General:

1. **What authorities do you possess that would enable you to mandate standards or requirements (technical, performance, reporting, authentication/identity management, etc.) with respect to the trustworthiness, resilience, reliability, security, and survivability of the communications and information systems and infrastructure used by your regulated entities?**

   Please find attached to this response the Government Accountability Office Report GAO-08-1075R - *Information Technology- Federal Laws, Regulations, and Mandatory Standards for Securing Private Sector Information Technology Systems and Data in Critical Infrastructure Sectors* which identifies the authorities that the Federal Financial Regulators have in the area of cyber security. In addition, we have also attached the most recent draft of Appendix B of the Banking and Finance Sector Specific Plan, which includes, in more detail, both the statutory authorities and guidance and key selected documents that may assist your efforts.

   Finally, we call your attention to the Federal Financial Institutions Examination Council (FFIEC) Information Technology (IT) Handbook which was developed through a collaborative effort of the FFIEC's five member agencies (the Federal Reserve Board, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision The IT Handbook is made up of 12 booklets: Audit, Business Continuity Planning; Development and Acquisition; E-Banking; Fedline®; Information Security; Management; Operations; Outsourcing Technology Services; Retail Payment Systems; Supervision of Technology Service Providers; and Wholesale Payment Systems. Of particular interest to this review is the Information Security booklet which provides guidance for examiners and financial institutions to use in identifying information security risks and evaluating the adequacy of controls and applicable risk management practices of financial institutions. Information security is also addressed in other booklets as well. The following booklets address information security as it pertains to the topical subject of the booklet: Development and Acquisition; Electronic Banking; Fedline®; IT Management; Outsourcing Technology Services; Re-tail Payment Systems; and Wholesale Payment Systems

   We have also included a link to the "FFIEC InfoBase" (www.ffiec.gov/ffiecinfobase/index.html) that was developed by the Task Force on Examiner Education to provide field examiners, technology service providers and financial institutions with a quick source of introductory training and basic information. The long-term goal of the InfoBase is to provide just-in-time training for new regulations and for other topics of specific concern.

2. **What, if any, regulations, policies, or programs do you presently have in place that address these objectives?**

   Please see the answer to question number 1 and the material attached.

3. **[CSIS] How can we assess/identify the level of security that markets will naturally provide? Can this be done by government alone, or must it be in conjunction with industry?**
   a. **If gaps are identified between the upper threshold of market-based security and the level of security required for national security needs, what are the advantages and disadvantages of the following tools to fill this gap?:**
      i. **Direct regulation**
      ii. **Indirect regulation**
      iii. **Policy and economic incentives**
   b. **Any approach must:**
      i. **balance and harmonize security requirements, need to encourage (or at least not constrain) innovation, economic competitiveness for U.S. businesses, U.S. leadership in the global marketplace, and privacy rights and civil liberties of our citizens;**
      ii. **be flexible and agile to respond to rapid changes in technology and the threat/vulnerability landscape**
      iii. **be appropriately tailored to achieve objectives (avoid overbreadth or under-inclusion)**

      Do existing regulatory processes or mechanisms effectively enable this type of balancing, flexibility, and tailoring?

Unlike many commercial sectors and industries, the U.S. financial services sector is subject to a long-standing comprehensive statutory framework of regulation. Even before the modern banking and securities statutes and regulations were adopted, the financial industry was subject to a standard of care in the handling of customers' funds, securities and confidential financial information. Thus, financial institutions have a long-standing culture that emphasizes internal controls and physical and cyber security. This culture has been reinforced by the regulators through multi-tiered regulatory regimes that begin with each agency's specific statutory authorities. Then, for example, within the banking sub-sector, guidance is established by the Federal Financial Institutions Examinations Council (FFIEC) and, where appropriate, explained, enhanced, or expanded, at the regulatory agency level. [Note: The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS), and to make recommendations to promote uniformity in the supervision of financial institutions. In 2006, the State Liaison Committee (SLC) was added to the Council as a voting member. The SLC includes representatives from the Conference of State Bank Supervisors (CSBS), the American Council of State Savings Supervisors (ACSSS), and the National Association of State Credit Union Supervisors (NASCUS).] Additionally, compliance with the guidance is monitored through a combination of targeted examinations and ongoing supervision programs. Finally, the financial services sector firms that are covered under the Basel II accord are required to hold capital against operations risk. Operations risks include risks posed by the security and resilience of the IT and Telecommunications operations of financial firms. By requiring firms to hold capital against these risks, the issues of cyber security are

raised to Board room level attention.[1] Similar approaches exist within the other components of the financial sector.

This culture has resulted in a private sector, characterized by a concern for security issues; an awareness of and attention to security vulnerabilities; and a willingness to cooperate with each other, with the regulators, and with the federal government. The culture is exemplified by the FBIIC-FSSCC Cyber Security Working Groups which are working together to strengthen the cyber security and resiliency of the sector's current and future IT operations. The joint working groups that are addressing key issues like information sharing, cyber exercise and planning, and international cyber vulnerabilities.

Following a situational analysis that focused on barriers to effective information sharing on a (1) business to business level, (2) a business to business partner level and (3) a business to / from the federal government level, there was strong consensus among the joint working groups that the federal mechanisms governing transparency in information sharing between the public and private sectors - as well as processes governing the sharing of available cyber security tools and methodologies - were not effectively enabling private sector security initiatives and activities. To provide further background on this topic, we have attached a report from the Joint FSSCC/FBIIC Cyber Security Intelligence and Information Sharing Work Groups titled: ROADMAP FOR IMPROVED INFORMATION SHARING.

4. **[CSIS] To what extent can agencies coordinate regulatory actions with one another and with NIST to develop common benchmark standards and guidance for securing critical infrastructure communications and information systems and networks that could be adopted (with appropriate tailoring?) by each agency?**

Regulatory agencies currently work successfully together to develop standards and guidelines for securing critical infrastructure primarily through the Federal Financial Institutions Examination Council (FFIEC), described in the response to Question 1. The Securities and Exchange Commission (SEC), while not an official member, makes extensive reference to these guidelines when performing information technology reviews of security markets and clearing organizations. As explained in the response to Question 3, the FFIEC issued the Information Technology (IT) Handbook (comprised of 12 booklets: Audit, Business Continuity Planning; Development and Acquisition; E-Banking; Fedline®; Information Security; Management; Operations; Outsourcing Technology Services; Retail Payment Systems; Supervision of Technology Service Providers; and Wholesale Payment Systems). The FFIEC regularly updates these booklets to reflect new laws, rules and practices. In addition to the booklets, these agencies point to other guidelines when appropriate, from respected organizations such as ISACA, NIST, US CERT and ISO when needed.

---

[1] The Basel II Framework is a product of the Basel Committee under the Bank for International Settlements. Most countries adhere to the Basel principles regarding risk management. "The Basel II Framework describes a more comprehensive measure and minimum standard for capital adequacy that national supervisory authorities are now working to implement through domestic rule-making and adoption procedures. It seeks to improve on the existing rules by aligning regulatory capital requirements more closely to the underlying risks that banks face. In addition, the Basel II Framework is intended to promote a more forward-looking approach to capital supervision, one that encourages banks to identify the risks they may face, today and in the future, and to develop or improve their ability to manage those risks. As a result, it is intended to be more flexible and better able to evolve with advances in markets and risk management practices." http://www.bis.org/publ/bcbsca.htm

a. NIST – would your authorities enable you to work with the independent regulatory agencies to develop such standards and regulators (for example, with respect to certification metrics and standards for Industrial Control Systems)?

a. We believe that this question should be directed to NIST.

b. For example, should penetration testing be institutionalized and/or occur more frequently?

i. Should NIST 800-53A Appendix G be adopted as a framework for such testing?

i. NIST 800-53A constitutes one of the best practices for penetration testing, but an organization should not rely on it alone; rather, an organization should evaluate best practices from as many sources as possible and adopt those best suited to their particular needs.

Prevailing industry best practices include: the Information Systems Audit and Control Association's ("ISACA") Information Security Auditing Procedures; the FFIEC IT Examination Handbook; National Institute of Standards and Technology ("NIST") publications; NSA Guide to Hardening Windows, Unix, Routers and Switches, Wireless Architecture; the Software Engineering Institute CERT Coordination Center ("CERT") publications; SANS (SysAdmin, Audit, Network, Security) Institute best practices; Cisco and Microsoft best practices; the Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial Systems ("White Paper") (April 2003); the S.E.C. Policy Statement on Business Continuity Planning for Trading Markets (September 2003).

ii. What steps or conditions would be necessary to achieve consensus among the members of your respective sectors in support of a common "red-teaming" framework for system testing?

ii. During our inspections and examinations, the lead examiner requests that regulated financial institutions provide evidence of internal and external penetration testing and ensure they address identified gaps. While having a common approach could be helpful, each regulator will need to modify that approach to meet the unique needs of the organizations that it regulates.

iii. Assuming such a consensus could be developed, do standards or industry best practices establish timelines for mitigation or remediation of security vulnerabilities revealed by testing?

iii. During inspections and examinations, we currently request that regulated financial organizations identify remedial action to address any deficiencies or gaps in coverage, including penetration testing. In some cases, an organization would need to upgrade servers, network equipment or software to address a deficiency, which may take several budget cycles. We would expect financial institutions subject to our regulation to take remedial action on a timeline commensurate with

the gravity of the security issue -- that is, we would expect them to address significant problems immediately.

5. Each of your agencies maintains a "public private partnership" relationship of some kind with your regulated entities. How would you characterize the effectiveness of these collaboration frameworks (vice direct regulation) to achieve concrete improvements in the cyber security posture of the sector and auditable accountability on the part of individual companies?

The Banking and Finance sector has a robust public-private partnership. This partnership consists of the Financial and Banking Information Infrastructure Committee (FBIIC) on the public side and the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) and the Financial Services-Information Sharing and Analysis Center (FS-ISAC) on the private sector side. The FBIIC consists of 18 federal and state financial services sector regulators (see http://www.fbiic.gov/about/contacts.htm for members and a point of contact for each member). The FSSCC "is a group of more than 30 private-sector firms and financial trade associations that works to help reinforce the financial services sector's resilience against terrorist attacks and other threats to the nation's financial infrastructure."(see https://www.fsscc.org/fsscc/). The FS-ISAC "disseminates physical and cyber threat alerts and other critical information" to member organizations within the financial services sector. (see www.fsisac.com/about/). We have also attached a brief description of these organizations from the Banking and Finance Sector Specific Plan.

There have been several recent examples of where these organizations have assisted in increasing the cyber security posture of the banking and finance sector. The first situation involved a two wave distributed denial of service (DDoS) attack. As a result of the existing partnership and existing authorities, the federal government was able to quickly provide technical assistance to the organization involved to mitigate the possibility of additional DDoS attacks using the same vector. The parties are developing after action reports identifying lessons learned that can be shared with other organizations in the sector to increase the sector's security posture.

Cyber security has been increased within the sector as a result of increased distribution of cyber threat information between the public and private sectors. A second recent situation may be illustrative: Another organization became the target of a rather unique spear phishing attack. Information regarding this particular attack was created by several public sector organizations along with many private sector organizations. Upon the Treasury's receipt of the information, it was quickly distributed to the organization's primary federal regulator, who met with the entity to determine what resources could be brought to bear to assist the organization. In addition, the information was also shared with the private sector via distribution through the FS-ISAC. As a result of this sharing, the damage done by the attack was lessened.

Finally, we have also coordinated with other agencies such as DHS to obtain national security clearances for select individuals employed at certain financial organizations. These individuals hold senior positions in information security, business continuity/disaster recovery, or physical security within these organizations. The goal is to be able to share national security classified information with these individuals so as to be able to obtain feedback regarding potential threats to their institutions specifically and the financial sector generally.

6. **Electric Power, Communications (with IT) and Banking and Finance represent among the most critical of our nation's critical infrastructure sectors – To what extent do you communicate and coordinate among one another to ensure effective situational awareness and incident response?**

Starting in 2003, the FBIIC has hosted a series of series of meetings with the Electric Power, Communications (with IT), and Transportation Sectors to identify key interdependencies between the sectors. As a result of these meetings, a robust information sharing mechanism currently exists.

This sharing mechanism has been exercised several times over the last 5 years. For example, during the Northeast Power Blackout in August, 2003, the Treasury was able to quickly contact the Department of Energy to obtain information regarding the projected duration of the event and potential impacts the event might have on the sector. As a direct outcome of this event, the Treasury has partnered directly with the Department of Energy's Visualization Modeling Working Group to obtain estimated outage and impact information prior to landfall of Category 3 and above hurricanes. This information is shared with the members of the FBIIC so that they can position their field office personnel to deliver maximum assistance to persons and organizations impacted by the storm. Though our efforts, this information is made directly available to the financial sector through the FSSCC and FS-ISAC.

The financial sector is greatly dependent on the availability of telecommunications. In recognition of this critical dependency, the Federal Reserve Board (FRB) leads the FBIIC's efforts in developing a close working relationship with the Department of Homeland Security's National Communications System (NCS) and the private sector telecommunications industry representatives assigned to the NCS. A senior FRB employee is detailed to the NCS to provide subject matter expertise to the NCS regarding the needs of the financial services sector. This relationship has proven itself valuable many times. For example, in the aftermath of Hurricane Katrina, over 350 telecommunications circuits critical to the financial institutions in the impacted areas were rapidly restored on a priority basis by employing the Telecommunications Service Priority (TSP) program. In anticipation of the 2008 hurricane season, over 275 financial institutions in the Gulf States and along the Eastern Seaboard were issued Government Emergency Telecommunications Service (GETS) cards. During the Gustav, Hanna and Ike Hurricanes in 2008, over 2,000 GETS calls were placed with a 99% completion rate. The relationship paid off most recently during the January 2009 Kentucky ice storms. When telecommunications services were knocked out to an important financial services data center in the impacted region, the issue was quickly raised to the NCS via the FRB detailee and additional resources were added to the restoration efforts to minimize the disruption.

For Financial Regulators (FRB, OCC, SEC, CFTC):

1. **What are the major trends in attacks that you are seeing in your sector and what measures are being taken (voluntary or pursuant to mandates) to mitigate these threats?**

Information regarding particular attack trends is collected and distributed by the US-CERT and law enforcement organizations, along with several private sector organizations. The financial regulators do not gather or have the expertise to analyze what the criminal cyber underground may be working

on to attack financial institutions. An inquiry to US-CERT may provide information which is much more useful in the creation of your report. Posing this question in that direction may assist your efforts.

2. Are there available security measures that are not being used as much as they should be (e.g. multifactor authentication)?

We have found that the financial institutions subject to our regulation are aware of the need for adequate information security and adhere to the concept of "defense-in-depth" through building multiple layers of access controls to their systems and data. These strategies, however, are limited by the lack of available actionable information regarding threats to their systems.

3. Do existing auditing [inspection and examination] methodologies require updating?

Among those regulators who conduct audits, regulatory efforts under the topic of "auditing methodologies" cover a wide range: from guidance imposed on the industry to the processes used by the regulators in supervising the activities used by the internal and external auditors of financial institutions. Although agency terminology may differ, the approaches used are similar. For example, the FFIEC "Audit" booklet - one of 12 booklets that comprise the Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook (IT Handbook) - provides guidance to examiners, technology service providers, and financial institutions on the characteristics of an effective information technology (IT) audit function. It provides examiners a basis against which they can assess the quality and effectiveness of an institution's IT audit program. It describes the roles and responsibilities of the board of directors, management, and internal or external auditors; identifies effective practices for IT audit programs; and details examination objectives and procedures. In addition, each of the other subject-specific booklets contains an Appendix with the examination program for that subject area. The booklets not only explain the risks regulators expect institutions to address, but also provide an outline of the exam program that will be applied during an examination. The on-site examination team adapts the process based on their assessment of the institution's risk in the area under examination. All of the examination guidance is reviewed periodically and updated as required. Examination teams review both internal and external audit work-papers and reports during examinations and evaluate their effectiveness and completeness.

4. What are the obstacles to improving Suspicious Activity Reports?

That topic is one that is not narrowly focused within cyber security issues. As such, we suggest that you question the Treasury's Financial Crimes Enforcement Network.

5. Are additional measures required to improve protection of proprietary information?

We believe that the authorities that the financials regulators have for the protection of proprietary information entrusted to the regulator during an examination procedure are adequate. If, however, this question pertains to other programs, such as the Department of Homeland Security's Protected Critical Infrastructure Information (PCII) Program, we would suggest this question be directed to organizations in the private sector.

6. How prevalent is wire transfer via account takeover online?

We believe that the US-CERT and law enforcement organizations may be in the best position to answer this question.

7. Why have AICPA not updated the Statement on Auditing Standards (SAS) No. 70, *Service Organizations* in recent years?

As the American Institute of Certified Public Accountants is a private sector organization, we suggest that the AICPA is in the best position to answer this question.

8. For SEC: [CSIS] Is Y2K a valid model for cybersecurity regulation; where public-private partnership activities are reinforced by reporting requirements on publicly-traded companies to disclose security steps taken (*e.g.*, to ensure COOP, safeguard customer data., etc.)?

The President's Council on the Year 2000 Question (Y2K) model has validity for multiple applications in area of cyber security, however limitations do exist. On the one hand, the Y2K model did encourage transparency of an organization's efforts, by requiring firms to provide summary-level 10K status reporting. The federal and state financial sector regulators formed tighter communication networks to share information related to Y2K issues. The Year 2000 Disclosure Act (attached) raised the issue to corporate board level concern by imposing potential liability on board members. On the other hand, there has been discussion that the threat posed by Y2K may not have been as large as initially predicted (several countries that did not mount large scale remediation efforts did not have negative impacts). In addition, Y2K did have an end-certain date with a specific end state, whereas our current efforts related to cyber security do not have such bright line goals. While we believe that the Y2K model was sufficient to address a particular risk, such a model may not result in the same outcome against the much more sophisticated threats posed by today's cyber actors.