Department of Justice

STATEMENT OF
SCOTT S. SMITH
ASSISTANT DIRECTOR
CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

AT A HEARING CONCERNING
CYBER ROLES AND RESPONSIBILITIES

PRESENTED
OCTOBER 19, 2017

STATEMENT OF
SCOTT S. SMITH
ASSISTANT DIRECTOR
CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

AT A HEARING CONCERNING
CYBER ROLES AND RESPONSIBILITIES

PRESENTED
OCTOBER 19, 2017

Chairman McCain, Ranking Member Reed, and members of the Committee, thank you for the invitation to provide remarks on the FBI's role in defending the Nation against cyber threats.

As the Committee is well aware, the frequency and impact of cyber-attacks on our nation's private sector and government networks have increased dramatically in the past decade and are expected to continue to grow. We continue to see an increase in the scale and scope of reporting on malicious cyber activity that can be measured by the amount of corporate data stolen or deleted, personally identifiable information compromised, or remediation costs incurred by U.S. victims. Within the FBI, we are focused on the most dangerous malicious cyber activity: high-level intrusions by state-sponsored hackers and global organized crime syndicates, as well as other technically sophisticated attacks.

Cyber threats are not only increasing in scope and scale, they are also becoming increasingly difficult to investigate. Cyber criminals often operate through online forums, selling illicit goods and services, including tools that can be used to facilitate cyber attacks. These criminals have also increased the sophistication of their schemes, which are more difficult to detect and more resilient. Additionally, many cyber actors are based abroad or obfuscate their identities by using foreign infrastructure, making coordination with international law enforcement partners essential.

The FBI has worked with the rest of the intelligence and law enforcement community to address the unique set of challenges presented by the cyber threat. The information domain is an inherently different battle space, requiring government bureaucracies to shift and transform to eliminate duplicative efforts and stovepipes and move toward real-time coordination and collaboration to keep pace with the growing threat. Considerable progress has been made toward the shared goal of protecting the country from capable and unrelenting cyber adversaries, but there is still a lot to be done to ensure our government agencies have the proper resources,

structure, and mission to seamlessly work together on the cyber threat. The FBI will continue to be a leader in this area, and we have taken a number of steps in the last several years to ensure we are adequately structured to respond to threats in an agile and efficient way.

The decentralized FBI field structure is intended to support the investigation of crimes across the Nation. The FBI is made up of 56 field offices spanning all 50 States and U.S. territories, each with a multi-agency Cyber Task Force ("CTF") modeled after the successful Joint Terrorism Task Force program. The task forces bring together cyber investigators, prosecutors, intelligence analysts, computer scientists, and digital forensic technicians from various Federal, State, and local agencies present within the office's territory. Our field-centric business model allows us to develop relationships with local companies and organizations, putting us in an ideal position to engage with potential victims of cyber attacks and crimes. Cyber-trained special agents are in each field office, providing locally available expertise to deploy to victim sites immediately upon notice of an incident. Computer scientists and intelligence analysts are also stationed in field offices to support incident response efforts and provide intelligence collection and analysis as well as technical assistance and capability.

In addition to the resources in the field, the FBI has the Cyber Action Team ("CAT"), Cyber Division's elite rapid response force. On-call CAT members are prepared to deploy globally to bring their in-depth cyber intrusion expertise and specialized investigative skills to bear in response to significant cyber incidents. CAT's management and core team are based at headquarters, supplemented by carefully selected and highly trained field personnel. CAT members are available to supplement the technical capabilities in the field, and they are typically deployed in support of significant cyber incidents that have the potential to impact public health or safety, national security, economic security, or public confidence.

Cybersecurity threats and incidents are occurring around the clock, which motivated Cyber Division in 2014 to establish a steady-state 24-hour watch capability called CyWatch. Housed at the National Cyber Investigative Joint Task Force ("NCIJTF"), CyWatch is responsible for coordinating domestic law enforcement response to criminal and national security cyber intrusions, tracking victim notification, and coordinating with the other Federal cyber centers many times each day. CyWatch provides continuous connectivity to interagency partners to facilitate information sharing and real-time incident management and tracking as part of an effort to ensure all agencies are coordinating. CyWatch also manages FBI's Cyber Guardian program, through which more than 5,000 victim notifications were logged and coordinated in FY 2016.

In addition to these cyber specific resources, the FBI has other technical assets that can be utilized as necessary to combat cyber threats. Our Operational Technology Division develops and maintains a wide range of sophisticated equipment, capabilities, and tools to support investigations and assist with technical operations. The FBI maintains a robust forensic capability through its Regional Computer Forensic Laboratory Program, a national network of FBI-sponsored digital forensics laboratories and training centers devoted to the examination of

digital evidence. The Critical Incident Response Group ("CIRG") provides crisis support and incident management assistance. These resources can be leveraged throughout the FBI's response and investigative cycle to respond to cyber threats.

Given the international nature of cybercrime and the reality that the actors who seek to harm the U.S. through cyber means are often located abroad, the FBI relies on a robust international presence to supplement its domestic footprint. Through the Cyber Assistant Legal Attaché ("Cyber ALAT") program, the FBI embeds cyber agents, who are trained both at FBI Headquarters and in the field, with our international counterparts in 18 key locations across the globe where they build relationships with our international partners. These relationships are essential to working cyber cases that often involve malicious actors using computer networks worldwide.

In order to be successful in the mission of bringing cyber criminals to justice and deterring future activity in the cyber realm, the FBI relies on partnerships with the private sector. As frequent targets of malicious cyber activity, the private sector is on the front lines of defending our nation's critical information infrastructure, safeguarding its intellectual property, and preserving its economic prosperity. By building and maintaining partnerships with industry, the FBI is better able to share information about current and future threats, provide indicators of compromise for network defense, and provide context to help companies understand the intent behind the unnamed actors targeting their systems. These relationships also provide an optic into what kinds of nefarious activity they are observing on their systems, which helps the FBI better understand the threats.

The FBI has the capability to quickly respond to cyber incidents across the country and scale its response to the specific circumstances of the incident by utilizing all resources at its disposal throughout the field, at FBI headquarters, and abroad. Utilizing dual authorities as a domestic law enforcement organization and a member of the U.S. Intelligence Community ("USIC"), the FBI works closely with interagency partners in a whole-of-government approach to countering cyber threats. Presidential Policy Directive 41, signed by President Obama in July 2016, designates the Department of Justice, through the FBI and NCIJTF, as the lead Federal agency for threat response. Threat response is defined as activities related to the investigation of an incident and the pursuit, disruption, and attribution of the threat actor. Through evidence collection, technical analysis, disruption efforts, and related investigative tools, the FBI works to quickly identify the source of a breach, connect it with related incidents, and determine attribution, while developing courses of action.

The FBI is able to collect domestic intelligence on cyber threats, consistent with our authorities, to help us understand and prioritize identified threats, reveal intelligence gaps, and fill those gaps. By combining this intelligence with information from our interagency partners, the FBI contributes to painting a collective picture of cyber threats facing the Nation. This threat intelligence is critical to getting ahead of the threat and providing potential victims with information to assist them in better protecting their networks from compromise. The FBI liaises

with the other intelligence community components through standing coordination calls among the various watch centers; participation in standing interagency groups as well as incident- and threat-based working groups; through embeds and liaison officers at other agencies and within the FBI; and through memoranda of understanding allowing close coordination on topics of high importance.

The FBI along with the rest of the intelligence community understands the need to share information both within and outside the government with the potential victims of cyber attacks. The FBI disseminates information regarding specific threats to the private sector through various methods, including Private Industry Notifications ("PINs") and FBI Liaison Alert System ("FLASH") reports. PINs provide unclassified information that will enhance the private sector's awareness of a threat, and FLASH reports contain unclassified technical information collected by the FBI for use by specific private sector partners. These communication methods facilitate the sharing of information with a broad audience or specific sector. The FBI also works with industry partners in forums such as InfraGard and industry-based Information Sharing and Analysis Centers ("ISACs") to relay critical information. The FBI also works closely with its government partners to put out joint notifications and reports to help the private sector guard against potential cyber threats.

In some cases, the FBI receives indicators of potential compromise from various sources, including USIC partners and foreign governments, that are used in notification to victims of cyber attacks. Victim notification is critical in preventing continued cyber intrusion activity and mitigating the damages associated with the theft of sensitive data, intellectual property, and proprietary information. The goal of notification is to provide timely and meaningful notification to the victim while protecting sensitive sources and methods and balancing investigative and operational equities of the FBI and other USIC agencies. FBI and the Department of Homeland Security (DHS) have well defined policies and procedures which guide how victims are identified and how notification should be made; typically, the FBI, in coordination with DHS, will notify the individuals responsible for handling network security for the victim organization to discuss the necessary information related to the intrusion. The FBI will also provide open source information that may assist in the detection and identification of the intrusion. After the initial notification, some victims will contact the FBI to provide an update regarding the compromise of their network, while others will not. Typically, any post-notification engagement between the FBI and the victim is voluntary and its scope is determined by the company.

The FBI conducts its cyber mission with the goal of imposing costs on the adversary, and though we would like to arrest every cyber criminal who commits an offense against a U.S. person, company, or organization, we recognize indictments are just one tool in a suite of options available to the U.S. government when deciding how best to approach complex cyber threats. Working with the rest of the USIC, the FBI is able to share intelligence, better understand the threat picture, identify additional victims or potential victims of cyber intrusions, and help inform U.S. policymakers. The FBI and the intelligence community must work closely on cyber

threats to provide leaders with the information necessary to decide what tools are appropriate to respond to, mitigate, and counter cyber attacks, as well as deter cyber actors and reinforce peacetime norms of state behavior in cyberspace.

Using unique resources, capabilities, and authorities, the FBI is able to impose costs on adversaries, deter illicit cyber activity, and help prevent future cyber attacks. While much progress has been made toward leveraging the FBI's unique authorities and resources in real-time coordination with the interagency to combat cyber threats, there is still work to be done, specifically in ensuring agile and efficient incident response, seamless information sharing, and elimination of duplicative efforts. Although the resources of the FBI and of the Federal government are not growing in proportion to the rapidly evolving threat, we remain steadfast in our resolve to finds ways to work together better as a government, so that we may respond to cyber threats with agility, efficiency, persistence, and ferocity..

The FBI recognizes other agencies have technical expertise, tools, and capabilities to leverage as we work together against cyber adversaries, and is committed to working through challenges associated with sharing sensitive law enforcement information and intelligence with interagency partners. The FBI understands the importance of whole-of-government collaboration, and will continue to find ways to work with the interagency in responding to cyber incidents in a coordinated manner. Given the recent developments in structuring the Department of Defense to defend the Nation against cyber adversaries, the FBI is committed to finding ways to partner more closely with U.S. Cyber Command in its newly elevated role as a Unified Combatant Command and its Cyber Mission Force teams.

We at the FBI appreciate this committee's efforts in making cyber threats a focus and committing to improving how we can work together to better defend our nation against our increasingly capable and persistent adversaries. We look forward to discussing these issues in greater detail and answering any questions you may have.