WORKING GROUP 5: CYBER SECURITY INFORMATION SHARING

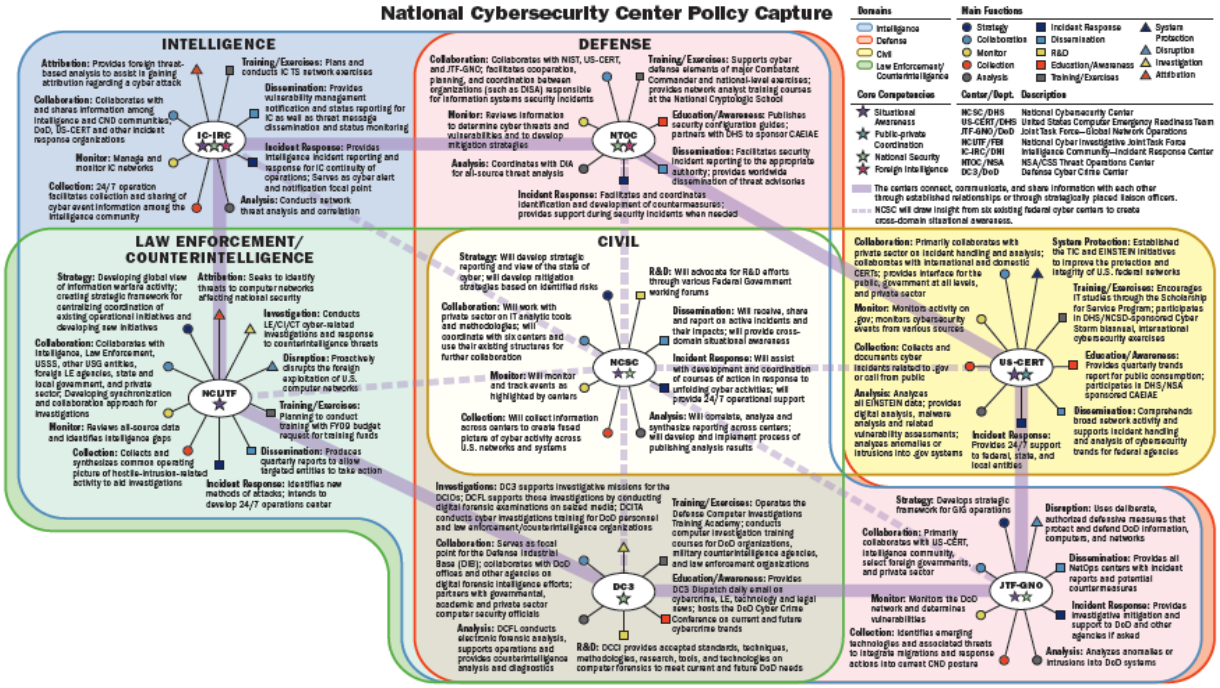
JUNE 2016 Information Sharing Barriers

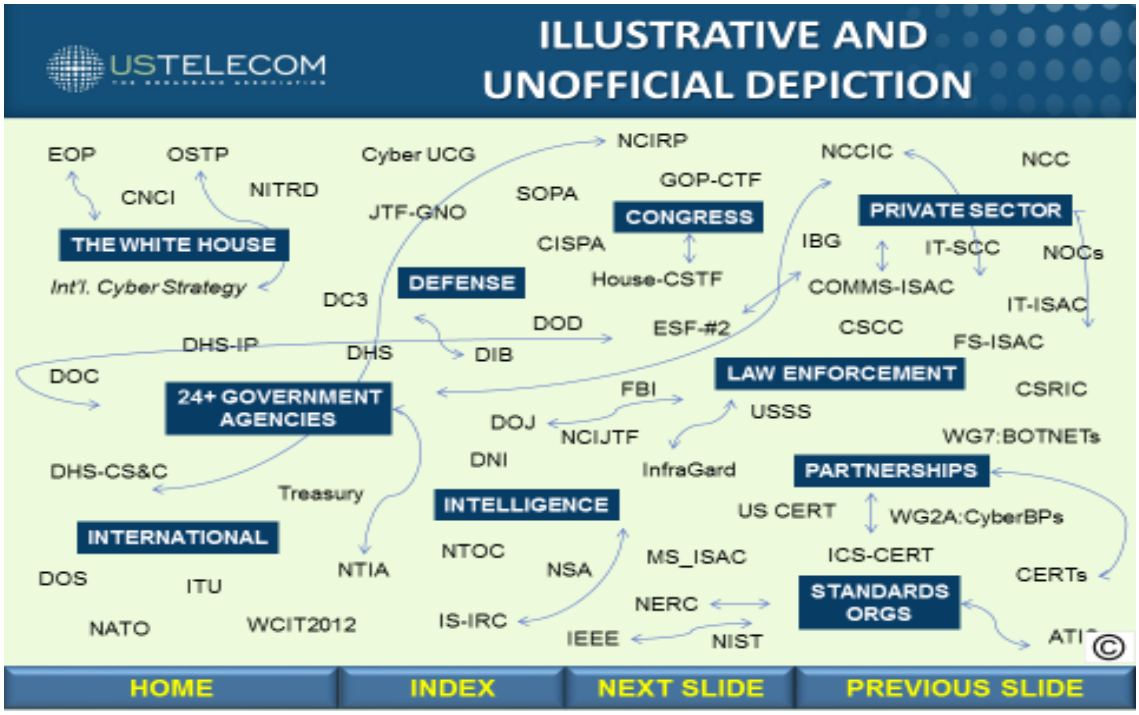
Introduction:

CSRIC V Working Group 5 (WG5) is currently tasked with identifying and assessing perceived technical, legal, financial, consumer/market, operational, and/or organization impediments to cyber threat information sharing and/or the implementation of the prospective use cases. WG5 also is directed to analyze potential solutions to the impediments, and develop recommendations that would enable cybersecurity information to be broadly shared across the communications sector. This interim update builds upon the working group's March 2016 Use Case Report. Following its March report, the working group analyzed potential organizational, operational, technical, consumer/market, financial, and legal and policy impediments to information sharing in the following sharing situations: private to private, private to government, and international information sharing. The working group also considered unique challenges for small and midsized communications companies sharing information in the private and public realms.

Organizational Challenges:

A critical organizational challenge facing the communications sector is the wide variety of private, public, public-private, and international groups, entities, and arrangements devoted to cyber threat information sharing. The proliferation of sharing entities and arrangements, illustrated below, threatens to dilute resources and expertise through redundant or conflicting activities and objectives.





A number of key communications companies are part of the Communications Information Sharing and Analysis Center (COMM-ISAC), which is coordinated by the Department of Homeland Security's National Coordinating Center for Communications (NCC). The COMM-ISAC is an established forum for gathering and exchanging information on vulnerabilities, threats, intrusions, and anomalies. Sector representatives also are involved in the development of – and will be working with – the new Information Sharing and Analysis Organizations (ISAOs), overseen by DHS, that will emerge in connection with effectuation of the President's 2015 Executive Order on information sharing. Communications companies also will be working with the DHS Automated Indicator Sharing (AIS), which is designed to facilitate real-time sharing of cyber threat indicators with DHS's National Cybersecurity and Communications Integration Center (NCCIC). CISA also designates the NCCIC itself as a principal Federal civilian interface for multi-directional and cross-sector information sharing related to cybersecurity risks, incidents, analysis and warnings. Sector companies also work the United States Computer Emergency Readiness Team (US-CERT). Thus, navigating the various DHS entities involved in information-sharing activities can be a challenge, due to the complexity of that agency's organizational structure and the potential for overlapping responsibilities.

Outside of DHS, communications companies are also the driving force behind the information sharing activities occurring in connection with CSRIC V. Companies may also be involved with the FBI-National Cybersecurity Industry Joint Task Force (NCI-JTF) and InfraGard, which is involved in botnet takedowns, repelling DDOS attacks and addressing other cyber threats. In addition to these entities, some communications companies may enter into arrangements with government agencies for the receipt and exchange of cybersecurity data, including threat vectors, attack signatures, anomalies, incursion patterns and other threat-related information. State and regional sharing entities also are beginning to emerge, with more such organizations anticipated following initial implementation of the Information Sharing and Analysis Organization (ISAO) EO.

In the wake of the laudable recognition of the value, benefits and importance of cybersecurity information sharing by legislators and policy-makers, a key objective going forward will be to streamline the mechanisms and venues for sharing and enhance coordination and cooperation among the various

Federal, State and regional entities involved in information sharing to promote efficient and effective sharing activities.

Industry members also may be involved in a number of cross-sector and multilateral organizations that exchange information on cybersecurity threats and issues, including the North American Network Operators' Group (NANOG), the Domain Name System Operations Analysis and Research Center (DNSOARC), and the Messaging, Malware and Mobile Anti-Abuse Working Group (M^3AAWG). Sector companies also enter into contractual arrangements with third-party security vendors for the receipt of threat data and tactical response information.

Organization impediments also generally exist in the private to private venue and are intensely felt by Small and Mid-sized Businesses (SMBs). Trust relationships have traditionally formed the basis for information sharing, but require time and effort to build and maintain. Sharing is often conducted on the basis of personal relationships built out of industry networks and at events such as NANOG and M3AAWG. Some organizations, and in particular, SMBs do not always have access to those events and aren't traditionally organized to share information effectively. Continued development and use of ISACs may alleviate some of these organizational barriers.

The distribution of classified information from government to private may also affect the quality of information shared between private entities. Access to classified information by cleared individuals may affect the scope and conditions in implementing operational activities. By the same token, not having knowledge of and access to classified information may have an effect on business activities. Classified information should be downgraded and distributed where possible.

Information sharing rules between and amongst organizations should take into account the trustworthiness of the recipient, the sensitivity of the shared information, and the potential impact of sharing (or not sharing) specific types of information.

Organizational impediments are most apparent in the context of international sharing. Many countries have Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) that vary in terms of procedural conformity, technology sophistication, financial support, and knowledgeable human resources, all of which impact domestic and international collaborative capabilities. Different governments also have different classifying mechanisms for sensitive information that also impact and prevent sharing among international response teams. DHS has also observed in the past that the amount and quality of information that come from CERTs is limited and often more robust between countries with similar cultures and language. Moreover, international information sharing does not have the same historical evolution as domestic sharing within the U.S. Establishing trust within international groups needs to be emphasized and supported.

In addition to the technical, financial, operational and legal barriers mentioned above, sharing internationally gives rise to additional impediments where transactions can involve multiple governments and industries with different time zones, sets of laws, norms, languages, cultures, motivations and competence.

In recent years a combination of factors has increased awareness and concerns about information sharing generally. Studies of multi-country corporate environments have identified various social norms that impact the usefulness of information sharing. In some instances, for example, there is hesitance to share information about threats and vulnerabilities because such information may be associated with weakness or shame. Sharing weaknesses or vulnerabilities in some countries may give rise to regulatory or other actions by governments more than in others.

Given the complexities of international sharing mechanisms and legal protections, industry should engage with international partners verbally and in person to continue to build trust relationships in a similar way that trust relationships have evolved organically over time in the United States.

Operational Barriers:

The results of information sharing initiatives will be highly dependent on the effectiveness of implementation from an operational standpoint. Operational barriers can vary based on the size of an organization but exist in available resources, or the re-allocation of resources, to meeting changing or competing demands in the cybersecurity landscape. Filtering the many sources of threat intelligence, validating what is applicable, and then defining the priority to implement can be complex and time consuming.

Changes in operations over time can take time and slow down the information sharing process. Any change to an operational process generally requires a well-defined process and procedure that must be communicated to all parties, and must be related to performance goals with measurable results. The process for changing operational procedures must be more dynamic to lessen the impact on timely information sharing.

Production of refined, reliable intelligence also takes time and, while reliable intelligence developed over time can be useful in forensic efforts, the amount of time sometimes required hinders usefulness live or proactive protection efforts. Refining intelligence too hastily, however, can result in unreliable or unusable intelligence. Striking the right balance is essential.

Technical Barriers:

Technical barriers to cyber threat information sharing include capacity, accuracy, quality, timeliness, and issues resulting from a lack of consistent, standard formats and accepted nomenclature that should be used to share information.

The most cited technical impediment to sharing could be broadly characterized as a lack of "standardization" of formats and terminology. That is, while there are a wide array of formats/protocols/schemas for sharing, there is no agreed upon terminology for malware across organizations, and there is no universal schema for incident progress. The lack of a standardized information format, for example, means shared data is integrated on an ad-hoc, customized basis, which necessarily takes time and resources, and may cause data quality issues.

Similarly, rectifying differing terminology for the same piece of information as it is shared causes confusion, adds time, and lessens the effectiveness of information sharing. Wide variances in formatting standards, and terminology amongst organizations could render a perfect organizational structure for exchanging information useless.

Lack of context and accuracy for indicators also impede sharing. For example, an indicator may be marked "suspicious," but only the originator knows why, which lessens the usefulness to the information recipient. Similarly, lack of information about the origin of shared information leads to testing, filtering, or potentially dropping information by the recipient.

Quality of data and relevance to use cases can also be an impediment to fruitful information sharing. Often data is shared formally initially, but follow up occurs informally and becomes more subjective, thereby deteriorating the data validating process. Additionally, as the pool of participants grows in the information sharing process, trust declines and information may become more generic limiting the quality of information shared, as more detailed, validated data is shared among members within the

same sector where the information is shared through a dedicated portal. Those who are not members of the specific sector or who don't have access to the portal may receive information that is generalized, or it may receive no information at all.

The timeliness, scale or capacity, and integration of the information into various security tools also create technical challenges. Production of refined intelligence can take time and may not enable real time protection. On the end of the spectrum, quickly produced intelligence can be fraught with peril leading to false positives and other negative outcomes. Also there are scaling challenges as information is integrated into security tools. At scale, a firewall can be overwhelmed with rules to block literally thousands of IP addresses. Meanwhile the collective set of botnets has millions of IP addresses they cycle through daily. Finally integrating the data into an intrusion detection system or firewall can create additional challenges and further development work.

It is important to emphasize that the group does not consider top-down regulation or government-mandated technical standards as the solution to any of the technical constraints identified here. Cyber threat information sharing is still in its nascency. Standards, tools, protocols, and best practices recommendations are being discussed, developed, and are starting to be implemented. As legislators and policy-makers have repeatedly recognized, this is not an area conducive to backward-looking, static, one-size-fits-all prescriptive regulation. The technical issues and constraints that companies will face will continue to change and evolve in accordance with new technological developments and the constantly-changing threat landscape, and it is vital that the sector be afforded the necessary flexibility and agility to adapt to these changes. WG5 firmly believes that the public-private partnership and cross-sector that is aimed at generating industry-driven solutions to the technical challenges to sharing, continues to be the best way to address those challenges.

Consumer/Market Considerations:

Consumer concerns about where their information is being stored and with whom it is being shared are potential barriers to information sharing. Transparency about protections for consumer information within an organization's system as well insight into use of information after it leaves the system is important to managing consumer expectations and allaying fears about information sharing. It will become increasingly important for organizations to identify and protect certain information as well as to educate consumers about protections related to information sharing. Government support for the protections taken by industry also will be important to reassuring consumers. Consumer understanding of, and confidence in, the importance of sharing and the role that it plays in securing their data is a key factor in fostering a frictionless and robust sharing environment.

Financial Barriers:

Financial disincentives to information sharing exist in all information sharing venues. Building requisite sharing infrastructure, buying a data feed, and dedicating human resources are all cost centers. Moreover, with structured data there are costs affiliated with receiving and analyzing data in multiple different formats

Financial resource restraints are most acute for small and mid-sized (SMB) communications companies who are often challenged by limited resources including access to financial capital, operational manpower, technical expertise, management buy-in, and other tools and resources needed to effectively participate in sharing venues. SMBs are often unable to dedicate an employee to fully engage in external information sharing, and even when they are they often lack the financial support to fully engage.

Legal/Policy Considerations:

In the past there were a variety of legal concerns surrounding cyber threat information sharing, as cybersecurity was a relatively undefined area with respect to U.S. law. For example, the Electronic Communications Privacy Act (ECPA), a criminal statute governing the conduct of electronic surveillance, contains several exceptions that are useful when conducting cybersecurity operations. While the exceptions permit carriers to monitor their own communications networks to "protect their rights in property," there were questions about whether that exception protected not only imminent or actual threats to a carrier's network, but also sharing activities designed to protect the ecosystem as a whole. Further, the overall nature of ECPA is to restrict sharing and in many cases the use of information is dependent upon customer consent, which inevitably restricts real time information sharing.

The potential for civil liability remains an impediment for information sharing in the private to private, and private to government cyber threat information sharing venues. Lack of legal clarity on the civil front, and the potential for criminal sanctions, in particular, have, in the past, led companies to take a conservative approach to information sharing. Uncertainty, and the not infrequent instances in which the permissibility of sharing necessitates protracted legal analysis, also hampers companies' ability to respond in real time.

The enactment of the Cybersecurity Information Sharing Act of 2015, which represented Congress' attempt to develop a clear legal framework to information sharing, was intended to address a number of these issues. Communications companies are in the process of working with their legal departments and are reviewing the guidance published by DHS and the Department of Justice based upon the legislation to determine the extent to which these issues remain a concern.

Recent joint guidance by the Department of Justice and the Federal Trade Commission in *Antitrust Policy Statement on Sharing of Cybersecurity Information*, was intended to address potential concerns over antitrust violations because of cybersecurity information sharing, recognizing that private parties play an important role in preventing cyberattacks and in sharing information.[1] In addition, contractual provisions in contracts with third-party security and tool vendors that affect sharing of certain information may impede the quality and timeliness of threat information sharing regardless of a generally permissive legal or policy environment.

Further, the impact of new service arrangements and offerings for end users of communications services may warrant additional legal review. As more and more customers consume broadband services and capabilities offered in a managed service environment, additional legal review may be necessary to assess whether an ISP can or should share security-related information they glean from third-party security specialists and vendors, other service providers, and end users themselves – consistent with all applicable legal obligations. The ongoing potential for conflict between communications service provider privacy obligations and security duties remains a serious potential impediment to robust sharing, particularly as the kind of packet metadata that have long been at the core of the work and sharing undertaken by network engineers and security specialists begins to fall under the rubric of privacy regimes. This potential impediment arises not only in connection with real-time sharing, but also with respect to threat intelligence sharing and research on attack vectors, defense tools, and remediation measures.

Indeed, an emerging challenge for communications companies engaged in information sharing activities is the potential for conflict between the FCC's privacy NPRM and CISA. Under CISA, companies may

[1] Issued April 10, 2014.

share cyber threat indicators for a "cybersecurity purpose" and are obligated only to remove from such indicators information not directly related to a cyber threat which the company "knows at the time of sharing to be personal information." However, under the FCC's proposal, sharing of cyber threat indicators that include customer proprietary network information (CPNI) – and the FCC defines commonly shared cyber threat data elements such as IP addresses and domain information as CPNI – would be subject to potential post-hoc liability assessments of whether the disclosure of such CPNI was "reasonably necessary" to protect against a threat. This more stringent standard could chill beneficial sharing activity, particularly with respect to sharing of threat intelligence and research related to threat vectors, attack strategies, and the efficacy of defensive measures.

Additional potential impediments also include the lack of human resources that may be needed to adequately balance privacy protections with the need for effective, timely sharing. Namely, that it may take more manual "eyes-on" analysis to effectively balance privacy protection concerns and effective and timely information sharing. In addition, development of required policies and procedures may lag as the size of the sharing community grows.

Legal barriers also exist in the international information sharing venue where the legal framework varies from state to state. Such barriers include freedom of information laws, anti-trust rules, restrictions on cross-border data flows and in-country data retention, and criminal jurisdiction and coordination. Diverse information classification regimes further complicate inter-government sharing, and re-sharing. Currently, the complex and uncertain legal regime slows down sharing arrangements to the point where real time sharing internationally is not possible. Harmonization of information sharing laws and further development of international liability protections are also desirable to build confidence in international sharing venues and to facilitate cyber threat information sharing across international borders.

In the absence of legal harmonization, industry should evaluate and dialogue with various international entities to determine how best to work within their frameworks to share cyber threat information internationally.

Summary:

In this interim report, CSRIC V WG5 has identified perceived technical, legal, financial, consumer/market, operational and/or organization impediments to cyber threat information sharing. This interim report builds upon the prior WG5 interim reports in which cyber information sharing relationships were identified and information sharing use cases were described. In its Final Report in March 2017, WG5 will synthesize the material presented in its interim reports, to include forthcoming reports on trust pools and conduits for information sharing, and make recommendations to enable cybersecurity information to be more broadly shared in order to effectively mitigate the cyber threats posed to the communications critical infrastructure.