INTELLIGENCE AND
NATIONAL SECURITY ALLIANCE

POSITION PAPER

June 2017

FINnet:

A Proposal to Enhance the Financial Sector's Participation in Classified Cyber Threat Information Sharing

Prepared By
THE INSA FINANCIAL THREATS TASK FORCE

EXECUTIVE SUMMARY

For almost 20 years, the government has facilitated the sharing of cyber threat information between federal entities and private sector organizations whose assets, systems, and proper functioning are essential to U.S. national security, economic security, and public safety.

The financial sector, one of 16 sectors designated as critical by the Department of Homeland Security (DHS), would gain tremendously from the real-time sharing of highly contextualized cyber threat indicators (CTI) and defense measures (DM) between key financial institutions and government agencies.

The Defense Industrial Base (DIB) Cybersecurity (CS) program is a robust model for such public-private sharing of information and analysis. This existing arrangement between the Department of Defense (DoD) and its core contractors has advanced detection and mitigation of malicious activity on DIB and DoD networks. The program's capabilities include DIBNet, a classified (Secret-level) web portal for real-time data exchange.

INSA encourages DHS, the Department of Treasury, the Federal Bureau of Investigation (FBI), and the Secret Service to partner with financial institutions to establish a public-private cybersecurity/ information assurance (CS/IA) program unique to the financial sector. Such a program should include a portal modeled on DIBnet – "FINnet" – that enables the real-time, secure flow of classified and unclassified cyber threat data between federal and non-federal entities.

BACKGROUND

Protecting critical infrastructure from cyber threats has been a national imperative of the past three U.S. presidents and surely will be a priority for those to follow. Beginning with President Bill Clinton's Presidential Decision Directive 63 in 1998, administrations have sought to establish and improve upon efforts to facilitate the sharing of cyber threat information between federal entities and elements of the private sector whose assets, systems, and proper functioning are essential to U.S. national security, economic security, and public safety.

The Defense Industrial Base (DIB) Cybersecurity (CS) program is perhaps the most robust model to date for public-private information sharing. Initiated in 2007, this arrangement between the Department of Defense (DoD) and its core contracting firms – whose intellectual property drives American innovation, global economic advantage, and military might – has been instrumental to advance detection and mitigation of malicious activity on DIB and DoD networks. Expanded as a voluntary program in 2012 to include the broader DIB membership, the program's capabilities include DIBNet, a classified (Secret-level) web portal for real-time data exchange with other program participants, including DoD's Cyber Crime Center (DC3). As the program's operational hub, DC3 offers "analytic support, incident response, mitigation and remediation strategies, malware analysis, and other cybersecurity best practices" to participating companies.[1] Classified connectivity, paired with a digital forensics powerhouse in DC3, makes the DIB CS program standard apart from similar endeavors.

> The financial sector… would stand to gain tremendously from a program with sharing and analysis capabilities comparable to the Defense Industrial Base Cybersecurity program.

The financial sector, like the DIB sector, is a part of U.S. critical infrastructure under the protective mission of the Department of Homeland Security (DHS). It would stand to gain tremendously from a program with sharing and analysis capabilities comparable to the DIB CS program. Financial institutions and related services industries face an astonishing range of cyber threats that are rapidly increasing in sophistication. The damage that cyber actors can unfurl is illustrated by a series of distributed denial-of-service (DDoS) attacks that started in September 2012 and by the March 2016 malware-aided theft of $81 million by hackers who falsified transactions between the central bank of Bangladesh and the Federal Reserve Bank of New York.[2]

Such attacks highlight the potential consequences of a severe and sustained disruption to the global financial system. A "FINnet" program that facilitates the real-time sharing of classified, highly contextualized cyber threat indicators (CTI) and defense measures (DM) between key financial institutions and government agencies would seem appropriate, if not overdue. Such a proposal may gain momentum today as the federal government begins to implement the Cyber Security Information Sharing Act of 2015 (CISA).

[1] 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 by the Federal Government Under the Cybersecurity Information Sharing Act of 2015," February 16, 2016, page 8. Available at https://www.us-cert.gov/sites/default/files/ais_files/Federal_Government_Sharing_Guidance_(103).pdf

[2] Arun Devnath and Michael Riley, "Bangladesh Bank Heist Probe Said to Find Three Hacker Groups," Bloomberg, May 10, 2016. Available at https://www.bloomberg.com/news/articles/2016-05-10/bangladesh-bank-heist-probe-said-to-find-three-groups-of-hackers.

CISA: SETTING THE STAGE

While not a panacea for all obstacles to more extensive public-private information sharing, CISA has fostered an environment in which a FINnet proposal may find traction. Signed by President Obama in December 2015, CISA charges the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General with developing procedures to facilitate "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" and to do so in a manner "consistent with the protection of classified information."[3]

For the private sector, CISA explicitly offered liability protections and other confidentiality safeguards, including exemptions from regulatory and open records requests, for the data they may provide. At minimum, the authorities and protections CISA has put in place would be key building blocks in a FINnet program. But more is needed.

CISA calls for the government to share in real-time classified cyber threat indicators and defensive measures with non-Federal entities that have appropriate security clearances.

[3] *CISA, sec. 103(a); 6 USC 1502.*

CHALLENGES TO FINANCIAL SECTOR PREPAREDNESS

The DIB CS program succeeded in part because DoD and the defense-oriented DIB companies that support it already shared a mindset of "intelligence-driven security." It allowed them to build upon an existing infrastructure in which their respective cleared personnel collaborated and operated along compatible guidelines. Financial organizations have developed cyber intelligence capabilities and hired personnel – predominantly from the military, government and DIB sector – to understand how to collect, share, and receive data. This data enables companies to categorize adversaries; identify tactics, techniques, and procedures (TTP); disrupt malicious activities; and harness unclassified cooperative forums like the Financial Services Information Sharing & Analysis Center (FS-ISAC).

Even fewer financial organizations are equipped to handle and share classified information, which requires access to secure facilities; specially secured phone, email and terminal connectivity; and personnel who have been granted security clearances by the government.

The financial sector also faces a personnel deficit the DIB sector largely bypassed. Multinational companies, unlike government contractors, tend to employ a large contingent of non-U.S. citizens (not uncommonly in leadership positions); consequently, obtaining security clearances for these staff members could prove challenging. To gather sufficient sector participation in a FINnet program, the government should pursue a consistent and comprehensive path for financial services companies to obtain facility clearances that meet the government's obligation to protect classified information but do not require private companies to change their operating structures. Executive Order (EO) 13691 of February 2015, "Promoting Private Sector Cybersecurity Information Sharing," speaks directly to this issue. This presidential directive:

- Designates the National Cybersecurity and Communications Integration Center (NCCIC), the primary DHS component in public-private information sharing, as a critical infrastructure protection program; and
- Authorizes the Secretary of Homeland Security to set guidance for "arrangements necessary to permit and enable secure sharing of classified information under a designated critical infrastructure protection program to such authorized individuals and organizations."[4]

> …the government should pursue a consistent and comprehensive path for financial services companies to obtain facility clearances…

Essentially, eligibility for facility and personnel clearances issued to enhance critical infrastructure protection is at the DHS Secretary's discretion, offering a potential path to guidelines less rigid than those governing clearances for defense contractors. In this respect, EO 13691 makes a FINnet proposal infinitely more viable.

[4] Executive Order 13691, "Promoting Private Sector Cybersecurity Information Sharing," February 13, 2015, 3 C.F.R. 13691 (2016). Available at https://www.gpo.gov/fdsys/pkg/CFR-2016-title3-vol1/xml/CFR-2016-title3-vol1-eo13691.xml.

RECOMMENDATIONS

In pursuit of a FINnet pilot program, the INSA Financial Threats Task Force encourages elements of DHS (including the NCCIC), the Department of Treasury, the Federal Bureau of Investigation (FBI), and the Secret Service to partner with essential financial institutions to establish a public-private cybersecurity/ information assurance (CS/IA) program unique to the financial sector. A DIBNet-model portal allowing for the flow of secure, real-time traffic of both classified and unclassified cyber threat data between federal and non-federal entities would be an essential component of the program. Other considerations to attract financial sector participation include but are not limited to the following:

1. **Designate the program under CISA.** Under the Act, the president may designate federal entities other than DHS to develop capability and process for the purpose of sharing cyber threat indicators in real time. Designating a FINnet pilot program as such an entity would ensure the full application of CISA – including the liability protections, safeguards for privacy and civil liberties, and open-records and regulatory exemptions – to program participants.

2. **Take a risk-based approach to membership, and include financial institutions designated as critical infrastructure.** The eight U.S.-chartered financial institutions named as "globally systemically important banks" by the Financial Stability Board in 2015 (and re-named in 2016) serves as a sufficient public proxy.[5] Those G-SIBs are Bank of America, Bank of New York Mellon, Citigroup, Goldman Sachs, JP Morgan Chase, Morgan Stanley, State Street and Wells Fargo. By virtue of their G-SIB status and E.O. 13636 (which addresses critical infrastructure at greatest risk),[6] the risk to national economic security associated with these institutions is of a magnitude greater than the financial sector at large. A FINnet pilot offers definitive value if it prioritizes the detection, mitigation and remediation of cyber threats directed at this foundational set of institutions "where a cybersecurity incident could reasonably result in catastrophic regional or national effects," as stated in the Executive Order. To this point, however, E.O. 13636 has conferred support more symbolic than substantial to many of these companies. A FINnet pilot could be its first tangible benefit.

   Leading U.S. banks took a significant practical step to enhance the identification and mitigation of cyber threats by establishing the Financial Systemic Analysis & Resilience Center (FSARC) as part of the FS-ISAC in October 2016. The FSARC's mission is to mitigate systemic cyber risks to the financial sector by promoting collaboration, information sharing, and analytic techniques between U.S. financial services firms and federal agencies.[7] With its deep understanding of the financial sector, the FSARC is well positioned to help the Intelligence Community focus its efforts on the most critical or vulnerable components of the banking sector.

3. **Identify a strategy to grow the sector's cleared workforce.** Under current practice and law, the federal government must bear the cost of clearing an individual or facility to handle classified information. This structure is neither cost-friendly to government nor efficient for the private sector.

4. **Plan for growth.** Although the DIB initially involved fewer than 20 core firms, it includes five times that many today, and Defense Department officials are reportedly considering adding hundreds more.[8] Should an initial, "G-SIB"-focused FINnet mechanism prove valuable, broadening participation to the additional 22 banks identified as "systemically important" would be appropriate.

[5] Financial Stability Board, "2015 update of list of global systemically important banks (G-SIBs)," November 3, 2015. Available at http://www.fsb.org/wp-content/uploads/2015-update-of-list-of-global-systemically-important-banks-G-SIBs.pdf. See also Financial Stability Board, "2016 list of global systemically important banks (G-SIBs)," November 21, 2016. Available at http://www.fsb.org/wp-content/uploads/2016-list-of-global-systemically-important-banks-G-SIBs.pdf.

[6] Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," February 12, 2013, 3 C.F.R. 13636. Available at https://www.gpo.gov/fdsys/pkg/CFR-2014-title3-vol1/xml/CFR-2014-title3-vol1-eo13636.xml.

[7] "FS-ISAC Announces the Formation of the Financial Systemic Analysis & Resilience Center (FSARC)," press release, October 24, 2016. Available at https://www.fsisac.com/sites/default/files/news/FS-ISAC%20Announces%20the%20Formation%20of%20the%20Financial%20Systemic%20Analysis%20%28FSARC%29.pdf.

[8] Shane Harris, @War: The Rise of the Military-Internet Complex (Boston: Houghton Mifflin Harcourt, 2014).

SHARING INFORMATION, BUILDING TRUST

Ten years in, the DIB CS program has both fans and critics. Yet it undoubtedly offers lessons on how sector-specific information sharing efforts can be initiated and sustained, even at the classified level. The viability of a DIBNet or FINnet hinges on fostering trust and good faith, which comes in part from the common experiences shared by the public and private entities involved and the joint understanding that develops between them. Defense-focused DIB companies encounter the same threats that DC3 already sees as it protects DoD networks; DIB companies, as government contractors, already inherently understand how to do business with federal agencies.

> The viability of a DIBNet or FINnet hinges on fostering trust and good faith…. The financial sector is only beginning to develop that rapport with its government counterparts.

The financial sector is only beginning to develop that rapport with its government counterparts. For many institutions, as in other private industries, regulation has been the overriding purpose of federal engagement. The very nature of the relationship between regulators and the institutions they oversee makes it difficult to build an equal, collaborative partnership. Trepidation exists on government's side too; just as the financial sector has concerns about the risk of sensitive data being publicly disclosed, federal entities want to protect investigative sources and methods. It would be imperative for FINnet pilot participants to discover early opportunities to provide value and demonstrate trustworthiness. In time, a FINnet pilot would offer immense contributions to the financial sector's defense from persistent, highly evolving cyber threats.

While DIBNet is in some ways an exemplar, it is also an exception. Alternate models to sensitive, public-private information sharing must be explored that capitalize on the authorities and protections provided by CISA and that build upon the framework established nearly 20 years ago. The FINnet would be just one of many.

ABOUT INSA

The Intelligence and National Security Alliance (INSA) brings together the public, private and academic sectors to collaborate on the most challenging policy issues and solutions. As a nonprofit, nonpartisan, public-private organization, INSA's ultimate goal is to promote and recognize the highest standards within the national security and intelligence communities. INSA has over 160 corporate members and several hundred individual members who are leaders and senior executives throughout government, the private sector and academia.

ABOUT INSA'S FINANCIAL THREATS TASK FORCE

INSA's Financial Threats Task Force works to provide a deeper understanding of the broad range of financial threats to U.S. national security; strengthen public-private cooperation and information sharing regarding financial vulnerabilities; and establish tools and processes to counter efforts to exploit such vulnerabilities.

ACKNOWLEDGEMENTS

INSA appreciates the efforts of everyone who contributed to the development of this paper:

Financial Threats Task Force

Bill Wansley, *Booz Allen Hamilton;*
Chair, INSA Financial Threats Task Force

James Katavolos, *Citigroup;*
Vice Chair, INSA Financial Threats Task Force

Rob Knake, *Council on Foreign Relations*

Byron Collie, *Goldman Sachs*

Errol Weiss, *Bank of America Merrill Lynch*

INSA Leadership and Staff

Chuck Alsup, *President*

Suzanne Wilson-Houck, *Chief Operating Officer*

Larry Hanauer, *Vice President for Policy*

Ryan Pretzer, *Policy and Public Relations Manager*

Amy Cooper, *Intern*

Eric Bigelow, *Intern*

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

Building a Stronger Intelligence Community

(703) 224-4672 | www.INSAonline.org