William B. Nelson
President & CEO
FS-ISAC
20496 Partridge Place
Leesburg, VA 20175

703-777-2803 (Direct)
509-278-2412 (Fax)
bnelson@fsisac.us www.fsisac.com

April 10, 2009

Ms. Melissa Hathaway
Acting Senior Director for Cyberspace
National Security and Homeland Security Councils

Dear Ms. Hathaway:

On behalf of the Financial Services Information Sharing and Analysis Center (FS-ISAC), I want to thank you for this opportunity to provide input to the interagency cyber security review and the development of a strategic framework to ensure that U.S. Government cyber security initiatives are appropriately integrated, resourced, and coordinated with Congress and the private sector.

Provided below are comments offered by the FS-ISAC Threat Intelligence Committee addressing the four subjects you requested concerning various cyber security issues of potential national security significance.

By way of background, the FS-ISAC is a nonprofit private sector organization designed, developed and owned by the financial services sector. Its mission is to enhance the ability of the financial services sector to prepare for and respond to cyber and physical threats, vulnerabilities and incidents, and to serve as the primary communications channel for the sector. The FS-ISAC stood up operations in 1999 and has grown from 68 members at the beginning of 2004 to over 4,000 members today.

The FS-ISAC Threat Intelligence Committee (TIC) is comprised of several dozen volunteer information security professionals from small and large financial services firms. They are assisted in this effort by full-time information security staff from the FS-ISAC's Security Operations Center. In their role on the TIC, the Committee members and SOC staff are responsible for protecting critical infrastructure within the financial services sector. TIC members take this responsibility very seriously and welcome this opportunity to submit these comments on the subjects you have outlined.

Question 1: "What is (should be) the government's role in securing/protecting the critical infrastructures and private sector networks from attack/damage (e.g., from nation states?)"

In the situation where cyber attacks are suspected or confirmed as being of terrorist, state sponsored, or nation state origin, we suggest that government's role should be to:

- Work with the Telecommunications industry and NSTAC to implement a capability to block attacks at the national ISP level at the US network boundaries when requested to by an authorized representative of the sector.

- Engage in diplomatic, law enforcement, military, or other appropriate means to deter, prevent, and mitigate the attack.

- Provide incident response support to the Financial Sector through such means as forensic analysis and system recovery assistance to ensure the continued availability of the infrastructure.

- Provide appropriate detective and preventative threat signatures to allow the Financial Sector to detect and mitigate any attacks using internal security controls.

- Share appropriate classified contextual intelligence with cleared Financial Sector crisis management and threat intelligence groups to allow provision of sector impact assessments and response coordination.

- Clarify roles and responsibilities for authorities such as: NSA, DHS, USCERT, etc., to support the Financial Sector in response to incidents with minimal bureaucratic overhead. This might be implemented through the FBI or US Secret Service and then having other government agencies, including the intelligence community, engaged with the firm under the law enforcement agency's auspices.

- Establish a system for the management of Protected Critical Infrastructure Information (PCII). This system should provide the capability to track the process of classifying, submitting, and accounting for PCII by the private sector in a timely manner.

- Provide clarity as to what the US government's response would be to network attacks carried out overseas that have major domestic implications for the Financial Sector. For example:

    - An overseas attack against a major international payments system overseas that is critically relied on for day to day transactions.

    - An overseas attack against a telecom or IT infrastructure overseas, such as the undersea cable infrastructure in the Middle East.

    - An attack against a US firm's overseas operations that impacts its domestic operations. Ultimately, the effects of any one of these types

of attacks could be as significant as a direct cyber attack against US interests.

Question 2: "Based on what you know, what are the key intersections between the Economic Stimulus Package and cyber security activities within the sectors (e.g., Smart Grid)?"

- "Smart Grid" and "Rural Broadband" may exacerbate domestic security concerns by increasing the number of potential points for attack. Without appropriate downstream security of this domestic user base, the possibility increases significantly for these consumer systems to be compromised and employed in botnets and other automated attack activities.

- Ensuring that Internet Service Providers have established programs and are funded to implement BCP 38/RFC 2827 ingress filtering, DNS hardening, and infrastructure attack mitigation, and other measures to ensure the broader attack surface being exposed by these programs is not used against the US and Allied Critical Infrastructure/Key Resources (CI/KR.)

Question 3: Much of the success of the current Internet architecture has stemmed from the fact that it ensures there is a unique, authoritative root. How would the security and stability of the Internet be affected if the single, authoritative root were to be replaced by a multiple root structure? What would be the economic and technical consequences of a multiple root structure? What, if any, influences do you see that may (a) move the Internet in the direction of greater fragmentation; or (b) help to preserve and maintain a single, interoperable Internet? What are the implications of these forces?

For a variety of reasons, the potential for fragmenting the Internet environment is significant.

- Dissolution/dissatisfaction with ICANN and the subsequent move to other management organizations.

- Implementation of IPv6 and future protocols on a national level supporting a technological barrier for IP and Domain Name management. China and the national mandate of implementation of IPv6 is an example of this potential technological fragmentation.

- Issues and challenges facing the Financial Sector include the following:

    - Because many of the financial sector firms are global in nature, nationalistic name and technological fragmentation would make network management significantly more complex.

- Clear identification of organizations by URLs would become significantly more difficult, thereby increasing the already soaring phishing threat.

- Organizations would be forced to incur the expense of registering their trademarks and service marks as URLs in each of the national top-level domains or run the risk of losing this protection.

- There is also a high likelihood of "cyber-squatting" regarding these domains with the associated costs of purchasing the rights to the URLs in question.

- Firms will face increased costs to combat phishing and related services.

- This question also poses the opportunity for the Government to ask the following questions of CI/KR organizations:

  - How many firms have registered IPv6 spaces in preparation to IPv6?

  - How many firms have registered Autonomous System Numbers to serve as distinct peering points for IPv6?

Question 4: "Do you have or do you recommend thresholds for reporting cyber incidents for the government, private sector, quasi private sector?"

- The Financial Sector is already heavily regulated with respect to cyber security and incident reporting. For example, financial institutions must submit Suspicious Activity Reports in cases of intrusion into financial institution customer information systems. This reporting is well understood and implemented within the sector.

- For significant incidents, depending on a financial institution's regulatory circumstances, it may already be required to report the circumstances of the incident and subsequent actions to their federal regulator. We do not propose changing this requirement for the sector.

- In terms of less significant incidents within the financial services sector, the FS-ISAC assists its member firms in submitting incidents to the Government through the use of an incident submission template. This allows a firm to explicitly select sharing of the information with public and/or private organizations including Treasury, DHS, and other ISACs. We should also consider leveraging other global resources (e.g., the UK's Center for the Protection of National Infrastructure, or "CPNI").

- The Financial Sector currently has no visibility into the cyber security status of those sectors on which it is dependent, such as the Telecommunications,

Energy, and IT Sectors. Providing a common view (a.k.a. Common Operating Picture) of these CI/KR areas would benefit all.

- In addition to a Common Operating Picture, we would benefit from a common incident reporting framework. In this way we could share attack data for correlation and analysis between sectors and possibly with other government/DoD sources. We, therefore, recommend that existing ISAC capabilities be leveraged to create a more effective mechanism to share or report cyber incidents between CI/KR sectors and the government. It is important, too, that the private sector be involved in the analysis of incidents to ensure results are accurate, correctly interpreted, appropriately risk rated, and properly managed.

Thank you again for the opportunity to provide these comments. Please do not hesitate to contact me if there are any further questions. I would be happy to coordinate putting your team in contact with the members of our Threat Intelligence Committee who are more than willing to assist in this important endeavor.

Sincerely,

William B. Nelson
President and CEO
Financial Services Information Sharing & Analysis Center

cc: Shawn Johnson, Chair, Financial Services Sector Coordinating Council, State Street Global Advisors

Brian Perretti, Program Manager, Financial Services Sector Agency Representative, U.S. Department of the Treasury, Office of Critical Infrastructure Protection

Guy Copeland & Stuart Brindley, Co-Chairs, Partnership for Critical Infrastructure and Security, Cross-Sector Cyber Security Working Group