

STATEMENT

OF

CATHERINE A. ALLEN

CEO, BITS

BEFORE THE

UNITED STATES CONGRESS

HOUSE COMMITTEE ON HOMELAND SECURITY

SUBCOMMITTEE ON ECONOMIC SECURITY,

INFRASTRUCTURE PROTECTION AND CYBERSECURITY

HEARING ON

H.R. 285, THE DEPARTMENT OF HOMELAND SECURITY

CYBERSECURITY ENHANCEMENT ACT OF 2005

APRIL 20, 2005

TESTIMONY OF CATHERINE A. ALLEN CEO, BITS

Introduction

Thank you, Chairman Lungren and Ranking Member Sanchez, for the opportunity to submit testimony before the House Committee on Homeland Security's Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity about proposed legislation to elevate the Cyber Security Director at the Department of Homeland Security (DHS) to the Assistant Secretary level.

I am Catherine Allen, CEO of BITS, a nonprofit industry consortium of 100 of the largest financial institutions in the U.S. BITS is the non-lobbying 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' activities are driven by the CEOs and their direct reports—CIOs, CTOs, Vice Chairmen and Executive Vice President-level executives of the businesses. 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. Attached to this statement is an overview of our work related to cyber security, crisis management coordination, critical infrastructure protection, and fraud reduction.

The importance of cyber security cannot be overstated. Our nation's economic and national security relies on the security, reliability, recoverability, continuity, and maintenance of information systems. IT security has a direct and profound impact on the government and private sectors, and the nation's critical infrastructure. Further, the security and reliability of information systems is increasingly linked to consumer and investor confidence.

As I speak, hackers are writing code to compromise systems. Viruses are epidemic. Hackers are closing the window between the discovery of a flaw and the release of a new virus. Fraudsters are finding new ways to trick consumers into providing personal information that can facilitate ID theft. Beyond threats to our nation's infrastructure, leaders in the financial services industry are growing increasingly concerned with the impact on consumer confidence.

The financial services industry has been aggressive in its efforts to strengthen cyber security. We are sharing information, analyzing threats, urging the software and technology industries to do more to provide more secure products and services, and combating fraud and identity theft. Just last week, BITS and The Roundtable announced the results of a pilot of the Identity Theft Assistance Center (ITAC). The ITAC has helped nearly 700 consumers restore their financial identities since it became operational last August. The ITAC is a free service to financial institution customers. It is a key part of industry efforts to help victims and address the causes of identity theft.

Last year I submitted a letter in support of a proposal to elevate the position of Cyber Security Director at the Department of Homeland Security to the Assistant Secretary level (Attachment A). BITS and The Financial Services Roundtable support this effort to increase the administration's focus on cyber security concerns and address our sector's concerns. While much of DHS' focus has been on physical security, it has not focused enough attention on addressing cyber security concerns. Elevating the cyber security position is a small step as part of a broader strategy to strengthen cyber security. Cyber security is handled at a level far below where most corporations handle the issues today. Elevating this critical position and ensuring that adequate funding is provided will help to focus greater attention on cyber security issues within the government and throughout the private sector and thus implement many areas identified in the Administration's National Strategy to Secure Cyberspace.

Since the creation of DHS in March 2003, BITS has worked closely with many DHS officials, including the director and acting director of the Cyber Security Division. We have provided numerous suggestions for DHS actions to strengthen cyber security and ways it can work in partnership with leaders in the private sector. Earlier this year, the National Cyber Security Division convened a "retreat" of representatives from the major associations (e.g., BITS, Center for Internet Security, Cyber Security Industry Alliance, Educause, Information Technology Association of America, ISAlliance, Technet, SANS Institute, U.S. Chamber of Commerce), individual companies (e.g., IBM, Microsoft, RSA), law enforcement (e.g., Federal Bureau of Investigations, U.S. Secret Service) and government (e.g., Central Intelligence Agency, Commerce Department, Defense Department, Homeland Security Department, House of Representatives, Justice Department, Treasury Department, National Security Agency). DHS played an important leadership role in convening the meeting and other meetings of the US-CERT program. Attachment B is a summary of answers to several questions DHS officials asked in advance of the meeting.

More Can Be Done

As an organizational and symbolic step, elevating this critical position will help to focus greater attention on cyber security issues within the government and throughout the private sector. However, this should be viewed as just one of many steps that must be taken to strengthen cyber security.

Government plays an enormous role. Our nation's economic and national security relies on the security, reliability, recoverability, continuity, and maintenance of information systems. IT security has a direct and profound impact on the government and private sectors, and the nation's critical infrastructure. Further, the security and reliability of information systems is increasingly linked to consumer and investor confidence. In recent years, members of the user community that rely on technology provided by the IT industry—private-sector companies, universities and government agencies—are demanding greater *accountability* for the security of IT products and services.

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.

The Financial Services Industry Is Leading the Way in Responding to the Cyber Security Challenge

The financial services sector is a key part of the nation's critical infrastructure. Customer trust in the security of financial transactions is vital to the stability of financial services and the strength of the nation's economy. At the same time, our sector is a favorite target of cyber criminals as well as of terrorists, as was made clear on 9/11.

Since 9/11, the financial services sector has taken major strides to respond to the risks we face today. BITS has made coordinating financial services industry crisis management efforts a top priority. Senior executives at our member companies have dedicated countless hours to preparing for the worst. We have convened numerous conferences and meetings to bring together leaders and experts, developed emergency communication tools, strengthened our sector's Information Sharing and Analysis Center (FS/ISAC), conducted worst case scenario exercises, engaged in partnerships with the telecommunications sector and key software providers, compiled lessons learned from 9/11 and the August 2003 blackout, developed best practices and voluntary guidelines, created a model for regional coalitions, developed liaisons and pilots with the telecommunications industry for diversity and redundancy, and combated new forms of online fraud. Additionally, BITS is now developing best practices in collaboration with the electric power industry.

Lessons Learned

BITS regularly gathers and disseminates “lessons learned” from its membership. These lessons are a critical building block for BITS’ best practices. Below are some of those lessons for the Committee to consider.

We must work with other parties in the private and public sectors to address these issues sufficiently. We understand that the risks for national security and economic soundness cannot be underestimated. Neither can the importance of our working together to address them.

We need to look strategically and holistically at the nation’s critical infrastructures and what can be done to enhance resiliency and reliability. We urge the Committee to consider all aspects of critical infrastructure—the software and operating systems, the critical infrastructure industries, and the practices of firms, industries and the government—in addressing software security and vulnerability management.

Preparation is critical. The events of 9/11 and subsequent preparations by the private sector and government enhanced mutual trust and the ability to communicate, shift to backup systems, and continue operations. Prior to the August 2003 blackout, BITS conducted a scenario exercise that included the West Coast power grid being out for seven days and the impact that might have on the sector. That exercise helped the industry think through things like communications, water shortages, backup for ATM operations, and fuel for generators.

Critical infrastructure industries and the public need to have an 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. If it had been a terrorist event, other communications and directives such as “shields up”—in which external communications to institutions are blocked—might have occurred.

Diverse and resilient communication channels are essential. Diverse elements—such as cell phones, wireless email devices, landline phones, and the Internet—are required. Both diversity and redundancy are needed within critical infrastructures to assure backup systems are operable and continuity of services will be maintained.

The power grid must be considered among the most vital of critical infrastructures and needs investment to make sure it works across the nation. The cascading impact on the operation of financial services, access to fuel, availability of water, and sources of power for telephone services and Internet communications cannot be overstated.

Recognize the dependence of all critical infrastructures on software operating systems and the Internet. A clear understanding of the role of software operating systems and their “higher duty of care,” particularly when serving the nation’s critical infrastructures, needs to be explored. Further, the Committee should 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.

Financial Industry Efforts to Strengthen Cyber Security

In October 2003, BITS began its Software Security and Patch Management initiative to respond to increasing security risks and headline-sweeping viruses. Since then, BITS has worked to mitigate security risks to financial services consumers and the financial services infrastructure, ease the burden of patch management caused by vendor practices, and help member companies comply with regulatory requirements. BITS also began forging partnerships with the software vendors most commonly used in our industry.

In February 2004, BITS and The Financial Services Roundtable held a Software Security CEO Summit. The event launched BITS and Roundtable efforts to promote CEO-to-CEO dialogue on software security issues. More than 80 executives from financial services, other critical infrastructure industries, software companies, and government discussed software vulnerabilities and identified solutions. A “toolkit” with software security business requirements, sample procurement language, and talking points for discussing security issues with IT vendors was distributed to 400 BITS and Roundtable member company executives. One important deliverable from this Forum is the set of Software Security Business Requirements, which are essential from the perspective of the financial services sector. These requirements and the full “toolkit” are available in the public area of the BITS website, at www.bitsinfo.org.

A theme of the event was the importance of collaborating with other critical infrastructure industries and government. Since the Summit we have worked with all the associations representing the

financial services industry, as well as The Business Roundtable, the Cyber Security Industry Alliance and other relevant groups.

In April 2004, BITS and The Financial Services Roundtable announced a joint policy statement calling on the software industry to improve the security of products and services it provides to financial services customers. The policy statement calls on software providers to accept responsibility for their role in supporting financial institutions and other critical infrastructure companies. BITS and The Roundtable support incentives and other measures that encourage implementation of more secure software development processes and sustain long-term R&D efforts to support stronger security in software products. We also support protection from antitrust laws for critical infrastructure industry groups to discuss baseline security specifications for the software and hardware that they purchase. Additionally, as part of the policy, BITS and The Roundtable are encouraging regulatory agencies to explore supervisory tools to ensure critical third-party service providers and software vendors deliver safe and sound products and services to the financial services industry.

We continue to work with software companies to create solutions acceptable to all parties. In 2004 BITS successfully negotiated with Microsoft to provide additional support to BITS member companies using Windows NT. We have provided Microsoft and other software and hardware companies with Software Security Business Requirements. (See Attachment A.) BITS members agree that these requirements are critical to the soundness of systems used in the financial services industry.

In July 2004, BITS published best practices for software patch management in response to the increasing urgency of patch implementation, given the speed with which viruses are targeting new vulnerabilities. This document is available to the public at no cost and applicable to industries outside of financial services.¹

In July, BITS published *The Calculator: BITS Key Risk Measurement Tool for Information Security Operational Risks*. This tool helps financial institutions evaluate critical information security risks to their businesses. Financial institutions use the *Calculator* to score their own information security risks based on the likelihood of an incident, the degree to which the organization has defended itself

¹ Patch management and implementation alone can cost one financial institution millions of dollars annually. A BITS survey of member institutions found that costs to the financial services industry associated with software security, including patch management, are approaching \$1 billion annually. BITS' best practices help companies mitigate these costs.

against the threat, and the incident's possible impact. The tool brings together an extensive body of information security risk categories outlined in international security standards and emerging operational risk regulatory requirements. Like the patch management best practices, the *Kalculator* is available to the public at no cost and applicable to industries outside of financial services.

BITS participated in the Corporate Information Security Working Group (CISWG) sponsored by Congressman Adam Putnam, then-Chairman of the House of Representatives' Subcommittee on Technology, Information Policy, Intergovernmental Relations on the Census. CISWG is made up of corporate, industry and academic leaders and is working to pursue a private sector-driven approach to enhancing the protection of the nation's corporate computer networks. BITS is active in the best practices, incentives, and procurement subgroups. In addition, BITS has participated in task forces established by DHS and several technology associations.

Finally, the BITS Product Certification Program is another important part of our work to address software security. The BITS Product Certification Program is a testing capability that provides security criteria against which software can be tested. A number of software companies are considering testing. The criteria are also used by financial institutions in their procurement processes. We are working to hand this over to DHS and secure ongoing funding for it.

Identity Theft and Phishing: Prevention and Victim Assistance

Just as financial institutions are a key target for hackers and other cyber criminals, our industry is increasingly the target of fraudsters operating online. BITS and The Financial Services Roundtable are responding to the escalation in identity theft with a series of steps to facilitate prevention of the crime and assist victims when it occurs. The goals of these efforts are to help maintain trust in the financial services system, assist member companies' customers, and mitigate fraud losses. BITS and The Roundtable are working with the Administration, Congress, and law enforcement and regulatory agencies to accomplish these goals.

A cornerstone to these efforts is the Identity Theft Assistance Center (ITAC). Developed by BITS and The Roundtable, with the support of 50 founding member institutions, the ITAC helps victims of identity theft restore their financial identity. If a consumer or a member company suspects a problem, the consumer and the company resolve any issues, and if the problem involves identity theft, the customer is offered the ITAC service. The ITAC walks the consumer through his or her credit report to find any other suspicious activity. Then, the ITAC notifies the affected creditors and

places fraud alerts with the credit bureaus. The ITAC also shares information with the Federal Trade Commission and law enforcement agencies, to help arrest and convict the perpetrators and prevent future identity theft crimes.

Because a consistent understanding of the problem is essential to finding solutions, a 2003 BITS white paper on identity theft outlines the full identity theft landscape, establishing key terms as well as identifying factors that contribute to identity theft. The paper provides background about the legislative and policy environment, including existing and proposed laws, as well as industry best practices.

Along with the white paper, BITS developed guidelines for financial institutions to use to prevent identity theft and restore victims' financial identities. The guidelines include processes for providing a "single point of contact" at companies to whom victims may report cases of identity theft.

Additionally, the BITS Fraud Reduction Steering Committee and the Federal Trade Commission have created a Uniform Affidavit to simplify the recovery process for victims. The Uniform Affidavit streamlines the reporting process by recording the victim's information about the crime, so that victims only have to tell their story once.

BITS is also responding to "phishing" through its Fraud Reduction Program. Phishing is the practice of luring consumers to provide bank account and other personal information to fraudsters through bogus email messages. In response to these and other online scams, BITS has created a Phishing Prevention and Investigation Network. The Phishing Network provides member institutions with information and resources to expedite investigations and address phishing/spoofing incidents. The Phishing Network includes a searchable database of information from financial institutions on their phishing incident and response experience, including contacts at law enforcement agencies, foreign governmental agencies, and ISP Web administrators. The Phishing Network also provides data on trends to help law enforcement build cases and shut down identity theft operations.

Financial institutions are regulated to "know your customers." However, financial institutions currently do not have access to various government databases to validate information provided at new account openings. For instance, financial institutions cannot validate that a passport number belongs to the individual providing it and matches the address given at a new account opening. This is also true of driver's license and tax ID numbers. (A pilot is underway with Social Security numbers; BITS is hopeful that financial institutions will finally be able to validate Social Security

numbers.) Financial institutions do not want direct access to the information; they would like to have access to a “yes” or “no” response through a trusted third party.

Complying with Regulatory Requirements

As you know, financial institutions are heavily regulated and actively supervised by the Federal Reserve, Federal Deposit Insurance Corporation, Office of the Comptroller of Currency, Office of Thrift Supervision, National Credit Union Administration, and the Securities and Exchange Commission. Regulators have stepped up their oversight on business continuity, information security, third party service providers, and critical infrastructure protection. Our industry is working consistently and diligently to comply with new regulations and ongoing examinations. In addition, BITS and other industry associations have developed and disseminated voluntary guidelines and best practices as part of a coordinated effort to strengthen all critical players in the sector.

Regardless of how well financial institutions respond to regulations, we simply cannot address these problems alone. Our partners in other critical industry sectors—particularly the telecommunications and software industries—must also do their fair share to ensure the soundness of our nation’s critical infrastructure.

Recommendations

The Congress can help the financial services sector meet the challenges of a post 9/11 environment in a number of ways. We have developed these key recommendations for the Committee to consider:

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. 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, the Congress should encourage providers of software to the financial services industry 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 U.S. 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 the financial services industry.**
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 telecommunications circuits are adequately protected and that redundancy and diversity in the telecommunications networks are 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.

On behalf of both BITS and The Financial Services Roundtable, thank you for the opportunity to testify before you today. I will now answer any questions.

Attachment A

Letter from BITS and The Financial Services Roundtable

THE FINANCIAL SERVICES ROUNDTABLE



BITS
FINANCIAL SERVICES
R O U N D T A B L E

Sent via Fax: 202.225.3486

July 13, 2004

Representative Christopher Cox
Chairman, Select Committee on Homeland Security
2402 Rayburn House Office Building
Washington, DC 20515

Representative Jim Turner
Ranking Member, Select Committee on Homeland Security
330 Cannon House Office Building
Washington, DC 20515

Representative Mac Thornberry
Chairman, Cybersecurity Subcommittee
2457 Rayburn House Office Building
Washington, DC 20515

Representative Zoe Lofgren
Ranking Member, Cybersecurity Subcommittee
102 Cannon House Office Building
Washington, D.C. 20515

RE: Cybersecurity Concerns

Dear Representatives Cox, Turner, Thornberry and Lofgren:

Thank you for the opportunity to discuss the concerns of financial institutions with regard to strengthening software security.

The Financial Services Roundtable (FSR) and BITS want to offer our support for the recommendation to elevate the position of cybersecurity director to the level of Assistant Secretary. We support this effort as a way to increase the administration's focus on cybersecurity concerns and address issues such as those outlined in the attached BITS/FSR Software Security Policy Statement.

Furthermore, we believe that this elevation to Assistant Secretary will provide support for those areas identified by the National Strategy as requiring additional actions.

Finally, we would like to acknowledge the responsiveness of the National Communications System (NCS) to meeting the needs of the financial services industry. As such, we would like to ensure that moving the NCS into the Cybersecurity Division will not undermine the excellent work of the NCS.

Best regards,

Steve Bartlett
President
The Financial Services Roundtable

Catherine A. Allen
Chief Executive Officer
BITS

Enclosure: BITS/FSR Software Security Policy Statement

BITS

FINANCIAL SERVICES
R O U N D T A B L E

SOFTWARE SECURITY

Security is a fundamental building block for all financial services. It is also a regulatory requirement. The financial services industry relies upon software to operate complex systems and provide services, as well as to protect customer information.

Financial services companies comply with a host of legal and regulatory requirements to ensure the privacy and security of customer information. Recently, the prevalence of security risks, threats and viruses, combined with a lack of accountability for software vulnerabilities, has saddled financial institutions with significant risks and skyrocketing costs.

In early 2004, BITS surveyed its members to estimate the costs to financial institutions of addressing software security and patch-management problems. Based on the survey, BITS and Financial Services Roundtable members pay an estimated \$400 million annually to deal with software security and patch management. Extrapolated to the entire financial services industry, these costs are approaching \$1 billion annually.

The members of BITS and The Financial Services Roundtable believe:

- Because the financial services industry plays a central role in the nation's critical infrastructure and is dependent on the products and services of software providers, such providers of mission critical software to the financial services industry need to accept responsibility for the role their products and services play in supporting the nation's critical infrastructure and should exhibit and be held to a "higher duty of care" to satisfy their own critical infrastructure responsibilities.
- Software vendors should ensure their products are designed to include security as part of the development process using security-trained and security-certified developers on product development and lifecycle teams.
- Software vendors should ensure through testing that their products meet quality standards and that financial services security requirements are met before products are sold.
- Software providers should develop patch-management processes that minimize costs, complexity, downtime, and risk to user organizations. Software vendors should identify vulnerabilities as soon as possible and ensure that the patch is thoroughly tested.
- Software vendors should continue patch support for older, but still viable, versions of software.
- Collaboration and coordination among other critical infrastructure sectors and government agencies are essential to mitigate software security risks.

The members of BITS and The Financial Services Roundtable:

- Support measures that make producers of software more accountable for the quality of their products.
- Support incentives (e.g., tax incentives, cyber-insurance, liability/safe harbor/tort reform, certification programs) and other measures that encourage implementation of more secure software development processes and sustain long-term R&D efforts to support stronger security in software products.
- Seek protection from U.S. antitrust laws for critical infrastructure industry groups that agree on baseline security specifications for software and hardware that they purchase.
- Encourage regulatory agencies to explore supervisory tools to ensure that critical third-party service providers and software vendors deliver safe and sound products to the financial services industry.
- Support and incorporate, where possible, the BITS Product Security Criteria into security policies, and encourage technology vendors to test products to meet these criteria.
- Apply a risk-management approach to software security by assessing risks and applying appropriate tools and best practices to ensure the most secure deployment and application of software possible across the entire enterprise.
- Participate in and support efforts to strengthen the Financial Services Information Sharing and Analysis Center (FS/ISAC) in order to share vulnerability information on the products deployed by financial institutions.
- Educate policy makers on the significance of the risks posed to the financial services sector and other critical infrastructure industries and the need to take action to mitigate these risks.

**BUSINESS REQUIREMENTS
FOR
SOFTWARE SECURITY AND PATCH MANAGEMENT**

Members of BITS and The Financial Services Roundtable believe software vendors should take responsibility for the quality of their products. Especially when selling products to companies that are within critical infrastructure industries, certain minimum requirements should be met. Following are recommended critical infrastructure sector Business Requirements.

Provide a higher “duty of care” when selling to critical infrastructure industry companies.

To meet this higher duty of care, vendors should:

- Make security a fundamental component of software design.
- Support older versions of software (e.g., NT), particularly if existing programs are functional and not past the end of their estimated life cycle.
- Make upgrading easier, less cumbersome and less costly, and offer more support.
 - Products should be less prone to failure and have an automated back-out feature.
 - Components (including embedded components used in other products) should be clearly defined in order for the customer to assess the cascading effect of the upgrade or installation.
- Publish metrics on security of new and existing products.
- Expand coordination and establish better communication with individual clients and industry groups.
 - Vendors should give customers an aggressive “patch playbook” which would provide clear guidance and explicit instructions for risk mitigation throughout the patch management process and especially in times of crisis.
 - Vendors should offer critical infrastructure customers access to one-on-one, private, early vulnerability notice prior to notifying the general public, possibly by establishing “preferred” customer levels. (Some vendors offer financial institutions advanced notification if they agree to serve as a “beta” site, however, this is not practical as an industry-wide solution.)
- Provide better security-trained and security-certified developers on product teams.
- Establish Regional Centers of Excellence to service major financial institutions in their area. Centers would keep IT profiles for each institution in order to:
 - Inform institutions of the likely effects of a new vulnerability on their specific IT environment.
 - Continually advise institutions on how to best apply patches.
 - Expedite patch installation by visiting the financial institution site.
 - Make on site or remote consultation available when patches affect other applications.

Comply with security requirements before releasing software products.

Vendors should:

- Meet minimum security criteria, such as BITS software security criteria and/or the Common Criteria.
- Thoroughly test software products, taking into consideration that:
 - Testing needs to address both quality assurance as well as functionality against known and unknown threats.
- Conduct code reviews.
 - Whether conducted internally or outsourced, code reviews should involve tools or processes, such as code profilers and threat models, to ensure code integrity.

Improve the patch-management process to make it more secure and efficient and less costly to organizations.

Vendors should:

- Issue patch alerts as early as possible.
- Continue patch support for older software.
 - Vendors should be clear about the level of support provided for each software version.
 - Vendors are strongly encouraged to provide support for up to two versions of older software, i.e., the N-2 level.
- Provide automatic, user-controlled patch-management systems, such as uniform, reliable, and, possibly, industry-standard installers.
- Ensure all patches come with an automated back-out function and do not require reboots.
- Support clients who purchase third-party installer tools (until a standard is established).
- Thoroughly test patches before release.
 - Testing should include patch-to-patch testing to identify any cascade effects and in-depth compatibility testing for effects on networks and applications.
- Issue better patch and vulnerability technical publications. Publications should include more thorough analyses of the impact of vulnerabilities on unpatched systems as well as data on the environments and applications for which the patches were tested. Impact on other patches should also be addressed.
- Conduct independent security audits of the patch-development and deployment processes.
- Distribute a communication and mitigation plan, including how vulnerability/patch information will be relayed to the customer, for use in times of crisis.

Attachment B
BITS Response to DHS Questions on Cyber Security
January 4, 2005

The National Cyber Security Division of DHS hosted a retreat at Wye River, Maryland on January 6-7, 2005 to assess private and public sector progress in meeting the goals and objectives of the Administration's National Strategy to Secure Cyberspace. DHS asked participants in advance of the meeting to answer three questions. BITS submitted the following answers to these questions.

Question 1: What are the top three initiatives your organization is currently involved in to advance cybersecurity (such as the goals articulated in the National Strategy to Secure Cyber Space)?

BITS is involved in numerous efforts to address cyber security and protect the Nation's critical infrastructure. **For 2005, BITS will focus on the following top three initiatives to advance cybersecurity: 1) urge major software vendors to address software security business requirements; 2) combat on-line fraud and identity theft; and 3) support efforts to develop meaningful software product certification programs.** In addition to the three initiatives outlined below, BITS also will continue to educate policy makers on cyber security risks and steps that can be taken to protect the Nation's critical infrastructure. (See appendix B for a summary of BITS' accomplishments in 2004.)

A. Urge major software vendors to address the BITS/FSR software security business requirements. In April 2004, BITS and The Financial Services Roundtable announced a joint policy statement calling on the software industry to improve the security of products and services it provides to financial services customers. The policy statement calls on software providers to accept responsibility for their role in supporting financial institutions and other critical infrastructure companies. BITS and the Roundtable support incentives (e.g., tax incentives, cyber-insurance, liability/safe harbor/tort reform, certification programs) and other measures that encourage implementation of more secure software development processes and sustain long-term research and development efforts to support stronger security in software products. (The BITS/FSR Software Security Business Requirements are attached to the April 2004 BITS/FSR Software Security Policy statement which is available at <http://www.bitsinfo.org/bitssoftsecuritypolicyapr04.pdf>) In addition, BITS is working with major software vendors to discuss business requirements. In June 2003, BITS announced it had successfully negotiated with Microsoft to provide additional support to BITS member companies for Windows NT. We have provided Microsoft and other software and hardware companies with the Software Security Business Requirements. BITS members agree that these requirements are critical to the soundness of systems used in the financial services industry. BITS also is working with or has plans in early 2005 to work with Cisco, IBM and RedHat on software security issues.

B. Combat on-line fraud and identity theft and explore appropriate authentication strategies. BITS is involved in supporting the pilot of the BITS/FSR Identity Theft Assistance Center (ITAC), developing the BITS Phishing Prevention and Investigation Network, and focusing on authentication practices and strategies.

The ITAC is a one-year pilot program intended to help victims of identity theft by streamlining the recovery process and enabling law enforcement to identify and prosecute perpetrators of this crime. ITAC is an initiative of The Financial Services Roundtable and BITS, which represent 100 of the largest integrated financial services companies. Fifty BITS and Roundtable Members are participating and funding the ITAC pilot program as a commitment to their customers and maintain trust in the Nation's financial services system. The ITAC's services are free-of-charge to customers and made available based on referrals to the ITAC by one of the 50 members of the ITAC pilot program. BITS has also published several business practices guidelines and white papers on various aspects of identity theft and fraud reduction strategies.

The BITS Phishing Prevention and Investigation Network has three primary purposes. First, the Network helps financial institutions shut down online scams. Second, it aids in investigations of scam perpetrators by providing law enforcement with trend data. Law enforcement agencies can use the data to build cases and stop scamming operations. Finally, the BITS Network facilitates communication among fraud specialists at financial institutions, law enforcement agencies and service providers, resulting in a "united front" for combating online scams. Financial institutions can also use the BITS Network to share information about online scams. Through its searchable database, fraud professionals at BITS member institutions learn from other institutions' phishing incidents and responses. The database provides quick access to contacts at law enforcement agencies, foreign governmental agencies, and ISP administrators. Founded under the auspices of the BITS eScams Subcommittee of the BITS Internet Fraud Working Group, the Network is hosted by the Financial Services Information Sharing and Analysis Center (FS/ISAC). Resources to develop the Network were contributed by Microsoft Corporation and RDA Corporation.

On March 8, 2005, BITS will host a Forum entitled "A Strategic Look at Authentication" in Washington, DC. Authentication issues have emerged in a number of BITS' working groups. This strategic Forum will focus on the following issues: business issues that drive the need for authentication; business challenges to implementation; public policy implications; and emerging technologies in the authentication area.

C. Support efforts to develop meaningful software product certification programs.

The BITS Product Certification Program (BPCP) is an important part of our work to address software security. The BPCP 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 initiated discussions with 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). DHS has expressed support for broad-based, not sector specific, certification programs. Moreover, DHS wants "buy in" from the broader user community. Consequently, BITS has been in discussions with The Business Roundtable, NIST, and the Cyber Security Industry Alliance (CSIA) to develop a joint proposal.

Question 2 & 3: Aside from funding, what can the government (if appropriate, specify which agency(ies)) do to help advance the cybersecurity agenda/priority(ies)/initiative(s) of your organization? What else should government and the private sector be doing to help facilitate enhanced cybersecurity?

Our Nation's economic and national security relies on the security of information technology (IT). This security depends on the reliability, recoverability, continuity, and maintenance of information systems. The issue of secure information technology has a direct and profound impact on both the government and private sectors, and includes the Nation's critical infrastructure. The security and reliability of information systems are increasingly linked to consumer and investor confidence. Financial institutions (and others that make up the "user" community) are demanding greater accountability for the security of IT products and services. The federal government can play an important role in protecting the Nation's IT assets. The following are steps the U.S. government can and should take to secure information technology.

- ***Strengthen the Information Sharing and Analysis Centers (ISACs) by providing complete and adequate federal funding.*** Information sharing and trend analysis within a sector is essential to protecting information security and responding to events. The ISACs are a good vehicle for such sharing, but they require additional resources.
- ***Encourage sharing of essential information among industry ISACs.*** Threats to cyber security will reach some sectors before others – oftentimes resulting in simultaneous or cascading effects. Mandatory sharing among the ISACs will provide valuable advance notice to sectors not immediately threatened.
- ***Utilize the ISACs to inform critical infrastructures of cyber threats discovered through national intelligence and law enforcement.*** As a primary target of cyber attacks, the government expends substantial resources to protect, detect and respond to attacks. The information gathered by the government regarding present, imminent, or gathering threats should be shared with sectors that are widely understood to be critical to the security of the country. ISACs represent a centralized way of quickly disseminating important security information.
- ***Create an emergency communication system in the event of a massive cyber attack.*** Such an attack 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 relies on the BITS/FSR Crisis Management Process and Manual of Procedures, including the BITS/FSR Crisis Communicator.
- ***Create and promote security standards for technology products which address the Common Criteria certification concerns noted by the National Cyber Security Partnership (NCSP).*** These concerns include:
 - Cost and delay of the certification process
 - Need to make certification applicable to the needs of both government and industry
 - Uniform tying of federal procurement policies to the certification system

In the alternative to repairing the Common Criteria, a new system should be developed that would address from the beginning the limitations of the Common Criteria. DHS has expressed interest in such a certification program if it is not sector specific. The BITS Product Certification Program may well be able to serve as a model for such a certification program.

- ***Increase staffing, funding, and prominence of cyber security in the DHS.*** Cyber security is a unique threat to national security. As such, it should be elevated in importance at DHS.
- ***Create a more senior level policy level position within DHS to address cyber security issues and concerns.***
- ***Provide tax or other incentives for achieving higher levels of Common Criteria certification.*** Presently, Common Criteria certification is the primary uniform means of evaluating the security of software and hardware. Incremented incentives, based upon the level of certification achieved, would help to compensate companies for the time and cost of certification. This should encourage more 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 and not a single build or version of a product.
- ***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.*** Regulatory controls may be necessary to prevent the wider broadcast of such information, but it is vital that the critical infrastructure receive immediate notice of serious vulnerabilities. Regulatory action will also be necessary to police software provider compliance with such an information sharing requirement.
- ***Establish requirements which improve the patch-management process to make it more secure and efficient and less costly to organizations that use software.***
- ***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.***
- ***Provide tax or other incentives for industry cyber security awareness campaigns.*** Because security should not be grounds for competitive advantage, cyber security awareness campaigns undertaken on an industry-wide basis should be encouraged.
- ***Educate corporate executives and officers regarding their duties under Sarbanes-Oxley, GLBA, and HIPAA as relates to cyber security.***
- ***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.
- *Assign to the Commerce Department or another appropriate agency the responsibility of tracking and reporting such costs and the impact on the economy.* Measuring and making transparent these costs will aid law makers and regulators as they assign resources to cyber security programs.
- *Fund research and development of more secure software development practices, testing and certification programs.*
- *Facilitate collaboration with the users and suppliers of information technology to develop standards for safe practices.*
- *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 curriculum.*
- *Encourage law enforcement to enforce, investigate and prosecute cyber crimes here and abroad.*
- *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, share information and identify and prosecute offenders.*