

STATEMENT
OF
JOHN CARLSON
ON BEHALF OF BITS
AND THE FINANCIAL SERVICES ROUNDTABLE
BEFORE THE
UNITED STATES CONGRESS
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
ORGANIZATION, AND PROCUREMENT AND
SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND
NATIONAL ARCHIVES
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES
HEARING ON
FEDERAL IT SECURITY: THE FUTURE FOR FISMA
JUNE 7, 2007

TESTIMONY OF JOHN CARLSON, EXECUTIVE DIRECTOR, BITS

Introduction

Thank you Chairman Towns and Chairman Clay for the opportunity to submit testimony before your subcommittees about information security best practices within the financial services industry and how these practices may be of use to Federal agencies in meeting the goals of the Federal Information Security Management Act (FISMA).

I am John Carlson, the Executive Director of BITS. BITS focuses on technology and operations issues such as information security, fraud prevention, business continuity and vendor issues where industry cooperation serves the public good. In our ten years, BITS has worked with our member financial institutions, affiliate associations such as the American Bankers Association and Credit Union National Association, government agencies, technology companies, and others to achieve our mission to promote best practices and a strong national financial infrastructure. BITS is a division of The Financial Services Roundtable, a national association that represents 100 of the largest integrated financial services companies providing banking, insurance, investment products, and other financial services to American consumers. Roundtable member companies provide fuel for America's economic engine, accounting directly for \$65.8 trillion in managed assets, \$1 trillion in revenue, and 2.4 million jobs.

In your invitation letter, you asked me to provide testimony regarding BITS' work and how both the government and private sector can benefit through shared best practices, procurement models, and life-cycle stewardship activities for information technology systems and assets. In my testimony, I will cover three areas. First, I will discuss the risk and threat environment financial institutions currently face and why securing our information technology infrastructure is so important. Second, I will outline some recommendations for the government to strengthen information security programs. Third, I will highlight our efforts to address information security challenges and how these approaches may benefit the government in strengthening information security.

Risk and Threat Environment

Our nation's economic and physical security relies on the security, reliability, recoverability, continuity, and availability of information systems. Information technology security has a direct and profound impact on the government, the private sector, and the nation's critical infrastructure. The financial services sector is an important part of the nation's critical infrastructure. 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 a favorite target of cyber criminals as international crime rings, using the Internet for fraud and financial gain, are propagating. The financial sector is also a target for terrorists, as was made clear on 9/11.

The cybersecurity threat environment is constantly evolving and some risks are increasing. Criminals are writing code to compromise systems. Phishing, cybersquatting, viruses, worms, and other forms of attack are endemic.¹ Hackers are closing the window between the discovery of a software flaw and exploitation of that flaw. Criminals are using social engineering to trick consumers into providing personal information that can facilitate fraud and identity theft. Highly-publicized breaches and the resulting loss or theft of personally-identifiable information undermine consumer confidence.

Anxiety about identity theft remains high. However, the combined efforts of the financial services industry, law enforcement, federal financial regulators, and the Federal Trade Commission (FTC), are showing results. For example, The Identity Theft Assistance Center (ITAC), another division of The Roundtable which BITS helped to create, fights identity theft by helping victims recover from this serious crime, partnering with law enforcement to catch and convict criminals, and conducting research on the causes of and solutions to identity theft. The ITAC provides a free victim assistance service to customers of member

¹ Phishing is the use of technology and social engineering to entice consumers to supply personal information such as account numbers, login IDs, passwords, and other verifiable information that can then be exploited for fraudulent purposes, including identity theft. Phishing is most often perpetrated through mass emails and spoofed websites. According to the Anti-Cybersquatting Consumer Protection Act, cybersquatting is registering, trafficking in, or using a domain name with bad-faith intent to profit from the goodwill of a trademark belonging to someone else.

companies. Since it opened in 2004, ITAC has helped 16,000 consumers restore their financial identity. ITAC's research into the experience of actual victims is providing important insight into the causes of identity theft. A recent ITAC survey of 275 victims showed that 42% of identity theft victims knew how the fraud occurred. Of those, the most frequently cited cause was friends, family, and in-home employees

Recommendations for Government

Over the years, BITS members have collaborated to develop numerous guides, toolkits and other publications to identify and address challenges facing the financial services. Many of these efforts may be useful for government agencies in procuring more secure software, sharing information, notifying citizens following a data breach, developing testing/training procedures, managing third party outsourcing, and funding research and development. Most of these documents are publicly available on the BITS website².

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.

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

² See www.bitsinfo.org.

- 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.

Several years ago, BITS 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: 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.

During the past year alone, the Federal government has taken several important steps to strengthen cybersecurity, many of which The Roundtable and BITS 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 2001.³
- Release of the Administration's Identity Theft Task Force Report. The report includes a number of helpful recommendations, including support for a uniform national standard for breach notification, endorsement risk-based approaches and strategies to render lost or stolen data useless by identity thieves, and the

³ The Convention on Cybercrime is the first and only international, multilateral treaty specifically addressing the need for cooperation in the investigation and prosecution of computer network crimes. It requires global law enforcement cooperation with respect to searches and seizures and provides timely extradition for computer network based crimes covered under the treaty.

recommendation that public and private sectors to limit use of Social Security Numbers (SSNs). The report also appropriately acknowledges the need for financial institutions and law enforcement to use SSNs as identifiers, recommends greater involvement by law enforcement in investigating and prosecuting identity theft crimes, and recommends additional studies. Further, the report includes information on financial services industry efforts to protect data, educate consumers, and assist victims of identity theft and the role of financial regulators in overseeing industry efforts in these areas.

- 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.
- U.S. Office of Management and Budget requirements for executive departments and agencies to strengthen information security programs.

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

Financial Industry Efforts

I want to highlight some examples of the financial services industry's leadership in information security, privacy protection, fraud reduction, vendor management, and identity theft assistance. These efforts are helping the financial services industry mitigate some of the risks it faces.

Members of The Roundtable and BITS are sharing information, analyzing threats, creating best practices, urging the software and technology industries to do more to provide more secure products and services, and combating fraud and identity theft.⁴ For example, 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

⁴ Many BITS best practices and other deliverables are publicly available on the BITS website (http://www.bitsinfo.org/p_publications.html).

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.

Applying the same **PREPARE** template, let me reference some of financial services industry efforts and how these efforts may benefit the government in strengthening information security.

Promote. As part of an effort to promote secure information technology, financial institutions have developed tools to secure data and respond more effectively to data breaches. The sources of data breaches vary from lost or stolen computers or backup tapes containing sensitive data to insider abuse and hacking. While research by ID Analytics, Inc. indicates that most data compromises do not lead to fraud or identity theft, consumers are understandably concerned about the possible risks posed to their personal and/or account information. Notifying customers of a breach is a complicated and complex process that, if poorly done, can undermine confidence in the financial institution. Care must be exercised in alerting consumers to steps they can take to protect themselves from identity theft and other forms of fraud while averting needless alarm as well as apathy caused by too many false alarms.

The breach involving customers of TJX Companies, Inc. several months ago provides a good example of how BITS and our member companies responded.

- First, we convened information sharing calls among experts in our member companies to discuss the current and potential impact of fraud and identify theft and response strategies of financial institutions that included card re-issuances, increased monitoring of accounts, and customers notification.
- Second, we analyzed the impact of breaches and engaged other organizations to address challenges. While most breaches have involved the compromise of credit and debit card information, the TJX Companies, Inc.'s breach is reported to have compromised check and driver's license information. The theft of this information can be used to access a consumer's checking account and may result in account takeover, counterfeits, new account fraud, and identity theft. We recognized that

there was no known network or industry association that served as the point of contact for the general merchant/retail sector when checking account information has been breached. In light of this gap, we worked with the American Bankers Association (ABA) and Certegy, the check processor for TJX Companies, Inc., to facilitate the distribution of files for Demand Deposit Accounts (DDAs) processed by Certegy from early 2003 to the present. In addition, we reached out to the leadership of the National Retail Federation (NRF) to discuss how the financial services industry and the retail industry can work together more collaboratively prior to and in response to breaches that involve more than credit or debit card information.

- Third, we reminded members of the tools we have developed to help experts in the financial services industry to prevent data breaches and to respond to them more effectively. Examples include the *BITS/ABA Key Considerations for Responding to Unauthorized Access to Sensitive Customer Information*, *BITS Key Considerations for Securing Data in Storage and Transport*, and *BITS Consumer Confidence Toolkit: Data Security and Financial Services*.
 - BITS and the ABA completed the *BITS/ABA Key Considerations for Responding to Unauthorized Access to Sensitive Customer Information* in 2006 to help financial institutions develop and execute response programs when confidential and sensitive information is accessed or misused by unauthorized individuals. The paper covers the evolving legal and regulatory requirements, potential elements of a response program, and suggestions for managing third party service provider relationships as they relate to data security programs and customer notification.
 - The *BITS Key Considerations for Securing Data in Storage and Transport* paper provides financial institutions with a framework to evaluate the risks associated with the transport and storage of physical media and the destruction or erasure of data on various media. The framework helps risk managers by outlining key questions, identifying risks that can (and cannot) be mitigated, educating key vendors about the needs of financial institutions, implementing appropriately secure storage and transport procedures, and developing effective audit procedures.

- 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.
- Fourth, individual financial institutions communicated with their customers and in many cases issued new cards and/or increased monitoring to detect fraudulent activity.
- Fifth, we maintained contacts with Federal financial regulators and responded to questions about this breach and the impact on related efforts involving information security, outsourcing, business continuity planning, vendor management, payments, and identity theft and fraud reduction.

As another example of promoting secure information technology, we have encouraged government agencies to provide fraud and identity theft prevention tools for use by the industry. For instance, BITS and The Roundtable are encouraging the Social Security Administration (SSA) to provide a robust verification system that will help prevent fraud and identity theft and assist financial institutions in complying with numerous legal requirements. Financial institutions support efforts to establish a consent-based Social Security Number verification program (CBSV) that will allow financial institutions to affirmatively verify a consumer's name, SSN and date of birth against SSA databases. Establishing a real time verification system capable of high volume at low cost would significantly reduce the incidence of identity theft by providing a means of validating key information used at account opening. Consumers would also benefit from industry's ability to verify SSN information by reducing the incidence of fraud and errors.

In July 2006, BITS completed the *BITS Business and Technical Requirements for an Effective and Secure Social Security Number Verification Program to Combat Fraud and Identity Theft*. These requirements provide a framework for cooperation between the SSA and financial institutions to partner on a consent-based verification program that meets the needs of the customers, the industry, and the agency. In July 2006, BITS, The Roundtable, and senior SSA officials met to discuss the business and technical requirements document. Following the meeting, BITS gathered information from member financial institutions regarding their

anticipated participation in a consent-based Social Security Number Verification program. In November 2006 BITS transmitted the results of the survey to members and the SSA. The survey did reveal strong interest from U.S. financial institutions for a CBSV program, but it also indicated several impediments to broader participation in a verification program if changes were not made to the current proposed structure. Financial institutions noted that more would participate in the CBSV program if it:

- is automated;
- does not require paper consent forms;
- has minimum delays in verifications;
- includes a reasonable cost for verification;
- has reasonable record keeping requirements; and
- addresses the need for ID verification processes for non-U.S. citizens.

Participants indicated that the greatest value to the financial institutions via an enhanced CBSV program would be the ability to: verify the identity of an applicant; reduce instances of identity theft; facilitate compliance with the Customer Identification Program (CIP) as required by Section 326 USA PATRIOT Act); reduce losses due to fraud or loan defaults; enhance customer service, as financial institutions would not have to ask customers to go to their local SSA office to validate their SSN; and detect and reduce erroneous tax reporting.

Another important area is government-issued credentials. The DHS recently issued for comment a proposal that outlines the minimum standards for state-issued driver's licenses and identification cards in compliance with the REAL ID Act of 2005. The proposal establishes minimum standards for state-issued driver's licenses and identification cards that Federal agencies could accept for official purposes, such as boarding Federally-regulated aircraft and entering Federal facilities. These standards may also impact financial institutions because financial institutions rely on government-issued credentials to verify identity for everyday functions including opening customer accounts, establishing loans, and hiring employees. Financial institutions also are required by government regulations to identify their clients and gather relevant information before doing business with them. Therefore, it is extremely important that when issuing identification under this proposal, states take all

steps necessary to verify both the identity of the individual and the authenticity of the documents presented to them. Improving credentials, such as state driver's licenses and state-issued identification cards, will provide an important opportunity to improve financial institutions' ability to "know their customer" as mandated by the USA Patriot Act and other laws and regulations.

Responsibility. For many years BITS and our members 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.

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).

Collectively, these efforts raised the level of awareness of leaders in the technology, financial services and government communities and have resulted in positive change as more technology companies deliver more secure products and services.

Educate: 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*.⁵

Recently, we have 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. We also have learned that without proper protocols, email is insecure and lacks controls that can ensure confidentiality and integrity. In April 2007, we released the *BITS Email Security Toolkit: Protocols and Recommendations for Reducing the Risk*.⁶ The toolkit recommends email technology protocols for financial services, Internet Service Providers, and other business partners. We 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.

Procure: In the procurement area, our members are focused on getting the best performance from their investments and ensuring that risks are appropriately managed. An example of this is the Financial Institution Shared Assessments Program (FISAP) which is designed to improve the cumbersome and expensive service provider assessment process. The FISAP 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, nearly 50 organizations are involved in the FISAP and there is increasing interest in overseas firms that provide services

⁵ See <http://www.bitsinfo.org/downloads/Publications%20Page/bitsconscon.pdf> and <http://www.bitsinfo.org/downloads/Publications%20Page/bitssecaware.pdf>.

⁶ See <http://www.bitsinfo.org/downloads/Publications%20Page/BITSSecureEmailFINALAPRIL1507.pdf>.

to financial institutions. The FISAP 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*.⁷ 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*.⁸

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.⁹ The guide is a comprehensive tool that is used by our member financial institutions to better understand the risks and strategies for working with telecommunications companies to deliver more diverse and secure telecommunication services.

In recent years, there has been increased focus on authentication which has implications for procurement. In October 2005, the Federal financial regulators issued supervisory guidance requiring financial institutions to improve authentication of electronic banking applications.¹⁰ In response to this guidance and changing threats, financial institutions have implemented stronger authentication technologies and procedures while trying to keep the process simple and convenient for customers.

In late April 2006, BITS participated in the Federal Trade Commission's workshop on authentication. The workshop revealed a number of challenges facing government and the private sector:

⁷ See <http://www.bitsinfo.org/downloads/Publications%20Page/bits2003framework.pdf> and <http://www.bitsinfo.org/downloads/Publications%20Page/bits2003framework.pdf>

⁸ See <http://www.bitsinfo.org/downloads/Publications%20Page/bitsbcheck.pdf> and <http://www.bitsinfo.org/downloads/Publications%20Page/bitsexitsstrategy.pdf>.

⁹ See <http://www.bitsinfo.org/downloads/Publications%20Page/bitstelecomguide.pdf>

¹⁰ See FFIEC "Authentication in an Internet Banking Environment"
http://www.ffiec.gov/pdf/authentication_guidance.pdf.

- The complexities of how identity theft is perpetrated and the limitations of authentication technologies currently available to prevent fraud and identity theft.
- Difficulties that governments face in implementing national and state identification programs given the costs and citizen expectations and concerns.
- Promises and perils of biometrics in light of consumer concerns that criminals might access biometric information and perpetrate fraud, in addition to concerns as to how government may use biometric information.
- Greater appreciation for the notion that identity is a relationship and that people adopt identities for different purposes. This creates a dynamic tension for advocates of a national identification system in which there is a unique identifier for each individual.
- Greater understanding of the consumer acceptance challenges and why banks implemented risk-based device authentication technologies to comply with the FFIEC authentication guidance.
- Greater understanding of the importance of interoperability given the many systems used to identify, verify, and authenticate identity.
- Greater use of wireless devices and mobile phones for authentication and for mobile payments.
- Gradual emergence of smart cards for access to government facilities and computer networks.
- Concern over the security of devices given the rise of spyware and botnets and other malware.

Another example with implications for procurement is encryption technology. Encryption is an important and useful tool and a key component of a financial institution's information security programs. However, encryption of data poses a number of significant challenges that financial institutions must consider. First, its application must be measured against the need for interoperability with clients, business partners and regulators, and the ability to access data today as well as to meet recovery and retention requirements in the future. Second, encryption should be used only after identifying the threat before applying a control. For instance, encryption does not protect against abuse of legitimate access to information; whereas better access control requirements, data masking, or other controls could be much

more effective. Third, there are consequences to encrypting data that must be weighed against the benefits. For example, there are potential negative effects on computer networks, the ability to detect intrusions, the reduced speed of computing, and the ability to retrieve data for back-up restoration or business continuity requirements. There also are implications upon mandatory monitoring requirements and the ability to provide regulators records of communications. Fourth, encryption in itself cannot guarantee data security. Given that many of the publicly announced data breaches in recent years were from stolen paper documents or data sold to fraudulent businesses, it is important to recognize that encryption would not have prevented the information from being viewed or compromised. The threshold issue in a compromise is the usability of the compromised data. Encryption is only one class of factors that can affect the usability of data.

Some government agencies do not allow financial institutions to transmit sensitive data in encrypted formats. We encourage government agencies, such as the Internal Revenue Service (IRS), to permit the transmission of encrypted data when our member financial institutions share data with government agencies.

Analyze and Research: In the analysis and research areas, financial institutions have encouraged the government and academic community to collect and analyze information on the costs and impact of information security risks, vulnerabilities and threats. In 2006, the Departments of Justice and Homeland Security initiated a National Cyber Security Survey (via The RAND Corporation). BITS supported this effort and encouraged our members to participate in this survey. Our hope was for more accurate data on the cybersecurity challenge and its impact on society. Since initiating the study last year, our members have not received feedback or results of the study.

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:¹¹

- 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.

Enforce. Under the category of encouraging law enforcement to enforce, investigate and prosecute cyber crimes here and abroad, the financial services industry is playing a leadership role. Financial institutions have an obligation under existing laws and regulations to file Suspicious Activity Reports on computer crimes, identity theft and others. This information is a major source for regulator and law enforcement agencies to investigate crimes. Another example that is purely a private sector driven effort is the work of the ITAC in partnering

¹¹ For more information, please see the current FSSCC Research Agenda at: www.fsscc.org/reports/2006/Research_Agenda_Booklet_061108.pdf

with law enforcement to catch and convict criminals while assisting victims of identity theft. With the consumers' consent, ITAC shares information about these crimes with the United States Postal Inspection Service (USPIS) and hundreds of other law enforcement agencies through the FTC Consumer Sentinel database. Data supplied by ITAC is helping law enforcement catch the individuals who commit these crimes. The USPIS reports that for the fourth quarter of 2006, data from ITAC helped produce eighteen arrests and the execution of three search warrants. The success of law enforcement efforts is heavily dependent on front-line law enforcement officers having the knowledge and forensic skills essential to the investigation of computer-based crime. For that reason, ITAC is working closely with the United States Secret Service and the Alabama District Attorneys Association on the National Forensic Computer Institute which will train hundreds of law enforcement personnel each year in computer forensic techniques.

Conclusion

I would like to close by stating that securing information is no easy task and there are no simple solutions. Securing information and protecting privacy is an ongoing process. It requires constant vigilance, constant enhancement to address new and emerging threats, and collaboration with partners. Members of BITS are sharing information, analyzing threats, creating best practices, urging the software and technology industries to do more to provide more secure products and services, and combating fraud and identity theft. These efforts are helping the financial services industry mitigate some of the risks facing the financial services industry and can be applied by government agencies in complying with the goals of FISMA. Our members also want to encourage the Congress to improve information security by urging government agencies to develop more secure credentials that can be used to identify individuals, by implementing a Social Security verification program to reduce fraud and identity theft, and by encouraging government agencies to permit financial institutions to transmit sensitive information in encrypted formats.

Thank you for the opportunity to testify before you today.

APPENDIX: PREPARE: RECOMMENDATIONS FOR GOVERNMENT

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.
- 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 employs a system for industry-specific events through 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.

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:

- Enhance criminal penalties for cyber crimes.
- Make cyber crimes and identity theft enforcement a higher priority among law enforcement agencies.