

STATEMENT  
OF  
WILTON DOLLOFF  
EXECUTIVE VICE PRESIDENT  
OPERATIONS AND TECHNOLOGY  
HUNTINGTON BANCSHARES INCORPORATED  
ON BEHALF OF  
BITS AND THE FINANCIAL SERVICES ROUNDTABLE  
BEFORE THE  
HOUSE FINANCIAL SERVICES COMMITTEE  
UNITED STATES CONGRESS  
HEARING ON  
CRITICAL INFRASTRUCTURE PROTECTION

SEPTEMBER 8, 2004

**TESTIMONY OF WILTON DOLLOFF  
EXECUTIVE VICE PRESIDENT, OPERATIONS AND TECHNOLOGY  
HUNTINGTON BANCSHARES INCORPORATED**

**Introduction**

Thank you, Chairman Oxley and Ranking Member Frank, for the opportunity to testify before the House Financial Services Committee about the ways the financial services sector is addressing critical infrastructure protection.

I am Wilton Dolloff, executive vice president for operations and technology at Huntington Bancshares Incorporated. I am pleased to appear before you today on behalf of BITS and The Financial Services Roundtable (The Roundtable). Huntington is a \$31 billion regional bank holding company headquartered in Columbus, Ohio. Huntington provides innovative retail and commercial financial products and services through more than 300 regional banking offices in Indiana, Kentucky, Michigan, Ohio and West Virginia. Huntington also offers retail and commercial financial services online, through its 24-hour telephone bank and through its network of nearly 700 ATMs. Financial services activities are also conducted in other states including Florida, Georgia, Tennessee, Pennsylvania, Maryland, New Jersey, and Arizona.

I am also a member of the Executive Committee of BITS, a nonprofit industry consortium of 100 of the largest financial institutions in the US. BITS is the sister organization to The Financial Services Roundtable. 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, acting quickly to address problems and galvanize the industry. BITS' activities are driven by the CEOs and their appointees—CIOs, CTOs, Vice Chairmen and Executive Vice Presidents—who make up the BITS Executive Committee and BITS Advisory Council. BITS is not a lobbying organization. Our work in crisis management coordination, cyber security, critical infrastructure protection and fraud reduction is shared not only among our member companies but throughout the financial services sector. We have set industry-wide technology standards and business requirements for enhancing security, managing vendors and reducing fraud, including best practices for preventing and reducing Internet fraud and managing service provider relationships. BITS works with other critical infrastructure sectors, government organizations including US Department of Homeland Security, US Department

of the Treasury, Office of the Comptroller of the Currency (OCC), the Federal Reserve, technology providers and third-party service providers to accomplish its goals.

We are fortunate to have excellent leadership within our sector. While BITS takes pride in its own role in enhancing the sector's preparedness, we recognize that collaboration and joint efforts with many of the other financial services industry associations can magnify the value of what we have contributed. One principal vehicle for this collaboration is the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC), in which BITS participates. The FSSCC is chaired by the financial services sector coordinator, Don Donahue, Chief Operating Officer, Depository Trust and Clearing Corporation. The FSSCC fosters and facilitates financial services sector-wide activities and initiatives designed to improve critical infrastructure protection and homeland security, based on the close alliance and cooperation among BITS and the other FSSCC members to achieve these ends. BITS and other FSSCC members work closely with the Federal Banking Infrastructure Information Committee under the leadership of Wayne Abernathy, Assistant Secretary for Financial Institutions, US Department of the Treasury, and with the active participation of numerous government agencies responsible for the safety and soundness of the entire financial services sector.

### **Responding to the Challenge**

Since 9/11, our sector has done a lot to respond to the risks we face today. Protecting our Nation's critical financial services infrastructure is a top priority. Senior financial services executives have dedicated countless hours to prepare for the worst and to deal with the associated challenges. These efforts have played a major role in helping financial institutions prepare for and respond to crises.

The financial services sector is a key part of the Nation's critical infrastructure. Ensuring that the payments system operates during times of crisis is essential to the Nation's wellbeing. Among industry sectors, the financial sector is particularly aware of the challenge, in part because customer trust is so 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.

Protecting our Nation's critical financial services infrastructure is a top priority. Among other things, we have convened numerous conferences and meetings to bring together leaders and experts, developed emergency communication tools, strengthened our sectors' 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 the 9/11 attacks and the August 2003 blackout, developed best practices and voluntary guidelines, and combated new forms of online fraud.

There are a variety of important elements of our strategy to protect the financial services sector and its critical infrastructure. These include improving communications during crises, enhancing the resiliency of telecommunications services and the energy sector, improving the security of software and cyber space, addressing new forms of online fraud, and improving oversight of third party providers—all of which in total is focused on assuring the safety, soundness, security and stability of the financial services critical infrastructure. I'd like to briefly highlight several efforts.

### **Improving Communications**

A fundamental foundation of BITS' approach to critical infrastructure protection is effective communications. As one example, Crisis Management Coordination is one of BITS' highest priorities. BITS has opened participation in the Crisis Management Coordination Working Group to nonmembers, embracing public partners as well as representatives of member financial institutions. Among its key roles today is coordinating the industry during times of crisis through the BITS/FSR Crisis Communicator. This high-speed alert system rapidly notifies appropriate members of conference calls, during which industry leaders share information and make decisions. Most recently, BITS used the Crisis Communicator following the threat level escalation for the financial industry in certain regions on August 1. On that date, a Sunday, BITS held a conference call for members to ensure business continuity and the safety of personnel and physical assets. Senior executives from the nation's top 100 banks participated, including vice chairmen, CIOs, chief information security officers and chief technology officers. In addition, Assistant Treasury Secretary Abernathy participated in a call of the FSSCC to discuss the DHS announcement and the impact on the entire sector. In response to the August 1 announcement by DHS, financial services firms (beyond the four named institutions) took additional steps to increase physical security.

Many firms relied on the "considerations document" that BITS and the Securities Industry Association jointly developed in 2003 at the request of the FSSCC on behalf of the sector. This confidential document addresses security specifics for financial institutions to consider at each threat level of the Homeland Security Advisory System. This detailed series of suggested "threat level considerations" provides sector members with specific guidance on appropriate steps that individual organizations can implement to reduce vulnerabilities and provide additional protection for their employees. This guidance has played a key role in educating sector members about appropriate

measures in raising and lowering the intensity of their security precautions as appropriate at different threat levels. The financial services sector was the first to create such comprehensive guidelines, which have served as the basis for similar templates for other sectors.

The BITS Crisis Management Coordination Working Group has also helped member companies establish cross-industry crisis management procedures through the *BITS and FSR Crisis Management Process: Members' Manual of Procedures*. Additionally, members of this group share information and establish best practices to improve the industry's ability to prepare for and recover from large-scale business interruptions.

### **Strengthening the FS/ISAC**

Our sector has continued to support enhancements to the Financial Services Information Sharing and Analysis Center (the FS/ISAC), which was initially launched in 1999, to help secure the financial services sector against cyber attacks. Membership in the FS/ISAC continues to grow, providing an important tool for members to share and analyze threat and vulnerability information. Recently, the FS/ISAC has agreed to serve as the repository for an anti-phishing data base, developed through the leadership of the BITS Fraud Reduction Program, and described in more detail below.

### **Enhancing the Resiliency of Telecommunications Services**

One of the key “lessons learned” in recent years is our sector’s dependence on other critical infrastructure sectors, namely telecommunications and power. As a part of our strategy to address reliability and resiliency issues, BITS approached the telecommunications industry in 2002 in an effort to identify and mitigate vulnerabilities and enhance recoverability. The cooperation between these two sectors has been unprecedented. BITS has worked with the National Communications System, Federal Reserve Board,, Federal Communications Commission, and telecommunications companies. Additionally, BITS CEO Catherine Allen sits on the board of the Network Reliability and Interoperability Council (NRIC), representing the interests of the financial services industry. The NRIC’s mission is, in part, to assess telecommunications vulnerabilities and determine how to best address them.

Results of this collaboration include:

- A detailed and confidential assessment of interdependencies in a specific geographic area as a replicable model for other areas;
- Best practices in telecommunications and financial industry procurement practices and policies;

- Greater awareness of telecommunications industry priority access and recovery tools, such as the Government Emergency Telecommunications System (GETS) cards, Wireless Priority Service (WPS) and Telecommunications Service Priority (TSP) program;
- Pilots to model the costs of attaining greater diversity and redundancy in telecommunications services to the financial services industry;
- Completion of the NSTAC Financial Services Task Force Report on telecommunications resiliency issues;
- Adoption by BITS and Financial Services Roundtable CEOs of the Network Reliability and Interoperability Council (NRIC) best practices in physical and cyber security; and
- Education of both sectors on the importance of working closely together to identify and address issues.

The FSSCC, at its meeting next week, is expected to approve for widespread distribution throughout the financial sector a statement on telecommunications resiliency issues, intended to provide guidance to all financial firms—from the largest to the smallest—on how they can act to improve the resiliency of their own telecommunications infrastructure. This FSSCC statement will build further on the efforts undertaken by BITS and others I mentioned above.

### **Strengthening the Power Grid**

BITS is also working with the electric power industry on interdependency issues. The August 2003 blackout in the Northeast provided an opportunity to test our assumptions about what would happen with a large scale loss of power. In general, the electric power industry performed well. Backup systems operated, alternate communications systems were used, and there was no measurable impact on settlements and payments. There was excellent cooperation and communications among the financial services regulators, Treasury and the private sector. And, despite the absence of landline telephones and waning cell phone batteries, the BITS and Financial Services Roundtable Crisis Management Coordination process functioned as it should—providing members with a real-time forum to exchange information.

In June 2004, BITS held the BITS Critical Infrastructure Forum, “Strengthening Resiliency of the Telecommunications and Energy Sectors.” More than 100 executives from the financial services, telecommunications, energy, and chemical sectors attended. In addition, senior officials from Treasury, DHS and Federal Reserve Board participated. We discussed critical issues related to interdependencies among our sectors and developed an action agenda to address them.

### **Establishing Regional Coalitions**

BITS was a key player in the outstanding success of ChicagoFIRST, a cross-sector coalition to address crisis and security issues within Chicago's financial community. In cooperation with the US Department of the Treasury, and the Boston Consulting Group, BITS today is writing a manual to help other coalitions apply that model in their regions. The purpose is to address region-specific needs for resilience, recoverability and continuity of financial services in a time of crisis. The FSSCC, again, plans to work to get this material broadly distributed throughout the sector to encourage these types of preparations.

### **Financial Industry Steps to Strengthen Cyber Security**

Our industry has been working hard to strengthen cyber security. We have stepped up our efforts by sharing information, analyzing threats and urging the software and technology industry to do more to provide more secure products and services.

The state of cyber security is an alarming issue and critical to protecting the nation's infrastructure. 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. They are employing the tactics of spammers to rapidly spread their destructive code globally. We are increasingly concerned that a coordinated cyber attack of some kind could impact communications, Supervisory Control and Data Acquisition (SCADA) systems, or first responder systems and put all of us at terrible risk.

In October of last year, BITS increased its focus on flawed software with a Software Security and Patch Management initiative to respond to increasing security risks and headline-sweeping viruses. Our goal is 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.

Also in October of 2003, BITS began forging partnerships with key software vendors most commonly used in our industry. In February of 2004, BITS and The Financial Services Roundtable held a Cyber 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 key Software Security Business Requirements, essential from the perspective of the financial services sector. These requirements and the full “toolkit” are available in the public area of the BITS web site, at [www.bitsinfo.org](http://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, The Business Roundtable and some sector-specific associations.

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 R&D efforts to support stronger security in software products. We are also seeking protection from US antitrust laws for critical infrastructure industry groups that agree on 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.

Today, we are working with software companies to create solutions acceptable to all parties. In June 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.

This summer, BITS published best practices for patch management from the user’s perspective. This document is available to the public at no cost and applicable to industries outside of financial services. It was created by BITS in response to the increasing urgency of patch implementation, given the speed with which viruses are targeting new vulnerabilities. Security issues aside, patch management and implementation alone can cost one financial institution millions of dollars annually. A BITS survey of member institutions, extrapolated to the financial services industry in total, yielded

this estimate—costs to the financial services industry associated with software security, including patch management, are approaching one billion dollars annually. The best practices help companies mitigate these costs.

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. The tool starts with a list of common information security threats and vulnerabilities and matches them with corresponding controls to mitigate those risks. Using the tool, financial institutions score their own information security risks based on the likelihood of an incident, the degree to which the organization has defended itself against the threat, and an incident's possible impact. An institution can use the results to boost its ability to assess and mitigate risks to its information security program. The tool brings together an extensive body of information security risk categories outlined in international security standards and emerging operational risk regulatory requirements and combines them in one tool. Financial institutions can modify the tool to meet their unique needs.

BITS is participating in the Corporate Information Security Working Group (CISWG) which is sponsored by Congressman Adam Putnam, 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 set up by DHS and several technology associations.

In October, BITS will hold an invitation-only Forum called "Protecting the Core." This event will allow executives from member companies, government, and invited vendors to come together to discuss how the significant risks and costs resulting from insecure devices, untrusted systems, and new threats/vulnerabilities impact core operations.

The Forum will focus on sharing best practices and identifying solutions, focusing on three critical areas: 1) creating strategies for evaluating internal and external risk; 2) deploying preventative measures in a dynamic environment; and 3) identifying incident-management best practices.

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.

BITS is also working with other critical infrastructure industries and industry associations to help motivate a larger user movement. BITS' consultation and collaboration with The Business Roundtable resulted in that organization's widely publicized response to the state of software security. The Business Roundtable called on software producers and end users to work together to build a more unified defense against the increasing number and growing cost of cyber attacks.

### **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 BITS/FSR Identity Theft Assistance Center. Developed by BITS and the Roundtable, with the support of 50 founding member institutions, the ITAC is in pilot at this time. The concept is to provide a simplified recovery process that benefits victims by relieving much of the current burden of reporting the theft and restoring one's financial identity. Once an individual has reported a theft to his or her financial institution, and the problem has been solved at that institution, with the victim's permission, the ITAC will work with the consumer to determine whether accounts at any other institutions have been affected. If so, the ITAC will step in to notify all other companies where there may be an affected account. By working with the Federal Trade Commission and law enforcement agencies, information collected by the ITAC will be used to 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. Background about the legislative and policy environment, including existing and proposed laws, is provided 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 a victims' financial identity. Included are 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 is creating a Phishing Prevention and Investigation Network. The Phishing Network will provide member institutions with information and resources to expedite investigations and address phishing/spoofing incidents. The Phishing Network will include a searchable database of information from other financial institutions on their phishing incident and response experience, including contacts at law enforcement agencies, foreign governmental agencies, and ISP Web administrators. The Network will also provide data on trends to help law enforcement build cases and shut down identity theft operations.

The BITS Phishing Prevention and Investigation Network will:

- Help member institutions monitor and shut down e-scams faster and more effectively.
- Reduce financial institution manpower costs and losses.
- Increase phishing investigations and arrests of perpetrators.
- Facilitate communication among fraud specialists at financial institutions, service providers and law enforcement agencies.

### **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, organizations like 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 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.

### **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 had 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 early understanding of the scope and cause as early as possible when a major event occurs.** During the August 2003 blackout, the announcement that the problem was not the result of a terrorist event alleviated public concerns and made for orderly execution of business continuity processes. 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.

### **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. During the August 2003 blackout, the announcement that the problem was not the result of a terrorist event alleviated public concerns and made for orderly execution of business continuity processes. Diverse communication channels such as cell phones, wireless email devices, landline phones, and the Internet are necessary. Both

diversity and redundancy are needed within critical infrastructures to assure backup systems are operable and continuity of services will be maintained.

3. **Recognize the dependence of all critical infrastructures on software operating systems and the Internet. Given this dependence, 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 US antitrust laws for critical infrastructure industry groups that agree on baseline security specifications for the software and hardware that they purchase.
4. **Encourage regulatory agencies to review software vendors—similar to what the regulators currently do in examining third-party service providers—so that software vendors deliver safe and sound products to 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 telecom circuits are adequately protected and that redundancy and diversity in the telecommunications networks assured.
6. **Invest in the power grid because of its critical and cascading impact on other industries and other critical infrastructures.** The power grid must be considered among the most vital of critical infrastructures and needs investment to make sure it works across the nation.
7. **Establish improved coordination procedures across all critical infrastructures and with federal, state, and local government when events occur.** Coordination in planning and response between the private sector and public emergency management is inadequate and/or inconsistent. For example, a virtual national command center for the private sector that links to the Homeland Security Operations Center would help to provide consistency.

8. **Encourage law enforcement to prosecute cyber criminals and identity thieves, and publicize U.S. government efforts to do so.** These efforts help to reassure the public and businesses that the Internet is a safe place and electronic commerce is an important part of the Nation's economy.

Protecting critical infrastructure is a collaborative and cooperative effort. Only by working together can we address the challenges we face today. On behalf of Huntington Bancshares, BITS, and The Financial Services Roundtable, thank you for the opportunity to testify before you today.