Questions for Kevin Mandia, Chief Executive Officer, FireEye, Inc.
February 23, 2021, Hearing: "Hack of U.S. Networks by a Foreign Adversary"

From Chairman Warner and Vice Chairman Rubio

1. What information, as cybersecurity firms, are you required to share with the government when looking at cyber threats? What factors influence your decisions?

We are unaware of any general mandatory disclosure requirement for cybersecurity firms to share cyber threat information with the U.S. government unless the government legally compels a cybersecurity firm to disclose information via a subpoena or another legal mechanism. There are a number of other laws that require disclosure of a cyber incident to the government depending on, for example, the industry, the type of information affected and/or the severity of the cyber incident. For example, there are industry-specific laws such as the defense industry that might require a DoD government contractor to disclose information under certain circumstances pursuant to DFARs. § 252.204-7012.

In the normal course, cybersecurity firms are servicing clients during a cyber incident when gathering cyber threat information and the consent of such client would typically be required before any information is shared. We understand federal legislation and/or other legal instruments are being considered to mandate that certain information be shared with the government during cyber incidents and support those initiatives in order to better protect the Nation and inform the security community at large.

When FireEye chooses to share cyber threat information with the government, it is through our intelligence subscription service with paying (government) customers. We adhere to our Victim Notification program and policy process to protect our government and non-government customers from cyber attacks. It is designed to rapidly collect and analyze relevant and actionable threat intelligence from a variety of FireEye sources and disseminate to potential victims in a secure manner.

Additionally, we may choose to notify certain government partners, including the Department of Homeland Security, the Federal Bureau of Investigation, and the National Security Agency, when we have discovered a major cyber incident, such as recent the recent Pulse Secure, SolarWinds, and Colonial pipeline incidents. Factors for providing notification and/or sharing threat data associated with such incidents include the sophistication of the techniques used by the adversary, the likelihood of the threat actor being a nation state, and/or potential impacts and disruptions to critical infrastructure.

2. Does the Cybersecurity Information Sharing Act of 2015 provide sufficient legal protections for the sharing of information? In what ways could it be improved?

Although the 2015 information sharing law provides liability protections, they do not go far enough. Organizations are hesitant to share data in trusted-group or not-publicly-accessible environments for fear of retribution in the courts; the media; and possibly with shareholders and current and prospective customers.

Current statute provides companies liability protections, but only if *all* the sharing requirements are followed. The law reduces liabilities but does not eliminate them. For example, organizations

must remove all personally identifiable information (PII) from whatever is shared with the government. This may be easily accomplished for some prior to sharing, but difficult for others. The loss of protections under the law for unintentionally sharing PII is too big a risk for some companies. Updating the sharing program to mitigate against such risks might include the ability to share data anonymously in a repository. Furthermore, using that repository to also analyze and aggregate cyber risks and sharing findings with the security community might incentivize companies to share threat data.

The current information sharing law is challenged beyond limited liability protections. Additional challenges including the following:

- Today's sharing model is voluntary. There are no incentives for a private entity to share information with the federal government, especially for fear of reputational harm; reduction in shareholder value; criticism from the government, the media, etc.
- Participation in the program is low, thus, the information that's shared is minimal and not helpful to the government or participating entities. According to an Inspector General report at the Department of Homeland Security, less than 300 public and private entities were participating in the program as of 2018.
- Cybersecurity workforce issues are not accounted for – if the right cybersecurity experts aren't posted in private entities, they cannot correctly identify or conceptualize what should be shared with the government. There needs to be greater technical assistance from the federal government to help private entities share information.
- Operational capability issues are not accounted for – some companies don't have the capability to make the intelligence actionable or are unable to share intelligence effectively.
- The Department of Homeland Security is not necessarily sharing information back out to the community. Information that is shared is not actionable. The DHS IG report found that the Cybersecurity and Infrastructure Security Agency (CISA) increased the number of participants in the Automated Indicator Sharing (AIS) program and the volume of cyber threat indicators it has shared since the program's inception in 2016, but CISA has made limited progress "improving the overall quality of information it shares with AIS participants to effectively reduce cyber threats and protect against attacks."
- CISA is not staffed appropriately to manage the AIS Initiative, thereby reducing the quality of indicators that are shared back out to the community.
- The AIS technology, as well as relevant standards, are outdated.

We are encouraged by the requirements laid out in the President's recent executive order on cybersecurity, including mandatory disclosure requirements for federal contractors. We look forward to participating in and reviewing feedback and criteria established by DHS to share cyber threat information and to disclose incidents. FireEye maintains that these two activities should not be conflated and requirements surrounding each should be considered separately.

Additionally, CISA should consider (as well as Congress through any compulsory legislative requirements):

- Utilizing "cybersecurity first responders" to assist in identifying, contextualizing, and sharing cyber threat data.

- Establishing a small group of cyber first responders to prevent or mitigate the impact of cyber incidents through sharing information quickly and confidentially; first responders would include those who assess the events surrounding unlawful access to a network; these first responders would have an obligation to share threat intelligence to a government agency without being concerned about liabilities.
- Ensuring that all shared data is fully anonymized and 100% confidential.

From Senator Wyden

In 2019, FireEye released two free hacking tools, which automated the theft and use of encryption keys from Microsoft's Active Directory Federation Services (AD FS) software to access accounts in the cloud. The Golden SAML hacking technique that these tools automated was used by the adversary in the Solarigate campaign. In January, I wrote to your company to seek information about the steps that FireEye took to protect itself and warn the U.S. government about this hacking technique. FireEye's February response letter did not answer any of the questions I asked. Please respond to the information requests that I made in my January letter. Those information requests are:

3. Please describe and provide a timeline for all efforts by FireEye to warn Microsoft about the vulnerabilities exploited by adfsdump and adfspoof and of the importance of adding defenses against these exploitation techniques to Microsoft's enterprise products. Please provide copies of any relevant communications between FireEye and Microsoft.

4. Please describe and provide a timeline for all efforts by FireEye to warn the Department of Defense, the Office of the Director of National Intelligence, the National Security Agency, and the Cybersecurity Infrastructure and Security Agency, about the vulnerabilities exploited by adfsdump and adfspoof and the importance of the government deploying defenses against these exploitation techniques. Please provide copies of any relevant communications between FireEye and the U.S. government.

5. Please describe and provide a timeline for all efforts taken by FireEye to defend its corporate network against adversaries using adfsdump and adfspoof.

6. Please describe all efforts by FireEye to warn Congress about the need for organizations, including government agencies, to better protect AD FS encryption keys.

With respect to questions 3, 4, and 6, FireEye viewed the activities associated with ADFSDump and ADFSSpoof as a technique versus a vulnerability. As such, as is common practice, we did not disclose these activities via formal channels to any government agencies or the U.S. Congress, as we would through our typical responsible disclosure process for vulnerabilities or incidents. In general, for the latter cases, we use this process to notify vendors, who then in turn notify the appropriate agencies, government entities, etc.

As typically practiced within the security community, we discussed ADFSDump and ADFSSpoof in a number of informal channels:

- March 2019 – held informal conversations with Microsoft employee about the tool and response of "no feedback" from the ADFS team
- March 2019 – mentioned technique during a talk at a public conference, TROOPERS 19, in Germany
- July 2019 – mentioned technique during an informal "Tech Talk" at Fort Meade
- August 2020 – mentioned technique during a talk at a virtual public conference, Blackhat

With respect to question 5, we followed proper internal security protocols and took appropriate actions to defend and instrument our environment against the technique.