Testimony of
Robert K. Knake
Senior Research Scientist, Global Resilience Institute
Northeastern University
&
Senior Fellow for Cybersecurity Policy
The Council on Foreign Relations

Before

The U.S. House of Representatives
Subcommittee on Cybersecurity and Infrastructure Protection
of the Committee on Homeland Security

"Maximizing the Value of Cyber Threat Information Sharing"

Wednesday, November 15, 2017
2:00pm

Room 210
House Visitors Center

Introduction

Thank you Chairman Ratcliffe, Ranking Member Richmond, and members of the Committee for the opportunity to testify on this important matter. While much work remains to be done, I believe it is important to start by noting that much has been accomplished. Information sharing has been the focus of the cybersecurity community for the better part of a decade and has enjoyed bipartisan support.

When I was Director for Cybersecurity Policy at the National Security Council from 2011 to 2015, I had a productive bipartisan working relationship with Congress that resulted in several successful pieces of legislation. Important with respect to the topic of today's hearing, was the passage of the Cybersecurity Information Sharing Act of 2015 that succeeded in resolving many of the reasons private companies believed they were unable to participate in cybersecurity information sharing. By explicitly offering liability protections and other safeguards, CISA has removed major barriers to information sharing.

The primary challenges that remains are creating meaningful incentives whereby the sharing of cyber threat information has real value for network defenders and providing a secure operational environment for allowing the most sensitive information to be shared. In my testimony today, I will focus on two areas that I believe deserve the committee's attention: 1) the need for a secure network for classified information sharing, collaboration, and operations for use by critical infrastructure; and 2) the need for a mechanism to quickly investigate and share information on the causes of cyber incidents.

Developing a Secure Network for Classified Information Sharing, Collaboration, and Operations

Through programs like Automated Indicator Sharing (AIS) and the Cyber Information Sharing and Collaboration Program (CISCP), the Department of Homeland Security is fulfilling its mandate to broadly share information the government has with private companies and state, local, territorial, and tribal governments that need it to protect themselves. When combined with vendor products and private sector collaboration through Information Sharing and Analysis Centers, Information Sharing and Analysis Organizations, and efforts such as the Cyber Threat Alliance, these programs meet the needs of most companies.

Yet, government policy recognizes that a small set of private companies that operate the nation's critical infrastructure are under near constant threat from sophisticated actors. These "Section 9 list" companies (those identified pursuant to Section 9 of Executive Order 13636), require the ability to communicate with the government over classified channels in order to protect the nation's critical infrastructure from our adversaries.

Solutions to the problem of classified information sharing to date have been partial at best. Federal agencies continue to try and declassify or "tearline" more cyber threat information, separating out actionable threat information from intelligence. Federal agencies are also routinely providing classified in-person briefings to cleared individuals in the private sector.

These measures can never fully address the challenge of providing detailed and timely information to key infrastructure owners and operators. Given the clear and present ongoing threat of cyber attacks, Section 9 companies must be able to receive classified threat information in real time and to be able to coordinate securely with government and other private companies on network defense. What they need is a classified network for sharing critical infrastructure information. In addition to information sharing on cyber threats, I believe that such a network could address two other challenges.

President Eisenhower famously said, "If a problem cannot be solved, enlarge it." There is a tendency to view the idea of a classified network for critical infrastructure as too costly and difficult to manage for the value it would provide. As one government leader who considered the topic asked, "is the juice worth the squeeze?" My answer to that is an emphatic yes. The government owes it to its partners in the private sector to provide them the detailed and timely intelligence that they need to protect themselves and this cannot be done in unclassified form;. Providing a classified network for Section 9 companies would help to ensure a higher degree of assurance for critical infrastructure operations and provide a necessary fall back communications system in the event that the public Internet is disrupted. Given the ongoing threat and the significant economic and security consequences associated with disrupting the nation's critical infrastructure, there is ample justification to develop a new network.

Sharing Classified Information and Threat Collaboration

When the government has information that private companies need to protect themselves, it has an obligation to provide that information. A duty to warn exists as one of the rationales for the collection of intelligence and is embedded in the authorities granted to the Department of Homeland Security at its creation. To this end, the intelligence community, the FBI, and DHS deserve credit for initiating a program in 2013 to provide notification to private companies if they were the victim or target of malicious cyber activities. Government notification is now one of the leading ways that companies discover cyber incidents.

Through this program and related efforts, the government has wrestled with the challenge of sharing classified information with private companies. Declassification remains a slow and cumbersome process in large part because there is, in most cases, a good reason that classified information should not be put into the public realm.

When information cannot be declassified, government agencies have attempted to address the challenge in two ways. Through in-person briefings, they convey information to cleared personnel at relevant companies. These briefings are valuable for raising awareness but are not useful for operational purposes. The Enhanced Cybersecurity Services (ECS) program attempted to address the operational challenges associated with classified information by deploying classified signatures to managed security service providers that could be used to block attacks. ECS, based on a successful pilot effort within the Defense Industrial Base (DIB), is certainly part of an overall solution.

What ECS does not provide is context and multi-party communication. A signature alone is not sufficient to protect companies. Organizations under threat from the nation's adversaries need to

understand who is targeting them, why they are being targeted, how to protect themselves against the threat, and what threat actors may do next.

The Department of Defense has largely solved this problem for DIB companies. DoD successfully piloted and moved into production the Defense Industrial Base Network (DIBnet), a classified network for communicating with DIB companies. The network is used both to share classified information on threats and to securely convene to coordinate incident response. For DIB companies, DoD has shown the importance of being able to deploy both classified indicators and to communicate the context around threats. The DIBnet concept should be extended by the Department of Homeland Security to other critical infrastructure sectors.

Several colleagues of mine and I worked with the Intelligence and National Security Alliance (INSA) to develop a proposal for creating a classified network for sharing classified information and threat collaboration for the financial services industry based on DIBnet. I have included the paper, "FINnet: A Proposal to Enhance the Financial Sector's Participation in Classified Cyber Threat Information Sharing" for the record.

In the paper, we argue that the authority to establish a classified network for critical infrastructure is already vested in the President and the Secretary of Homeland Security. Executive Order 13691 of February 13, 2015 "Promoting Private Sector Cybersecurity Information Sharing" gave the Secretary of Homeland Security the necessary authority to establish a classified network for critical infrastructure companies. That order also directed the updating of the National Industrial Security Program Operating Manual (known as "the NISPOM") to better accommodate the needs of private companies that are not part of the Defense Industrial Base. Congress followed this action by charging the Federal government with developing mechanisms to allow for "the timely sharing of classified cyber threat indicators and defensive measures in the possession of the federal government with representatives of relevant federal entities and non-federal entities that have appropriate security clearances…" as part of CISA.[1]

We believe that DHS, Treasury, FBI, and Secret Service should work together to pilot the FINnet concept with a small number of financial services firms that have mature security organizations and are willing participants. Companies from other sectors could also be brought into the pilot. This pilot should be launched right away and initially operate at the secret level, using secure phones, laptops, and encryption cards to communicate securely over the public network infrastructure. If the pilot is successful, it could be migrated to dedicated network infrastructure that would provide higher degrees of assurance.

Crucial to the success of the DIBnet is that it is backed by the Defense Cyber Crime Center (DC3). DC3 provides companies connected through the DIBnet with "analytic support, incident response, mitigation and remediation strategies, malware analysis, and other cybersecurity best practices to participating companies."[2] In short, DC3 takes a customer service approach to the

[1] 6 USC 1502

[2] *Office of the Director of National Intelligence, Department of Homeland Security, Department of Defense, and Department of Justice, "Sharing of Cyber Threat Indicators and Defensive Measures*

DIB. It fosters information sharing among participating companies by providing valuable services when companies share information with it. Such an approach is critical to replicating the success of the DIBNet for other sectors. Each sector needs a government partner with a deep understanding of its sector, strong relationships with members of the sector, and the ability to provide value back to participating companies when they share information.

Protecting Critical Infrastructure Operations

The second challenge that such a network should address is the protection of critical infrastructure operations. As critical infrastructure grows more dependent on information technology, particularly given the growth of the so-called "Internet of Things", companies are connecting their operational technology to the public internet. While it is economical to use the public Internet for this purpose, the risk that critical infrastructure could be disrupted through a cyber attack highlights the need for higher levels of assurance provided by a separate network. As the National Infrastructure Advisory Council (NIAC) concluded in its latest report, "Industrial control systems connected to business IT systems and the Internet constitute a systemic cyber risk among critical infrastructure."[3]

The NIAC report recommends the establishment of "separate, secure communications networks specifically designated for the most critical cyber networks, including 'dark fiber' networks for critical control system…" The NIAC called for a pilot project to identify dark fiber that could be used for the network and test whether critical infrastructure could be operated if separated from the public network. Some utilities have already begun to migrate their operations to dedicated networks that they own instead of continuing to use the public Internet. Piloting this concept is well warranted given the threats our connected infrastructure faces.

Coordinating Network Restoration

The third problem that such a network could address would be coordinating network restoration in the event of an attack that destabilizes the public Internet. While the Internet has grown increasingly robust, it is not immune from disruptive cyber attacks. Some botnets have grown so large that a distributed denial of service attack could take down portions of the network. They have become so sophisticated that it can be difficult for network operators to separate the signal from the noise and filter out the attacks.

In the period after 9/11, the Bush Administration recognized the need to have a backup, redundant communications system to coordinate network restoration in the event of an Internet outage. The Critical Infrastructure Warning Information Network (CIWIN) was created with two purposes: it would serve on a daily basis to provide information on threats to critical infrastructure and provide a backup communications capability in the event of an Internet outage.

---

by the Federal Government Under the Cybersecurity Information Sharing Act of 2015," February 16, 2016, page 8.

[3] https://www.dhs.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf

CIWIN ran over the Internet's physical infrastructure but on dedicated circuits that would allow users to continue to communicate as long as the core routing infrastructure was still operational. In the face of budget cuts, the Department of Homeland Security canceled the program in 2013. The system had not been routinely exercised and no information was flowing over it.

The need for such a system remains. The problem with CIWIN was that the information that was shared over it was unclassified and could also be shared over the public Internet so it was essentially a redundant network that would only be used if the public Internet was compromised. However, the need to routinely share classified information would mean the network would be used on a daily basis as part of operations. Business needs will dictate use of the most expedient medium for sharing information. Absent the presence of classified information that cannot legally be shared on enterprise networks, operators will routinely fall back to sharing over unclassified email, phone, and other systems.

Taken together, I believe that the need to share classified threat information, the need to provide higher levels of assurance for critical infrastructure operations, and the need for a redundant communications system in the event of an Internet outage amply justifies the development of a dedicated secure network.

Creating a "National Transportation Safety Board" for Cyber Incidents

Over the last decade, cybersecurity professionals have recognized that, try as they might, incidents will still occur. The concept of "cyber resilience" is emerging to capture the idea that, while we may not be able to stop all harms from occurring in cyberspace, we can rapidly respond, recover, and adapt, becoming stronger than we were before. Achieving resilience, however, is not something any individual organization can do alone. Instead, it requires a collective effort so that the lessons learned from an individual incident at a company are widely disseminated and countermeasures implemented.

While a small number of defense contractors and financial services firms have recognized that sharing this kind of information is vital and, if done in the proper context, does not introduce risk to the firm, most companies fear the downside of sharing and see no potential upside. Companies fear that sharing information about a breach, even if it did not result in the loss of any data, will cause a public relations nightmare and result in a loss of stock value. It could lead to the firing of the CISO and even CEO. Even if these concerns were addressed, that would simply mean that there is limited downside. It would not mean that there is an upside or any kind of positive incentive to share this information. After all, sharing this kind of information does not directly help the company that has been breached; it only helps other companies detect or prevent a breach. Simply put, the challenge for information sharing is that the last thing a company that has experienced a breach wants to do is tell anybody else that it happened, let alone how it happened. Yet, it is in the national security interest that they do so as soon as possible.

To address this problem, many in the security community have long advocated for the equivalent of the National Transportation Safety Board (NTSB). When a plane crashes or a train derails,

NTSB shows up on the scene to investigate. The goal of NTSB is not to assign blame but to figure out what went wrong and to rapidly develop recommendations to prevent an incident like that from ever happening again. This information and those recommendations are rapidly shared with other airlines who quickly work to implement them. Such a virtuous cycle is what we need in cyber.

The challenge is that a plane crash is a public event and a cyber incident is usually, at least initially, a private one. An NTSB for cyber incidents requires a new system of notification and disclosure. It also requires developing a rubric under which companies that are busy trying to contain an incident are also willing to cooperate with an investigation that is not about helping them but about helping everyone else learn from their mistakes. Constructing such a system is no simple task.

A straightforward approach, which I do not recommend, would require disclosure of breaches to the Federal government and would give a government agency the authority to investigate and disseminate lessons learned. I do not believe such an approach I do not believe would be in the spirit of the public-private partnership we have worked to construct over the last two decades. It would create an adversarial relationship to the detriment of the cooperative environment we need to foster.

Instead, I believe what is necessary is a voluntary program under which companies are incentivized to agree that in the event of incident they will disclose it and cooperate with investigators that have a mission to surface and share the causes of the incident with the rest of the community.

One option that has worked well in a few incidents is to have US-CERT accompany the FBI on the bureau's investigation to advise the firm on "asset response" with a secondary purpose of collecting and sharing information for dissemination. The challenge with this approach is that companies may not cooperate with law enforcement investigations and often have little interest in receiving assistance from the government.

In my view, a better approach is to use cyber insurance to establish an obligation to disclose and to allow an independent investigation into the causes of the incident to take place for the purpose of disseminating that information to other companies. Such a system need not require public disclosure of either the fact of the breach or the findings. A Council on Foreign Relations paper that I authored on, "Creating a Federally Sponsored Cyber Insurance Program,"[4] called for an NTSB-like program be established as a requirement for participation in any federally back-stopped cyber insurance program.

While I support this recommendation, I do not believe that a government-backstopped program must be a prerequisite for advancing this kind of information sharing. Insurance companies, if they banded together, could set participation in this kind of disclosure and investigation program as a requirement for their underwriting commercially-available insurance or in order to receive a discount on policies. Doing so would be in the interest of insurance companies, as it would help

[4] https://www.cfr.org/report/creating-federally-sponsored-cyber-insurance-program

to reduce their aggregate risk by speeding the containment of related breaches that may yet to be discovered.

Congress should work with the insurance industry to identify whether there are any legal impediments to establishing this sort of program.

What We are Doing at Northeastern University

I recently joined the Global Resilience Institute (GRI) at Northeastern University. GRI's mission is to is to lead a university-wide interdisciplinary effort to advance resilience-related initiatives that contribute to the security, sustainability, health and well-being of societies. As with all efforts to create and sustain global change, they must start locally. Thus, we are working within the metro-Boston area to bring together the stakeholders who are willing to develop, test, and pilot the concept of a secure, redundant communications system that could be used for information sharing, collaborating on incident response, and restoring public networks should they become inoperable or compromised.

Mapping Critical Infrastructure and Dark Fiber in the Boston Area

We are beginning this effort by developing a map of critical infrastructure in the metro-Boston area. Initially, because of the challenges associated with getting detailed infrastructure information, this will not be a comprehensive model, but it will provide a foundation for identifying critical assets that can potentially be connecting to the available dark fiber in the Boston area. This will allow us to identify the practical barriers for making these connection, focusing in particular on the "last mile" challenge – how much additional fiber would need to be strung to connect control systems to the network. Our initial assessment suggests that the costs are likely to significantly lower than many expect.

Technical Design of a Secure Network

We have also begun work to design the architecture for this network. As indicated elsewhere, a dark fiber network is the preferred option at this stage; however, we are investigating other transmission mediums for where fiber is either not practical or desirable. For instance, long distance transmissions in rural areas might suggest microwave or other "over the air" technologies; likewise, in a coastal area like Boston, an over-the-air system might prove more resilient than fiber running underground or strung on telephone poles.

While it is tempting to think of a secure network as a closed loop, such a network would have limited use. Data will need to be securely moved on and off the network. For cybersecurity operations, incident data will need to be pulled up from the public Internet or enterprise business networks to be analyzed. Indicators of compromise extracted through analysis will need to be pushed down to be of use to network defenders. For industrial control systems, while communications with operations centers could take place on the closed network, signals from devices (at homes for instance) will need to be pulled up. Thus, it will be essential that the network allows, but strictly limit and monitor, communications to and from untrusted sources on the Internet.

The secure movement of data on and off the network can be accomplished with a series of "guards" or "cross domain solutions" that are used in government systems to move data from unclassified domains to classified domains. We are exploring the commercial application of these technologies and believe a viable system can be developed.

Admittedly, a perimeter approach such as we are advocating here is not a silver bullet. In fact, it has become popular in the cybersecurity community to declare that "the perimeter is dead". We think that such a notion is more marketing hype than reality for most companies. In the critical infrastructure space, it would not be responsible risk management to give up on limiting access to connected devices. Yet, we recognize that a "hard exterior" and "soft middle" is not the right solution. Even a separate network with the most advanced cross domain solutions and best inspection technologies can be breached. We are also painfully aware of the risk of insider threats, particularly when dealing with industry. Thus, the design of the network needs to account for both the threat from external actors as well as malicious insiders.

To address insider threats or to detect external threats that have compromised the security of the network, we believe that it is possible to develop a viable approach that will take advantage of new technologies that have been difficult or costly to implement in legacy networks. On a basic level, advances in software-defined networking and related technologies can allow the segmentation of traffic at multiple classifications. The network could easily accommodate sensitive but unclassified operational communications for critical infrastructure as well as classified communications on cyber threats for network defenders. Traffic moving across the network can be inspected, not just on exit and entry, and data accessed by users tracked to monitor for potential malicious conduct. In short, advances in technology together with the proper governance structure can limit access to data to those who need to know. Objections to extending this connectivity to the private sector based on concerns over security can be effectively addressed.

Business Model

As we have begun to develop this concept, a persistent question has been raised that should be familiar to all members of the committee: who will pay for it? I generally tend to favor the view that the necessary investment for cybersecurity is best treated as the cost of doing business for modern enterprises; however, I believe it is unlikely that the private sector will fund the development of a secure network on its own. A model in which the government selects an independent network operator and pays the initial cost of a pilot project that guides the development of the network is likely the most viable path. After it is established, use of it by critical infrastructure companies could incur a fee to cover its costs. The process for selecting the Electric Reliability Organization established by the Energy Policy Act of 2005 may be a model worth investigating.

Next Steps

As we continue to develop the concept of a classified network for critical infrastructure, we will look for opportunities to collaborate with critical infrastructure companies in the metro-Boston

area and beyond. Our plan is to be able to present a feasibility study on this topic within the next six months and to engage in a regional pilot within a year.

Conclusion

Thank you for the opportunity to testify on these important issues. As I hope my testimony conveyed, I believe that the remaining challenges in information sharing require identifying discrete problems and working to collaboratively develop specific solutions. As we pursue the development of these solutions and identify roadblocks, I look forward to continuing to engage with you, your staff members, and with my colleagues in the executive branch to further develop these important concepts.

I would be happy to answer any questions at this time.