FSSCC/FBIIC Cyber Security Intelligence and Information Sharing Work Groups
ROADMAP FOR IMPROVED INFORMATION SHARING
Situational Analysis and Recommendations for Action

Background: ***This Roadmap for Improved Information Sharing was developed by the Joint FSSCC/FBIIC Cyber Security Intelligence and Information Sharing Work Groups from June 2008 through October 2008, finalized in November 2008 and approved for implementation by the FSSCC/FBIIC Cyber Security Steering Committee in December 2008. Implementation activities are currently underway.***

I. SITUATIONAL ANALYSIS

A. PROBLEM STATES

1. Business to Business Information Sharing
2. Business to Business Partner Information Sharing
3. Business to / from Government Information Sharing

Threat information, best practices and solutions (intellectual property) within each area listed above would be derived from the following sources:

- Classified or Non-Classified (either by Government Scheme or Private Sector Scheme)
- Cross-sector (inter-sector) or intra-sector
- Domestic or international

B. BARRIERS TO EFFECTIVE INFORMATION SHARING

Business to Business / Business to Business Partner

- The method for marking documents for the purpose of distribution needs to be clearer so recipients fully understand their responsibilities and restrictions regarding disclosure.
  - The lack of a Private Sector marking and labeling scheme
  - The lack of agreements on how shared information may be distributed with private sector organizations.
- There needs to be better ways to stimulate dialogue on information sharing conference calls.
- There needs to be more effective mechanisms for members to share information via email and to provide their own comments in response to member submissions.
- Solutions must address the issues of anonymity, confidentiality and control of proprietary information; and provide for the establishment of required metrics.

Business to/from Government

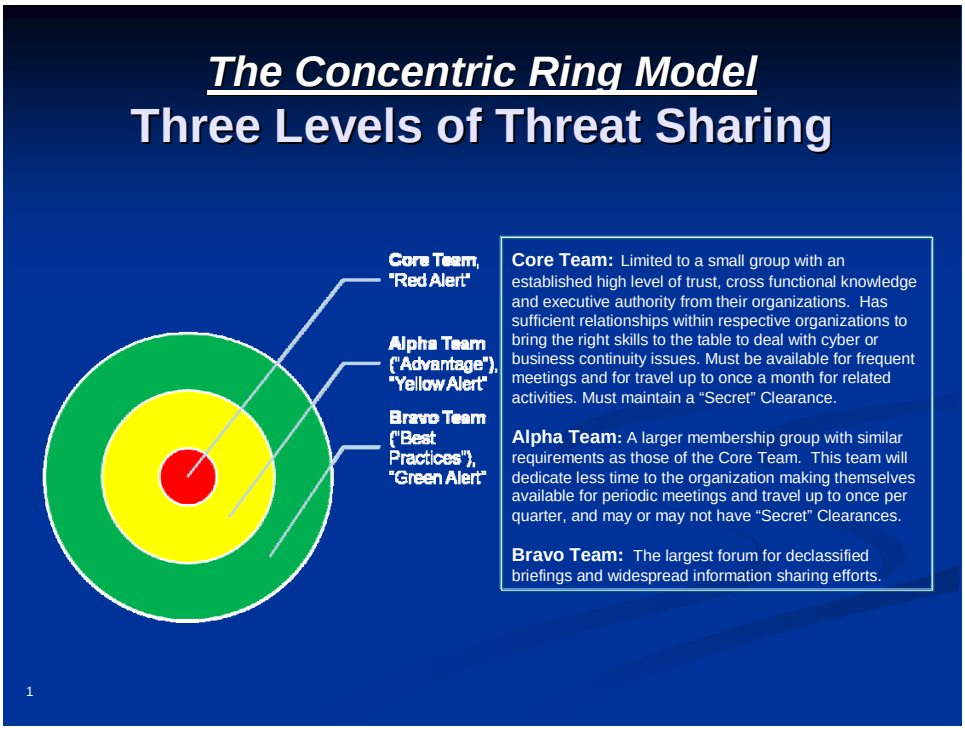
- The quality of information received from some government sources is viewed as pedestrian.
- The private sector needs to more effectively demonstrate the sharing of information among each other before asking the government to modify its processes.
- Available Facilities (SCIFs, STUs, and STEs) for sharing classified information.
- Sharing information with non-cleared executives within the private sector
- Sharing classified/unclassified information with staff based outside of US within the private sector.
- Solutions must address potential FOIA issues.

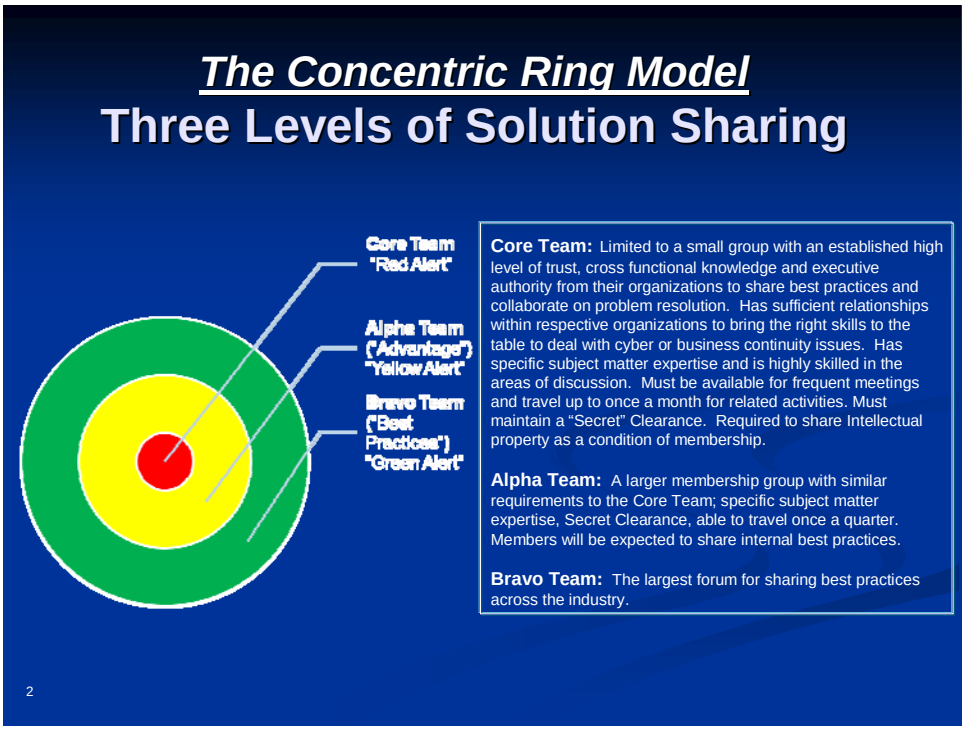
II. RECOMMENDATIONS FOR ACTION (ST= Short-term Action, MT= Mid-term, LT= Longer-Term)

Short-term activities require some effort but are implementable within a one-year timeframe.
Mid-term tasks require more effort and may require a one to two-year timeframe for full implementation.
Long-term tasks are expected to require significantly more effort and coordination, and more than two years for implementation.

1. That FS-ISAC (for the private sector) and FBIIC (for the public sector) adopt the concentric ring model for sharing cyber security threat and vulnerability information and solutions; and that the model be used for Business to Business, Business to Business Partner, and Business to/from Government interactions. Further, the Working Groups suggest that FSSCC, FS-ISAC and FBIIC consider the same model for sharing physical security and business continuity threat and vulnerability information.

The following examples show how the Concentric Ring Model can be used for Cyber Threat Sharing and for Cyber Solution Sharing. FS-ISAC and FBIIC should determine whether separate 3-level team structures are required for threat vs. solution sharing, or whether a single 3-level team structure is appropriate. It is the position of the Work Group that separate teams are needed.





For whichever approach (separate 3-level team structures or single 3-level team structure) is used,

a. (ST) That for the FS-ISAC: the CORE TEAM be comprised of the Threat Intelligence Committee; the ALPHA TEAM be comprised of all members at or above the Standard membership level, as well as the participants on the Threat/Intelligence listserv; and the BRAVO TEAM be comprised of all other FS-ISAC members and all FSSCC members.

b. (ST) That for the FBIIC: the CORE TEAM be comprised of the members of the Cyber Security Working Group; the ALPHA TEAM be comprised of the US Treasury, the CFTC, the FDIC, the FRB, the NCUA, the OCC, the OTS and the SEC; and the BRAVO TEAM be comprised of all other FBIIC members.

c. (ST) That to ensure the sustainability and continuity of the teams, the agreed-upon team structure be endorsed by the FSSCC and formally incorporated into the governance models of the FS-ISAC and FBIIC.

d. (MT) That for SOLUTION-SHARING, the FS-ISAC and FBIIC recognize the potential need for ad hoc Core Teams to address solutions requiring extensive research and development.

e. (ST) That the standing FS-ISAC and FBIIC Core Teams (and ad hoc Core Teams, where appropriate) establish an ongoing joint working relationship to ensure that their efforts for the financial sector are optimized.

> (i) (LT) Form trusted active, day-to-day operational partnerships among security operations centers (SOC) of relevant agencies, the FS-ISAC SOC and member firm SOC to allow real-time collaboration and discussion of threats, vulnerabilities and incidents.

(ii) (LT) Develop a project plan to implement activities identified in the Final Report and Recommendations of the NIAC Public-Private Sector Intelligence Coordination Working Group, specifically,

Recommendation 3: Existing Mechanisms
Leverage existing information-sharing mechanisms as clearinghouses for information to and from critical infrastructure owners and operators. This takes advantage of the realities that exist sector by sector.
Recommendation 4: National-Level Fusion Capability
Establish or modify existing government entities to enable national- and state-level intelligence and information fusion capability focused on Critical Infrastructure Protection (CIP).
Recommendation 7: RFI Process
Develop a formal, and objectively manageable, homeland security intelligence and information requirements process, including requests for information (RFIs). This should include specific, bi-directional processes tailored sector by sector.
Recommendation 8: Standardize SBU Markings and Restrictions
The Federal government should rationalize and standardize the use of SBU markings, especially "For Official Use Only" (FOUO), and publish standard handling instructions clearly for all intended recipients.

f. That, to the extent possible, individuals selected for the FS-ISAC and FBIIC Core Teams provide a cross-disciplinary perspective; and that they be empowered as organizational points of contact with as-required access to subject matter experts and decision-makers.

(i) that the FBIIC and FSSCC define the process to identify and designate those individuals in the Core Teams.

g. That the FS-ISAC and FBIIC Core Team members, in addition to the inherent duties of the models, function as two-way communication channels facilitating the flow of information to and from organizational members.

2. That the following actions be taken to support the implementation of the concentric ring model:

a. FS-ISAC (ST) – Coordinate and establish Information Classification policies. These policies should be vetted with FSSCC and FS-ISAC Members and Partners.. Establish a process for marking documents and provide guidance to members to ensure that members understand handling requirements and the restrictions on disclosure applicable to the classification.

(i) Implementation should address identified concerns regarding anonymity, confidentiality and control of proprietary information; and provide for the establishment of required metrics.

(ii) Implementation should provide a more effective mechanism for members to share information via email and to provide their own comments in response to member submissions

(iii) As part of the implementation, initiate a project to facilitate identification and definition of the specific types of information that all members commit to share (i.e., provide to the Common Operating Picture);

b. FS-ISAC (ST) – Identify and document industry Points of Contact (POC) for information sharing initiated by the government with sector member firms;

(i) FBIIC (ST) Obtain agreement from appropriate government organizations to utilize the identified POC to ensure appropriate corporate management chains are followed. This agreement is not intended to replace or interfere with contacts that have been or will be established for regulatory purposes.

3. That the following actions be taken to enhance information sharing within the financial sector:

a. FSSCC / FBIIC Cyber Security Intelligence and Information Sharing Working Groups (MT) – **Communications** – Develop a single communications strategy to provide CEOs and other Senior Executives with an understanding of the importance and usefulness (i.e. the value proposition) of a common operating picture for the financial sector, including annual threat briefings to further high level understanding and support for requirements to mitigate threats to the sector.

b. FSSCC / FBIIC Cyber Security Intelligence and Information Sharing Working Groups (MT) – **Education and Awareness** – Develop an education / awareness plan to ensure that recipients can effectively use distributed threat information. Explore leveraging programs like those offered by the Interagency OPSEC Support Staff (IOSS) which was created to support the National OPSEC Program by providing tailored training, assisting in program development, producing multimedia products and presenting conferences for the defense, security, intelligence, research and development, acquisition and public safety communities.

c. FS-ISAC (ST) – **Governance** – Establish Operating Rules and **Memoranda of Understanding** and/or Non-Disclosure Agreements (where appropriate) governing how shared information may be distributed with private sector organizations.

d. FSSCC / FS-ISAC (ST) – **Regional Coalitions** – Implement a communications program to encourage firms to engage with local, state and federal agencies in formal and informal information sharing initiatives through Regional Coalitions and other geographically focused programs.

e. FSSCC / FBIIC Cyber Security Intelligence and Information Sharing Working Groups (MT) – **Facilities** – Develop a plan for making facilities available to the private sector for the sharing of government classified information. Consider the use of existing intelligence and law enforcement facilities (e.g. DHS, the FBI and the USSS) and fusion centers as well as the creation of private sector owned and operated facilities. For private sector communications, consider establishing an out of band secure communication channel that includes multi factor authentication and message encryption with members being required to pass periodic security background checks.

f. FSSCC – **FOIA and related issues** – Work with appropriate member legal departments to identify perceived FOIA and PCII issues related to information sharing and review findings with the FSSCC / FBIIC Cyber Security Intelligence and Information Sharing Working Groups.

(i) Leverage the work done by the NSTAC in its recommendation to the President on this subject.

4. That the following actions be taken to improve the utility and effectiveness of the FS-ISAC:

a. FS-ISAC (ST) – Stimulate greater dialog on scheduled bi-weekly and ad hoc calls.

b. FS-ISAC (ST) – Market the listserv capability of the FS-ISAC to the membership.

c. FS-ISAC (ST) – Implement a Request for Information (RFI) capability for relevant member submissions and alerts concerning new threats, incidents and vulnerabilities.

d. FS-ISAC (MT) –Evaluate the cost/benefit of providing members mobile-based information sharing capabilities which utilize, for example, SMS / IM, feeds and other new technologies like Jabber servers.

e. FS-ISAC (MT-LT) – Improve steady-state information sharing with other key ISACs, including IT communication and electricity, establishing SLAs where appropriate. Potential improvement opportunities for consideration by the FS-ISAC are included in the Appendix.

f. FSSCC (MT-LT) – Improve information sharing with other key sectors, including the telecommunications, IT, energy, and transportation sectors to ensure availability of critical information to the FS-ISAC on a timely basis.

(i) FS-ISAC – Identify specific areas / situations in which FSSCC can provide assistance.

g. FS-ISAC (MT) – Work with the DHS National Cyber Security Division (NCSD) to arrange for access to its list of ISPs and then provide members the ability to query that list by service.

(i) As a follow-on effort, request access to a list of hosting providers, registrars, and providers of anonymous access services that have been known to provide safe haven and services to cyber criminals; and couple the request with an offer to help the NCSD build such a list if it is not available.

h. FS-ISAC Core Team (Ongoing) – Identify and document improvements needed to the information sharing products of US CERT, HITRAC, the FBI and the USSS; then meet with those organizations to discuss specific recommendations.

(i) Review the effectiveness of the current distribution mechanisms for confirmed threat information, as well as the ability to deliver threat information to a broader audience of private sector security partners.

(ii) Work with the intelligence and law enforcement communities (e.g. DNI, DHS, the FBI and the USSS) to ensure their understanding that non-US financial sector executives with appropriate host country clearances need to be included in the distribution of threat information.

(iii) Work with the intelligence and law enforcement communities (e.g. DNI, DHS, the FBI and the USSS) to ensure their understanding that the financial services sector needs to be included in the distribution of threat information related to those sectors on which the sector has a critical reliance, especially the telecommunications, IT, energy, and transportation sectors.

(iv)Work with the intelligence and law enforcement communities (e.g. DNI, DHS, the FBI, and the USSS) to ensure their awareness of critical terminology / keywords they should consider when evaluating threat information for potential impact on the financial sector.

5. FSSCC / FBIIC Cyber Security Intelligence and Information Sharing Working Groups (ST):

a. That a Program Oversight and Evaluation Team (POET) be established to monitor the implementation and progress of these recommendations; and that the POET consist of the co-chairs, the team leaders and others as required.

Appendix – Potential Information Sharing Improvement Opportunities Associated with Recommendation 4.e

1- Work with the IT ISAC and the Communications ISAC to establish steady state communications to improve levels of trust and information sharing during a crisis.

2- Work with the IT-ISAC to facilitate greater interaction of the FS and IT ISAC memberships around cyber security trends, specific threats and vulnerabilities, and development of mitigation strategies.

3- Work with the Communication ISAC and / or the telecommunications carriers to obtain meaningful information on physical and logical circuit routing information; concentration points; outages and meaningful and relevant information on restoration of services from disasters.

4- Work with the Communications ISAC and the NCS to determine how best to proactively influence carrier design of the next generation of network services, including prioritization of IP packets and Service Oriented Networks.

5- Work with the Communications ISAC and the NCS on how best to ensure that ISPs are required to install software patches for significant vulnerabilities (such as the recent Kaminsky DNS server cache poisoning vulnerability).

6- Work with the Communications ISAC and NCS on how best to encourage industry collaboration and cooperation, and adherence to best practices to improve availability and enhance resiliency. For example, should carriers be incented or legislated to pressure downstream ISPs to deploy basic anti-fraud mechanisms such as IP address spoofing controls? Or should ISPs be mandated to respond, investigate, and enforce reported violations by malicious users or cyber criminals for whom they are providing network services? Or should Hosting providers be required to deploy timely security patches to content management system frameworks and web servers that are being used to host phishing sites or are serving as malware distribution points?

7- Work with the communications ISAC and NCS on the provisioning of cyber security related services from carriers to the financial sector. For example, access to real time IP address feeds for known malicious sites and nodes so that we can determine if we have communication occurring to these destinations; having carriers provide data showing known and rogue internet proxies; and having carriers provide an IP reputation lookup service that includes quantitative scoring based on the risk of a particular IP address - covering behavior seen from this address as well as traffic going to other malicious sites from the address in question.