agencies to adopt these protocols too and work in partnership with financial institutions, Internet Service Providers and others to increase the security of email as a communication channel.
- One critical area of security and reliability is that of managing third-party service providers. The Financial Institution Shared Assessments Program, launched by BITS and managed by The Santa Fe Group, is helping to facilitate risk management of service providers, consolidate various security standards, and provide a rigorous program that introduces efficiencies in the service provider assessment process. The Shared Assessments Program grew out of the efforts of the BITS IT Service Provider Working Group, which has been addressing managing third-party risk since BITS' inception in the mid-90s. The Shared Assessments Program is based on two essential documents: the Standardized Information Gathering Questionnaire (SIG), which gives financial institutions a detailed "snapshot" of the security controls at the service provider's location and the Agreed Upon Procedures (AUPs), whose 45 control points can be used by assessment firms or qualified CPAs to create detailed reports regarding the effectiveness of the controls. To date, more than 50 organizations are involved in the Shared Assessments Program and there is increasing interest in overseas firms that provide services to financial institutions. The Shared Assessments effort is based on previous work of the BITS IT Service Provider Working group which developed the *BITS Framework for Managing Technology Risk for IT Service Provider Relationships* and the *BITS IT Service Provider Expectations Matrix.* Other major documents produced through

the BITS IT Service Provider Working Group include the *BITS Key Considerations for Global Background Screening Practices* and *Key Contractual Considerations for Developing an Exit Strategy*.

- Another example is the work BITS did on telecommunications resiliency and diversity. The *BITS Guide to Business-Critical Telecommunications Services* was completed in 2004 based on extensive work by BITS members, participation by all the major telecommunications companies, and involvement by the National Communications System as well as the President's National Security Telecommunications Advisory Council. The guide is a comprehensive tool that is used by financial institutions to better understand the risks and strategies for working with telecommunications companies to deliver more diverse and secure telecommunication services.
- In 2005, BITS urged the FSSCC to establish a committee to outline research and development priorities based on recommendations in the Administration's National Strategy to Secure Cyberspace and National Strategy for Physical Protection of Critical Infrastructures and Key Assets. The FSSCC's R&D Committee, working in partnership with the Treasury Department, issued a list of research challenges designed to further strengthen the security and resilience across the sector and then published a research agenda. The FSSCC research agenda identifies the most promising opportunities for research and development initiatives in the following areas:
    - Secure Financial Transaction Protocol
    - Resilient Financial Transaction System
    - Enrollment and Identity Credential Management
    - Suggested Practices and Standards
    - Understanding and Avoiding the Insider Threat
    - Financial Information Tracing and Policy Enforcement
    - Testing
    - Standards for measuring ROI of CIP and Security Technology

The FSSCC is working in partnership with the Treasury Department and Federal financial regulators involved in the Financial and Banking Infrastructure Information Committee (FBIIC) to develop the Sector Specific Plan (SSP) for the Banking and Finance Sector and research and development priorities. The Banking and Finance Sector Specific Plan SSP was completed earlier this year and joined with 16 other sector specific plans as part of the National Infrastructure Protection Plan (NIPP). The Banking

and Finance SSP outlines a strategy for working collaboratively with public and private sector partners to identify, prioritize and coordinate the protection of critical infrastructure, including information security. It describes how this public-private partnership has become part of the fabric of our sector over the past four years and identifies areas where work remains to be done.

The financial services industry, through the FSSCC and FBIIC, sponsored by the US Department of the Treasury and the Securities Industry and Financial Markets Association (SIFMA), recently completed a pandemic exercise. More than 2,700 companies participated. One aspect of the exercise looked at systemic risks to the sector, including potential disruptions of the Internet if overloaded by demand from people working at home.

Additional examples of these leadership initiatives include:

- The Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) and Information Sharing and Analysis Center (FS/ISAC) initiatives to strengthen the industry's infrastructure
- Industry's contributions to the National Strategy for Critical Infrastructure Assurance
- Convening of numerous conferences, meetings and calls to bring together leaders and experts to discuss security and business continuity issues
- Developing industry emergency communication tools
- Conducting worst-case scenario exercises for multiple threats, including cyber threats
- Engaging in partnerships with the telecommunications sector and key software providers on interoperability issues
- Compiling lessons learned from 9/11, the August 2003 blackout and Hurricane Katrina
- Publishing best practices and voluntary guidelines, from telecommunications resiliency to recoverability should there be a power failure affecting financial services
- Creating a model for regional resiliency and disaster-recovery coalitions and helped establish ChicagoFIRST
- Collaboration and pilots with the telecommunications industry and National Communications System for diversity and redundancy of telecommunications circuits and facilities

- Public presentations and Congressional testimony that have raised the public's and policy makers' awareness of the interdependencies among the sectors at the same time demonstrating that the financial services sector is far ahead of other sectors
- Publishing a study of industry security investments for the Council on Competitiveness's Task Force on Competitiveness and Security.
- Contributing to the Business Roundtable's publication of "Essential Steps Toward Strengthening America's Cyber Terrorism Preparedness."
- Publishing the Financial Services Roundtable's Report of the Blue Ribbon Commission on Mega-Catastrophes

**Recommendations**

The 2006 GAO Report, *Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan* outlines some of the key challenges to establishing a plan for recovering from an Internet disruption, much of which related to DHS legal and organizational issues. It recommends to Congress that it consider clarifying the legal framework guiding Internet recovery. It also makes recommendations to the Secretary of DHS to strengthen the Department's ability to effectively serve as a focal point for helping to recover from Internet disruptions by establishing clear milestones for completing key plans, coordinating various Internet recovery-related activities, and addressing key challenges to recovery planning. Our industry agrees with this recommendation. But there is much more to be done.

Financial institutions are heavily regulated and supervised. Financial regulators, primarily through interagency efforts of the Federal Financial Institutions Examination Council (FFIEC), have issued numerous regulations and supervisory guidance on information technology covering many aspects including management, information security, outsourcing, business continuity planning, and consumer protection. Regulators constantly examine financial institutions to ensure compliance with these dynamic requirements. In response, financial institutions continue to demonstrate that they have adequate controls in place to mitigate these risks.

Collectively, these efforts by financial institutions and the financial regulators are helping to improve the resiliency of the financial services industry, as well as the Internet. We believe these

same practices and policies should apply to the government and other critical infrastructure industries, especially IT, telecommunications, and power.

Several common steps serve as the foundation for many of our tools that are relevant to government programs:

- **Secure and maintain senior management commitment to ensure that organizations have the appropriate incentives, adequate funding, and training for technicians and users.**
- **Assess risks on an ongoing basis and participate in information sharing and analysis programs.**
- **Implement appropriate controls (e.g., access controls, authentication, physical security, encryption, employee background checks, insurance) based on changing risks.**
- **Manage third party providers effectively and focus on critical interdependencies with other sectors.**
- **Establish meaningful metrics to measure and understand risks, assess gaps, and measure progress.**
- **Educate users through training and awareness programs.**
- **Test regularly to ensure that the technology, people, and processes are working effectively at appropriate levels of assumed residual risk.**
- **Measure progress through meaningful and independent audits.**

These steps and risk-based policies need to be adopted by critical infrastructure industries.

Congress can help critical infrastructure industries meet the challenges of a post-9/11 environment in a number of ways. We ask that the committee consider these recommendations:

1. **Recognize that the financial sector is driven by its "trusted" reputation as well as regulatory requirements.** Other industries do not have the same level of regulatory oversight, liability, or business incentives. However, we rely on other sectors because of our interdependencies. Responsibility and liability need to be shared.
2. **Maintain rapid and reliable communication.** Critical infrastructure industries and the public need to have an early understanding of the scope and cause as early as possible when a major event occurs. During the August 2003 blackout, the announcement that the

problem was not the result of a terrorist event alleviated public concerns and made for orderly execution of business continuity processes. Diverse communication channels such as cell phones, wireless email devices, landline phones, and the Internet are necessary. Both diversity and redundancy are needed within critical infrastructures to assure backup systems are operable and continuity of services will be maintained.

3. **Recognize the dependence of all critical infrastructures on software operating systems and the Internet.** Given this dependence, Congress should encourage providers of software to critical infrastructure industries to accept responsibility for the role their products and services play in supporting the nation's critical infrastructure. In so doing, Congress should support measures that make producers of software more accountable for the quality of their products and provide incentives such as tax incentives, cyber-insurance, liability/safe harbor/tort reform, and certification programs that encourage implementation of more secure software. Congress also could provide protection from US antitrust laws for critical infrastructure industry groups that agree on baseline security specifications for the software and hardware that they purchase.
4. **Encourage regulatory agencies to review software vendors—similar to what the regulators currently do in examining third-party service providers**—so that software vendors deliver safe and sound products to critical infrastructure industries.
5. **Encourage collaboration and coordination among other critical infrastructure sectors and government agencies to enhance the diversity and resiliency of the telecommunications infrastructure.** For example, the government should ensure that critical telecom circuits are adequately protected and that redundancy and diversity in the telecommunications networks assured.
6. **Invest in the power grid because of its critical and cascading impact on other industries and other critical infrastructures.** The power grid must be considered among the most vital of critical infrastructures and needs investment to make sure it works across the nation.
7. **Establish improved coordination procedures across all critical infrastructures and with federal, state, and local government when events occur.** Coordination in planning and response between the private sector and public emergency management is inadequate and/or inconsistent. For example, a virtual national command center for the private sector that links to the Homeland Security Operations Center would help to provide consistency.
8. **Encourage law enforcement to prosecute cyber criminals and identity thieves, and publicize U.S. government efforts to do so.** These efforts help to reassure the public and

businesses that the Internet is a safe place and electronic commerce is an important part of the Nation's economy.

Several years ago, BITS, on behalf of the financial services industry, outlined seven elements that the Government can pursue to strengthen cybersecurity. We call these seven steps **PREPARE.** The full **PREPARE** statement is included in the Appendix to this testimony, but immediately below are several important elements of these recommendations:

**Promote:** Government can play an important role in promoting the importance of secure information technology.

**Responsibility:** Government should promote shared responsibility between suppliers and end users for developing, deploying, and maintaining secure information networks. Government can play an important role in establishing incentives and making producers of software and hardware accountable for the quality of their products.

**Educate:** Government can help communicate to all users of information technology the importance of safe practices.

**Procure**: Using its purchasing power and leveraging security requirements and best practices developed by the public and private sectors, government can play an important role in encouraging the information technology industry to deliver and implement more secure systems.

**Analyze:** Government should collect information and analyze the costs and impact of information security risks, vulnerabilities, and threats and provide this analysis to policy makers.

**Research:** Government can play an important role in funding research and development in the areas of secure software development practices, testing, and certification programs.

**Enforce:** Law enforcement must do more to enforce, investigate, and prosecute cyber crimes here and abroad. Government needs to properly fund enforcement.

During the past two years, the Federal government has taken several important steps to strengthen cybersecurity, many of which the financial services industry supported. Examples include:

- Creation and appointment of an Assistant Secretary for Cyber Security and Communications to the Department of Homeland Security (DHS).
- U.S. Senate ratification of the Council of Europe's Convention on Cybercrime, signed by the United States in November 2001.
- Completion of the Sector Specific Plans for all of the nation's critical infrastructures, including the Banking and Finance Sector Plan, as part of the Administration's National Infrastructure Protection Plan.
- Requirements by U.S. Office of Management and Budget for executive departments and agencies to strengthen information security programs.

These are positive steps but much more needs to be done.

**Conclusion**

I would like to thank you, Chairman Clay and Subcommittee members, for this opportunity to testify. Insuring Internet resiliency and security in light of increased cyber criminal and potential terrorist attacks is a daunting task. It requires the coordinated and collective efforts of the IT, telecommunications and power industries, the user communities like financial services companies, and the government to create the incentives, policies, best practices and technological innovations needed to prevent disruptions where possible and recover quickly when they happen. I would be happy to answer any questions.

## APPENDIX

### PREPARE

The federal government can play an important role in protecting the nation's IT assets. The following are seven key elements that the U.S. government should support to secure information technology.

**Promote.** Government can play an important role in promoting the importance of secure information technology. Also, government should do more to facilitate collaboration among critical infrastructure sectors and government. Some sectors, such as financial services, are heavily regulated and supervised to ensure that customer information is protected and that financial institutions operate in a safe and sound manner. Examples of actions the government can take include:

- Government should lead by example by ensuring that the issue of cyber security receives adequate attention in the Department of Homeland Security. Today, cyber security is handled at a level far below where most corporations handle these issues. Congress could create a more senior-level policy level position within DHS to address cyber security issues and concerns and ensure that adequate funding is provided.
- Strengthen information sharing coordination mechanisms, such as the Information Sharing and Analysis Centers (ISACs), by ensuring adequate funding is made available to Federal agencies sponsoring such organizations. Information sharing and trend analysis within a sector is essential to protecting information security and responding to events. Information sharing among sectors is equally important as cyber threats sometimes reach some sectors before others.
- Create an emergency communication and reconstitution system in the event of a major cyber attack or disruption of information networks. Such an attack or disruption could potentially cripple many of the primary communication channels. To allow maximum efficiency of information dissemination to key individuals in such an event, a thorough and systematic plan should be in place. The financial services industry has developed such a plan for industry-specific events in the BITS/FSR Crisis Communicator. Other organizations have developed similar communication mechanisms. These emergency communications programs should be examined as potential models for a national cyber security emergency communication system.

- Reform of the Common Criteria/National Information Assurance Partnership (NIAP). The current software certification process is costly, inefficient, used on a limited basis by the Federal government, and virtually unknown to the private sector. NIAP should be reformed so that it is more cost effective for vendors to seek certification while ensuring consistent Federal procurement practices and expanded commercial adoption of NIAP-certified products. The BITS Product Certification Program may well be able to serve as a model.

**Responsibility.** Government should promote shared responsibility between suppliers and end users for developing, deploying, and maintaining secure information networks. Government can play an important role in establishing incentives and making producers of software and hardware accountable for the quality of their products. Examples of actions the government can take include:

- Provide tax or other incentives for achieving higher levels of Common Criteria certification. Incremented incentives would help to compensate companies for the time and cost of certification. This should encourage certification and increase the overall security of hardware and software.
- Provide tax or other incentives for certification of revised or updated versions of previously certified software. Under Common Criteria, certification of updated versions is costly and time consuming. Incentives are necessary to ensure that all software is tested for security
- Require software providers to immediately notify ISACs of newly discovered cyber threats and to provide updated information on such threats until an effective patch is provided. It is vital that critical infrastructure companies receive immediate notice of serious vulnerabilities.
- Establish requirements that improve the patch-management process to make it more secure and efficient and less costly to organizations.

**Educate.** Communicate to all users of information technology the importance of safe practices. Public confidence in e-commerce and e-government is threatened by malicious code vulnerabilities, online fraud, phishing, spam, spyware, etc. Ensuring that users (home users, businesses of all sizes, and government) are aware of the risks and take appropriate precautions is an important role for government and the private sector. Examples of actions the government can take include:

- Fund joint FTC/DHS consumer cyber security awareness campaign. The FTC should focus its efforts on building consumer awareness, and DHS should coordinate more detailed

technical education regarding specific serious threats. In addition, government employees should be trained in proper cyber safety measures.

- Train government employees on proper cyber security measures.
- Educate corporate executives and officers regarding their duties under Sarbanes-Oxley, GLBA, and HIPAA as they relate to cyber security.

**Procure.** Using its purchasing power and leveraging security requirements and best practices developed by the public and private sectors, government can play an important role in encouraging the IT industry to deliver and implement more secure systems. Examples of actions the government can take include:

- Require high levels of cyber security in software purchased by the government through procurement procedures. Extend such requirements to software used by government contractors, subcontractors, and suppliers.
- Provide NIST with adequate resources to develop minimum cyber security requirements for government procurement. NIST should include software developers and other stakeholders in the standard-creation process.

**Analyze.** Government should collect information and analyze the costs and impact of information security risks, vulnerabilities and threats and provide this analysis to policy makers. Examples of actions the government can take include:

- Assign to the Commerce Department or another appropriate agency the responsibility of tracking and reporting such costs and their impact on the economy. Measuring and making these costs transparent will aid law makers and regulators as they assign resources to cyber security programs.

**Research.** Government can play an important role in funding R&D in the development of more secure software development practices, testing and certification programs. In addition, training future generations of programmers, technicians and business leaders that understand and manage information security can be accomplished by establishing university and educational/certification programs. Government can help by facilitating collaboration with the users and suppliers of IT to develop standards for safe practices. Examples of actions the government can take include:

- Enhance DHS, NSF, and DARPA cyber security R&D funding.
- Carefully manage long- and short-term R&D to avoid duplication.
- Establish a mechanism to share educational training and curricula.

**Enforce.** Law enforcement must do more to enforce, investigate and prosecute cyber crimes here and abroad. Examples of actions the government can take include:

- Ratify the Council of Europe's Convention on Cybercrime.
- Enhance criminal penalties for cyber crimes.
- Make cyber crimes and identity theft enforcement a priority among law enforcement agencies.
- Encourage better coordination among law enforcement agencies in order to detect trends.