MARCH 2017 WORKING GROUP 5: CYBER SECURITY INFORMATION SHARING

FINAL REPORT

The Communications Security, Reliability and Interoperability Council V
Cybersecurity Information Sharing Working Group 5
FINAL REPORT

TABLE OF CONTENTS

The Communications Security, Reliability and Interoperability Council V
Cybersecurity Information Sharing Working Group 5
FINAL REPORT

1. EXECUTIVE SUMMARY

Working Group 5 (WG 5), Cybersecurity Information Sharing, was tasked with developing recommendations to the Federal Communications Commission (FCC or the Commission) to encourage sharing of cybersecurity information between companies in the communications sector. This report represents the culmination of multiple work streams highlighting the robust level of information sharing that is already underway within the sector and between industry and government. As illustrated in this document the Communications Sector is uniquely situated given our integrated role with the Department of Homeland Security (DHS) at the National Coordinating Center (NCC) which serves as the Communications Information Sharing and Analysis Center (Comms-ISAC). Much of the material presented here outlines how the industry functions today, highlights the types of sharing that occurs and brings to light the extensive level of private to private sharing within the industry and concludes with a series of recommendations building on this foundation to improve sharing throughout the sector.

In order to facilitate the development of this report the Working Group completed five interim reports in the following areas: (1) a Notional Diagram illustrating information sharing within the sector, (2) information sharing use cases, (3) barriers to information sharing, (4) trust pools, and (5) a discussion of conduits or means to share information within the sector. This report summarizes each of those items and then concludes with recommendations for both the FCC and the sector.

The Notional Diagram – Communications Sector Information Sharing (included on page 7) illustrates the various means by which the sector shares information today. This diagram delineates information sharing (1) among private sector partners and (2) between the private sector and government entities. The use cases then build upon this by providing examples of information in each of these categories. For private to private information sharing, the working group describes a categorization model based upon two primary factors: (1) the *formality of the relationship*, and (2) the *structure of the data*, and use cases for each of the four resulting categories. For private to government and government to private information sharing, ten use cases provide representative and diverse examples of how the communications private sector shares with government to address cyber threats.

In the next section, the working group goes on to discuss various barriers to information sharing including organizational, technical, operational, financial, and legal/policy issues impacting information sharing. The working group also considered unique challenges for small and midsized communications companies (SMBs) sharing information in the private and public realms. In the "Information Sharing Trust Pools," section, the working group identified optimal information sharing "Trust Pools" to inform the working group's recommendations to the Commission. The intent of this effort was to identify, assess, analyze, and develop recommendations for how industry engages in information sharing with other trusted entities. Finally, the working group discusses Conduits for Information Sharing, described as identifying and assessing structures and platforms for the communications sector stakeholders to routinely share cybersecurity information (threat indicators, warnings, anomalous indicators, and post-incident information).

The working group's proposed recommendations are based on facts and conclusions drawn from each of the sections discussed above. These recommendations include the following:

- The FCC should acknowledge the breadth and depth of cyber-threat information sharing that

currently takes place between and among industry and government entities, and recognize that DHS is leading in government information sharing with the private sector. To the extent the FCC wants to participate in information sharing it should do so in the context of the broader efforts organized by DHS and not duplicate efforts within the FCC.

- Industry should continue its efforts to conduct and expand on the current pilot that it has underway regarding information sharing using STIX/TAXII, and determine if these protocols meet the needs of communications sector. Industry should also explore the opportunities and challenges related to sector-wide operational use of DHS' Automated Indicator Sharing (AIS) portal.

- Industry should enhance the Communications ISAC by developing a hosted, private website on which government entities, industry partners, and stakeholders representing SMBs may register to access a cybersecurity resource repository and message board. At the same time, the ISAC should consider the best means to encourage international involvement in information-sharing processes balanced against the challenges outlined in this document.

- The public and the private sector should continue to work together to develop, promote, and enhance cybersecurity education and awareness within the sector, including by educating SMBs regarding the depth and breadth of existing venues that offer cyber-threat information-sharing opportunities.

- The government should explore a grant program to provide funding to SMBs so that they may obtain or develop resources necessary to robustly participate in the cybersecurity information sharing ecosystem.

- There is currently a considerable amount of threat intelligence gathering and client-tailored information sharing provided on a proprietary basis by commercial entities. Policy makers should continue to encourage and support such sharing. Proprietary information sharing tools and managed security services that incorporate this information provide a reliably agile, effective, and innovative mechanism to both heighten awareness of cyber threats and tactics and can play a role in mitigating attacks.

2. WORKING GROUP MEMBERS

Name	Company	Name (cont.)	Company (cont.)
Chris Boyer (Co-Chair)	AT&T	Robert Gessner	MCTV
Rod Rasmussen (Co-Chair)	Infoblox	Mark Hoffer	MCTV
Greg Intoccia (FCC Liaison)	FCC	Bill Mertka	Motorola (ATIS)
Vern Mosley (FCC Liaison)	FCC	Larry Walke	NAB
Martin Dolly	AT&T (ATIS)	Loretta Polk	NCTA
Rosemary Leffler	AT&T	Matt Tooley	NCTA
Trace Hollifield	Bright House Networks	Dr. Donald H. Sebastian	NJ Institute of Tech
Kathryn Condello	CenturyLink	Frank Menzer	NOAA
Paul Diamond	CenturyLink	Kathy Whitbeck	Nsight
Mary Haynes	Charter Communications	Jesse Ward	NTCA
John Kelly	Comcast Cable	Kazu Gomi	NTT America
Jorge Nieves	Comcast Cable	Shinichi Yokohama	NTT America
Paul Fournier	Comcast Cable	Michael Brown	RSA

Rudy Brioche	Comcast Cable	Richard Perlotto II	Shadowserver
Kevin Kastor	Consolidated	Jason Jenkins	SilverStar
Jemin Thakkar	Cox Communications	Jeff England	SilverStar
Matt Carothers	Cox Communications	Allison Growney	Sprint
John Marinho	CTIA	Brian Scarpelli	TIA
Chris Alexander	DHS	Joe Viens (Co-Chair Sub-Group 1 Private to Government Sharing)	Charter Communications
John O'Connor	DHS (Co-Chair Sub-Group 1 Private to Government Sharing)	Chris R. Roosenraad (Chair Sub-Group 2 Private to Private Sharing)	Charter Communications
Alexander Gerdenitsch	Echostar	Arthur "Trey" Jackson	T-Mobile
Jennifer Manner	Echostar	Cindy Carson	T-Mobile
David Colberg	EMC	Harold Salters	T-Mobile
Daniel Cashman	FairPoint Communications	Howard Brown	Tulalip Data Services
Carlos Carrillo	FireEye	Robert Mayer	US Telecom
Thomas M. MacLellan	FireEye	Eric Osterweil	Verisign
Tony Cole	FireEye	Shawn Wilson	Verisign
Dave Keech	Frontier	Nneka Chiazor	Verizon
Ethan Lucarelli	Iridium (Wiley Rein)	Dorothy A. Spears-Dean	VITA
Michael O'Reirdan	MAAWG	Greg Lucak	Windstream
Greg Holzapfel	Sprint	Stephen Swanson	WOW, Inc.
Myrna Wilson	DHS (Support for Sub-group 1 Private-Government Sharing, Editor/Drafter for reports)		

3. OBJECTIVE

CSRIC Working Group 5 was tasked with reviewing and making recommendations on the state of cybersecurity information sharing within the communications industry. As stated in the working group description, "in order to improve the communication sector's ability to identify, protect, detect, respond, and recover from cyber-attacks, Working Group 5 will develop recommendations to the Council to encourage sharing of cybersecurity information between companies in the communications sector."

The working group was further instructed to build upon the CSRIC Working Group 4 efforts by developing recommendations on how communications companies can improve information sharing about cyber risks to communications critical infrastructure within the private sector. The description further states that, to develop the recommendations, WG5 will organize into four study efforts: (1) Use Cases, (2) Information Sharing Barriers, (3) Information Sharing "Trust Pools," and (4) Conduits for Information Sharing.

4. SCOPE

As noted in the working group description, the primary focus on the working group's efforts is to develop guidance on how communications companies can effectively share cyber risk information pertinent to communications critical infrastructure within the private sector. Thus the scope of this effort is centered on critical infrastructure which was defined by each of the five sub-sectors -- wireline, wireless, cable, satellite, and broadcast -- in 2015 in the final CSRIC Working Group 4 report. In that report, critical infrastructure was defined consistent with Executive Order 13636,

which defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

As such, the type of information in scope for this report is information relevant to ensuring the availability, reliability, resiliency, and integrity of each segment's critical infrastructure with their respective communications networks rather than the entirety of their end-to-end network paths. However, given the wide variety of information sharing that is currently underway in the industry, the use cases are focused on providing a holistic picture of how information sharing is conducted today so that the working group could assess those models or examples to identify both barriers and recommendations related to securing critical infrastructure.

5. USE CASES

Baseline Communications for Information Sharing

The first step taken by the working group was to develop a baseline diagram to reflect the level of information sharing currently underway in the sector. The diagram below was presented at the December 2015 CSRIC meeting and is intended to provide this baseline view. As illustrated, there are a variety of groups that the industry is sharing with today from trusted peers and commercial partners, government agencies under contract, law enforcement, industry peers as part of the sector policy and planning process, the DHS via the National Coordinating Center and the National Cybersecurity and Communications Integration Center (NCCIC) and other affiliated organizations like US-CERT, public and private partners, and finally by ISPs for their own internal use and to protect customers. The type of information also will vary, as depicted by the various colors in the diagram. For example, information about threats to ISPs' own networks is generally shared, to the extent an individual ISP or sector member is willing to share this information, with a variety of trusted peers and commercial partners, formal and informal peer organizations and with commercial partners as is reflected in the box in the far upper left corner of the diagram. This information also may, at the ISP's discretion, be provided to other entities such as DHS. Because this information is specifically about an attack on ISP infrastructure itself, it raises fewer concerns than, for example, information directly related to a customer.

Customer information is generally *not shared* within industry due to a variety of concerns related to customer privacy, but can be used with the impacted customer directly (reflected by the red line) to aid them in addressing a cyber incident. Typically, this occurs in the form of managed security services provided to the customer itself. It is important to draw a distinction between customer information and network infrastructure information given the privacy and business considerations that must be considered. For these reasons the primary focus within industry is on sharing information with respect to attacks on ISP core network infrastructure which is consistent with the mission of this working group.

Other examples include sharing with law enforcement. In this case, as noted in the diagram, the example is intended to cover situations in which the ISP may be the victim of an attack; e.g., a fraud case etc., and information about that attack needs to be shared with law enforcement as part of a criminal investigation. It is *not intended to indicate that customer information would be shared with law enforcement*. While enactment of the Cybersecurity Information Sharing Act has helped to clear away some of the legal underbrush that inhibited sharing under a variety of circumstances, there are still a variety of privacy related statutes that are implicated by a prospective sharing of customer information including, among others, the FCC's CPNI rules, and the Electronic Communications Privacy Act (ECPA) that must be analyzed by counsel prior to sharing that form of information today. Also there are a myriad of business reasons such as contractual limitations that would prevent ISPs, notwithstanding legal concerns, from sharing this information. For these reasons most of the working group's focus here is on sharing infrastructure related information.

Likewise, pursuant to government contracts some ISPs may share information with government agencies about the agencies' own network traffic that may be monitored by an ISP as part of services that they provide to the Federal government. Finally, information shared with public and private sector partners, such as the FCC or other government entities, as noted on the diagram, is less about cyber threat indicators and more general information about how ISPs are designing and implementing their

cybersecurity risk management programs.

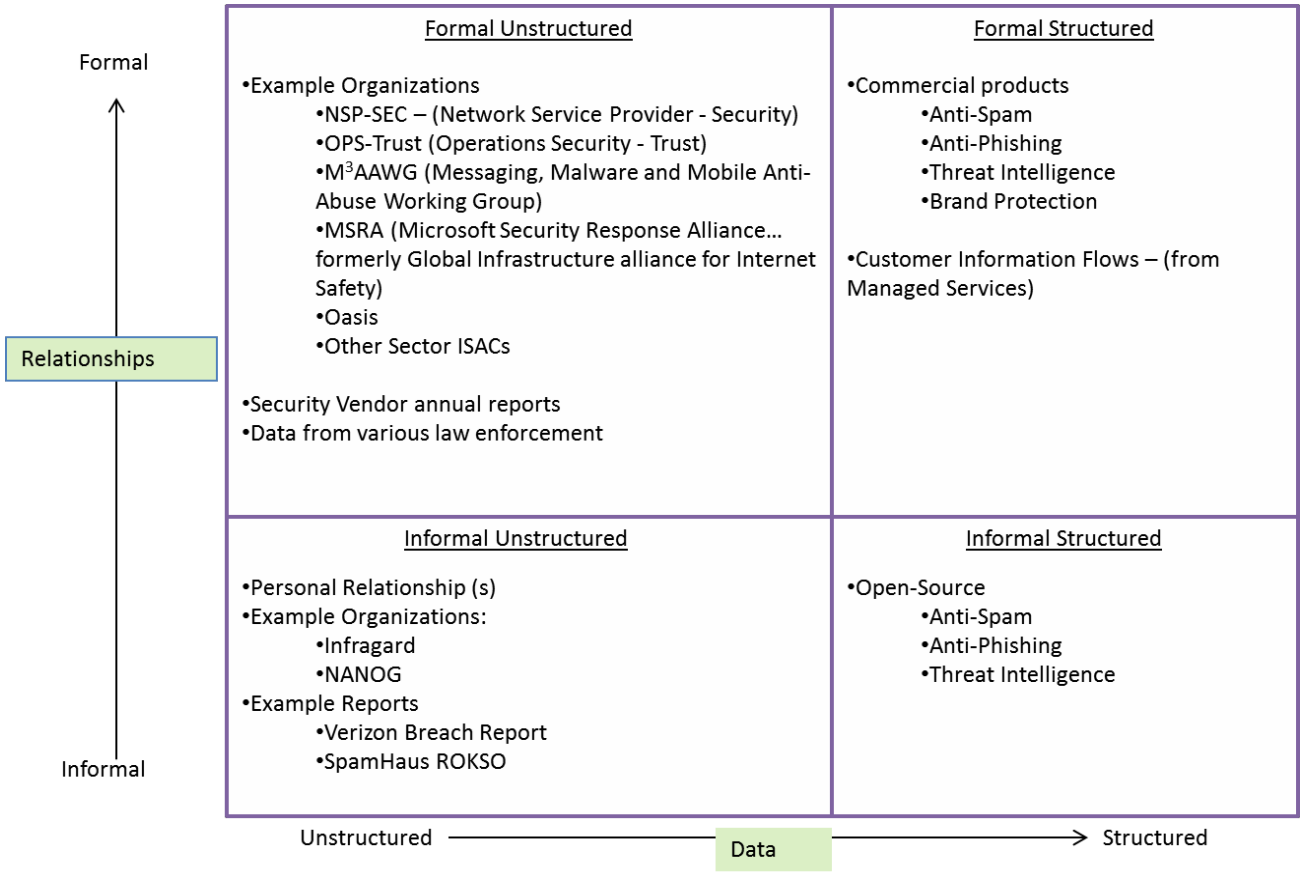
Based upon the diagram, the working group determined that there are in effect two fundamental buckets of use cases that would accurately reflect the work being done in the industry: (1) private to private sharing encompassing the bulk of the upper left quadrant of the diagram, and (2) private to government and government to private information sharing reflected predominantly by the box associated with the DHS information sharing process and other government related activities. Accordingly, the working group broke into two sub-groups focused on developing use cases in each category.

5.1 Private to Private Sharing

The first subgroup was chartered to describe the various forms and methods of private to private sharing. The conclusions of the group included: that there are literally dozens of examples; that the group wanted to avoid using names, in particular as it relates to some peer groups that may not wish to be named in a public document and/or or to avoid any potential indication of a vendor preference; that these relationships can change relatively quickly; and that there are many ways to categorize the private to private sharing relationships. Finally, the sub-group observed that for many smaller sized carriers and participants in the communications sector, information sharing today is one- way (e.g., carriers are consumers of information).

Thus it was recommended that an objective of the working group is to make it easier for all sizes of service providers to participate more robustly. The sub-group settled on a categorization model based upon two primary factors: (1) the *formality of the relationship* that can be either *formal* such as a contractual relationship or *informal,* which could include sharing via personal relationships or open sourced sharing, and (2) the *structure of the data* between *structured*, such as data feeds, anti-spam, anti-virus, machine readable feeds of data and *unstructured* such as mailing lists, phone calls, conferences, formal presentations, hallway conversations etc. aimed at humans. The group then proceeded to develop the following quadrant chart to illustrate examples of each of these categories.

As noted from the diagram there are multiple examples within each quadrant from formal unstructured, formal structured, informal unstructured, and informal structured. The sub-group then proceeded to develop a model use case for each of these quadrants without focusing on the specifics of any one entity or relationship. The working group elected to develop a standard template for the use cases that includes a description, discussion of the ISP and entity relationship, the relationship type, discussion of the information that is shared, benefits of information sharing, preliminary discussion of the gaps in information and process, and preliminary discussion of barriers and challenges. Each of those use cases is listed below.



5.1.1 Formal Structured

ISP & Entity Relationship	Formal, structured, information sharing between two entities with a defined relationship, such as a legal agreement. This may be a commercial or non-commercial agreement.
Relationship Type	Formal - structured
Information that is Shared	To whom: Typically, this involves sharing from an entity to an ISP, e.g. from a vendor to a customer, but other arrangements may exist as well. For instance, the ISP may share data rather than money.
	Content & Value: Content is machine-readable IOCs. The format may be as simple as CSV files delivered over HTTPS, or it may be as complex as STIX delivered over TAXII.
	Timeliness: This may be anything from real time in the case of automated detection systems or sinkholes to weeks delayed in the case of manual investigation.
	Sharing Process: The process varies depending on the source of the data and the technology they have chosen.

Benefits of Information Sharing	Compromises prevented or at least identified. Vulnerabilities revealed, potentially prior to exploitation. Vendors can tailor information feeds to the risks and vulnerabilities that predominate for a ISP customer. Can be used for victim notification in the case where a vendor sends an ISP lists of compromised customer IPs.
Gaps in Information & Process	Every vendor has a different format for their data and a different method of delivery. Every source requires custom integration. Quality of data varies, and there is no standard to assess that quality.
Barriers & Challenges	Vendors can be prohibitively expensive in some instances. Integration is costly and time consuming. Contextual data is often missing, e.g., an IP is listed as bad, but there's no further information as to why it is bad or how an ISP can determine whether a detection is a false positive.

5.1.2 Formal Unstructured

ISP & Entity Relationship	Informal conversations between the SP and a vendors/partners. Content may be derived from conversations or simple communications such as email. Often the content comes in the form of a formal written report.
Relationship Type	Formal - unstructured
Information that is Shared	To whom: The data is almost always shared from the vendor/partner to the SP.
	Content & Value: Content may be derived from conversations or simple communications such as email, or be contained within a larger report or analysis
	Timeliness: This may be either real time (conversations) or near real time (email).
	Sharing Process: The delivery method will vary based on the relationship of the ISP and the source in addition to the nature of the data being shared. The higher the degree of sensitivity the more likely that the sharing method will be verbal. The less sensitive the data the more likely that it will be shared via email or other electronic means.
Benefits of Information Sharing	Compromises prevented or at least identified. Vulnerabilities revealed, potentially prior to exploitation. SP – SP conversations often lead to enhanced understanding of threats as they relate to the SP environment. Heightened awareness. Information often comes in the form of a warning "we've seen this threat elsewhere" or a post-mortem "here is what we determined happened to you".

Gaps in Information & Process	There is no formal process. The nature of this sharing is ad hoc. Can sometimes arise from vendors seeking to demonstrate value of their service. Often it is best used for awareness and not as an input for automated tools.
Barriers & Challenges	Validating the data is a major concern. Information shared in conversation and email can be highly subjective. SPs will often treat this information as useful context but not make decisions based upon it.

5.1.3 Informal Structured

ISP & Entity Relationship	Informal, structured, information sharing between two entities with no defined relationship
Relationship Type	Informal - structured
Information that is Shared	To whom: Typically, this involves the service provider downloading information from a publicly available source. There is almost never data sharing back.
	Content & Value: Content is machine-readable IOCs. The format may be as simple as CSV files delivered over HTTPS, or it may be as complex as STIX delivered over TAXII.
	Timeliness: This may be anything from real time in the case of automated detection systems or sinkholes to weeks delayed in the case of manual investigation.
	Sharing Process: The process varies depending on the source of the data and the technology they have chosen.
Benefits of Information Sharing	Compromises prevented or at least identified. Vulnerabilities revealed, potentially prior to exploitation. Effective for conveying ecosystem-wide threats. Can be used for victim notification in the case where a vendor sends an ISP lists of compromised customer IPs.
Gaps in Information & Process	Every source has a different format for their data and a different method of delivery. Every source requires custom integration. Quality of data varies, and a sense of “you get what you pay for”.
Barriers & Challenges	Lack of contract means data is by default provided best effort Integration is costly and time consuming. Contextual data is often missing. E.g. an IP is listed as bad, but there’s no further information as to why it is bad or how a SP can determine whether a detection is a false positive.

5.1.4 Informal Unstructured

ISP & Entity Relationship	Informal, unstructured, information sharing between two entities with a casual, undefined relationship.
Relationship Type	Informal - unstructured
Information that is Shared	To whom: This may involve SP – SP, SP – customer and/or SP to vendors/partners.
	Content & Value: Content may be derived from conversations or simple communications such as email.
	Timeliness: This may be either real time (conversations) or near real time (email).
	Sharing Process: The delivery method will vary based on the relationship of the ISP and the source in addition to the nature of the data being shared. The higher the degree of sensitivity the more likely that the sharing method will be verbal. The less sensitive the data the more likely that it will be shared via email or other electronic means.
Benefits of Information Sharing	Compromises prevented or at least identified. Vulnerabilities revealed, potentially prior to exploitation. SP – SP conversations often lead to enhanced understanding of threats as they relate to the SP environment. Heightened awareness.
Gaps in Information & Process	There is no formal process. The nature of this sharing is ad hoc. Often it is best used for awareness and not as an input for automated tools. Quality of data varies, and there is no standard to assess that quality.
Barriers & Challenges	Validating the data is a major concern. Information shared in conversation and email can be highly subjective. SPs will often treat this information as useful context but not make decisions based upon it.

5.2 Private/Government Sharing

Sub-group 2 was tasked with developing use cases for private to government and government to private sharing. The subgroup developed several use cases to provide examples of how the communications sector shares with government to address cyber threats. The list of use cases includes the following. Each of these use cases is provided in Appendix A to this document. It should be noted that these example use cases are not intended to be all inclusive but to cover a range of examples raised by both the industry and the FCC during the working group.

EAS Service Disruption
Data Breach Investigative Report

Foreign Government to U.S. Industry
TDOS Government and Industry Use Case
Heartbleed
NCFTA Government and Industry Use Case
Government to Industry Solar Flares
Hacktivist Threats to Law Enforcement and Public Officials
Qakbot Botnet
Social Engineering

6. BARRIERS TO INFORMATION SHARING

6.1 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 existing cyber threat information sharing landscape, as illustrated below, is complex and, therefore, may be challenging to navigate, especially for those previously unfamiliar with the breadth and depth of entities noted below. Further, the proliferation of sharing entities and arrangements threatens to dilute resources and expertise through redundant or conflicting activities and objectives. Several communications operators and trade associations are part of existing information sharing trust pools convened in coordination with the Federal government including the Communications-ISAC, which is coordinated by DHS via the NCC. The Communications-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) that will emerge in connection with effectuation of President Obama's 2015 Executive Order on information sharing.

Communications companies also will be working with the DHS AIS portal, which is designed to facilitate real-time sharing of cyber threat indicators with DHS's NCCIC. The Cybersecurity Information Sharing Act of 2015 (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 with the Hunt and Incident Response Team (HIRT), the computer emergency readiness team, which is part of NCCIC. 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 the driving force behind a variety of information sharing activities. Companies also may be involved with the FBI-National Cybersecurity Industry Joint Task Force (NCI-JTF) and InfraGuard, which are 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 ISAO Executive Order. 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. These existing trust pools should also be publicized across the sector so that organizations of all sizes are aware and informed of the opportunity to participate.

Regarding existing private-to-private trust pools, industry members may be involved in several 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 (M3AAWG). Sector companies also enter into contractual arrangements with third-party security vendors for the receipt of threat data and tactical response information.

However, organizational impediments generally continue to exist in the private-to-private venue. Trust relationships have traditionally formed the basis for information sharing, but require resources 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. However, these events may not be widely publicized to communications sector companies. As such, some organizations, and in particular, SMBs may not be aware of these events, may not be invited to attend, and/or may not have the resources to participate. Continued development and use of ISAOs and ISACs may alleviate some of these organizational barriers, particularly for SMBs.

The distribution of classified information from government to private sector partners also may 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 consider the trustworthiness of the recipient, the sensitivity of the shared information, and the potential impact of sharing (or not sharing) 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 also has 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 should 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.

6.2 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. Filtering the many sources of threat intelligence, validating what is applicable, and then defining the priority to implement can be complex and time consuming. This is especially pertinent for SMBs, which face cybersecurity workforce challenges. For instance, service providers located in rural and remote regions often have difficulty attracting and retaining employees, especially those with much-needed technical expertise. Further, at small company employees often wear many different hats, and as such, the company may suffer from a lack of internal resources with the time and technical skill sets required to contribute to the larger information-sharing environment. In addition, an operator may lack sufficient financial support to fully engage in the more formal or structured categories or mechanics of info sharing. Further, SMBs may not be aware of the existence of more formal information sharing venues, especially those that are operated by the private sector and accessed via exclusive invitation.

For larger and more complex organizations, changes in operations 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 in live or proactive protection efforts. Refining intelligence too hastily, however, can result in unreliable or unusable intelligence. Striking the right balance is essential.

6.3 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 also can 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. This limits the quality of information shared. More detailed, validated data is shared among members within the same sector when the information is shared through a dedicated portal. Those who are not members of the sector or who don't have access to the portal may receive information that is generalized, or 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 other 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 working 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 infancy. Standards, tools, protocols, and best practices recommendations are being discussed, developed, and are starting to be implemented. As legislators and policy-makers have recognized repeatedly, this is not an area conducive to backward-looking, static, one-size-fits-all prescriptive regulation. Additionally, metrics should not be imposed by policy-makers with the intention of providing a relative measure of information sharing effectiveness. Such metrics are not likely to be accurate or effective. 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. The working group firmly believes that the public-private partnership and cross-sector initiatives and coordination aimed at generating industry-driven solutions to the technical challenges to sharing continues to be the best way to address those challenges.

6.4 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 as insight into use of information after it leaves the system is important to managing consumer expectations and allaying fears about information sharing. Not only is it necessary It will become increasingly important for organizations to identify and protect consumer information in accordance with applicable law and consumer expectations, but it is becoming increasingly important as well as to educate consumers about protections related to cyber threat 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.

6.5 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 formats. Financial resource restraints are most acute for SMBs within the communications sector, which 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. At base, lack of sufficient monetary resources negatively impacts a company's ability to participate within both public and private information sharing trust pools. However, the solution to these issues is not to discourage commercially-available threat intelligence capabilities and proprietary information sharing tools and services, since the existence of such offerings often provides the most up-to-date information and facilitates reaching the most agile solutions to real-time threats and vulnerabilities. Threat intelligence and threat analysis are properly viewed as business resources that are the product of recurring investment and training, and preserving the incentive to invest in such capabilities is critical to the overall health of the ecosystem.

6.6 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 for the "protection of the rights or property of the provider," among other things, 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. Further, the overall nature of ECPA is to restrict sharing and in many cases the use of information is dependent upon customer consent, which could in some circumstances limit 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 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 (CISA), which represented Congress' attempt to develop a clear legal framework to information sharing, was intended to address several these issues.

Joint guidance from the Department of Justice and the Federal Trade Commission issued in 2014, the "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. 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 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 relief provided by CISA from legal liability concerns under certain circumstances is not absolute or unqualified. Thus, 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 broadband privacy rules NPRM and CISA. While the Commission's broadband privacy Order clarified that any sharing of information permitted under CISA would not be restricted by its broadband privacy rules, those rules constrain use and sharing of IP addresses, device identifiers, and other customer and device-related metadata that the Justice Department guidance makes clear are expected to be shared regularly under CISA. Companies may share cyber threat indicators for a "cybersecurity purpose" under CISA. 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. Further CISA does not directly and specifically address potential common law risks associated with actions (or inactions) in response to receiving (or not receiving) shared cyber threat information.

Moreover, the authorization to share under CISA carries with it the obligation to remove personal information not directly related to a cyber threat, which inevitably introduces delay into the process, as well as uncertainty since the concept of "personal information" can vary among different privacy regimes applicable to different industry sectors. And there remains considerable uncertainty and risk with respect to the sharing of defensive measures under CISA, due to the removal of liability protection for any shared defensive measure that causes harm to another network or data on such other network. Further, there are also concerns about the extent to which CISA's liability protections extend to sharing relationships with the government other than via AIS or the NCCIC web and email portals. 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.

7. Information Sharing Trust Pools

7.1 Definition

Information sharing trust pools are appropriately scoped groups based on communications sector needs and capabilities within the cybersecurity community who may identify, assess, analyze, and/or develop recommendations and potentially take action to share information. Information sharing trust pools encourage and enable the sharing of cybersecurity information across the communications sector to all stakeholders necessary to successfully execute the "protect, detect, respond, and recover" functions of the NIST Cybersecurity Framework.

7.2 Characteristics of Information Sharing Trust Pools

Information sharing trust pools come in a variety of sizes for a variety of missions, use multiple types of operational strategies and cover an undetermined length of time. It should be noted that how they perform or even unite for a purpose also varies. And, while all types have in common the need to share information in a trustworthy manner, they cannot be fit into a mold where one size of trust pool fits all requirements. Some of the key characteristics of trust pools are as follows.

- Participants define trust to include confidentiality, meaning that information is shared within a specific environment or regime responsibly, without leakage or retribution, and that only appropriate/authorized people have access to the information.
- Participants are stakeholders with common interests/goals, capabilities, and ownership (the ability and capability to initiate change affecting the group).
- Participants within a trust pool are credible members building on an initial informal relationship based on the common scope of interest.
- The trust pools have a rally point, focus area, or purpose to unite for a common mission and utilize subject matter experts to act upon the needs of the group.

7.3 Examples of Information Sharing Trust Pools

Entities including, but not limited to, those discussed here are examples of information sharing trust pools participating within the Communications sector. They are broken into two categories: operator and sector. Operator level trust pools encompass those groups which may be informal or non-structured and more easily accessible for small to medium sized business members. Sector level trust pools represent formal and structured groups encompassing all sizes of businesses as well as all government levels.

7.3.1 Operator Trust Pools

- **US Telecom Cybersecurity Working Group** was established in 2004 as the focal point for member engagement and information sharing related to Cybersecurity strategic, operational and planning activities, supporting the wireline communications sector. The group includes policy and technical representatives from wireline service providers of all sizes and discusses the multitude of industry and public-private partnership initiatives across the entire government landscape. The Working Group has served as the primary vehicle for establishing policy positions on regulatory and non-regulatory matters and provides the association with guidance that is used to represent industry interests in discussions with government officials and legislators.

- **CTIA/CTIA Cybersecurity Working Group – The US Wireless Association,** originally known as the Cellular Telephone Industries Association, is an industry trade group representing all wireless communication sectors including cellular, personal communication services and enhanced specialized mobile radio. CTIA sponsors the CTIA Cybersecurity Working Group (CSWG), comprised of leading industry security experts from across the wireless ecosystem to address the mobile cyber threat landscape. Established in June 2012, CSWG sponsors key cybersecurity initiatives such as an automated Cyber-Threat Information Sharing Pilot, as well as advanced technical research programs targeted at cyber-threat trends and coordination amongst wireless companies and with government agencies. One of the principle findings from the information sharing pilot is that the current STIX and TAXI schema in use by DHS may not support all of the telecom use cases analyzed in the pilot. Thus the STIX and TAXI schema needs to be extended or adapted to support telecom use cases and this limits the communications sector's ability to share communications network related cyber threat indicators under the current model.

- **NCTA – The Internet & Television Association/NCTA Cybersecurity Working Group.** The NCTA is the principal trade association for the U.S. cable industry, representing cable operators that deliver digital services to consumers and businesses throughout urban and rural America and more than 200 cable program networks that product TV's most creative and popular shows. NCTA's Cybersecurity Working Group was established in 2012 and is the focal point for member engagement and information sharing related cybersecurity strategic, operational, and planning activities for the cable sector. The group includes policy and technical representatives from its member companies and cybersecurity experts from CableLabs.

- **A Network Service Provider (NSP)** is a business or organization that sells bandwidth or direct network access to the Internet and usually access to its network access points. Also known as Internet Service Providers (ISPs), NSPs may consist of telecommunications companies, data carriers, wireless communications providers, and cable television operators offering high-speed Internet access.

- **Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) –** This global organization formed in early 2004 is a technology-neutral, non-political working body focused on operational issues of Internet abuse including technology, industry collaboration and public policy. The group's purpose is to bring industry together to work against bots, malware, spam, viruses, denial of service attacks and other online exploitation. With a membership which

includes Internet Service Providers (ISPs), telecommunications companies, Email Service Providers (ESP), social networking companies, hardware and software vendors, major brands, major antivirus vendors and security vendors, M3AAWG develops and publishes best practice papers, position statements, training and education videos, and other materials to help the online community fight abuse with a focus on operational practices.

- **California Utilities Emergency Association (CUEA)** serves as a point of contact for critical infrastructure utilities and the California Office of Emergency Services (Cal OES) and other Governmental Agencies before, during and after an event to facilitate communications and cooperation between member utilities and public agencies; and with non-member utilities; to provide emergency response support for electric, petroleum pipeline, telecommunications, gas, water and wastewater utilities; and to support utility emergency planning, mitigation, training, exercises and education. CUEA was chartered by the Governor of California in 1952 as part of the State's Civil Defense Plan, growing from a four-member group to include nearly 100 members and geographically covering the entire state of California.

- **Informal Information Networks of Trust –** Preceding the very earliest days of the Internet, in the ARPANET era, operational issues across networks including security arose routinely. Early operators would exchange messages, typically via e-mail, with colleagues responsible for other networks to solve such problems. To this day, informal sharing continuously occurs between professionals within different organizations that know and trust each other to assist in security responses. In order to make such informal communications more efficient several security mailing lists were formed which number into the hundreds. These include open mailing lists that anyone can join and closed lists where a moderator will invite or review requests for membership. All manner of security topics may be discussed from vulnerabilities and patching to investigations of particular botnets or malicious actors.

- **Vetted Security Communities –** In the early 2000's, with the rise of e-crime, informal security mailing lists and communities began creating more formal rules of membership and adopting important concepts such as formal vetting processes, membership criteria, and mission statements. These groups may focus on one particular issue (e.g. the DNS Changer Working Group coordinated the handling of the response to the DNS Changer malware) or tackle general security issues that may affect network operators, software vendors, government bodies, or any organization. In such groups, existing members follow criteria to carefully expand membership while providing vetting in three main realms – sphere of trust, sphere of action, and need to know. While no formal organization typically exists that manages these communities, these groups are still highly organized and generally infer trust transitively via their membership activities. This trust is based on individual rather than organizational trust and is supported by the network of trust inherent in the combination of one-to-one trust relationships.

- **Information Sharing and Analysis Organizations (ISAOs)** – An ISAO is a group created to gather, analyze, and disseminate cyber threat information through a more flexible, self-organized approach of information sharing activities amongst communities of interest such as small businesses across sectors: legal, accounting, and consulting firms that support cross-sector clients, etc. In February 2015 Executive Order 13691 was issued directing the Department of Homeland Security (DHS) to encourage the development of ISAOs. The ISAO

Standards Organization is currently collaborating with public and private sector entities to form an official definition of ISAO.

7.3.2 Sector Level Trust Pools

- **Anti-Phishing Working Group (APWG)** is the coalition unifying the global response to cybercrime across industry, government and law enforcement sectors and nongovernment organization (NGO) communities. APWG manages three parallel enterprises including clearinghouses for cybercrime-related machine event data to inform members on security applications, forensic routines, and research programs; an annual symposium on electronic crime research; and an international cybersecurity awareness campaign (STOP.THINK.CONNECT). Established in 2003, APWG conducts its mission through: a US-based 501(c)6 organization; the APWG.EU European chapter (established in 2013), a non-profit research foundation incorporated in Spain and managed by an independent board; and the STOP. THINK. CONNECT. Messaging Convention, Inc., a US-based non-profit 501(c)3 corporation. Membership is open to financial institutions, retailers, solutions providers, ISPs, ESPs, telephone companies, defense contractors, law enforcement agencies, trade groups, treaty organizations, researchers in relevant fields of study and government agencies.

- **The Communications Sector Coordinating Council (CSCC)** fosters and facilitates the coordination of sector-wide policy-related activities and initiatives designed to improve both the physical and cyber security of the communications critical infrastructure. CSCC, chartered in June 2006, represents the communications sector within cross-sector/interdependency matters, including provision of representation to activities such as the ANSI Homeland Security Standards Panel, the Critical Infrastructure Partnership Advisory Council (CIPAC), National Infrastructure Advisory Council (NIAC) Working Groups, and the Partnership for Critical Infrastructure Security. CSCC improves equitable information sharing among and/or between the communications sector, sector members, government entities, and other industry sectors. The basis for CSCC's coordinated approach is Homeland Security Presidential Directive 7 (HSPD-7) and the National Infrastructure Protection Plan (NIPP).

- **Cyber Ecosystem Key Players** represent the functional capabilities—services and operations shared and used throughout the world—which have broad visibility of the global environment, deep technical expertise within their functional space, and an understanding of the roles and functions of numerous enablers within the community. Their customer base drives their activities towards ensuring all customers have full access to the capabilities and services they provide and they take significant care to ensure even-handed treatment of their global customer base. Because of the variance in non-disclosure and privacy laws globally, cyber ecosystem key players generally choose to operate under stricter non-disclosure and privacy environments than entities operating within only one national border. Given the interconnectedness of the cyber ecosystem, a cyber-attack against any two key players either independently or in close proximity gives rise to systemic consequences. In such cases a cyber incident(s) of significant magnitude would require a concerted response beyond a single enterprise or sector. These cyber ecosystem key players utilize their independent, dedicated computer security incident response teams to maintain functionality but also have dedicated security incident response teams for product lines or commercial networks to ensure global service continuity. Additionally, they share global product and service information through tightly controlled private sector trust groups.

- **Forum for Incident Response Teams (FIRST) –** FIRST is a global organization of incident response teams from government, military, commercial and educational organizations fostering cooperation and coordination in incident prevention, stimulating rapid reaction to incidents, and promoting information sharing among members and the community at large. Formed in 1990 in response to a major incident called the "Wank worm," FIRST provides value added services such as access to up-to-date best practice documents, technical colloquia for security experts, hands-on classes, an annual incident response conference, publications and web services, and special interest groups. FIRST members include 356 teams (72 in the US) and 77 countries.

- **Government Coordinating Councils (GCCs) –** GCCs are formed as the government counterpart for each Sector Coordinating Council (SCC) to enable interagency and cross-jurisdictional coordination. The GCCs, including one specifically for the Communications sector, are comprised of representatives from across various levels of government (federal, state, local, or tribal), as appropriate to the operating landscape of each individual sector. They coordinate strategies, activities, policy and communications across government entities within each sector to include providing interagency strategic communications and coordination at the sector level, participating in planning efforts related to the development, implementation, update and revision of the National Infrastructure Protection Plan (NIPP) and the Sector-Specific Plans (SSPs), coordinating strategic communications, discussion and resolution of issues among government entities within the sector, and coordinating with and supporting the efforts of the SCC to plan, implement, and execute the nation's critical infrastructure protection mission.

- **Information Sharing and Analysis Centers (ISACs)** are nonprofit organizations that provide a central resource for gathering information on cyber threats to critical infrastructure and providing two-way sharing of information between the private and public sectors.

- **Multi-Association Framework Development Initiative (MAFDI) –** The initiative, co-chaired by the US Telecom Association vice president and the Information Technology Industry Council vice president, includes 32 US-based trade associations. The MAFDI group's four key goals are: (1) to include engaging multiple stakeholders in coordinating views of the use and evolution of the NIST framework and any external factors that could affect the viability of the model; (2) to share information across sectors on specific NIST framework activities and experiences with regulators and other stakeholders; (3) to work to promote the framework as an international model; and (4) to bring key influencers from government to hear their perspectives, learn of new initiatives and share industry interests and concerns.

- **National Coordinating Center for Communications (NCC),** as part of the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC), is the Communications ISAC. The White House designated NCC as an ISAC in January 2000 in accordance with Presidential Decision Directive-63. It continuously monitors national and international incidents and events that may impact emergency communications and facilitates the exchange of vulnerability, threat, intrusion and anomaly information amongst government and industry telecommunications participants. Incidents include not only acts of terrorism, but also natural events such as tornadoes, floods, hurricanes, and earthquakes. In cases of emergency, NCC functions as national coordinator for emergency communications response and recovery efforts under Emergency Support Function #2 of the National Response Framework. NCC works with both the US Computer Emergency Response Team (US-CERT) and

the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) to monitor and resolve issues impacting cyber and communications during an emergency. The NCC joint government and industry partnership consists of over 60+ communications sector entities comprising expertise from wireline, wireless, cable, broadcast, satellite, equipment manufacturers, and associations.

- **National Council of ISACs** (**NCI),** formed in 2003, is a coordinating body designed to maximize information flow across the private sector critical infrastructures and with the government. NCI comprises 24 organizations designated by their sectors as their information sharing and operational arms. Sharing and coordination are accomplished through daily and weekly calls between ISAC operations centers, daily reports, requests for information, monthly meetings, exercises, and other activities as situations require. NCI also organizes its own drills and exercises as well as participates in national exercises. Council members are present on the National Cybersecurity and Communications Integration Center (NCCIC) watch floor, are embedded with the National Infrastructure Coordinating Center (NICC) during significant incidents, and collaborate with other federal government agencies, fusion centers, the State and Local Tribal Territorial Government Coordinating Council (SLTTCC), the Regional Consortium Coordinating Council (RCCC), the Partnership for Critical Infrastructure Security (PCIS) and international partners.

- **National Cyber-Forensics & Training Alliance (NCFTA)** – NCFTA, founded in 2002, is a non-profit corporation focused on identifying, mitigating, and neutralizing cyber-crime threats globally by conducting real time information sharing and analysis with subject matter experts in the public, private, and academic sectors. Collaboration with national and international partners across private industry, law enforcement, government and academia has resulted in criminal and civil investigations which otherwise may not have been addressed. NCFTA provides physical and remote forums to meet with public, private and academic partners; dedicated and trained staff who specialize in respective initiatives; focused meetings and events for each initiative; intelligence feeds built and maintained by NCFTA; monthly initiative calls including trend updates, law enforcement efforts and intelligence gaps needing attention; contacts to help inform and encourage coordination amongst public and private sector partners; and assessments and reports based on NCFTA intelligence, including focused benchmarking and success metrics for each initiative.

- **Network Security Information Exchanges (NSIE)** – Industry and Government coordinate through NSIE, which was formed in 1991 as a subcommittee of the Network Security Telecommunication Advisory Committee (NSTAC), to voluntarily share sensitive information on threats to operations, administration, maintenance, and provisioning systems supporting the telecommunications infrastructure. Government NSIE members include departments and agencies that use national security and emergency preparedness (NS/EP) communications services, represent law enforcement, or have information relating to network security threats and vulnerabilities. The President's NSTAC NSIE representatives include industry subject matter experts engaged in prevention, detection, and/or investigation of communications software penetrations or who have security and investigative responsibilities.

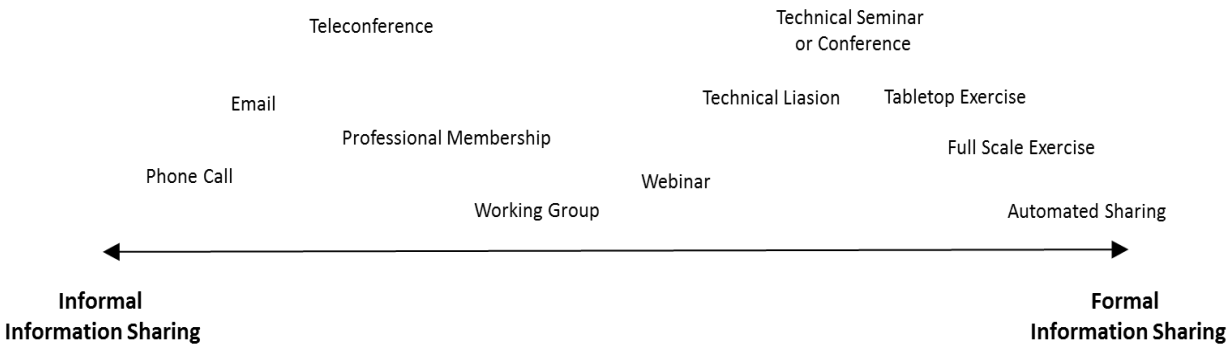
- **Sector Coordinating Councils (SCCs)** are self-organized and self-governed councils that enable critical infrastructure owners and operators, their trade associations, and other industry representatives to interact on a wide range of sector-specific strategies, policies, and activities. The SCCs coordinate and collaborate with sector-specific agencies (SSAs) and related Government Coordinating Councils (GCCs) to address the entire range of critical infrastructure security and resilience policies and efforts for that sector.

8. Conduits for Information Sharing

For the purposes of this report the working group defined "conduits" as the following: a means by which something is transmitted[1]; a channel through which anything is conveyed[2]; an agency or means of access, communication, etc.[3] Based upon this definition there are many conduits for information sharing within the communications sector ranging from informal items such as phone calls, emails, distribution lists to more sophisticated formal automated sharing such as that conducted by DHS. In its previous efforts to develop use cases, the working group found that information follows as a stream from informal to formal. Simple items such as phone calls or emails represent the most informal with automated machine to machine sharing representing the most formal arrangements.

As noted above there are a variety of mechanisms for sharing information ranging from informal items such as a phone call, email, distribution list, teleconference, meeting, briefing, professional membership, working group, professional conference, online seminar, technical liaisons, technical seminars or conferences, tabletop exercises to more formal items such as automated information sharing. Table 1 below lists the various forms of information sharing ranging from informal to formal:

Table 1: Mechanisms for information sharing from informal to formal



A **telephone call** between two people who may be business acquaintances is the most informal way of sharing information. A phone call would be used in a situation where basic information should be shared, i.e., whether either party is aware of open source reporting (i.e., on the radio or television) about a cyber-attack and whether the attack affects them.

[1] American Heritage Dictionary of the English Language, Fifth Edition. Copyright © 2011 by Houghton Mifflin Harcourt Publishing Company. Published by Houghton Mifflin Harcourt Publishing Company. All rights reserved.
[2] Random House Kemerman Webster's College Dictionary, © 2010 K Dictionaries Ltd. Copyright 2005,1997, 1991 by Random House, Inc. All rights reserved.
[3] Collins English Dictionary—Complete and Unabridged, 12th Edition 2014 c HarpersCollins Publishers 1991, 1994, 1998, 2000, 2003, 2006, 2007, 2009, 2011, 2014

Using **electronic mail** between the two parties is the next most informal avenue. An email could be used when the two parties wish to share slightly more detailed basic information, i.e., one organization wishes to share information to remedy a type of cyber-attack with another related to a specific cyber-attack which affected one organization and may have affected the other organization. Of course information sharing through email can be transmitted from one to several parties or more formally through a distribution list of participants. When more than one organization is involved in the specific cyber event, information regarding the event and precautions or practices to alleviate the issues resulting from the event can be shared among trusted partners. This occurs when members of a trust pool contact each other and a government entity.

These participants can take the information sharing to a concerted organizational level through a designated bridge for a **teleconference**. A teleconference may be convened when a cyber or physical event requires discussion and coordination among the affected parties, whether industry or government entities. The next step would be a face to face meeting among participants. At a briefing, a subject matter expert could share information with several participants with a need to know and a shared understanding. A meeting or briefing may occur to provide information to participants because of an event or in anticipation of an event to coordinate organizational activities which may affect a large population.

Professional membership in an organization, i.e., one of the recognized trust pools, provides a more concentrated focus. Information sharing through professional membership occurs when some, most or all members of the profession may be affected by an event. A **working group** -- an ad hoc group of subject matter experts in the same industry working together to achieve specified goals -- may come together regarding a domain and focus on discussion or activity around a subject area.

At a **professional conference**, subject matter experts may share information pertaining to their profession as well as a cyber or physical event. Because all the professionals may not be available to attend a conference, a webinar-- a seminar or other presentation that takes place on the Internet allowing participants in different locations to see and hear the presenter, ask questions, and sometimes answer polls -- also provides a means for the information sharing process. A **webinar** may be initiated to provide professionals with best practices or lessons learned as the result of a cyber-attack.

In a **technical liaison relationship**, a subject matter expert from an organization provides technical expertise to communicate and coordinate activities, i.e., share cybersecurity information, with another organization with the goal of resolving an issue or event. Technical liaisons generally occur in conjunction with a cyber event or may be initiated because of a cyber event. The organization's liaison officer may be collocated at a security operations center as part of a memorandum of agreement between the organization and the center.

A **technical seminar or conference** may be convened to discuss an event or issue among liaison officers. Such a seminar or conference may occur because of one or more cybersecurity events affecting several critical infrastructure organizations and government entities. Because this type of information sharing opportunity may require extensive collaboration and coordination, lead time for this activity may be several months after the occurrence of the event or issue.

Thus, or because of the likelihood of a cybersecurity event, a **tabletop exercise** involving executives of various organizations and government entities may provide strategic information sharing. A **full scale exercise** involving likely affected organization liaison officers and government entities provides the

best opportunity for practicing the information sharing process. As with the technical seminar or conference, a tabletop or full scale exercise may require several months to a year to organize and execute.

The ultimate means of sharing cybersecurity information and the most formal would be an organization's application for membership in and use of an **automated information system** such as Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII). STIX and TAXII are community-driven technical specifications designed to enable automated information sharing for cybersecurity situational awareness, real-time notification, and response. Information shared through an automated system is validated before distribution.

8.1 Information Sharing Conduit Examples

The following are a few real world examples of information sharing using both industry and government entities. In the first example, an industry engineer discovered the Heartbleed vulnerability and, after committing and applying a patch, shared the information with an international organization via email. The international organization used a distribution list to send out an advisory sharing the information. A government entity used the advisory to post a technical alert to its portal, to which trusted partners had access. Information regarding this vulnerability led to convening a trust pool members' meeting and associated teleconference. To further share information about the vulnerability, a government entity used a distribution list to request information on confirmed exploits from trust pool members. Once the vulnerability was patched by more affected government and industry partners, another government entity conducted webinars on the vulnerability, sharing analysis and mitigation actions.

In another example of the information sharing process, a foreign government's commercial banks and government agencies experienced heavy distributed denial of service attacks from over 150 countries and contacted its government computer emergency response team. The foreign government computer emergency response team (CERT) contacted by email through an international cyber organization distribution list the US Computer Emergency Readiness Team for mitigation assistance, providing the pertinent attacking information for cross data analysis. US-CERT notified via email another US government entity, the Communications ISAC, which in turn contacted the potentially associated sector members via email. Sector members researched and identified the problems and implemented mitigation strategies to alleviate the attacks. Once mitigation was completed, the US-CERT emailed and telephoned the foreign government CERT to ensure the activity had ended.

8.2 Information Sharing Conduit Challenges

There are some challenges related to sharing information, most of which result from scalability concerns. These issues appear to shape the cybersecurity information sharing processes for the communications sector. Table 2 Challenges and Scalability, provides lists of proactive and conflicting issues which the working group recognizes.

Table 2: Challenges and Scalability

PROs	CONs
Established trust pools support through personal relationships	SMBs may have neither dedicated, on-staff cyber personnel nor capital to expend
Use cases provide evidence of previous info sharing activity and substance for increasing and improving incident response	Desired degree of information sharing attention may not be realized until cost benefit can be justified for SMBs
Use cases include annual cybersecurity incident study, incident responses and various exercises involving private sector and/or government entities at state, regional, national, and international levels	Need for additional cybersecurity personnel will strain availability as more private sector/government entities participate, especially personnel with security clearances
For networks with less (relative) traffic, anomalies/incursions may be easier to detect, thereby shrinking operator and industry response time	

The list of issues above is not intended to be all inclusive but highlight some of the main challenges identified by the working group.

8.3 Future Activities

With all private sector partners, and especially in the case of SMBs, the capabilities to fully engage in a two-way information sharing process are dependent on upon cost effectiveness and workforce availability for each business. Many SMBs may currently participate as consumers of information through informal means (personal/professional relationships) instead of formal means (organized trust pools which cater to larger private sector partners).

The creation and increased use of ISAOs and the establishment of the ISAO Standards Organization in October 2015, may improve the nation's cybersecurity posture regarding SMB involvement. ISAOs may provide an information sharing link between the government and SMBs. The ISAO Standards Organization may help with this effort by identifying standards and guidelines for robust and effective information sharing and analysis related to cybersecurity risks, incidents, and best practices.[4]

For their part, government entities and larger private sector partners may continue to use the identified trust pools and the array of cybersecurity legislation and guidelines to further enhance and refine information sharing processes. As necessary, additional trust pools, cybersecurity legislation[5], [6] and other guidance may evolve to further define and refine the cyber environment

[4] ISAO Standards Organization, https://www.isao.org/ viewed 19 August 2016.
[5] U.S. law enforcement and intelligence officials said on 15 September 2016, they are building legal cases to respond to growing Russian attempts to disrupt and discredit the November elections without sparking an open confrontation with the Russian President. See http://www.reuters.com/article/us-usa-cyber-russia-idUSKCN11M00H, viewed 19 September 2016.
[6] The National Bank of Belgium, the New York Fed, and the Society for Worldwide Interbank Financial Telecommunication (SWIFT) this summer set up a task force with representatives from some 25 central banks to set cybersecurity standards around inter-bank transfers that may be adopted globally. The new principles or guidance could cover responsibilities of banks that send and receive

and, in succession, information, and the sharing processes. Human to human information flow processes may continue to be supplemented with machine to human information flow processes. Machine to machine information flow processes also may be added as the cost or benefits are discovered and the value of and need for additional information flows are realized and incorporated as part of the business model for all entities.

8.4 Technology

Finally, the working group discussed the various technologies available to facilitate information sharing. For information flow processes involving machines, available structures and platforms include automated information systems (AIS), such as Structured Threat Information eXpression (STIX), and Trusted Automated eXchange of Indicator Information (TAXII). STIX, a collaborative effort to develop a standardized, structured language to represent cyber threat information, conveys the full range of potential cyber threat elements and strives to be expressive, flexible, extensible, automated, and human-readable. TAXII, a set of services and message exchanges, empowers organizations to share the information they choose with partners they choose.[7]

These technological means have the potential to be instrumental in sharing information among private sector and government entities. However, the working group finds, while the technology is beneficial, it is still developing. For instance, the STIX and TAXII schemes are not structured to share telecom-specific use cases, and will need to be customized for the sector's needs. Further, AIS is often time intensive to set up and requires significant monetary resources. As such, Currently, it is suited to large businesses and government entities;[8] SMBs remain inhibited by resource constraints.

Finally given the diversity of sharing that is currently underway in the sector, policymakers should be careful not to artificially constrain these activities by attempting to force all sharing through the AIS portal or via government and DHS. What is important is that information is being shared. Government should encourage all forms of sharing and the protections afforded via CISA should apply when sharing meets the requirements of the statute. As a policy matter attempting to push sharing via government could have a limiting impact contrary to the overall goal of the legislation.

money transfers and networks like SWIFT that transmit payment instructions in correspondent banking. This is in response to the 81 million dollar Bangladesh bank heist. See http://www.reuters.com/article/us-cyber-heist-basel- taskforce-idUSKCN11L269, viewed 19 September 2016.

[7] Information Sharing Specifications for Cybersecurity, https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity, viewed 30 Aug 2016.

[8] As of 27 Sep 2016, about 50 agencies, private companies and organizations have joined the DHS automatic information sharing network, STIX/TAXII. http://federalnewsradio.com/cybersecurity/2016/09/dhs-50-agencies-private-companies-cyber-information-sharing-network/, viewed 28 Sep 2016.

9. Recommendations

The goals and objectives of this report were to improve the communication sector's ability to identify, protect, detect, respond, and recover from cyber-attacks through information sharing and to develop recommendations to encourage sharing of cybersecurity information between companies in the communication sector and government agencies. After careful consideration of the details noted in the use case examples and the barriers to information sharing sections, the working group has identified the following generic and encompassing recommendations.

- The FCC should acknowledge the breadth and depth of cyber-threat information sharing that currently takes place between and among industry and government entities, and recognize that DHS is leading in government information sharing with the private sector. To the extent the FCC wants to participate in information sharing it should do so in the context of the broader efforts organized by DHS and not duplicate efforts within the FCC.

- Industry should continue its efforts to conduct and expand on the current pilot that it has underway regarding information sharing using STIX/TAXII, and determine if these protocols meet the needs of communications sector. Industry should also explore the opportunities and challenges related to sector-wide operational use of DHS' Automated Indicator Sharing (AIS) portal.

- Industry should enhance the Communications ISAC by developing a hosted, private website on which government entities, industry partners, and stakeholders representing SMBs may register to access a cybersecurity resource repository and message board. At the same time, the ISAC should consider the best means to encourage international involvement in information-sharing processes balanced against the challenges outlined in this document.

- The public and the private sector should continue to work together to develop, promote, and enhance cybersecurity education and awareness within the sector, including by educating SMBs regarding the depth and breadth of existing venues that offer cyber-threat information-sharing opportunities.

- The government should explore a grant program to provide funding to SMBs so that they may obtain or develop resources necessary to robustly participate in the cybersecurity information sharing ecosystem.

- There is currently a considerable amount of threat intelligence gathering and client-tailored information sharing provided on a proprietary basis by commercial entities. Policy makers should continue to encourage and support such sharing. Proprietary information sharing tools and managed security services that incorporate this information provide a reliably agile, effective, and innovative mechanism to both heighten awareness of cyber threats and tactics and can play a role in mitigating attacks.

APPENDIX A: PRIVATE TO GOVERNMENT USE CASES/EXAMPLES

1. EAS Service Disruption

Description	Poor password security allowed hackers to broadcast a bogus warning on TV networks. The FCC published an urgent advisory to change passwords on all manufacturers' equipment that forces emergency broadcasts on television networks, interrupting regular
	programming and to ensure the gear was secured behind firewalls. They should also inspect systems to ensure hackers had not queued "unauthorized alerts" for future transmission.
ISP & Entity Relationship	Industry to Government
Relationship Type	Formal - structured
Information that is Shared	To whom: Communications ISAC members and Government
	Content & Value: Emergency Alert System for three MI television stations breached, sending audio messages of zombie citing and avoidance alerts (hacking)
	Timeliness: Contacted Michigan Association of Broadcasters, State Police, and FCC same day
	Sharing Process: Email notification from TV stations to MAB, police and FCC as well as NCCIC/NCC
Benefits of Information Sharing	Research, identification, and mitigation of the problem at affected stations and notification of other stations to mitigate possibility of the problem being repeated
Gaps in Information & Process	None
Barriers & Challenges	Contacting all stations nationwide to reset passwords from the factory standard; message could have involved a different code causing public concern and/or panic

2. Data Breach Investigative Report

Description	An annual report presenting the threats, vulnerabilities and actions that lead to cyber security incidents and how those incidents impacted victim organizations
ISP & Entity Relationship	Industry to Industry; Industry to Government
Relationship Type	Formal structured
Information that is Shared	To whom: Industry and Government

	Content & Value: For calendar year 2014, 70 contributing organizations provided information on 79,790 security incidents with 2,122 confirmed data breaches affecting organizations in 61 countries
	Timeliness: Annual report shared on a regular basis provides trend analysis from year to year since 2004
	Sharing Process: Gathered data from individual organizations, reviewed and converted into a framework to create a common, anonymous aggregate data set, then wrote and published report through open sources
Benefits of Information Sharing	Shows changes in aspects of the threat space, longer term trends and findings while providing a traditional focus on interesting developments over the previous year. Provides communication providers (small, medium, and large) with greater visibility to the threat landscape. Provides government and private enterprise with visibility to trends for planning purposes.
Gaps in Information & Process	(Extra Space) Diverse enterprise environments with numerous differences in baseline security practices limit the usefulness of data collection. After trends and types of compromise are shared among organizations and governments for strategic and informational purposes, follow-up becomes informal.
Barriers & Challenges	Comprehensive and information is most helpful when making cybersecurity-related planning decisions. The volume of indicators shared overall may be dependent on factors ranging from frequency of activity, fidelity and availability of attack information and available resources to produce the information. Some subsectors experience different threats than those faced by the majority. Many subsectors in different industries share closer threat profiles than do subsectors in the same overall industry. Information sharing, compliance and regulatory standards imposed on an industry level is less than optimal and may be counterproductive.

3. Foreign Government Sharing

Description	A foreign government's commercial banks and government agencies experienced heavy distributed denial of service attacks from 168 countries utilizing the User Datagram Protocol (UDP) amplification. The government computer emergency response team (CERT) contacted DHS/NCCIC/US-CERT for mitigation assistance through an international cyber organization, FIRST.org, email distribution list. The foreign government CERT provided US based attacking Internet Protocol (IP) addresses and timestamp information which was passed to another component, DHS/NCCIC/NCC, for cross data analysis. NCC contacted 21 potentially associated Communications sector members who researched and identified the problems and implemented mitigation strategies.

APPENDIX A: PRIVATE TO GOVERNMENT USE CASES/EXAMPLES

ISP & Entity Relationship	Government to Industry
Relationship Type	Formal - structured
Information that is Shared	To whom: Communications ISAC members
	Content & Value: Attacking IP addresses located within the US involved in UDP and amplification attacks targeting port 1900 (SSDP)
	Timeliness: Provided 1 week after onset of DDoS attacks
	Sharing Process: Email notification from country CERT to US-CERT passed to NCC for cross data analysis and shared with 21 Communications ISAC members
Benefits of Information Sharing	Research and identification of the problems and implementation of mitigation strategies
Gaps in Information & Process	A week delay in receiving the request; a lack of beginning and ending timestamps for the events against the different IP addresses (quality control check); and a corrupted open source database for IP address identification slowed the process
Barriers & Challenges	Time difference between the two countries' CERTs and possible language barriers as well as a lack of an incident severity schema for incident progress in addition to post event and request for information time lines and methodology

4. Telephony Denial of Service (TDOS)

Description	Telephony Denial of Service (TDOS)
ISP & Entity Relationship	Government to Industry
Relationship Type	Formal structured
Information that is Shared	To whom: Communications ISAC member/Carrier
	Content & Value: Phone number located within the US involved in TDOS attack on PSAP, originating across international borders
	Timeliness: Immediate notification to carrier, however international coordination through DOJ to international counterparts experienced significant delay (several days)

	Sharing Process: PSAP notification to carrier, carrier tracking call originations to an IP address outside the US, carrier notifies Dept of Justice
Benefits of Information Sharing	Research and identification of the threat and implementation of mitigation strategies across international boundaries, ability to aggregate information across sector for government, and best practices
Gaps in Information & Process	A lack of beginning and ending timestamps for the events against the originating IP addresses; and lack of coordination guidelines across international jurisdictions between law enforcement groups
Barriers & Challenges	Time difference between countries, as well as a lack of an incident severity schema for incident progress in addition to post event and request for information time lines and methodology; the law enforcement perspective and process across country borders

5. Heartbleed

Description	An industry engineer discovered the Heartbleed vulnerability, committed, and applied a patch, then notified an international organization which issued an advisory. US-CERT posted a technical alert, which led to DHS/NCCIC convening a Cyber Unified Coordination Group meeting. NCC distributed a request for information to Communications ISAC members and government partners seeking shared information confirmed exploits. After patching the vulnerability, DHS' the Telecommunications Service Priority (TSP) system database service was patched and updated removing the OpenSSL vulnerability. ICS-CERT conducted webinars on the vulnerability sharing analysis and mitigation actions.
ISP & Entity Relationship	Industry to Industry
Relationship Type	Formal - structured
Information that is Shared	To whom: Industry and government
	Content & Value: The vulnerability is a Heartbeat extension (RFC6520) to OpenSSL's Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) protocols which allows malicious actors to send specially crafted heartbeat requests to the vulnerable server and obtain sensitive information stored in the server's memory. Harvested data can be pieced together to develop a broader understanding of the acquired information.
	Timeliness: Notification of vulnerability to the world within 3 weeks of initial discovery
	Sharing Process: Information shared via email to distribution lists, through a dedicated website, technical advisory, and webinars

Benefits of Information Sharing	Industry partners revoked and reissued certificates after remediation, changing credentials/ passwords as needed.
Gaps in Information & Process	Slow in setting up Cyber UCG meeting
Barriers & Challenges	Providing notification of the vulnerability and mitigation actions through as many channels as possible in a timely fashion

6. NCFTA

Description	Non-Profit organization focused on cybersecurity training and awareness.
ISP & Entity Relationship	Informal, unstructured, information sharing between private sector, academia and government – "trust group".
Relationship Type	Informal - Unstructured
Information that is Shared	To whom: Private sector, academics and government security professionals participate in an informal communication via email list or one-one conversations.
	Content & Value: Private, academic or government can ask questions, share examples (e.g. "Is this a new sample of a distributed denial of service, DDOS, toolkit?") or seek security contact for off-line investigation.
	Timeliness: This may be real-time, 'off-list' or distributed via email list.
	Sharing Process: The delivery method will vary based on the type of information to be shared. Private industry, law enforcement, government, and academia may reach out verbally or one-on-one if the information is highly sensitive. List members may 'share' security-related information or questions to the group as appropriate.
Benefits of Information Sharing	Research and identification of threat indicator awareness and discussion of possible mitigation strategies across international boundaries. Ability to quickly identify if this is a new or known threat. For example, in the case of the new DDOS toolkit, information is shared to the entire list for awareness and feedback. Ability to communicate with security personnel at a specific agency, country, or private entity quickly.

Gaps in Information & Process	Information is shared organically. Participating members will informally vet information shared to determine relevance, accuracy, scope of the threat, and mitigation strategies. Indexing or categorizing and tracking of threats will occur in other venues.
Barriers & Challenges	As the pool of participants grows, trust levels decline and list information becomes more generic.

7. Government to Industry Solar Flares

Description	Solar Flares have caused negative impacts on Electric Power Transmission; Cellphone, Radio and Satellite Communications; GPS and other electronic communications. The Quebec Blackout Storm of 1989, caused by a Solar Flare, resulted in the entire 9,500-megawatt output from Quebec's La Grande Hydroelectric complex to experience massive power swings and a collapse of the Quebec power grid. The Halloween Storm of 2003 swamped the sensors of dozens of satellites and the Astronauts hid deep within the body of the ISS, but still reported radiation effects and ocular "shooting stars". More recently, low strength solar flares have caused cellphones to drop calls resulting in numerous complaints directed at the Telecommunications Industry.
ISP & Entity Relationship	Government to Industry Provide predictions of Solar flare activity.
Relationship Type	Formal-Structured
Information that is Shared	To whom: Communications ISAC members
	Content & Value: NOAA' Space Weather Prediction Center (SWPC) provides predictions of solar flare activity. Solar flares can cause satellite drag and disrupt radio and satellite communications, GPS signals, and eclectic power transmission. The predictions can alert ISAC members of the potential disruptions so they can take precautions and more quickly correlate cause and effect.
	Timeliness: Predictions are available ranging from monthly, weekly and daily forecasts.
	Sharing Process: The predictions are posted on the SWPC web site http://www.swpc.noaa.gov/products-and-data or by signing up to their subscription service http://www.swpc.noaa.gov/content/subscription-services. Information is further distributed through the DHS NCC. The NCC provides acts as a conduit for feedback and impact assessment, as needed.
Benefits of Information Sharing	The Citizens and Government rely on the communications capabilities provided by Industry.

Gaps in Information & Process	Industry may not be aware of the resources available from SWPC.
Barriers & Challenges	None

8. Hacktivists

Description	Hacking collectives are leveraging open source, publicly available information in social media to identify and target law enforcement officers, public officials, their employers or associates and families
ISP & Entity Relationship	Government to Industry
Information that is Shared	To whom: Industry and Government
	Content & Value: Product provides threat actor targeting techniques and suggests the targeted groups maintain an enhanced awareness of the content they post and how it may reflect on them or be used against them in court or during online attacks
	Timeliness: Information provided as part of an ongoing investigation
	Sharing Process:
Benefits of Information Sharing	Provides operational mitigation support to countermand potential cyber attacks
Gaps in Information & Process	Limited details on the threat actor as well as targeted individuals or organizations as the information comes from an ongoing investigation
Barriers & Challenges	Announcement is based on information from an ongoing investigation, limiting details

9. Qakbot Botnet

Description	Qakbot (Qbot) is an information stealing botnet capable of spreading across a network through network shares. Although Qakbot has been infecting computers since 2009, NCCIC/US-CERT observed a recent increase of new infections in January 2016
ISP & Entity Relationship	Government to Industry
Information that is Shared	To whom: Industry and Government

	Content & Value: Bulletin published jointly by FBI and DHS/NCCIC/US-CERT provides indicators related to this activity
	Timeliness: Increased activity cited in open source reporting on 22 January 2016 spurred indicator information sharing published 28 January 2016
	Sharing Process: FBI shared indicators with DHS/NCCIC/US-CERT and together they published a joint indicator bulletin for informational purposes to industry partners
Benefits of Information Sharing	Highlights known cyber threat indicators to government and industry partners
Gaps in Information & Process	There may be other indicators not included in this bulletin
Barriers & Challenges	Bulletin is based on information from an ongoing investigation, limiting details

10. Social Engineering

Description	Private Industry Notification to inform industry partners of a trend in criminal actors conducting social engineering scams targeting phone and email service providers to target government officials and corporate executives, ultimately gaining access to personal banking information.
ISP & Entity Relationship	Government to Industry
Information that is Shared	To whom: Industry
	Content & Value: Precautionary measures to mitigate social engineering threats
	Timeliness: Information provided during the course of associated investigations
	Sharing Process: FBI Cyber Division provides these notification reports in conjunction with a statutory requirement outlined in 42 USC 10607
Benefits of Information Sharing	Provides awareness for participating organizations and peers within the broader community or sector
Gaps in Information & Process	None
Barriers & Challenges	Information provided follows the Traffic Light Protocol for distribution