Statement for the Record

Robert Kolasky
Director
National Risk Management Center
National Protection and Programs Directorate
U.S. Department of Homeland Security

FOR A HEARING ON

"Cyber Threats to Our Nation's Critical Infrastructure"

BEFORE THE
UNITED STATES SENATE
COMMITTEE ON JUDCIARY
SUBCOMMITTEE ON CRIME AND TERRORISM

Tuesday, August 21, 2018

Washington, DC

Chairman Graham, Ranking Member Whitehouse, and members of the Subcommittee, thank you for today's opportunity to testify regarding cyber threats to critical infrastructure. The Department of Homeland Security (DHS) serves a critical role in safeguarding and securing cyberspace, a core homeland security mission. The National Protection and Programs Directorate (NPPD) at DHS leads the Nation's efforts to ensure the security and resilience of our cyber and physical infrastructure.

DHS is responsible for assisting Federal agencies in protecting civilian Federal Government networks and collaborating with other Federal agencies, as well as state, local, tribal, and territorial governments, and the private sector to defend against cyber threats. Our work enhances cyber threat information-sharing across the globe to stop cyber incidents before they start and help businesses and government agencies to protect their cyber systems and quickly recover should such an attack occur. By bringing together all levels of government, the private sector, international partners, and the public, DHS is taking action to protect against cybersecurity risks, improve our whole-of-government incident response capabilities, enhance information sharing of best practices and cyber threats, and to strengthen resilience.

Threats

Cybersecurity threats remain one of the most significant strategic risks for the United States, threatening our national security, economic prosperity, and public health and safety. Regarding cyber threats to our critical infrastructure, the Director of National Intelligence recently said that "the warning lights are blinking red." We have seen advanced persistent threat actors, including cyber criminals nation states and proxies, increase the frequency and sophistication of malicious cyber activity. Our adversaries have been developing and using advanced cybersecurity capabilities in attempts to undermine critical infrastructure, target our livelihoods and innovation, steal our national security secrets, and threaten our democracy.

Although the intelligence community has not yet seen evidence that Russia intends to conduct a robust campaign aimed at tampering with our election infrastructure or influencing the makeup of the House or Senate in 2018, Russia has previously demonstrated the capability and intent to interfere with our elections. Russian efforts to influence the 2016 elections were one of the most recent expressions of Moscow's longstanding desire to undermine the US-led liberal democratic order. The Russian government conducted malicious cyber operations by compromising and leaking emails from U.S. political figures and institutions, and targeting election infrastructure. These activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations. Accordingly, we view the 2018 midterm elections as a potential target for Russian cyber operations and are working aggressively to mitigate any foreign threats to our election systems or infrastructure.

Global cyber incidents, such as the "WannaCry" ransomware incident attributed to North Korea and the "NotPetya" malware incident attributed to the Russian military in May and June 2017, respectively, are examples of malicious actors leveraging cyberspace to create disruptive effects and cause economic loss. These incidents exploited known vulnerabilities in software commonly used across the globe. Prior to these events, DHS had already taken actions to help protect networks from similar types of attacks. NPPD's National Cybersecurity and

Communications Integration Center (NCCIC) publishes a list of known software vulnerabilities and pushes this information out to stakeholders on a routine basis. Additionally, through requested vulnerability scanning, we helped stakeholders identify vulnerabilities on their networks so they could be patched before incidents and attacks occur. Recognizing that not all users are able to install patches immediately, we shared additional mitigation guidance to assist network defenders. As the incidents unfolded, we led the Federal Government's incident response efforts, working with our interagency partners, in providing situational awareness, information sharing, malware analysis, and technical assistance to affected government and critical infrastructure entities.

In a series of incidents since at least May of last year, working with U.S. and international partners, DHS and FBI have identified Russian government actors targeting government entities and businesses in the energy, nuclear, water, aviation, and critical manufacturing sectors. DHS assesses that this campaign ultimately collected information pertaining to industrial control systems with the intent to gain access to industrial control systems environments. The intrusions have been comprised of two distinct categories of victims: (1) staging and (2) intended targets. Through the Department's incident response actions, we identified activities by Russian government actors to target certain entities that then become pivot points, leveraging existing relationships between the initial victim and the intended targets to hide their activity, as part of a multi-stage intrusion campaign to gain access to networks of major, high-value assets that operate components of our Nation's critical infrastructure. Based on our analysis and observed indicators of compromise, DHS has confidence that this campaign is still ongoing, and threat actors are actively pursuing their ultimate long-term campaign objectives. DHS and FBI continue to conduct incident response related to this activity and have published a joint technical alert and hosted public webinars to enable network defenders to identify and take action to reduce exposure to this malicious activity.

Since 2015, the U.S. Government received information from multiple sources—including public and private sector cybersecurity research organizations and allies—that cyber actors are exploiting large numbers of network infrastructure devices (e.g., routers, switches, firewall, Network-based Intrusion Detection System devices) worldwide. Earlier this year, DHS, FBI, and the United Kingdom's National Cyber Security Centre published a publicly-available joint technical alert attributing this activity to Russian state-sponsored actors. Targets are primarily government and private-sector organizations, critical infrastructure providers, and Internet service providers supporting these sectors. Several days after publication of the alert, an industry partner notified DHS and FBI of related malicious cyber activity in which the actors redirected certain queries to their own infrastructure and obtained sensitive information, which included the configuration files of networked devices. Russian state-sponsored actors are using compromised routers to conduct man-in-the-middle attacks to support espionage, extract intellectual property, maintain persistent access to victim networks, and potentially lay a foundation for future offensive operations.

Cybersecurity Priorities

DHS, our government partners, and the private sector are committed to a more strategic and unified approach as we work to improve our Nation's overall defensive posture against this malicious cyber activity. Presidential Policy Directive – 21, *Critical Infrastructure Security and Resilience*, recognized that only a more integrated approach to managing risk would enable the Nation to counter malicious cyber activity our adversaries. In May of this year, DHS published a Department-wide Cybersecurity Strategy, providing DHS with a strategic framework to execute our cybersecurity responsibilities during the next five years.

This Administration has leaned forward even further, prioritizing the protection and defense of our people and economy from the range of threats that exist today, including those emanating from cyberspace. Last year, the President signed Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. This Executive Order set in motion a series of assessments and deliverables to enable the improvement of our defenses and lower our risk to cyber threats.

Executive Order 13800 requires continued examination of how the Federal Government and industry work together to protect our Nation's critical infrastructure, prioritizing deeper, more collaborative public-private partnerships in threat assessment, detection, protection, and mitigation. In collaboration with civilian, defense, and intelligence agencies, we have worked to identify authorities and capabilities that agencies could employ, soliciting input from the private sector, and developed recommendations to support the cybersecurity efforts of those critical infrastructure entities at greatest risk of attacks that could result in catastrophic impacts. It is only through this collective defense model that we will be successful against this threat.

NPPD's NCCIC operates at the intersection of the private sector, state and local governments, federal departments and agencies, international partners, law enforcement, intelligence, and defense communities. The Cybersecurity Information Sharing Act of 2015 established DHS as the Federal government's central hub for the automated sharing of cyber threat indicators and defensive measures. The NCCIC's automated indicator sharing (AIS) capability allows the Federal government and the private sector network defenders to share technical information at machine speed,. The NCCIC also provides entities with information, technical assistance and guidance they can use to secure their networks, systems, assets, information, and maintains confidentiality with our data, by reducing vulnerabilities, ensuring resilience to cyber incidents, and private partners supporting their holistic risk management priorities. DHS does this in a way that protects privacy and civil liberties.

National Risk Management

We are facing an urgent, evolving crisis in cyberspace. Our adversaries' capabilities online are outpacing our stove-piped defenses. Working together with the private sector and our government partners, we are addressing this problem and taking collective action against malicious cyber actors.

Specifically, there is a need to enhance and promote the Department's cross-sector, cross-government coordination on critical infrastructure security and resilience.

We must improve our focus on examining the critical functions that drive our economy and facilitate national security. In other words, we need to continually advance our ability to organize and collaborate on risk strategies, planning, and solutions. For many years, DHS has worked closely with the private sector, but it has become clear that it must be a focal point for turning threat intelligence into joint action.

At the Department's first National Cybersecurity Summit this summer, in response to a clear demand signal and after extensive consultation with industry and government partners, Secretary Nielsen announced the rebranding of the Office of Cyber and Infrastructure Analysis (OCIA) as the National Risk Management Center (NRMC). Housed within DHS, the NRMC is the logical evolution of the ongoing improvements made over the last several years in information sharing and partnership building between the government and industry. The NRMC draws on existing resources and functions from across NPPD, the Department and our Federal and international partners to bring our risk management efforts to the next level in effectiveness.

The NRMC's mission is to continually facilitate analysts and planners, from both public and private sector, in their efforts to assess our country's cyber risks, plan to combat those risks and — most importantly — enable implementation of tailored solutions to protect our networks. The full expertise of the Federal government should be brought to bear on these challenges. With this in mind, the NRMC will provide the private sector with an entrance point for project teams to access programs from all departments and agencies and coordinate defenses against cyber threats that can affect all sectors.

Perhaps most importantly, the Center's core mission focuses on the systems or functions that cut across sectors. Ultimately, the Center will facilitate a partnership among and across government and industry that can provide a unified, collective approach to the defense that the nation needs to achieve superiority over our adversaries.

We cannot fail to evolve as the threats continue to come. The NCCIC and National Infrastructure Coordination Center (NICC) will continue to carryout current operations but the NRMC will enhance their efforts. The NRMC will support NCCIC and NICC operations by helping with prioritization and other needs, while also looking ahead to plan more strategically, and leveraging feedback from the operations and other partners.

Election Security

DHS is committed to ensuring a coordinated Federal Government effort to assess vulnerabilities and mitigate risk to election infrastructure. We understand that working with election infrastructure stakeholders is essential to ensuring a more secure election. Based on our assessment of activity observed in the 2016 elections, DHS and our stakeholders are increasing awareness of potential vulnerabilities and providing capabilities to enhance the security of U.S. election infrastructure as well as that of our allies.

Under the Constitution and our system of laws, state and local election officials in thousands of jurisdictions administer federal elections. Risk management for election officials did not begin in 2016. State and local election officials across the country have a long-standing history of working both individually and collectively to reduce risks and ensure the integrity of U.S. elections. DHS is working with all 50 states to provide value-added – yet voluntary – services to support their efforts to secure elections.

This year our Nation is in the midst of primary and special elections as well as the general election in November. We have been working with election officials in all states to enhance the security of their elections by offering support and by establishing essential lines of communications at all levels – public and private – for reporting both suspicious cyber activity and incidents. This information sharing is critical and our goal is to enhance transparency and have visibility of aggregated elections-related cybersecurity efforts. We are also working with election officials, vendors, the Election Assistance Commission (EAC), and National Institute of Standards and Technology (NIST) to characterize risk to election systems and ensure appropriate mitigations are understood and available in the marketplace. As a part of this process, we work with these stakeholders to recommend best practices to ensure a secure and verifiable vote. Through the Government Coordinating Council, we also developed guidance for States on how best to spend funding received through the Help America Vote Act grant issued by the EAC.

DHS has made tremendous progress and has been committed to working collaboratively with those on the front lines of administering our elections—state and local election officials and the vendor community—to secure election infrastructure from risks. Engagement with all 50 States and the establishment of the Election Infrastructure-Information Sharing and Analysis Center with nearly 1,000 members reflects the advances we have made in building a coalition committed to securing elections from cyber threats. The establishment of government and sector coordinating councils will build the foundations for this enduring partnership not only in 2018, but for future elections as well. We will remain transparent as well as agile in combating and securing our physical and cyber infrastructure. However, we recognize that there is a significant technology deficit across State and local governments, and State and local election systems, in particular. It will take significant and continual investment to ensure that systems are upgraded and insecure or vulnerable systems are retired.

Conclusion

In the face of increasingly sophisticated threats, DHS employees stand on the front lines of the Federal government's efforts to defend our nation's critical infrastructure from natural disasters, terrorism and adversarial threats, and technological risk such as those caused by cyber threats. Our infrastructure environment today is complex and dynamic with interdependencies that add to the challenge of securing and making it more resilient while not endangering freedom of speech, freedom of religion or failing to protect an individual's privacy. Technological advances have introduced the "Internet of Things" and cloud computing, offering increased access and streamlined efficiencies, while increasing access points that could be leveraged by adversaries to gain unauthorized access to networks. As new threats emerge, we must better integrate cyber and physical risk management in order to secure effectively the Nation.

Expertise in cyber-physical risk assessments and cross-sector critical infrastructure interdependency evaluation is where NPPD brings unique experience and capabilities.

We must ensure that NPPD is appropriately organized to address cybersecurity threats both now and in the future, and we appreciate this Committee's leadership in working to establish the Cybersecurity and Infrastructure Security Agency to accomplish this goal. We are committed to working with Congress to ensure that we address cybersecurity in a way that cultivates a safer, more secure and resilient Homeland.

Thank you for the opportunity to appear before the Committee today, and I look forward to your questions.