Commercial/Civil Cyber Community Snapshot[1]

PUBLIC/PRIVATE PARTNERSHIPS

CSCSWG

Description: Established to improve cybersecurity protection efforts across the Nation's CIKR sectors; highlights cyber dependencies and interdependencies; and shares government and private sector cybersecurity products and findings.

Policy/Strategy: Identifies opportunities to improve sector coordination around cybersecurity issues and topics.

System Protection: Engages in cybersecurity protection efforts that span all 18 CIKR sectors.

Collection/Analysis: Identifies cross-sector cyber dependencies and interdependencies to address shared risks among the sectors.

Education/Training: Receives regular presentations and briefings to keep informed of the latest developments in cybersecurity trends. Utilizes the group's contributions to enhance personal and professional cybersecurity practices.

Collaboration: Establishes and maintains cross-sector cybersecurity partnerships and aims to improve information sharing mechanisms.

InfraGard (led by FBI)

Description: Information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. Its goal is to promote ongoing dialogue and timely communication between members and the FBI. InfraGard members gain access to information that enables them to protect their assets and in turn give information to government that facilitates its responsibilities to prevent and address terrorism and other crimes.

Dissemination/Awareness: Provides members value-added threat advisories, alerts, and warnings.

Collaboration: Increases the level of information and reporting between InfraGard members and the FBI on matters related to counterterrorism, cyber crime and other major crime programs; Also works with local, state and federal agencies and departments, including DHS, NIST, and the Small Business Administration.

Education/Training: Provides members a forum for education and training on counterterrorism, counterintelligence cyber crime and other matters relevant to informed reporting of potential crimes and attacks on the nation and U.S. interests.

OSAC (led by DoD)

Description: Federal Advisory Committee with a USG Charter to promote security cooperation between American business and private sector interests worldwide and the Department of State (DOS).

Policy/Strategy: OSAC has outlined the private sector position on such issues as the protection of proprietary information, and technology and encryption needs overseas.

Monitor: The Research and Information Support Center (RISC) within OASC tracks social, political, and economic issues that impact the security of the private sector operating overseas, and gauges threats to U.S. private sector investment, personnel, facilities, and intellectual property abroad.

Collection/Analysis: The RISC staff conducts research to provide time-sensitive unclassified analytical products and updates.

Education/Training: Recommends methods and provides material for coordinating security planning and implementation of security programs to protect the competitiveness of American businesses operating worldwide.

Collaboration: Provides for regular and timely exchange of information between the private sector and DOS concerning developments in the overseas security environment; Member organizations also include USAID, DOC, and Treasury.

DSAC (led by FBI)

Description: Strategic partnership between the FBI and the U.S. private commercial sector, enhances communications and promotes the exchange of information. The DSAC advances the FBI mission in preventing, detecting, and investigating criminal acts, particularly those affecting interstate commerce, while also advancing the ability of the U.S. private sector to protect its employees, assets, and proprietary information.

Collaboration: Facilitates the exchange of information by and among its corporate members and the FBI.

CERT/CC

Description: Charged by DARPA to coordinate communication among experts during security emergencies, respond to major security incidents, and analyze product vulnerabilities; Develops and promotes use of appropriate technology and systems management practices

Policy/Strategy: Helps organizations, including the federal government, to improve cybersecurity strategies and posture.

System Protection: Conducts reserach in survivable systems engineering and includes analyzing how susceptible systems are to sophisticated attacks and finding ways to improve the design of systems.

Incident Warning/Response: Develops tools to enable network admins to become effective first responders to network security incidents. CERT/CC helps US-CERT respond to the effects of cyber attacks across the Internet.

Monitor: Monitors public sources of vulnerability information and regularly receives reports of vulnerabilities.

Collection/Analysis: CERT collects information through multiple channels to help organizations improve network security; Conducts in-depth network security and vulnerability analyses; Developing techniques that will enable the assessment and prediction of current and potential threats to the Internet.

Academic Research: Affiliation with a major university enables close collaboration with academia on network security issues.

R&D: CERT/CC is now part of the larger CERT Program, which develops and promotes the use of appropriate technology.

Education/Training: Offers public training courses for technical staff and managers of computer security incident response teams and other technical personnel interested in learning more about network security.

Collaboration: FFRDC; Participates with US-CERT, FIRST, IETF, and the NSTAC NSIE; Has also provided assistance to the National Threat Assessment Center, National Security Council, Homeland Security Council, OMB, and GSA.

Dissemination/Awareness: Disseminates information through multiple channels, including by publishing articles, research and technical reports, and papers. Staff give presentations at conferences and advises legislative and executive entities. The public can also access the USENET newsgroup.

IT-SCC

Description: Brings together companies, associations, and other key IT sector participants to coordinate strategic activities and communicate broad sector member views associated with infrastructure protection, response and recovery that are broadly relevant to the IT Sector

Policy/Strategy: Identifies IT CIP policy topics; Focal point for CIP policy strategy collaboration within the IT sector; Develop sector recommendations for incident response and recovery; Responsible for IT-SSP.

Collaboration: Partners with the GCC led by DHS; Seeks to improve information sharing between IT sector, Government entities, other sector members. Serves as base for IT sector representation to the Partnership for Critical Infrastructure Security.

R&D: The IT SCC and IT GCC will facilitate awareness and coordination of IT security research through the establishment of an R&D Working Group that will engage with research-oriented partner organizations to help implement proposed initiatives.

IT-ISAC

Description: Community of security specialists from companies across the IT industry dedicated to protecting the IT infrastructure that propels today's global economy by identifying threats and vulnerabilities to the infrastructure, and sharing best practices on how to quickly and properly address them.

Policy/Strategy: Provide thought leadership to policymakers on cyber security and information sharing issues.

Collection/Analysis: The 24x7 IT-ISAC Operations Center serves as a centralized hub allowing IT-ISAC members to submit and receive information.

Dissemination/Awareness: Disseminates threat and vulnerability information related to the IT infrastructure to ISAC members through secure communication channels.

Collaboration: Communicates with other ISACs; Shares information with DHS as appropriate; Reports and exchanges information concerning electronic incidents, threats, attacks, vulnerabilities, solutions and countermeasures, best security practices and other protective measures.

AFCEA

Description: International, non-profit membership association serving the military, government, industry, and academia as a forum for advancing professional knowledge and relationships in the fields of communications, IT, intelligence, and global security. AFCEA's vision is to be the premier information technology, communications, and electronics association for professionals in international government, industry and academia worldwide.

Dissemination/Awareness: Produces SIGNAL, a monthly international news magazine serving government, military and industry professionals active in the fields of communications, intelligence, information security; research and development; etc.

Collaboration: Promotes exchange of information among AFCEA's members, including engineers, programmers, managers, government officials and military personnel, about communications, intelligence, imaging and information systems technologies.

Education/Training: Offers conferences that provide problem-solving opportunities to intelligence, homeland security and information technology professionals. AFCEA Professional Development Center (PDC) provides a wide-ranging program of continuing education and technical training courses.

Hiring/Recruiting: Presents $1.4 million annually in scholarships, grants and awards to students in the hard sciences attending the five service academies, ROTC programs, graduate schools and other educational institutions.

NSTAC (serves EOP)

Description: Provides industry-based analyses and recommendations to the President and the executive branch on national security and emergency preparedness telecommunications.

Policy/Strategy: Develops policy and technical recommendations for improving the security and effectiveness of national security communications to the EOP and executive branch. NSIE develops risk assessments regarding the security of the public network.

Collection/Analysis: Subject matter experts participate in NSTAC task forces, which produce analytical reports to the President on critical telecom issues.

Dissemination/Awareness: Most NSTAC reports are publicly available on the NCS Website.

R&D: Conducts periodic research and development exchanges between industry, government, and academia alike, and recommendations raised during these exchanges help shape the national security communications agenda.

Collaboration: DHS/NCS is the designated government support entity for the NSTAC. NSTAC seeks USG participation in task force meetings; NSIEs are forums for public-private network security information exchange. Sensitive information is shared, including classified information on occasion.

FS-ISAC

Description: Established to enable public and private sectors to share information about physical and cyber security threats and vulnerabilities to help protect the U.S. critical infrastructure. The mission of the FS-ISAC is to serve as the primary communications channel for the sector.

System Protection: Identify, prioritize and coordinate the protection of critical financial services, infrastructure service and key resources.

Monitor: Identify critical financial services sector operational support issues and requirements and articulate those to the Department of Treasury (DOT) and DHS.

Collaboration: Works with DOT, DHS, FSSCC, and FBIIC; Facilitates sharing of information pertaining to physical and cyber threats, vulnerabilities, incidents, potential protective measures and practices.

SAMPLE COMPANIES[2]

Google Enterprise

Description: Provides innovative technologies that help government agencies organize information and make it accessible & useful to the citizens & to authorized government employees. Some of Google's solutions include search, geospatial data, and communication & collaboration tools.

Collaboration: Serves government and commercial clients; Participates in OASIS and several open source organizations.

McAfee

Description: Supplier of network security and availability solutions; Creates computer security solutions to prevent intrusions on networks and protect computer systems from the next generation of blended attacks and threats.

Policy/Strategy: In order to effectively fight cybercrime and make a meaningful impact to this problem, McAfee is focusing on three core areas: Legal Frameworks and Law Enforcement, Education and Awareness, and Technology and Innovation.

System Protection: Created "Shredder" to effectively remove any and all traces of confidential files from a computer and provides identity protection and anti-theft encryption.

Incident Warning/Response: Its cyber crime response center will provide help assessing the situation, including advice on what evidence to gather for law enforcement to bring a case, and refer victims to the appropriate law enforcement agencies, credit agencies, support agencies, and other organizations.

Collaboration: Serves as a security advisor to federal government and provides them with solutions such as: Anti-spyware, Anti-virus, Data loss prevention (DLP), Encryption, Host intrusion prevention, Messaging and web security, Network intrusion prevention, Risk and compliance analysis, System security management, Vulnerability management.

Symantec

Description: Helps consumers and organizations secure and manage their information-driven world. Provides software and services to protect against risks.

Collaboration: Offers government clients solutions such as Endpoint Security, Messaging Security, Policy & Compliance, Email Archiving, Data Loss Prevention, Security Management, Security Information & Event Management

Microsoft

Description: Partners with governments, communities, and other businesses around the world on digital inclusion; investing in long-term research that makes possible new breakthroughs in science and technology; and nurturing local innovation that expands social and economic opportunities for communities worldwide.

Collaboration: Government clients receive the some of following services: DOD—Business intelligence solutions, Combat collaboration solutions, DefenseReady; Federal Enterprise Architecture, Federal Server Core Configuration (FSCC), HSPD-12 smart card; Financial Management—Balanced Scorecard Accelerator, Earned value management; HHS—Chronic condition management, Electronic health records management

Education/Training: Funding several programs to gather more information and promote new solutions to the problem of ensuring global access to technology; Offers IT-Pro Training and Certification.

AT&T

Description: Communications provider that serves millions of customers on six continents, including all of the Fortune 1000.

System Protection: Launched a new network-based security service that provides advanced Web content and instant-messaging filtering.

Collaboration: Provides clients with solutions such as web security; business continuity, firewall & client security, security consulting, threat management.

ACADEMIC INSTITUTIONS AND THINK TANKS

Berkman Center

Description: Entrepreneurial non-profit research center whose mission is to explore and understand cyberspace; to study its development, dynamics, norms, and standards; and to assess the need or lack thereof for laws and sanctions.

Policy/Strategy: Develops reports on cyber policy issues (for example, the Global Network Initiative: In partnership with many commercial, academic and public groups, the Berkman Center has participated in an initiative to protect and advance individuals' rights to free expression and privacy on the Internet through the creation of a set of principles and supporting mechanisms for ICT companies).

Academic Research: Engages with a wide spectrum of Net issues, including governance, privacy, intellectual property, antitrust, content control, and electronic commerce.

Education/Training: Sponsors events, lectures, and online forums to promote dialogue and awareness; Supports Harvard cyber-based curriculum; Distributes a monthly newsletter and authors blog posts.

Collaboration: Regularly partners with commercial, academic and public groups.

CSIS

Description: A bipartisan, non-profit organization that provides strategic insights and policy solutions to decision makers in government, international institutions, the private sector, and civil society.

Policy/Strategy: Publishes reports on relevant technology policy issues and provides recommendations regarding policy changes to the Government; Sponsored the CSIS Commission on Cybersecurity for the 44th Presidency, which released its final report in Dec. 2008.

Academic Research: Conducts research and analysis to inform the policy landscape; sponsors initiatives that make policy recommendations to the Government (e.g. CSIS Cybersecurity Report).

Education/Training: Sponsors a variety of open events and publications to promote education and awareness of emerging policy issues.

Collaboration: Collaborates with the Government on strategic policy documents; receives partial funding from Government.

Sans Institute

Description: Provides information security training and certifications; Develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system—Internet Storm Center (ISC).

Incident Warning/Response: Internet Storm Center (ISC) provides a free analysis and warning service to thousands of Internet users and organizations, and is actively working with Internet Service Providers to fight back against the most malicious attackers.

Monitor: The all-volunteer ISC team monitors the data flowing into the database using automated analysis and graphical visualization tools and searches for activity that corresponds with broad based attacks.

Collection/Analysis: ISC uses the DShield distributed intrusion detection system for data collection and analysis. DShield collects data about malicious activity from across the Internet. This data is cataloged and summarized and can be used to discover trends in activity, confirm widespread attacks, or assist in preparing better firewall rules.

Academic Research: SANS Free Resources include developing and maintaining cybersecurity research documents and operation of the Internet's early warning system.

Education/Training: SANS provides intensive, immersion training to help people take practical steps necessary for defending systems and networks against cyber threats.

Collaboration: Collaborates with Government and industry on training courses; industry and government make up instructors and students (e.g. JTF-GNO, NSC, IBM).

Dissemination/Awareness: Disseminates both technical as well as procedural information to the general public; Report their findings to the Internet community through the ISC main web site, directly to ISPs, and via general emails; SANS distributes newsletters and publications to educate and inform the public on cyber vulnerabilities.

ASSOCIATIONS

ITAA

Description: Represents and enhances the competitive interests of the U.S. information technology and electronics industries. Provides leadership in business development, public policy advocacy, market forecasting and standards development to more than 350 corporate members.

Policy/Strategy: Works to educate decision-makers in Washington, D.C. and in state capitals about the many ways public policy affects innovation and the U.S.' ability to compete. Serves as a nexus for the industry's only grass roots to global network of industry executives.

Collaboration: Works to facilitate meetings with federal agency CIOs, state and local CIOs, program managers, and other key decision makers, and actively influence the outsourcing/procurement issues with agency and congressional officials.

ICASI

Description: Trusted forum for addressing international, multi-product security challenges that extends the ability of IT vendors to proactively address complex security issues and better protect enterprises, governments, and citizens, and the critical IT infrastructures that support them.

Dissemination/Awareness: Shares the results of its work with the IT industry through papers and other media. Alerts available online at ICASI's Website.

Collaboration: Members proactively collaborate to analyze, mitigate, and manage multi-vendor security challenges.

INSA

Description: Forum in which the once-independent efforts of intelligence professionals, industry leaders and academic experts come together to gain needed perspective on important intelligence and security issues.

Policy/Strategy: Positions itself as the non-partisan source of essential information and strategic analysis that is shaping policy to enhance our intelligence and national security communities.

Collection/Analysis: Provides strategic analysis on intelligence and national security issues.

Collaboration: INSA is one of the industry alliances partnering with the ODNI for the DNI Private Sector Initiative, a series of workshops bringing together experts from the government and the private sector on issues relating to national security, including Energy, China, and Emerging Technologies.

R&D: Innovative Technologies Council evaluates the applicability of new technologies, discusses cutting-edge concepts, and inspires innovation.

Education/Training: Sponsors symposiums, white papers, and debate; Engages the broader public to help find solutions. Working to create the workforce from which the leaders of the next generation will rise through education, advocacy and unclassified programs.

INTERNATIONAL MULTI-SECTOR COMMUNITIES

IETF

Description: Open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet; Produces relevant technical and engineering documents that influence the way people design, use, and manage the Internet.

Policy/Strategy: Develops technical and protocol standards, current Internet practices, and informational documents to ensure the Internet works more efficiently

Collaboration: Involves collaboration with a variety of Internet communities through an open process

ICANN

Description: International, non-profit consensus-based entity responsible for the management and oversight of the coordination of the Internet's domain name system and its unique identifiers.

Policy/Strategy: Facilitates policy development through a bottom-up, transparent process involving all necessary constituencies and stakeholders in the Internet Community; Key issues involve IPv4/IPv6, DNSSEC, and IDNs.

System Protection: Manages the IANA function, which is responsible for the global coordination of the DNS Root, IP addressing, and Internet protocol resources.

Collaboration: Open to all who have an interest in global Internet policy as it relates to ICANN's mission of technical coordination; NTIA holds contractual agreements with ICANN; USG Internet Governance community participates in ICANN policy making.

KEY

Functions

- Policy/Strategy
- System Protection
- Incident Warning/Response
- Monitor
- Collection/Analysis
- Dissemination/Awareness
- Collaboration
- Education/Training
- R&D
- Hiring/Recruiting
- Academic Research

Center/Dept.	Description
AFCEA	Armed Forces Communications and Electronics Association
Berkman Center	Berkman Center for Internet & Society at Harvard University
CERT/CC	CERT Coordination Center
CSCSWG	Cross Sector Cyber Security Working Group
CSIS	Center for Strategic and International Studies
DSAC	Domestic Security Alliance Council
FS-ISAC	Financial Sercices Information Sharing and Analysis Center
ICANN	Internet Corporation for Assigned Names and Numbers
ICASI	Industry Consortium for the Advancement of Security on the Internet
IETF	Internet Enginnering Task Force
INSA	Intelligence and National Security Alliance
ITAA	Information Technology Association of America

Center/Dept.	Description
IT-ISAC	Information Technology Information Sharing and Analysis Center
IT-SCC	Information Technology-Sector Coordinating Council
NSTAC	President's National Security Telecommunications Advisory Committee
OSAC	Overseas Security Advisory Council
AT&T	
Google Enterprise	
InfraGard	
McAfee	
Microsoft	
Sans Institute	
Symantec	

Notes

1 There are numerous civil/commercial sector communities. Some additional cyber-related groups include those in the following issue areas: technical/architectural (IEEE, ISO, IAB, ARIN, W3C), policy (IMPACT, GIIC, ITU, IGF, ICC, OECD), infrastructure/operations/security (FIRST, NANOG, ISPs, peering and transport providers) and research and development (PlanetLab, Clean Slate Project, CAIDA, Internet 2). This graphic simply offers a snapshot of the broad commercial/civil community to highlight the variety of cyber groups.

2 Represents small sample of companies that focus on cyber to illustrate connections.