Homeland Security Strategy

for Critical Infrastructure Protection in the Financial Services Sector

Version 2

May 2004

This ***Homeland Security Strategy for Critical Infrastructure Protection in the Financial Services Sector*** (the "Financial Services Strategy") has been adopted by the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (the "FSSCC"). The FSSCC was created in 2002 under the auspices of the United States Department of the Treasury as a private-sector organization to foster and facilitate financial services sector-wide voluntary activities and initiatives designed to improve Critical Infrastructure Protection and Homeland Security. The FSSCC consists of senior leaders from 28 of the financial services industry's key associations, utilities, exchanges and clearinghouses. Further information about the FSSCC is set forth elsewhere in this Financial Services Strategy, and is available on the FSSCC's website, www.fsscc.org.

PART ONE

INTRODUCTION

The *National Strategy for Homeland Security* identifies three national strategic objectives to secure the homeland:

i. Preventing terrorist attacks within the United States,
ii. Identifying and reducing vulnerabilities to such attacks, and
iii. Ensuring the resiliency of the nation to minimize the damage and expedite the recovery from attacks that do occur.

The *National Strategy to Secure Cyberspace* refines these objectives to focus on their implications on the national cyberspace. The *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* further refines these objectives to focus on the identification of critical infrastructures, steps to assure their protection, steps to provide for warnings in the event of foreknowledge of a threat and the development of a national approach to provide these benefits to additional critical infrastructures that may become the subject of a threat in the future. These three "National Strategies" set forth a comprehensive set of objectives for national resiliency and recovery capabilities. Each of the major economic sectors has been asked to articulate and implement a sector-specific strategy identifying how the sector will undertake to achieve these national objectives in the context of the sector's own activities.

STRATEGIC OBJECTIVES

The Financial Services Strategy identifies efforts in the financial services sector to achieve objectives for the sector consistent with the overall objectives of the National Strategies. Although the sector plays a key role in supporting national efforts to prevent attacks, strategic objectives in this area are more likely to be set and led by governmental authorities; therefore, the sector's efforts will focus more on the following overall objectives of the Financial Services Strategy:

i. Identifying and reducing vulnerabilities in the financial services infrastructure to such attacks,
ii. Ensuring the resiliency of the nation's financial services infrastructure to minimize the damage and expedite the recovery from attacks that do occur, and
iii. Promoting public trust and confidence in the financial services sector's ability to withstand and recover from attacks that do occur.

The Financial Services Strategy will address attacks by physical means or by cyber means (separately or in combination), with a principal focus on cyber security issues.*

* Although this Financial Services Strategy discusses the sector's planned efforts in the context of preparing for and responding to "attacks," it is, of course, the case that actions taken already by sector organizations and the initiatives planned under this Strategy also improve the sector's resiliency

STRATEGIC PRINCIPLES

Activities in the financial services sector to address sector issues relating to protection of critical infrastructures must be guided by certain key principles that identify crucial considerations in defining and implementing the strategy:

1. The financial services sector exists to service the personal and commercial financial needs of the people of the United States, and its continued ability to do so has a direct impact on public trust and confidence in the sector and on our nation's economy. The people of the financial services industry are the key means through which the sector meets this social need. The safety and security of the people of the industry must always be a principal objective of infrastructure protection efforts, since these people play a critical role in protecting the financial assets of the people of the United States.

2. The financial services sector is a decentralized and regionalized industry, with several different sector business components – banking, investments, insurance among others – and multiple centers of financial activity that are distributed throughout the United States. Many of the security issues relevant to the sector are most usefully defined at the business component level, since different vulnerabilities and issues exist in each of the components. In other cases efforts need to focus on the security vulnerabilities and issues for a particular financial center or region. The decentralized structure of the industry also means that some key infrastructures – markets and otherwise – can function independently and, in the event of an emergency, can be recovered at different times.

   Further, virtually all key infrastructures within the sector are privately owned, so efforts to address vulnerabilities and issues will require significant private sector participation and close coordination between involved private and public sector representatives. The Financial Services Strategy must reflect these factors, embracing decentralized solutions that focus on key sector business components and regional centers, with these solutions based on private sector contributions toward these national objectives.

3. The financial services sector is highly dependent on certain other critical sectors (most notably telecommunications), and the Financial Services Strategy should seek to identify means of addressing adverse impacts on the financial services sector from events affecting the other sectors, especially where there are specific vulnerabilities unique to financial services.

4. The Financial Services Strategy will evolve over time, as the industry develops more extensive experience with infrastructure protection, as new threats and vulnerabilities arise, and as improved approaches to protecting and restoring the financial services sector can be identified. The Financial Services Strategy, therefore, will need to be updated periodically to reflect progress made and new issues as they arise.

---

against other kinds of disruptive events resulting from power failures, extreme weather conditions or other causes.

5. The vulnerabilities of the financial services sector represent not only exposures to the national threat from terrorism, but also exposures to criminal and other damaging activities. The Financial Services Strategy will take a broader view of the vulnerabilities of the sector and seek to contribute to public trust and confidence in the sector through identifying means of addressing these risks and vulnerabilities.

SCOPE OF THIS STATEMENT

The areas of critical infrastructure protection and homeland security safeguards are viewed as particularly important priorities within the financial services sector today. Considerable industry efforts have been and are being directed to improving safeguards, identifying appropriate practices and strengthening resiliency. It is anticipated that the strategic objectives and principles identified above will remain the same for the sector in the future, but that specific areas of sector activity will evolve as practices and resiliency improve. Accordingly, the FSSCC anticipates that the sector's strategy statement will be updated periodically to identify and address key areas for strategic focus for the subsequent period. This "Version 2" statement is intended to encompass sector activities through mid-2006.

PART TWO

STRATEGIC SUCCESSES TO DATE

Many in the financial services sector have contributed to a broad range of initiatives addressing the strategic objectives articulated in the *National Strategy for Homeland Security*.[*] Some representative sector accomplishments, to date, include:

- **Helping to deter attacks**. The sector has provided important support for national efforts to deter attacks through such actions as the extensive sector efforts to promote awareness of and achieve compliance with the requirements of the Anti-Money Laundering Control Act, the anti-money laundering provisions of the Bank Secrecy Act, and Title III of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act). The sector's intense focus on these issues has aided the government's efforts to abate the financing of global terrorism through the establishment of anti-money laundering programs. The sector's efforts have included the development of internal policies, procedures and controls, ongoing staff training programs and independent audit and testing, together with efforts through sector associations and others to share information about requirements and "best practices" in this area. Such information sharing holds the potential to significantly augment the capabilities of any single financial institution to be aware of, and therefore guard against, money laundering and terrorist financing risks.[**]

- **Promoting trust and confidence**. The sector has acted to promote public trust and confidence in the sector's resiliency and recovery capabilities in a variety of ways, including, most notably, by establishing in May 2002 the FSSCC, to foster and facilitate voluntary activities and initiatives designed to improve critical infrastructure protection and homeland security in the sector. The FSSCC has undertaken a series of programs to coordinate sector activities related to infrastructure protection and homeland security issues and to promote sector awareness and education regarding these issues. More specifics regarding the FSSCC are set forth in Appendix B.[***]

- **Reducing vulnerabilities and ensuring resiliency**. The sector has taken a number of steps to identify and reduce vulnerabilities and to ensure the resiliency of the sector. In 1999, the sector launched the Financial Services Information Sharing and Analysis Center (the FS/ISAC), which was an early

---

[*] This section identifies certain initiatives that are representative of the sector's contributions over the past two years toward the strategic objectives identified in the *National Strategy for Homeland Security*, but the activities identified certainly are not all of the sector's efforts in these areas. Examples of the sector's accomplishments in these areas are set forth in Appendix A to this Statement.

[**] Examples of sector activities in this area are included in the section of Appendix A contributed by the American Council of Life Insurers.

[***] Examples of other sector activities in this area are included in the sections of Appendix A contributed by the American Bankers Association and the Investment Company Institute.

implementation of this information sharing capability to help secure the sector against cyber attacks. In its original implementation, the FS/ISAC membership grew to include 65 of the largest U.S. banking, securities, and insurance firms, which account for the overwhelming majority of the financial assets held. The FS/ISAC service allows these members to share and analyze threat and vulnerability information, and has helped sector members resist cyber attacks and take preventive steps to address exposures in their IT infrastructures.

Sector members also crafted and disseminated within the financial services industry a detailed series of suggested "threat level considerations" measures, providing sector members with specific guidance on appropriate steps that individual organizations can implement to reduce vulnerabilities and provide additional protection for their employees for different Threat Conditions under the Homeland Security Advisory System. This guidance 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 comprehensive guidelines, which have served as the basis for similar templates for other sectors.

Core infrastructure organizations within the sector responded to the events of September 11, 2001, with broad-ranging steps to reinforce their resiliency and business continuity capabilities, with efforts completed or under development by a number of these organizations to increase geographic diversity and to reinforce contingency data processing or operational capabilities. Sector organizations worked with governmental authorities to ensure resilience of sector communications through the national TSP and GETS programs.

Sector associations and organizations focused on business continuity and crisis management planning for key sector components. Considerable progress has been made in establishing cross-organizational procedures to coordinate and manage industry interactions in emergency situations. To date these plans have been implemented in a decentralized way, addressing the needs of particular markets or particular payment or settlement systems independently. Recent sector discussions have made clear that some degree of integration among these plans is needed to minimize duplication and ensure a coordinated response to any emergency across the markets.[*]

Each of these steps also contributed significantly to the sector's ability to preserve public trust and confidence in the security of the sector.

[*] Examples of the sector's extensive activities in this area are included in the sections of Appendix A contributed by the American Bankers Association, America's Community Bankers, BITS, ChicagoFIRST, the Independent Community Bankers of America, the Futures Industry Association, the National Association of Federal Credit Unions, the Securities Industry Association and others.

PART THREE

FUTURE STRATEGIC ACTION PLAN

The Financial Services Strategy seeks to address its strategic objectives and carry out its strategic principles through an action plan focused on the following key sector objectives:

A. To identify and reduce vulnerabilities in the financial services infrastructure to terrorist attacks:

1. The sector is implementing a revised action plan for the Financial Services/ Information Sharing and Analysis Center

Although the FS/ISAC has been quite effective in sharing information among its members, the events of September 11 demonstrated that the "membership model" followed in the original implementation of the FS/ISAC limited information dissemination, with most sector participants not having access to needed information. In a process beginning late in 2002, the FS/ISAC Board of Managers defined a new process for FS/ISAC operations that extends the reach of the FS/ISAC to nearly all firms within, or that provide supporting services to, the financial services sector.* The sector views this as one of the two principal sector strategic initiatives during the period for this "Version 2" strategy statement.

The enhancements to be implemented under this initiative include:

a. The FS/ISAC is transitioning to a new service model, evolving from a paid membership model into one that can provide rapid and timely basic information sharing and analysis services to all sector institutions and the associations that represent them. In 2003, as an interim step, the FS/ISAC modified its operating rules to allow sector associations to become full members of the FS/ISAC, with the right to distribute alerts that are marked "critical" or "urgent" to their members. This quickly enabled the FS/ISAC to extend its coverage to as many sector participants as possible as the transition to the new service model unfolded.

b. FS/ISAC coverage is being extended to include physical security threats, vulnerabilities and incidents in addition to those related to computer and network security. Further, FS/ISAC information sharing includes coverage of practical solutions, countermeasures, and best practices concerning CIP preparedness and management that are developed and endorsed by the sector participants or key sector organizations.

* The FSSCC and FSSCC member organizations have provided significant support to the FS/ISAC in this transition; note, for example, the section in Appendix A contributed by the BAI.

c. The FS/ISAC is linking to national alert and information sources being organized under the Treasury and DHS. It will link with other ISACs, especially the Information Technology/ISAC, the Telecom/ISAC and the Energy/ISAC, as well as a full range of private and public sector CIP services to maximize information flow and to provide scalable information services to all sector participants. On an ongoing basis the FS/ISAC will receive information from DHS and Treasury, and also will provide a path for sector participants to report their issues and a forum for sector participants to discuss respective threats, vulnerabilities, incidents, risks and solutions.

d. The FS/ISAC will define a process to report significant incidents to appropriate public and private sector organizations to support the aggregation of risk and threat data for broader and deeper analysis. These organizations can include other firms and government agencies charged with the protection of critical infrastructure components.

e. In addition to its information gathering and dissemination roles, the FS/ISAC is developing an internal analysis function that will analyze the information being gathered from a financial services sector perspective. As a result of this analysis, the FS/ISAC will alert sector member firms to those items of intelligence that it believes have the greatest import for the sector, along with its rationale for those conclusions. In this way, over time, the amount of analysis performed by individual firms should decrease. In addition this will benefit those smaller firms that have neither the resources nor the time to perform such an analysis of the raw data coming from the FS/ISAC.

f. The FS/ISAC Board of Managers is implementing the necessary administrative decisions to permit the FS/ISAC to achieve these objectives, including implementation of detailed Service Level Agreements (SLAs) with each of its service providers to ensure that sector participants have access to a high level of service and performance; a process of assessing service provider performance; and an appropriate funding model for the FS/ISAC which will allow for broad participation throughout the industry.

The FS/ISAC Board of Managers anticipates that these enhancements should be completely implemented by year-end 2004.

2. The sector will assist in the development of approaches to supporting individual sector members' efforts to reduce their individual vulnerabilities.

The financial services sector is comprised of a broad range of financial institutions of all types, servicing different financial markets and different customers. Virtually all of these institutions rely heavily on information

technology to deliver their services, but have widely varying levels of resources available to them to address technology issues. As a consequence, one critical area of individual institution and sector risk exposure is the prevalence of software vulnerabilities and the effort needed to address these vulnerabilities. The sector has been proactive in addressing these issues, pressing software providers to the industry to meet a higher standard of care when selling to the financial industry and other critical infrastructure companies.

Investments to assure the security of a particular institution's technology and information assets can be one significant source of demand on an organization's resources, since financial institutions must, on an ongoing basis, address issues arising from software product security defects and resulting patch management activities, as well as undertake duplicate testing and work force training necessary to address these issues. The varying levels of resources available to different institutions may impact their ability to meet these requirements. Finding more effective ways of addressing these issues, both at the sector level and at the individual institution level, can help reduce the resource investments required for these activities, and permit resources to be redirected to more preventive measures.

These disparities in resources are of particular concern with respect to information security, since the effectiveness and resiliency of the sector's information security protections are to a significant degree influenced by the effectiveness and resiliency of each individual member's protections. To the extent resource constraints, tolerance for risk, or other issues impair an individual institution's abilities in this area, a vulnerability is introduced – a "weakest link" – that may impact others in the sector and, potentially, result in a cascading failure that compromises the financial system itself. Improving the effectiveness of sector resource investments through a more proactive approach can help guard against the creation of these "weakest links."

The sector recognizes the need to accelerate its shift from a reactive to a proactive vulnerability management approach. At the same time, many of these information security issues are not unique to the sector, nor would solutions limited to the sector necessarily resolve all of the principal vulnerabilities. The sector, therefore, will seek to coordinate its activities in these areas with those pursued by other affected sectors. In particular, the sector will work in conjunction with the task forces initiated at the December 2003 National Cyber Security Summit to address these key issues. Sector representatives involved in these initiatives will emphasize the sector's focus on efforts to (a) reduce the need for individual sector members to ascertain the information security features in software products in common use in the sector through a certification program that ascertains compliance with sector-specified security requirements, (b) promote knowledge throughout the sector of appropriate standards for training and certification of security practitioners and application development staff in their information security responsibilities, and (c) participate in efforts to reduce

burdens in applying corrections to software products through the development of best practices in this area, potentially including a broadly available clearinghouse of information on such software patches and patch management. These three efforts – building on the sector's already extensive efforts in this area[*] – are described below.

(a) The sector will support efforts to assess approaches to promote testing and certification of technology products used within the sector. Software products have among the highest levels of defects of any products sold today, and there is very little accountability on the part of the producers of software products. Symptomatic of these defects are product patches, one of the major business and security impacts affecting the sector. These patches are released to address vulnerabilities that arise from defects in design and/or implementation and are, at best, analgesic. A more effective approach to addressing this issue would be to specify the minimum baseline security requirements a software product must meet, validate that the product properly implements these requirements through a formal testing procedure, and provide broader assurance to sector members that the product satisfies these requirements through a third-party certification process.

A first step in raising the level of information security resiliency in the sector would be to build on existing efforts to promote this more effective approach for software products in common use in the sector. To do this, we would work with appropriate parties to establish a "baseline level" of information security protections in these software products. We also recognize the need to implement programs that result in more effective testing of these products. These products need to demonstrate through a formal testing and certification process that they have successfully incorporated the minimum baseline security requirements (as defined by the industry) so that all sector members, regardless of the level of their sophistication in information security matters, can be assured that these products meet certain minimum standards.

The sector has invested heavily over the past several years in an effort to address product vulnerabilities, introduced by poorly created software products, which threaten our critical infrastructure. The sector has defined the baseline security requirements through a collaborative effort that brought together many sector organizations, technology providers and government agencies. By incorporating baseline criteria into their products, technology providers will increase the security and reliability of their offerings, reduce the risks associated with these products, and, ultimately, assist our sector and other sectors in improving the overall security and reliability of the products and services we provide using their products. Once the products incorporate the baseline criteria, it is necessary for products to demonstrate compliance with the criteria through a formal testing and certification process.

[*] See, for example, the section of Appendix A contributed by BITS.

In order to achieve this objective, members of the sector will work with appropriate counterparts from other sectors to increase awareness of this issue with technology providers and reach agreement on a mutually acceptable compliance certification process. Building on the sector's previous work on product testing and certification, the sector will promote the development of a plan for implementing a broader scale testing and certification process and effective program model, highlighting the benefits of testing and certification, encouraging organizations (within and outside the sector) to incorporate security requirements in contracts, and shifting of the liability of poor quality software from the users to producers of software products.

(b) The sector will assess approaches to promote training and certification of information security staff and application developers within the sector. The *National Strategy to Secure Cyberspace* recognizes the need for adequate training, awareness, and education programs to ensure the continued availability of trained cybersecurity professionals able to meet the Nation's cybersecurity needs. It also notes that a lack of trained personnel and of widely accepted, multi-level certification programs for cybersecurity professionals complicates the task of addressing cyber vulnerabilities. One of the initiatives the *National Strategy to Secure Cyberspace* identifies to address these issues is to promote private-sector support for well-coordinated, widely recognized professional cybersecurity certifications.

Determining the best approach will be a complicated and lengthy process, as there are a number of certification programs already in existence. These range from managerial-level certifications for information security professionals (such as the CISSP and CISA programs) to security certifications that are focused on key technology platforms for technical professionals responsible for the configuration and management of information resources, to security certifications that are focused on certifying proficiency in configuring, managing, and securing particular products. Further, although the initiative contemplated in the *National Strategy to Secure Cyberspace* appears to be primarily focused on the certification requirements for security practitioners, substantially more benefit might be derived if the approach also addresses the needs for training and, possibly, certifying of application developers and testers in cybersecurity matters.

Sector members agree that it is important that financial services institutions have available a constant and ready source of trained information technology professionals, including those who have demonstrated sufficient expertise in particular areas to achieve widely recognized certification credentials. Sector representatives will participate in a broader work effort to define the key elements of a cybersecurity certification program that meets the needs of the industry. A primary objective will be to examine the various IT job classifications applicable to the industry, to identify the security roles and responsibilities that each job classification might have, and to define security training requirements, and possibly certifications, appropriate to each job classification. The work effort also will ascertain which, if any, existing training programs can meet defined needs, or

how we might work with the certifying organizations to modify their programs to meet these needs. A key aspect of this task will be to work both with various certifying organizations and also with academic institutions to define how business and technical curricula might be enhanced so that future graduates attain higher levels of security knowledge and skills.

It is important to recognize that security training and certification does not stop at the security professional. Many known vulnerabilities in software products, which are the focus of the majority of patches issued, are attributable to gaps in the knowledge and training of developers with regard to security principles and practices, and to inadequate testing of products that permit these vulnerabilities to remain in products distributed into the marketplace. Training and certification of developers and testers needs to be considered as well.

Information regarding the standards and standard practices identified in this work effort will be disseminated widely throughout the financial services sector as a "best practice."

(c) The sector will assess how it can contribute to the development of a "software vulnerability patch clearinghouse" supported by an appropriate group.

The *National Strategy to Secure Cyberspace* and general industry commentary characterize the process of identifying vulnerabilities in software in common use within the financial services sector and implementing tested patches to remedy these vulnerabilities as key components of the effort to secure the national cyberspace. These commentaries, however, have not fully recognized the substantial burden involved in managing this process – each individual institution is required not simply to identify vulnerabilities and apply patches, but also to appropriately test each patch in the institution's own systems environment to ensure that it can be applied without causing other software to break or malfunction.

The burden the financial services sector now faces – along with other sectors – from remedying these defects cannot be underestimated. A survey of the largest US financial institutions was conducted in late 2003 on the estimated costs to financial institutions of addressing software security and patch management problems. These figures were then extrapolated to estimate the overall annual cost to the financial services industry. High-level results of the survey include:

- Software vulnerabilities are approaching a cost of $1 billion annually to the financial services industry.

- Patch management and implementation alone can cost one financial institution millions of dollars annually.

Some studies indicate that the "average" patch can cost up to $900 per server as a result of the testing and verification required before it can be applied in a particular systems environment.[*] Others estimate an average cost of $50 per desktop when an automated installation procedure fails to deploy the patch to all desktops. In large institutions with 20,000 or more devices, even a failure rate of 10% translates into costs in excess of $100,000 for a single desktop patch.[**] Conservatively, an institution can receive several patch notifications weekly given the number of technology providers and different platforms that it utilizes. Even if it receives just one or two weekly from all its major technology providers for the most widely-used software, a not unlikely scenario, the management burden and costs become readily apparent.

A more structured way to prioritize vulnerabilities and patches must be found, as well as a way to promote information about "best practices" in patch management, to minimize the burden of this process across all sector member firms. While sector members generally believe that the development of such a "software vulnerability patch clearinghouse" is more appropriately the responsibility of information technology vendors (and, conceivably, the Information Technology/ISAC), sector representatives will contribute to broader efforts aimed at creating a means of sharing information regarding patch testing and prioritization as these efforts are launched.

B. To ensure the resiliency of the nation's financial services infrastructure to minimize the damage and expedite the recovery from terrorist attacks that do occur:

1. Members of the sector will proceed with their plans to comply with the business resiliency standards articulated by the regulatory agencies in the April 2003 Interagency Paper.

The second principal sector strategic effort for this period involves the efforts of key sector participants to implement necessary changes in their infrastructures to meet the business resiliency standards set forth in the "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System" issued in final form by the Federal Reserve Board, the Office of the Comptroller of the Currency and the Securities and Exchange Commission on April 7, 2003. The paper identifies four "sound practices" that "core clearing and settlement

---

[*] Davidson, Mary Ann. "Automatic Patching -- Boon or Bane?", *Secure Business Quarterly*, vol 3, issue 2, Second Quarter 2003, [cited 30 July 2003], available at http://www.sbq.com/sbq/patch/sbq_patch_mdavidson.pdf

[**] Donner, Marc. "Patch Management -- Bits, Bad Guys, and Bucks!", *Secure Business Quarterly*, vol 3, issue 2, Second Quarter 2003, [cited 30 July 2003], available at http://www.sbq.com/sbq/patch/sbq_patch_mdonner.pdf

organizations" and "firms that play significant roles in critical financial markets" are expected to address and implement in the coming months:

a. Identify clearing and settlement activities in support of critical financial markets.

b. Determine appropriate recovery and resumption objectives (within stipulated guidelines) for clearing and settlement activities in support of critical markets.

c. Maintain sufficient geographically dispersed resources to meet recovery and resumption objectives.

d. Routinely use or test recovery and resumption arrangements.

Under the paper, core clearing and settlement organizations are expected to "substantially achieve" the sound practices by the end of 2004. Firms that play significant roles in critical financial markets are expected to move forward with plans that call for substantial achievement of the sound practices as soon as practicable, but generally within three years of the paper's publication (i.e., not later than Spring 2006).

The financial services sector views these efforts as critical to its ability to ensure resilience in the sector infrastructure against disruptions that may occur – from terrorist acts and for other reasons. Accordingly, the efforts of key sector participants to comply with these standards represent a major sector strategic initiative during the period for this "Version 2" strategy statement.

2. The sector will develop a rationalized approach to coordinate crisis management and recovery efforts within the sector.

As discussed above, sector organizations quickly responded to the "lessons learned" from the disruptions following the September 11 attacks by undertaking extensive efforts to coordinate emergency management efforts for different markets or for different payment and settlement systems. These efforts have included initiatives to establish rosters of emergency contact information, emergency "calling trees" to alert sector participants of relevant information, schedules of conference calls and other sessions to coordinate emergency response activities and similar preparatory steps. Importantly, these efforts have established emergency response structures that are aligned with the decentralized nature of the nation's financial markets (consistent with the Strategic Principles enumerated earlier). The sector's ability to respond to emergencies has been substantially strengthened due to these efforts.

Given the overlap among sector organizations and infrastructures, however, these sector efforts have produced some degree of duplication that could create some

problems in an actual emergency. Further, the sector's coordination of these decentralized efforts needs to be reinforced. To address this, the sector will form a working group of appropriate representatives who will identify the existing decentralized emergency response capabilities, identify any potential overlaps among them and resolve these overlaps, and determine what additional steps are needed to provide for coordination among these capabilities. It is anticipated that this effort will be completed by mid-2004.

3. **Members of the sector will participate in broader efforts to assess the security benefits of implementing version 6 of the Internet Protocol.**

The *National Strategy to Secure Cyberspace* identifies as a key Action and Recommendation (A/R 2-3) that:

> [t]he Department of Commerce will form a task force to examine the issues related to IPv6, including the appropriate role of government, international interoperability, security in transition, and costs and benefits. The task force will solicit input from potentially impacted industry segments.

The financial services sector relies on several key private telecommunications networks provisioned and/or managed by sector infrastructure organizations, and many of these networks are increasingly migrating away from older or more proprietary technologies to IP-based telecommunications. (Examples include the Securities Industry Automation Corporation's new Secure Financial Transaction Infrastructure (SFTI), the migration to SWIFTNet, the evolution of Depository Trust & Clearing Corporation's SMART network, and implementations in progress to networks supporting Fedwire and The Clearing House's CHIPS system.) As part of this migration, the sector infrastructure organizations necessarily are increasing their involvement with the security issues associated with the use of IP as it becomes more pervasive.

As the *National Strategy to Secure Cyberspace* indicates, the proponents of version 6 of IP believe that it offers certain advantages in terms of security, in addition to other benefits. While sector participants are somewhat skeptical in regard to these claims, sector representatives would be willing to contribute their expertise to any broader effort seeking to investigate the security benefits of Ipv6. In addition, sector members could work to identify a set of "best practices" for securing an IP network that would be broadly disseminated among sector member organizations. The sector will form a working group of appropriate representatives of industry organizations to consider the appropriate approach once any work effort under the *National Strategy to Secure Cyberspace* commences.

4. **Members of the sector will assess the viability of approaches to mutualized back-up for sector infrastructure organizations.**

   Under the auspices of the FSSCC representatives of sector infrastructure organizations ("core clearing and settlement organizations" for purposes of the April 2003 "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System") will form a separate working group to exchange information relevant to the resilience and business continuity preparations of these organizations. This working group will consider possibilities for sharing business continuity infrastructure among core clearing and settlement organizations, developing mutualized back-up capabilities or reciprocal back-up arrangements, and other such issues. This group will also seek to extend consideration and discussion of these issues to peer organizations in key financial markets in other countries as a proactive effort to extend critical infrastructure protection initiatives beyond the U.S. financial markets.

   This group will seek to provide a report of its progress in this area by mid-2005.

5. **The sector will continue with efforts to identify and implement appropriate protective measures addressing vulnerabilities resulting from dependencies on other economic sectors (e.g., telecommunications).**

   The financial services sector requires reliable and available services from other economic sectors, such as telecommunications, in order to perform its business operations and service its customers. This dependency is not unique to the financial services sector, but does have particular importance to and consequences for financial services.

   Understanding the nature and degree of these dependencies requires both a "top-down" and "bottom-up" approach to identifying adverse impacts and implementing protective strategies. Individual financial institutions must take a "bottom up" approach to assess risks, work closely with their service providers, and jointly develop contingency and disaster recovery plans and measures to address critical vulnerabilities that would seriously impact their business operations. It is equally important, however, that the sector itself take a "top down" approach to provide a strategic and systemic understanding of the most critical aspects of inter-sector dependencies and to prepare to manage these dependencies in a crisis. Again, the sector must particularly focus on the telecommunications sector as the most critical inter-sector dependency we must address.

   Sector members will continue efforts to better understand inter-sector dependencies on telecommunications and to address any resiliency issues identified. These initiatives will build upon activities conducted by sector organizations over the past two years, such as:

- A joint forum, held in June 2002, for representatives of the financial services and telecommunications sectors and governmental agencies to initiate cross-sector discussion of ways to improve resiliency and redundancy

- A working group, sponsored by the Industry Executive Subcommittee of the President's National Security Telecommunications Advisory Committee (NSTAC), that focused on the risks arising from the financial services sector's dependence on the telecommunications infrastructure to support the sector's core payment, clearance, and settlement processes to develop recommendations for actions to mitigate those risks.

- The Joint Pilot Recoverability Assessment Information Exchange, under which sector organizations collaborated with DHS/Office of the Manager of the National Communication System (NCS) and telecommunication service providers to examine a geographic area that has a high concentration of critical financial services that if not available for two or more hours could have national security and emergency preparedness implications, to determine the telecommunications assets/processes supporting these services and their associated recovery processes/timelines, and to identify any potential recovery issues or concerns.

- Sector participation in several national-level advisory committee efforts that have specific focus on telecommunications and cross-sector interdependency issues, including a National Infrastructure Advisory Committee (NIAC) effort to provide the President and federal government recommendations on inter-dependency issues among critical infrastructures, and the Network Reliability Interoperability Council (NRIC), a best practices body sponsored by the Federal Communications Commission, to develop recommendations on cyber and physical security for telecommunications.

- Sector collaboration with the Alliance for Telecommunications Industry Solutions (ATIS) CIO Council on a "National Diversity Assurance Pilot" to develop an effective process aimed at providing diversity assurance for critical national security/emergency preparedness circuits utilized by financial institutions.

- Intra-sector efforts to coordinate responses to telecommunications dependency issues through integrated approaches relying on sector infrastructures, such as the Payment Risk Committee's task force on telecommunications issues.

- Sector collaboration with Treasury on a draft tax incentives proposal that would provide long-term financial incentives for strengthening telecommunications resiliency.

The sector will continue to participate in these initiatives as they arise, and seek to disseminate to sector member institutions "best practice" standards for managing these dependencies as they are identified through these efforts.

6. **The sector will work to coordinate and support appropriate exercises to assess improvements in readiness and identify additional required enhancements.**

   The FSSCC will work with Treasury on improving the process for identifying, committing resources, and coordinating participation by financial institutions in exercises to assess sector preparedness for emergencies. The FSSCC, in conjunction with Treasury, will implement an approach to evaluate proposed exercises to determine which ones offer benefits to the sector in terms of assessing readiness and resiliency, and to suggest participation by sector organizations in exercises that are beneficial. Under this approach the FSSCC will "sponsor" appropriate exercises, as selected through this process, and work to promote sector participation in these "sponsored" exercises. Examples of exercises the FSSCC would encourage the sector to support would include TOPOFF-like exercises, now coordinated by DHS, which offer a significant opportunity for improving cross-sector, government and private sector coordination testing, and the planned National Cyber Exercise, being designed and coordinated under federal government sponsorship, that will focus on improving cross-sector coordination in the cyber area.

7. **The sector will work to develop and implement processes for ongoing sector readiness and risk assessments.**

   Within the sector, there must be an efficient and timely mechanism for gathering from critical sector members as to the state of their preparedness for emergencies or potentially disruptive events, consolidating that information into a sector-level readiness or risk assessment, and reporting those assessments to the appropriate regulators and governmental agencies. This would be in the form of an appropriately classified report provided on a regular basis, or as needed in the event of an emergency. The FSSCC recognizes, however, that this is a complex endeavor, and anticipates that a work group to develop such a consolidated process would not be initiated until later in 2004.

C. To promote public trust and confidence in the financial services sector's ability to withstand and recover from terrorist attacks:

The public's trust is the most valued asset of financial institutions and an essential part of the foundation for their ability to conduct business. Maintaining that trust is critical to the financial services sector's business and to the nation's economy. The sector will focus in two areas to accomplish this objective:

1. The sector will raise awareness of Critical Infrastructure Protection and Homeland Security issues throughout the sector by means of ongoing outreach programs.

For the public to have trust and confidence in the financial services sector's ability to recover from terrorist attacks, it is essential that financial services sector personnel, at all levels, are aware of the Critical Infrastructure Protection and Homeland Security (CIP/HLS) issues relevant to financial services and are committed to sector efforts to address those issues. Creating this awareness depends on sector "outreach" programs that are a critical supporting element of the sector's strategy. The primary objectives of these outreach efforts are to:

- Maximize general knowledge of CIP/HLS,
- Communicate the importance of our nation's and sector's CIP/HLS objectives and initiatives,
- Increase the sector's participation in CIP/HLS initiatives, and
- Maximize information sharing throughout the sector in support of these initiatives.

Within the sector, outreach efforts will target executive, business, operations, technology and security management. This would include contacts at the CEO, COO, CIO and CTO levels, and with Information Security and Security officers, executives with responsibility for Privacy and Risk issues, Business Unit officers, Boards of Directors and Board Committees such as Audit, Finance and Investment, and with other senior executives, product and service vendors and consultants. FSSCC members are the primary vehicle for communicating to these audiences.

The FSSCC will, as appropriate, reach out to the executive and legislative branches of the government and federal, state and local regulatory agencies to increase their awareness of sector-level CIP/HLS initiatives.

The FSSCC will work with key stakeholders and partners in the development and execution of its outreach efforts. This will include representatives of the Treasury and Homeland Security departments, the Financial and Banking Information Infrastructure Committee (FBIIC) agencies, the Partnership for Critical Infrastructure Security (PCIS), other critical infrastructure sectors, the National Infrastructure Advisory Committee (NIAC), and the Homeland Security Advisory

Committee (HSAC). The primary outreach effort is a forum jointly sponsored by the FSSCC and the FBIIC, established to provide educational opportunities for all financial services companies in major financial center cities. The forum covers best practices relating to physical security and cyber security, among other matters. Such programs have already been held in various cities around the country, and roughly a dozen additional locations are planned over the next half-year.

In addition to the awareness objectives outlined above, the following action steps have been incorporated:

- Development and distribution of uniform presentation materials to ensure common and consistent messages delivered by speakers
- Development and distribution of a list of concrete action items that industry and government can undertake to assist the sector in fulfilling its mission

It is anticipated that a cycle of these forums will be held roughly every two years to communicate new initiatives and actions that evolve to achieve our strategic objectives.

Other awareness efforts will include briefings to appropriate audiences, articles in the industry trade press and speaking engagements at industry conferences.

2. The sector will develop a public communications plan as part of the sector's crisis response and recovery process.

Maintaining public confidence in the sector's ability to ensure its resiliency, both in advance of and during a time of an actual crisis, needs to be a significant sector objective. Our sector goals in this area are as follows:

- Maintain public confidence both in times of crisis and on a regular, ongoing basis, and
- Establish clear, accurate, effective and timely communications relative to the safety of consumers' assets, and
- Handling communications during an incident or threat that may affect them.

It is important that the public know that, even during a crisis, the safest place for their assets is with their financial institution. The industry's back-up systems, business recovery and continuity plans, applicable regulatory requirements, and deposit insurance programs provide additional safeguards. These and other key messages need to be developed and agreed-upon throughout the sector and a communications plan and strategy will be developed around them.

The FSSCC will seek to develop a plan by the end of 2004 to achieve the sector's communication objectives in this area. Through our industry outreach programs and our public communications plan, the sector will provide the necessary elements to foster and maintain public confidence in all our financial institutions.

SECTOR SUCCESSES IN INFRASTRUCTURE PROTECTION ACTIVITIES 2001-2003

AMERICAN BANKERS ASSOCIATION

The American Bankers Association (ABA), an industry group whose membership includes community, savings, regional and money center banks, savings associations, trust companies and diversified financial holding companies, has an active, ongoing program for informing their membership of cyber security issues and providing cyber security resources.

As a member of the Financial Services Sector Coordinating Council, the ABA has taken a lead role in the current education and outreach initiative that is underway at the Council. This initiative is designed to apprise financial sector companies of existing organizations, including the Financial Services Information Sharing and Analysis Center, which can be utilized as a resource for information regarding physical as well as cyber threats and vulnerabilities. A second aspect of the initiative is to garner feedback from financial sector companies as to how the process of sharing such information should evolve, in terms of organization, services, and cost.

In relation to BugBear.B, the computer virus containing the domain name of over 1,200 financial institutions worldwide, the ABA sent an email or fax to the chief executive officer of the 550 member institutions that were listed in the virus' code. The alert was extremely beneficial in helping community-based financial institutions understand the import of FSSCC and FS/ISAC.

In its continuing outreach efforts, the ABA is developing a database of the primary and secondary cyber and physical security contacts at each of its member institution. This database will be used for direct submission of alerts as we transition to the next generation FS/ISAC, as well as for the purpose of ensuring that the proper individuals in each institution are solicited for direct FS/ISAC participation.

The ABA has developed a “Safeguarding Customer Information Toolbox,” made available free to members, to assist them in evaluating their information security and comply with Section 501.B of the Gramm-Leach-Bliley Act of 1999. The toolbox contains resources to assist financial institutions in building their security culture, assessing their information security and risk, managing vendor risk, reviewing their business continuity and recovery efforts, training employees and communicating their information security efforts.

The ABA holds a series of interactive Webcasts on a variety of critical infrastructure protection and cybersecurity issues. Additionally, in 2003 three ABA conferences, the Compliance Conference, the National Conference for Community Bankers, and the Foreword Financial Technology Convention, contained sessions on information security, as well as technology vendor due diligence and management. These conferences will also be held in 2004 and will contain an expanded series of information security sessions.

The ABA also distributes a bi-weekly electronic newsletter, the ABA eAlert, which focuses on electronic banking and information security concerns. The ABA website, aba.com, has a series of web pages addressing information security, pointing members to a variety of resources. Other ABA publications, such as the ABA Banking Journal, the ABA Compliance Magazine, and ABA Bankers News have recently contained lead articles regarding critical infrastructure protection and cyber threats.

Finally, the detection and prevention of identity theft is an area where the ABA has devoted a good deal of attention. For instance, the association has provided members with a Communications Kit that is designed to help bankers provide their customers with the resources and information they need to protect their

identity. The association, as part of its "Financial Privacy Toolbox," also made training aids available to assist front-line bank personnel in spotting pretext calling, a technique commonly used by identity thieves.

The ABA, in conjunction with Lexis/Nexis, has also recently released InstantID, a service that verifies customer account information across multiple databases, validating that such information as name, address, date of birth and social security number are authentic and identifying potentially high-risk data elements, for example, miss-matched addresses, prison or campground addresses, disconnected phone numbers, or Social Security numbers of deceased persons. In addition to helping reduce fraud and identity theft and complementing existing fraud tools, IDPoint can also play a valuable role in assisting the bank fulfill the new account opening requirements in the USA PATRIOT Act.

SECTOR SUCCESSES IN INFRASTRUCTURE PROTECTION ACTIVITIES 2001-2003

AMERICAN COUNCIL OF LIFE INSURERS

In response to developments concerning the USA PATRIOT Act and the Office of Foreign Assets Controls (OFAC), the American Council of Life Insurers (ACLI) formed a Money Laundering Subcommittee. The Subcommittee addresses a broad range of issues on the USA PATRIOT Act, OFAC, and other related items, as well as works with the U.S. Treasury Department. ACLI participated in numerous substantive discussions with Treasury and the Department of Justice to clarify the scope and intent of the Act and anti-money laundering standards as applied to life insurers and reinsurers. ACLI also spearheaded visits between Treasury, insurance companies, reinsurers, and insurance trade groups. As a result of these exchanges, Treasury regulations for insurance companies will not be developed in an informational vacuum.

ACLI developed and provided to member companies of the ACLI voluntary guidelines for life insurers to follow because insurance companies needed to develop these programs without the benefit of any actual or proposed instructional regulations. The Treasury expressed a favorable reaction to the ACLI guidelines, and commended ACLI for its prompt action and leadership. ACLI was positioned to react quickly to the Act because it has been following money laundering issues since the early 1980s, and has developed relationships wit the FBI, Postal Inspectors, Department of Justice, Treasury, and the SEC. ACLI has submitted substantive comments on numerous rulemaking initiatives under the Act.

The ACLI has been actively engaged in several significant policy development and information sharing groups. ACLI is one of the twenty-three founding members of the FSSCC CIP/HLS, which seeks to identify strategic initiatives enhancing critical infrastructure protection, and provides coordinated input to the federal government, for the financial services industry. ACLI formed a Homeland and Infrastructure Protection Working Group for our member companies in order for the life insurance industry to provide input to the FSSCC, as well as to provide a forum for discussion about and action on infrastructure and homeland security issues.

ACLI serves on Treasury's USA PATRIOT Act Task Force, to improve early policy development and effective rulemaking under the Act, for the insurance industry. ACLI actively participates in the *Intercept Forum* at The Clearing House in New York City, through which ACLI dialogues with federal regulators and law enforcement agencies about money laundering compliance, information sharing issues, and law enforcement responsiveness.

Treasury selected ACLI as a member of its U.S. delegation to an international forum on money laundering and terrorist financing designed to harmonize international standards for identifying and blocking assets of money launderers, and to promote

uniform sanctions. ACLI has twice been part of Treasury's U.S. delegation to the Financial Action Task Force (FATF), which develops anti-money laundering standards for international financial regulators, and submitted comments on FATF recommendations for anti-money laundering practices.

Additionally, immediately following the terrorist events of September 11, 2001, ACLI assumed a leadership role for life insurers regarding the USA PATRIOT Act, and in terrorist financing issues. At the request of the SEC, ACLI coordinated life insurer compliance with the Control List standards and procedures designed to isolate the assets of terrorists. On September 12, 2001, ACLI obtained emergency exemptive relief from the SEC concerning the pricing and redeemability of variable life insurance and variable annuities during the stock market closures. On September 20, 2001, ACLI obtained emergency relief from the Department of Labor so that life insurers could provide liquidity loans to pension plans following the stock market impairments of September 11th.

101 CONSTITUTION AVENUE, NW, Suite 700, WASHINGTON, D.C. 20001-2133
(202) 624-2183 FACSIMILE (202) 572-4756
www.acli.com

SECTOR SUCCESSES IN INFRASTRUCTURE PROTECTION ACTIVITIES 2001 – 2003

AMERICA'S COMMUNITY BANKERS

America's Community Bankers represents the nation's community banks. ACB members, whose aggregate assets total more than $1 trillion, pursue progressive, entrepreneurial and service-oriented strategies in providing financial services to benefit their customers and communities.

As a founding member of the Financial Services Sector Coordinating Council, America's Community Bankers recognizes the importance of keeping its members informed of current cyber and physical security threats that affect its member financial institutions, associate members and state organizations. ACB represents its members before the FSSCC.

ACB actively collects and maintains physical and cyber security contact information from its members and utilizes a variety of methods to keep its members informed of security threats on various levels. ACB collects and aggregates information from several security information service providers and disseminates the most critical information to its members. Most of the information communicated to members pertains to the latest virus threats and software security issues.

ACB and one of its business partners in the network security field recently joined with the FDIC to hold a series of seminars around the country to educate ACB members and other community banks on information security and the requirements of Gramm-Leach-Bliley Act. This involved working with the FDIC regional offices and their specialized information protection and security staff and examiners in the supervision division.

ACB communicated continuously and regularly with the federal banking agencies to ensure coordination of regulatory responses to cyber and physical security threats among insured depository institutions. One example of such coordination came recently after a series of bogus emails was distributed, claiming to be from the FDIC and the OCC. ACB coordinated with the FDIC and took quick action to get accurate information about these erroneous communications to its membership.

Information security and critical infrastructure protection are regularly featured topics at ACB conferences, including ACB's Annual Convention, ACB's National Operations/Technology Conference, and other ACB banking conferences. Through these forums, ACB discusses and educates community bank executives (and their board members) on the important issues surrounding information security, critical infrastructure protection and cyber-security.

ACB works to represent community banks on a variety of industry working groups such as the BITS Crisis Management Coordination Working Group, and the BITS Security and Risk Assessment Working Group. An ACB staff member was a contributing author of the "BITS Framework for Managing Technology Risk for IT Service Providers" (Version 1.0), which helps provide a roadmap for banks to manage IT security risk.

ACB sponsors regional network security/GLBA sessions for both ACB members and non-members.

For the past two years, ACB has been sending its members a weekly Security Alert which highlights the most critical network security issues threatening the industry.

Most recently, ACB monitors the threat alerts it receives from the FS/ISAC, and forwards this information to key staff of member institutions with security responsibilities.

In addition, ACB has integrated infrastructure protection into all aspects of its products and services, including program and meeting content and links to service providers.

ACB has created an area devoted to critical security issues that impact the financial sector on its “members only” area of its website.

In the past two years, ACB has distributed more than 4.7 million copies of identity theft brochures to community bank customers across the country in an effort to raise consumer awareness.

SECTOR SUCCESSES IN INFRASTRUCTURE PROTECTION ACTIVITIES
2001-2003

BAI®

BAI is an active participant in FSSCC initiatives to increase awareness of sector vulnerability and threat information resources and the need to build a greater focus on resiliency into the core business processes of banking companies. BAI has actively positioned the efforts of the FSSCC as good business practices to not only manage risk for financial services companies but as a tool to support consumer confidence in the financial services sector.

BAI has played a major leadership role in the FSSCC to ensure the success of the Next Generation FS/ISAC. In early discussions and planning stages, BAI identified the need for a comprehensive, coordinated and objective marketing strategy and plan to position and promote the launch of the new FS/ISAC capabilities and its clear value proposition. In June 2003,BAI committed to dedicate senior management resources to lead this strategic and tactical marketing effort. Since the time, BAI has worked closely with FSSCC leadership to form a FS/ISAC marketing sub-committee to ensure that our efforts were representative of the many segments of the financial services sector and that the FS/ISAC services design, packaging/pricing, value proposition, positioning and promotion of the FS/ISAC would resonate with all of the financial sector and provide a foundation for the FS/ISAC business model. In addition to BAI's own investment of resources, we funded and managed external consulting resources and production services to develop and execute on the agreed upon marketing plan.

In October 2003, BAI presented a comprehensive marketing plan to the FSSCC and has since developed execution and implementation tools and materials that can be leveraged by all Council members for soliciting FS/ISAC memberships. At the February 2004 FSSCC meeting, BAI launched an aggressive roll out of FS/ISAC marketing plan and a targeted recruiting program to support the FS/ISAC membership penetration goals.

To support the broader objectives of the FSSCC, BAI has integrated relevant content into its own extensive offerings including conference, education and training programs that reach thousands of banking professionals on an annual basis. We have provided various keynote speaker opportunities for Rhonda MacLean, and other FSSCC leaders, as well as regulators and subject matter experts. We have provided exhibit space and production services to FS/ISAC for the purpose of building visibility. BAI has also provided content development and program facilitation resources to support the FSSCC's Outreach programs.

BAI is the financial services industry's leading professional organization that delivers high-quality, relevant, objective information and education to enhance the organizational performance of financial services companies and the individual performance of banking professionals. BAI provides a comprehensive range of products and services that address the topical, strategic and operational issues in the financial services business.
BAI offers conferences, seminars and graduate schools, as well as full range of employee development tools including a comprehensive selection of a online and textbook training courses and employee opinion surveys. BAI also provides valuable insights on complex strategic issues through BAI KnowledgeBank, BAI Research and *Banking Strategies* magazine.

BAI is a non-lobbying organization located in Chicago, IL. BAI 's organizational members represent the vast majority of US commercial bank assets, global banking companies as well as other financial services companies.

ONE NORTH FRANKLIN STREET CHICAGO, ILLINOIS 60606 312-553-4600 FAX 312-683-2426

SECTOR SUCCESSES IN INFRASTRUCTURE PROTECTION ACTIVITIES 2001-2003

BITS
FINANCIAL SERVICES ROUNDTABLE

BITS was created in 1996 to foster the growth and development of electronic financial services and e-commerce for the benefit of financial institutions and their customers. A nonprofit industry consortium that shares membership with The Financial Services Roundtable (FSR), BITS seeks to sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions. 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. Membership in BITS and FSR is reserved for 100 of the nation's largest financial institutions. 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.

Security-related issues have always been—and remain—a priority for BITS. BITS has 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 cross-border outsourcing. In accomplishing its goals, BITS works with a number of government agencies, including the US Department of Homeland Security, Treasury Department, OCC, and Federal Reserve, and other agencies.

Through the BITS Security and Risk Assessment Working Group (SRA), BITS has played a key role in coordinating and drafting the financial services portion of the *National Strategy for Critical Infrastructure Assurance.* Made up of information-security leaders from member organizations, the SRA's mission is to strengthen the safety and soundness of financial institutions through sharing best practices and successful strategies to develop secure infrastructures, products and services; working with governmental agencies and regulators on supervisory guidance and regulations; and enhancing e-commerce and payments security. In 2004, the SRA is focusing on software security, legislation and regulation, operational risk, and critical infrastructure protection. The following priority areas operate under the direction of the SRA:

- **Crisis Management Coordination.** BITS provides its members the ability to communicate and coordinate with each other, government agencies and other sectors in order to implement the emergency response and recovery process for the financial services sector in a time of crisis. BITS has been instrumental in improving industry disaster preparedness. BITS created and maintains the BITS/FSR Crisis Communicator, a mechanism used to quickly convene meetings of member company CEOs and other leaders in times of crisis. BITS members also authored a key resource for members in developing internal crisis management procedures, the *BITS and FSR Crisis Management Process: Members' Manual of Procedures.* In all of its efforts, the Crisis Management Coordination (CMC) Working Group coordinates across institutions and sectors and cooperates closely with federal, state, and local authorities.

  Among the CMC Working Group's top priorities is to collaboratively address financial services interdependencies with other critical infrastructures, such as those between the telecommunications and financial services infrastructures. In 2004, BITS is also examining interdependencies with the electric power sector. The CMC Working Group facilitates efforts to establish regional coalitions to strengthen sector resilience in defined geographic areas. With ChicagoFIRST, a cross-sector coalition

of members of Chicago's financial community, BITS provided critical start-up resources and expertise during its first six months.

- **Software Security.** According to a survey conducted by BITS in December 2003, the cost of software vulnerabilities to the financial services industry is approaching $1 billion. In addition to the cost burden, software vulnerabilities have implications for the security of the nation's critical infrastructure. BITS has three primary goals in this area: to encourage a higher "duty of care" by software vendors that sell to critical infrastructure industry companies, to promote compliance with security requirements before software products are released, and to make the patch-management process more secure and efficient and less costly to organizations. BITS has developed business requirements for the software industry and is urging leaders in other critical infrastructure sectors to discuss security concerns with their software vendors. BITS is now in discussions with the financial services industry's major software suppliers. This group is also developing guidelines for patch management.

- **The BITS Product Certification Program (BPCP).** The BPCP was established by BITS members and other technology leaders to promote the security of software products used in the industry. A self-regulatory measure, the BPCP provides rigorous product testing by unbiased facilities against baseline security criteria established by the financial services industry. Those products that meet the criteria are awarded the *BITS Tested Mark*, indicating to financial services technology purchasers that the product has met industry requirements. Technology providers may also meet the product certification requirements via the internationally recognized Common Criteria certification.

- **IT Service Provider Relationships.** This effort raises awareness, develops voluntary guidelines, and shares successful strategies to assure the security and privacy of services provided by third parties to the financial services industry. BITS developed the first-of-its-kind *BITS Framework for Managing Technology Risk for Information Technology Service Provider Relationships* to provide detailed recommendations for managing IT service provider relationships. In 2004, BITS released the *BITS IT Service Providers Expectations Matrix,* a 33-page worksheet used by financial institutions and service providers to reduce risk while streamlining the financial institution service provider evaluation process.

- **Operational Risk Management.** This Working Group was formed in response to increased attention and evolving regulatory requirements related to operational risk management. Members work with the FSR to harmonize regulations and examination practices related to operational risk management. With the BITS Security and Risk Assessment Working Group, this group is developing risk-assessment elements for information security. The group is also developing a common body of baseline risk factors that influence operational risk and are related to information security.

Among BITS' other efforts to improve information security across the sector, BITS submitted detailed comments on the *National Strategy to Secure Cyberspace*. Working with the FSR, BITS responded to the "Draft Interagency White Paper to Strengthen the Resilience of the US Financial System." Through a matrix of sample scenarios and corresponding gaps in traditional insurance, the *BITS Technology Risk Transfer Gap Analysis Tool* provides guidance on e-commerce risk assessment and risk identification. The *Gap Analysis* can be used as a basis for discussions with management and insurance professionals, as well as for internal risk transfer analyses.

BITS is advancing the industry's interests in fraud reduction and payments. Additionally, BITS and the FSR are working together to create the Identity Theft Assistance Center (ITAC). As of March 2004, 50 member institutions have joined the ITAC. Developed by BITS and the FSR, the ITAC will provide a simplified recovery process that benefits victims by relieving much of the burden of reporting the theft. 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. The ITAC will be operational by 3Q04.

For more information about BITS, visit the BITS website at www.bitsinfo.org.

SECTOR SUCCESSES IN INFRASTRUCTURE PROTECTION ACTIVITIES 2001-2003

ChicagoFIRST

Regional Resilience

Recognizing that natural disasters and terrorist attacks have their greatest impact in the region in which they occur, financial institutions in the Chicago area formed a coalition for business continuity in 2003. The coalition, ChicagoFIRST, is the only regionally based organization in the U.S. dedicated to enhancing the resiliency of the financial community in a specific geographic region. ChicagoFIRST accomplishes this by fostering business recovery coordination and planning among its members and implementing a public/private partnership between its members and government at all levels.

The members of ChicagoFIRST include futures and options exchanges, commercial banks, brokerage firms, and clearing organizations. In January 2004, the organization became a limited liability company owned by the following firms: LaSalle Bank/ABN AMRO; Chicago Board Options Exchange; Chicago Mercantile Exchange; The Northern Trust Bank; UBS Warburg; Harris Bank; Archipelago; Chicago Stock Exchange; BankOne; William Blair & Company; Mesirow Financial; Mizuho Securities; The Options Clearing Corporation; and Bank of America.

ChicagoFIRST's key strategic partners include the City of Chicago, Department of Treasury, Department of Homeland Security, BITS, Securities and Exchange Commission, Commodity Futures Trading Commission, Federal Deposit Insurance Corporation, Illinois Commissioner of Banks and Real Estate, Federal Reserve Bank of Chicago, Board of Governors of the Federal Reserve, Office of the Comptroller of the Currency, U.S. Secret Service, Federal Bureau of Investigation, Financial Services Sector Coordinating Council, and the Futures Industry Association.

ChicagoFIRST Activities

Crisis Communication. ChicagoFIRST's highest priority had been to obtain a seat at Chicago's Joint Operations Center (JOC) to facilitate crisis communication. With the help of the Treasury Department, ChicagoFIRST achieved this goal in 2003. This will give the coalition's representative first-hand information about any disaster or emergency and how the city plans to respond. ChicagoFIRST is in the process of drafting policies and procedures for use of the seat and has identified individuals from the ChicagoFIRST membership to staff the center on a 24x7 basis when the Department of Homeland Security elevates its alert level to orange or red, or the JOC is otherwise activated by local authorities. Additionally, crisis management and coordinating procedures with the center are periodically being tested.

Credentialing. In the aftermath of the September 11 attacks, essential personnel whose physical premises were not destroyed lacked pre-authorized (by local officials) physical credentials to access restricted areas. Many businesses were unable to re-open in a timely manner or had great difficulty doing so. As a result, ChicagoFIRST has established a working project team with the City of Chicago, the City of Chicago Police Department, and Chicago's Building Owners and Management Association to develop an interim system to credential essential individuals. In addition, ChicagoFIRST and the City of Chicago recently co-hosted an information exchange on credentialing with New York City's Office of Emergency Management, which is testing a private sector approach to this issue in New York City in order to leverage critical lessons learned and avoid process pitfalls. At the same time, the City of Chicago is moving to adopt a longer term credentialing system of its own.

Evacuations/Sheltering in Place. ChicagoFIRST is working closely with the City of Chicago and the State of Illinois to both understand how the region will evacuate the central business district, if necessary, and ensure that the financial community's procedures complement those of the government. The organization has also participated in exercises with the City to test evacuation procedures, and more

exercises are planned. In addition, in 2004, ChicagoFIRST will develop best practices for sheltering in place, in conjunction with the City of Chicago and the Federal Emergency Management Agency.

ChicagoFIRST is the Regional Model

BITS, the Treasury Department, and the Financial Services Sector Coordinating Council (FSSCC) consider ChicagoFIRST a model that can be productively employed in other regions of the country. The structure and degree of formality can be tailored to meet the needs of any regional financial community. ChicagoFIRST has committed to work with BITS, the Treasury Department, and FSSCC to assist any such efforts and to foster the development of other regional organizations.

Leadership Breeds Success

The primary source of ChicagoFIRST's success can be traced to its leadership. Louis Rosenthal, Executive Vice President at LaSalle Bank/ABN AMRO, and Rohit Kumar, Chief Technology Officer at the Options Clearing Corporation, provided the vision and blueprint for the organization. In addition, BITS loaned able staffing assistance for ChicagoFIRST's initial six months in the person of BITS Chief of Staff Teresa Lindsey, who ensured that that vision became a reality. Furthermore, the members have not only funded the organization, but also have contributed time, ideas, and project leadership without which the blueprint could not be implemented.

For further information about ChicagoFIRST, please contact the Executive Director, Brian Tishuk, at brian.tishuk@chicagofirst.org.

SECTOR SUCCESSES IN INFRASTRUCTURE PROTECTION ACTIVITIES
2001-2003

INDEPENDENT COMMUNITY BANKERS OF AMERICA

In the wake of 9/11, the Independent Community Bankers of America, the nation's leading voice for community banks, has taken measures to ensure the security of its members. Working closely with the Financial Services Sector Coordinating Council (FSSCC) and the Financial Services Information Sharing and Analysis Center (FS/ISAC). ICBA is utilizing web-based technology to disseminate information of importance to its member base, the nation's community banks. ICBA has taken on the role as both a disseminator and clearinghouse of critical information. Some of the successes ICBA has encountered include:

- **ICBA Homeland Security Alert.** ICBA, a licensee of the FS/ISAC and member of the FSSCC, has developed an email alert service that notifies member banks of physical and cyber threats disseminated by the FSSCC and the FS/ISAC. When information has been received by ICBA, it is assessed and then disseminated via a list serve to those banks that have requested to be included in the dissemination. ICBA acts as a conduit between the FSSCC and FS/ISAC and ICBA's 5,000 community bank members. Banks have already responded with praise to the effectiveness and expedience of the ICBA Homeland Security Alert service.

- **ICBA Homeland Security Web Page.** In order to keep members frequently updated with information regarding Homeland Security, ICBA has created a Homeland Security section on its website devoted solely to cyber and physical security issues facing the finance and banking sector. The section, only accessible to members using valid passwords, contains a wealth of resources on preventive measures a bank can take to further ensure its security.

- **Outreach Meetings.** Using various communications media, ICBA has advertised symposia offered by the Financial Banking Information Infrastructure Committee and the FSSCC. ICBA encourages its members to attend these meetings that bring together federal, state and local government officials with sector representatives to advance sector protection.

SECTOR SUCCESSES IN INFRASTRUCTURE PROTECTION ACTIVITIES 2001-2003

FUTURES INDUSTRY ASSOCIATION

Organizational Successes

The Futures Industry Association (FIA) is the international trade association for the futures industry. Its membership includes more than forty of the largest futures commission merchants (FCM). FIA estimates that its members are responsible for more than eighty percent of all public customer business executed on U.S. contract markets. FIA's associate members include futures markets across the globe and domestic markets in the United States including the six U.S. futures exchanges (NYMEX, CME, NYBOT CBOT, MGE, and KCBT) and four equity options exchanges (CBOE, AMEX, PHLX, PECOS) as well as futures clearing houses and other firms servicing the industry.

The terrorist attacks of September 11, 2001 created tremendous disruption in the New York City financial markets and throughout the U.S. futures markets. However, the futures markets showed great resiliency as the industry reacted and re-opened the markets in a timely fashion. During the immediate hours and days after the terrorist attacks of September 11, 2001, FIA served as a communications hub, facilitator and industry information repository during the crisis. Since this event, FIA has built upon these industry successes and highlights of three of the many *strategic success to date appear below*:

Industry Communications and Coordination

FIA took the lessons learned from Sept 11th and formalized its role during crisis. FIA has added redundancy to its own technology and infrastructure to ensure it can perform vital industry functions of communications and coordination during a crisis. FIA continues to collect information for a Disaster Recovery Directory for key personnel from member firms. This information is distributed in hard copy format to members and posted online. The primary contact from these firms will provide a status report to a FIA Crisis Command Center in the event of an emergency. If the firm does not report within two hours of the event, then FIA will contact the firm for information. In addition, conference calls have been scheduled for 8:00 a.m., 12:00 p.m., 4:00 p.m. and 8:00 p.m. Wallet cards are to be distributed with conference call times and dial in information. In addition, FIA has established strategic partnerships with the Securities Industry Association and Chicago First to provide information on the futures sector and receive information on cities key to the futures industry.

Market Resiliency

Futures exchanges and FCMs have gone to great lengths over the last two years to review and update business continuity efforts, as well as their disaster recovery efforts. FIA has provided forums for discussion throughout this process and highlighted these efforts in various publications in order to ensure there has been communication and coordination throughout the industry. FIA is exploring industry-wide testing programs to test emergency preparedness.

Standards

Domestically, the futures industry is comprised of multiple exchanges. These exchanges have a complex communication backbone to communicate to trading members during and after trading hours. No standard protocol exists among the various network of exchanges and FCMs. As part of the industry wide business continuity efforts, FIA has established a Standards Working Group to consider a common communication protocol among communication systems. FIA has worked extensively with the FIX Protocol Organization to ensure that FIX is futures and options compliant and to establish standards for post-trade processing (FIXML). FIX Protocol Ltd. is a non-profit organization that owns the intellectual property rights of the Financial Information eXchange protocol (FIX), which is provided free in the public

domain. FIX is a globally recognized messaging standard enabling the electronic communication of pre-trade and trade messages between financial institutions, primarily investment managers, broker/dealers, ECNs and stock exchanges.

For more information on the Futures Industry Association or any of these activities contact: Mary Ann Burns, Senior Vice President of Communications at maburns@futuresindustry.org or Jeff Morgan, Chief Operating Officer at jmorgan@futuresindustry.org.

INVESTMENT COMPANY INSTITUTE

The Investment Company Institute (Institute) has continued to monitor or participate in numerous business continuity planning (BCP) initiatives directly focused on the financial services industry's emergency preparedness. Since 1999 the Institute has taken an active role in monitoring the development of the Financial Services Information Sharing and Analysis Center (FS/ISAC). Institute members are regularly updated by FS/ISAC participants on the increasing effectiveness of FS/ISAC's information sharing capability as well as threat and vulnerability analysis.

The Institute, primarily through its Committee structure, continuously updates members on regulatory, legislative and private organizations' (e.g. industry utilities) efforts to promote awareness of threats, limit vulnerability to attack, and develop best practice guidelines for business continuance. These initiatives include dissemination and discussion with Institute members on the USA PATRIOT ACT, Anti-Money Laundering Control Act, Inter-Agency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, National Strategy to Secure Cyberspace, Securities Industry Association's BCP Committee, and New York Stock Exchange and Nasdaq Stock Market BCP strategy.

The Institute, in October, will conduct a BCP Roundtable where Institute members will be able to discuss a wide range of BCP related strategies and challenges. Presentations tailored to the investment company industry will be delivered. It is expected that the Roundtable will be held periodically.

National Association of Federal Credit Unions
3138 10th Street North • Arlington, VA 22201-2149
(703) 522-4770 • 800) 336-4644 • Fax (703) 524-1082
www.nafcu.org • nafcu@nafcu.org

Critical Infrastructure Protection: NAFCU's Role

The National Association of Federal Credit Unions (NAFCU) is the only national trade association that exclusively represents the interests of our nation's federal credit unions. NAFCU is strongly committed to enhancing the resiliency of the nation's financial system. NAFCU is a founding member of the Financial Services Sector Coordinating Council (FSSCC) and has worked closely with it. NAFCU has also worked with the U.S. Department of the Treasury and the National Credit Union Administration on efforts to enhance security.

NAFCU actively participates in the activities of the FSSCC and the Financial and Banking Information Infrastructure Committee (FBIIC). NAFCU distributes information on the FDIC-sponsored regional outreach meetings to its members and strongly encourages attendance. A NAFCU representative generally attends these outreach meetings and meets with credit union attendees at the conclusion of the meetings for feedback. NAFCU is also working with the Financial Sector/Information Sharing and Analysis Center (FS/ISAC), including assembling a credit union focus group to meet with FS/ISAC representatives in September 2003.

On September 11, 2001, NAFCU provided key communication links for Pentagon Federal Credit Union and for XCEL Federal Credit Union, located in the World Trade Center in New York. NAFCU confirmed to Pentagon Federal Credit Union's main office that personnel working in its branch at the Pentagon were safe. Similarly, NAFCU confirmed the safety of XCEL staff to its CEO, who was traveling at the time.

NAFCU has a number of initiatives in place to educate its members on security issues. Training is an important part of NAFCU's mission. NAFCU holds a Compliance School at which the information security is always part of the curriculum. An annual Compliance Seminar usually addresses security issues as well. For example, a presentation on authentication was part of the October 2003 seminar. Finally, NAFCU holds an annual three-day Security Workshop devoted to safeguarding electronic information. NAFCU also sponsored a hacker lab at its Annual Conference in July 2003. NAFCU's attorneys are available to speak to credit unions on these and other issues as needed.

NAFCU publishes a variety of manuals designed to assist credit unions. NAFCU's Security Manual for Credit Unions covers both physical and cyber security. NAFCU's Contingency Planning, Disaster Recovery, and Record Retention for Credit Unions manuals focus on business continuity planning. Many other manuals have substantial sections on security. NAFCU also educates its member credit unions members on security issues in magazine and newsletter articles.

For additional information please call Robert Byrer, NAFCU's Regulatory Compliance Counsel, or Gwen Baker, NAFCU's Director of Regulatory Affairs, at (800) 336-4644.

Securities Industry Association
120 Broadway - 35 Fl. • New York, NY 10271-0080 • (212) 608-1500, Fax (212) 968-0703 • www.sia.com, info@sia.com

SIA BCP Background & Summary

Business Continuity Planning Steering Committee
September 2003

At its Annual Meeting on November 9, 2001 – The Securities Industry Association announced the launch of a new business continuity planning effort to coordinate and develop industry plans for disaster recovery and business continuity. As a result, a board level committee (Business Continuity Steering Committee) was created to direct these efforts.

The Business Continuity Planning Steering Committee has been charged with the following:

- Provide a forum for securities firms, industry organizations, and service providers to share specific plans and business continuity information.
- Identify and develop business continuity plans and projects that have an industry wide, rather than firm specific, focus.
- Provide liaison between the securities industry and government legislators, regulators, and service providers, as well as to related industries such as telecommunications and power utilities.

In fulfillment of its charter, the BCP Steering Committee has become the financial industry's hub for BCP related information and for the validation of BCP best practices. Beneath the BCP Steering Committee, the organizational structure currently consists of subcommittees with their own mission and deliverables. These include: Command Center, Exchange/Markets - Industry Utilities & Service Providers, Physical Infrastructure and Urban Renewal, Best Practices, Insurance, Catastrophic Events, Industry Testing, and Regional Issues. Committees meet at least once a month and also educate the industry with a yearly BCP conference and vendor exhibit.

Since their inception, the committees have made substantial progress in preparing the securities industry for unexpected outages while reducing vulnerabilities and ensuring resiliency. A dedicated web site http://www.sia.com/business_continuity has been developed to provide the latest information on the progress and work of the subcommittees. BCP website categories include: Reports, Press Releases, White Papers, Comment Papers, Regulatory Issues, Testing, Key Issues, and related links. You can also find the mission statements and current roster of the subcommittees.

In its short life, the committee has been involved in the NYC Transit strike preparation, software viruses, the east coast blackout, and hurricanes. The committee has initially released a Lessons Learned Document on the 9/11 attacks. They have also released comment letters representing the securities industry on the Amendments to NYSE rule 446 concerning BCP, the Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, and the NASD BCP proposals. SIA and the committee have also endorsed the Secure Financial Transaction Infrastructure (SFTI, pronounced "safety"), for resiliency within the industry's communication backbone. SFTI was developed by the Securities Industry Automation Corporation (SIAC). The Committee has also promoted the GETS and the TSP national programs.

Below is a summarization of several of the subcommittees:

Command Center-Procedures, roles and responsibilities have been developed by the subcommittee for communicating with various agencies i.e. NYC Office of Emergency Management (OEM) & other city agencies, state and federal agencies and other external groups such as BITS and FS/ISAC. The subcommittee conducts ongoing tests for the SIA/SIAC Emergency Notification System (ENS), which also identifies members who were not reachable under office hours and weekend testing scenarios. The tests are conducted quarterly.

Exchanges, Utilities & Service Providers-The American Stock Exchange, NASDAQ, Reuters, Bloomberg and other industry data and service providers have met with the subcommittee to describe their respective contingency plans. NYSE and NASDAQ have planned for trading NYSE stocks on NASDAQ and vice versa in the event of an emergency. The subcommittee also surveys service providers to distribute preparedness information to the entire BCP Steering Committee.

Urban Renewal and Critical Infrastructure- Has created a listing of New York Metro area critical infrastructure providers that will present their status to the committee on a regular basis. Also created is a listing of national and regional critical infrastructure industry regulatory groups relating to utilities. Additional reviews of scenario planning around widespread utility outages and/or the impact of regional outages on the financial industry as a whole have been initiated.

Best Practices- The subcommittee is developing a BCP 101 course outline to be released in September of 2003. The course outline will include specifics that will be published separately from the Best Practices Guidelines that were released last year.

Additional testing recommendations are being added to the Best Practices Guidelines in light of the accelerated interest in testing being expressed by the SEC and other regulators. An approach to this concern would be to include testing specifics in a BCP 101 course outline with general recommendations in the Best Practices Guidelines.

Industry Testing- The subcommittee has developed a strategy for holding an industry testing exercise. These will be scheduled on an ongoing basis.

Regional Issues-The Regional Issues Subcommittee works to provide a forum for the discussion of issues and concerns by regional firms. This includes ensuring that the work of the SIA BCP Committee and its subcommittees is geographically neutral. Members have reported on the formalized arrangements made with the Chicago OEM by the Chicago First organization. The subcommittee is also developing a template for developing relationships with local OEMs for use nationally.

THE FINANCIAL SERVICES SECTOR COORDINATING COUNCIL FOR CRITICAL INFRASTRUCTURE PROTECTION AND HOMELAND SECURITY

In May of 2002, Rhonda MacLean, Director for Corporate Information Security, Bank of America, was asked by the US Treasury Department to serve as the Financial Services Sector Coordinator for Critical Infrastructure Protection and Homeland Security. In order to represent the financial services industry in this area, and to work most effectively with Treasury and the Department of Homeland Security, a coordinating council was formed.

The Financial Services Sector Coordinating Council (FSSCC) for CIP/HLS was created to foster and facilitates financial services sector-wide voluntary activities and initiatives designed to improve Critical Infrastructure Protection and Homeland Security. The Council consists of senior leaders from 28 of the financial services industry's key associations, utilities, exchanges and clearinghouses. The Council's organization was formalized by establishing a limited liability corporation (LLC) in November of last year.

The goals of the Council are to:

- Improve CIP/HLS coordination of sector-related activities and initiatives among participating sector constituencies, and with private and public sector partners.
- Review ongoing strategic initiatives and identify voluntary efforts where improvements in coordination can foster sector preparedness.
- Identify barriers and develop initiatives to improve awareness, sector-wide voluntary CIP/HLS information and knowledge-sharing, and timely processes for critical information dissemination among all sector constituencies and government entities.

The Council has chosen six major areas of focus: Information Dissemination; Crisis Management; Outreach, including Cross Sector Outreach; Best Practices, Research & Development and the National Strategy for CIP/HLS.

Information Dissemination –A Task Group was established to support the Financial Services Information Sharing and Analysis Center (FS/ISAC) in its efforts to develop a sector-wide, information dissemination service. This working group, helped to develop the requirements that will result in a service that will permit timely, coordinated dissemination of information throughout the sector of both specifically targeted and general information on cyber and physical threats, alerts, and new vulnerabilities.

Crisis Management – When events occur with broad sector or national impact, a planned and adopted approach for sector-wide crisis management coordination as well as coordination with government entities is needed. Leveraging the leadership of BITS and the Securities Industry Association (SIA), a Task Group is developing a plan for sector-wide crisis management coordination.

Outreach – It is important for each organization to determine how to optimally support and commit efforts for achieving the goals of the executive orders and national strategies. Under the leadership of the American Bankers Association (ABA), a working group is developing a strategy for sector-wide outreach on homeland security and critical infrastructure protection initiatives.

Cross-sector Outreach - In addition, we are actively working to identify critical interdependencies with other sectors, and leveraging work being done by Council organizations in this area for potential Council endorsement. FBIIC and key members of the private sector Council are providing important leadership in cross-sector outreach.

Best Practices – There have been a variety of 'lessons learned', activities and knowledge sharing of "good practices" within various trade associations and among institutions and government entities. However, no organized repository is maintained to provide this information to authorized institutions and individuals for all current and future sector members. The FSSCC established a Web site for sharing this information and will continue to feature best practice presentations at our Council meetings.

Research & Development - A Task Group is being formed to identify a meaningful Research and Development agenda that would improve infrastructure protection within the financial services sector, and to share important research information among and between sectors for the benefit of the national infrastructure program.

National Strategy for Critical Infrastructure Assurance - A Task Group was formed to draft the sector's National Strategy for Critical Infrastructure Assurance. This will be the sector's primary vehicle for communicating its national strategies for critical infrastructure protection and homeland security.

Much has been accomplished since the formation of the Council. It is largely due to the Council organizations that contribute their time, energy, products and enormous intellectual capital, that we are able to be successful.

Through our Council members, the FSSCC engages nearly all financial services sector institutions, exchanges and utilities. Individual institutions can participate through their associations, and are represented on the Council through designated principals and points of contact from those associations. It is by all of the entities working together in a collaborative spirit, that the sector achieves excellence and ensures protection of our critical infrastructures.