Prepared Testimony and Statement for the Record of

Ann Barron-Dicamillo
Vice President, Cyber Intelligence and Incident Response
American Express

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

Hearing on “Maximizing the Value of Cyber Threat Information Sharing”

Wednesday, November 15, 2017

Chairman Ratcliffe, Ranking Member Richmond, members of the subcommittee, my name is Ann Barron-Dicamillo, and I am Vice President of Cyber Intelligence and Incident Response at American Express. Thank you for the opportunity to be here with you today. In my role at American Express, I'm responsible for managing cyber security operations and directing cyber threat intelligence globally for the company. I oversee an organization responsible for information security monitoring, security incident response, advanced cyber analytics as well as forensics and other applicable investigations. My organization is on the frontlines of defense against active cyber threats, and we actively participate in information sharing with industry and government partners. As an experienced information security executive with almost twenty years of extensive experience in operations and in the delivery of information security services, I have gained a deep knowledge of the cyber threat intelligence environment and a respected track record of assisting organizations make balanced and informed risk decisions.

From January 2013 to February 2016, I was Director of the United States Computer Emergency Readiness Team (US-CERT) at the Department of Homeland Security (DHS). My responsibilities included leading cybersecurity incident-response activities and network analysis, working to share relevant data with both the public and private sectors on cyber threat information sharing initiatives. At US-CERT, I supported DHS's efforts to improve the nation's cybersecurity posture, and I directly coordinated cyber information sharing to proactively manage cyber risks. My responsibilities also included driving the US-CERT mission with CERTs around the world, overseeing the 24×7 operations center, analyzing and reducing cyber threats and vulnerabilities, disseminating cyber-threat warning information and supporting incident-response activities with government and critical industry partners.

I've been a vocal proponent of Cyber Threat Intelligence (CTI) information sharing throughout my career in both my public- and private-sector roles. The fundamental importance of CTI information sharing comes down to one simple concept: "One entity's detection could be another entity's prevention." As computer network defenders, information sharing becomes the foundation upon which we can build a robust cybersecurity program in the continual fight to thwart cyber criminals and other adversaries. CTI information sharing happens even before first-line defenders are engaged; it enables security operation analysts and hunters to be proactive in the search for malicious activities; and it gains us a broader perspective on the threat environment as it perpetuates across the Web.

While at DHS, I engaged in efforts to mature public/private CTI information sharing programs like those created by the Cybersecurity Information Sharing Act of 2015

(CISA). This legislation addressed many of the concerns that had been expressed by critical infrastructure sector partners, including American Express, in engaging in CTI information sharing with the government. It created the ability for DHS to establish machine-speed sharing while protecting enterprises from associated liability concerns. American Express' support and position on this issue is one of the many reasons I joined their cyber operations team, as it was clear that American Express understood the importance of cyber threat information sharing for the betterment of our public and private partners, both domestically and abroad.

Since the passage of CISA, American Express has developed a more formal standard for sharing cyber threat information. We have engaged in more consistent sharing with the Financial Services Information Sharing and Analysis Center (FS-ISAC). We deployed and have matured a Threat Intelligence Platform (TIP), which currently ingests, on-average, hundreds of thousands of unique threat indicators per month. Our TIP is used by my organization to proactively search for threats, both emerging as well as trending, in the "Wild West" of the internet for potential relevancy to our unique environment. The information we receive from the TIP includes indicators from the FS-ISAC. These indicators of compromise (IOCs) include those shared by the U.S. Government through DHS's Cyber Information Sharing and Collaboration Platform (CISCP).

American Express is not a current participant in DHS's Automated Indicator Sharing (AIS) program. I understand the AIS bi-directional sharing program, to date, has had limited adoption and early challenges in demonstrating its full potential value. While AIS may be a good program for new entrants in cyber information sharing and a good start down the path of private/public sector information sharing, the program would be more effective at protecting organizations from cyber threats if it offered timelier indicator sharing, richer context around the indicator information, and continual improvements to ensure quality information. The following goes into greater detail regarding these points.

Improve Timeliness of Information Sharing

An issue that minimizes the potential value of the AIS portal information is that the agency that originated the information or indicator is in charge of the classification or declassification of that information. If the information provided is categorized as classified, the need to go through the process of declassification results in delays in DHS's information-sharing process, making the details of threats quickly obsolete because of the quickly shifting nature of attacks. Alternatively, if the information is

scrubbed of its classified status, the resulting shared information is often so cleansed or minimized that much of the relevant context needed to properly action the information has been removed.

Some proponents have suggested that the timeliness issue can be resolved by increasing the numbers of – and expediting the process to clear – private-sector individuals at companies, so as to be able to get access to classified information. However, increased access to classified information by critical infrastructure personnel provides little actionable data for those individuals to take back to their unclassified networks for implementation, as the data is still classified at a level that can't be removed or actioned on an unclassified fabric.

When I was at DHS, to try to help address the classification issue, I encouraged my partners in law enforcement and intelligence to work to "tear-line" more of their reporting so any actionable information could be shared more expeditiously with critical industry stakeholders. (Tear-lining is the process of sanitizing classified information below the tear line to convey the substance of the information without any identifying or sensitive sources or methods.) If relevant context is getting lost through the tear-line process, then the government should act to declassify the entire report as rapidly as possible.

In addition, the equities review process continues to be a stumbling block towards broader, more actionable information sharing from the government to private industry, and over-classification of entire reports continues to be an issue across the board in the intelligence community in all kinds of different contexts. In some instances, the usefulness of the information is essentially eliminated if the context is removed or if the limited information around the threat is misleading, leaving the private sector with a clue of a threat but not the ability to take meaningful, intentional steps to protect its network against an existing threat.

Having worked in these circles responding to cyber events while in the public sector, I fully understand the intelligence community must consider both public benefit and operational risks when disclosing confidential information about a threat. However, in light of the public sector's caution when it comes to cyber incidents, private industry turns to private cybersecurity firms for timelier and contextually complete information.

DHS can best address timeliness of cyber information sharing by working with the originating agency of the information to expedite the equities review process. Alternatively, DHS could work toward tear-lining the reporting, or better yet, if the information is found in an open source, work towards declassifying the reporting.

Provide Context for Effective Threat Mitigation

At American Express, we rely primarily on the FS-ISAC and other sources of external threat data from vendors and other communities of interest. We engage in outbound sharing primarily with the FS-ISAC and other financial institution partners. Threat sharing within the FS-ISAC occurs in two distinct ways: (1) the automated sharing of indicators via STIX (Structured Threat Information eXpression) and TAXII (Trusted Automated eXchange of Indicator Information); and (2) the sharing of unstructured, free-form emails that describe threats and provide context, including various indicators, and that are exchanged between different trust communities vetted by existing members for operational experience. The bulk of threat information sharing is still primarily via email, since it allows for communication of important context, including who saw it (e.g., sector-specific or wide-spread), what was seen (e.g., specific exploit to a known vulnerability or software version), when it was seen (e.g., when the activity began), where (e.g., impact to specific operating system endpoints or servers or hardware components) or on which part of the network it was seen (e.g., cloud-based, traditional network or mobile), and how it was mitigated or contained as relevant (e.g., whether there is a patch available or known signatures or scripts to mitigate the exploit ahead of the patch). These are the important details security analysts need in order to identify which indicators are the most relevant and important in their own networks, and how they relate to specific ongoing attack campaigns.

Today, the AIS program does not offer this type of valuable context for the indicators that are being shared. Just as the context is important to security analysts, the lack of context prevents users of the information from confirming that the indicators have been properly vetted and received from trustworthy sources. Providing mechanisms for representing and encouraging the supply of additional context, providing real-time feedback on data quality, and supporting different communities of trust are ways to advance the program. Additionally, private-sector organizations, like American Express, have shared feedback with DHS that they would like to see a higher volume of unclassified sharing versus a larger volume of less insightful information.

There are ongoing collaborative developments in information sharing, both in the formation and evolution of information sharing groups (ISACs, ISAOs, and other formal and informal threat-sharing communities) and in mechanisms for describing and sharing threat information. There are also efforts to make that threat information actionable by defensive measures, such as STIX and TAXII , the MITRE CAPEC (Common Attack Pattern and Classification) and ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge), and the newly developing OpenC2 (Open Command and

Control) standard. The implementation of STIX 2.0, which allows for representation of greater context and the identification of relationships between shared data, would be a beneficial step for AIS.

Continually Improve to Ensure Quality and Trustworthiness of Information

DHS should focus on ways to continually assess and improve the quality of the information sharing process through adoption of technology that automates the ability to apply confidence levels by source to the indicator-sharing process. DHS should consider working more closely with information recipients to learn what data and context are useful and pertinent to private industry so that private industry can easily ingest relevant information in real time. In addition, DHS should work with the private sector to gain confidence in the validity and credibility of the information (through the context sharing described above) while ensuring that the voluntary reporting of threats to the AIS program does not lead to attribution of any particular industry or entity.

Since CISA's passage, private- and public-sector sharing has come a long way and has made many positive advancements, but we believe there is more work to be done to overcome our adversaries. We strongly believe that timelier, more contextual and higher quality information sharing is the next step in the evolution of cyber threat information sharing that will lead to increased private-sector participation in DHS's information sharing programs.

I want to thank you again for inviting me to be here today to discuss this very important issue, and I look forward to answering any questions you may have.