Statement for the Record

Robert Kolasky
Director
National Risk Management Center
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

FOR A HEARING ON

"Securing U.S. Surface Transportation from Cyber Attacks"

BEFORE THE
UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY
SUBCOMMITETEE ON TRANSPORTATION AND MARITIME SECURITY
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

February 26, 2019

Washington, DC

Chairman Richmond, Chairman Correa, Ranking Member Katko, Ranking Member Lesko, and members of the subcommittees, thank you for the opportunity to testify regarding the U.S. Department of Homeland Security's (DHS) ongoing efforts to reduce and mitigate risks to our Nation's critical infrastructure. I have the privilege of serving as the Director of the National Risk Management Center (NRMC) at the Cybersecurity and Infrastructure Security Agency (CISA). The NRMC operates as a planning, analysis, and collaboration center bringing together industry and multiple parts of government to identify, analyze, prioritize, and reduce risks to critical infrastructure. The NRMC's efforts are centered on the 'secure tomorrow' mantle of CISA's mission – complementing and drawing from the day-to-day information sharing, technical analysis, and operational assistance missions from elsewhere in the agency.

My testimony today will focus on the cybersecurity of surface transportation systems, including pipelines, mass transit systems, freight rail systems, and highways. Both CISA and the Transportation Security Administration (TSA) play a critical role in accomplishing this mission. CISA is leading national efforts to defend the Nation's critical infrastructure today and secure tomorrow by partnering with industry and government to reduce risk from cyber, physical, and hybrid threats. Thanks to Congress's leadership and passage of the *Cybersecurity and Infrastructure Security Agency Act of 2018* (P.L. 115-278), we are now even better poised to further the maturation of the organization to best reflect our essential mission and role in securing cyberspace. CISA's efforts to secure surface transportation are carried out in close coordination with the TSA and Department of Transportation, the Sector Specific Agencies (SSA) for the surface transportation portion of the Transportation Systems Sector.

Cyber Threats

Cyber threats remain one of the most significant strategic risks for the United States, threatening our national security, economic prosperity, and public health and safety. The past several years have marked a growing awareness of the cyber domain in the public consciousness. We have seen advanced persistent threat actors, including hackers, cyber criminals, and nation-states, increase the frequency and sophistication of their attacks. Our adversaries have been developing and using advanced cyber capabilities in attempts to undermine critical infrastructure, target our livelihoods and innovation, steal our national security secrets, and threaten our democratic institutions.

Cybersecurity threats affecting surface transportation have the potential to impact the industrial control systems that operate pipelines, mass transit, freight rail systems, and our highway infrastructure. For example, America depends heavily on the 2.7 million miles of pipeline crisscrossing our country. Increasingly, the business operations and control systems that are vital to the continuity of this part of our energy posture are threatened by cyber-attacks from nation-states and other malicious actors. Many pipelines are now supplied with industrial control systems, automated pressure regulators, and control valves. If this pipeline infrastructure is intentionally attacked, control valves and pressure regulators could be affected. Failure of these technologies could lead to pressure surges causing emergency shutdowns, unexpected explosions and fires, and other serious consequences. The recently published Worldwide Threat Assessment of the Intelligence Community states, "China has the ability to launch cyber-attacks that cause localized, temporary disruptive effects on critical infrastructure – such as disruption of a natural gas pipeline for days to weeks – in the United States."

Similarly, trains are now supplied with onboard information technology (IT) systems that provide and receive real-time updates on track conditions, train position, train separation, car status, and other operational data. While such technologies are designed to provide faster and more reliable communications, these wireless communication advances result in trains no longer functioning as closed systems, thus increasing the cyber risks.

Today's industrial control systems within highway infrastructure are often not only automated but highly integrated. Interconnected road networks are controlled by numerous systems and devices such as traffic signal systems, ramp metering systems, road weather information systems, and field devices that feed into a traffic management center. If an individual system or device was deliberately attacked, the potential to affect multiple control systems would be a distinct reality.

Cybersecurity Priorities

CISA, our government partners, and the private sector are all engaging in a more strategic and unified approach towards improving our nation's overall defensive posture against malicious cyber activity. In May of last year, DHS published the Department-wide *DHS Cybersecurity Strategy*, outlining a strategic framework to execute our cybersecurity responsibilities during the next five years. Both the Strategy and Presidential Policy Directive 21- Critical Infrastructure Security and Resilience, emphasize that we must maintain an integrated approach to managing risk.

The *National Cyber Strategy*, released in September 2018, reiterates the criticality of collaboration and strengthens the government's commitment to work in partnership with industry to combat cyber threats and secure our critical infrastructure. Together, the *National Cyber Strategy* and *DHS Cybersecurity Strategy* guide CISA's efforts to secure federal networks and strengthen critical infrastructure. DHS works across government and critical infrastructure industry partnerships to share timely and actionable information as well as to provide training and technical assistance. Our work enhances cyber threat information sharing between and among governments and businesses across the globe to stop cyber incidents before they occur and quickly recover when they do. By bringing together all levels of government, the private sector, international partners, and the public, we are enabling a collective defense against cybersecurity risks, while improving our whole-of-government incident response capabilities, enhancing information sharing of best practices and cyber threats, strengthening our resilience, and facilitating safety.

CISA's National Cybersecurity and Communications Integration Center (NCCIC) provides entities with information, technical assistance, and guidance they can use to secure their networks, systems, assets, information, and data by reducing vulnerabilities, ensuring resilience to cyber incidents, and supporting their holistic risk management priorities. The NCCIC operates at the intersection of the Federal Government, state and local governments, the private sector, international partners, law enforcement, intelligence, and defense communities. The *Cybersecurity Information Sharing Act of 2015* (P.L. 114-113) established DHS as the Federal Government's central hub for the sharing of cyber threat indicators and defensive measures.

CISA's automated indicator sharing capability allows the Federal Government and private sector network defenders to share technical information at machine speed.

Much of our Nation's surface transportation infrastructure is dependent on industrial control systems to monitor, control, and safeguard operational processes. Many of the industrial control systems currently in use were built for operability, efficiency, and reliability during an era when security was a lower priority than it is today. CISA has a well-established history of working to secure industrial control systems across critical infrastructure. In 2004, DHS established the Control Systems Security Program to address growing concerns over the security of industrial control systems. Since 2009, DHS has maintained the Industrial Control Systems Joint Working Group as the primary body for communicating and partnering across all critical infrastructure sectors and the government at all levels to accelerate the design, development, and deployment of secure industrial control systems. CISA's industrial control systems cybersecurity capabilities include malware and vulnerability analysis; an operational watch floor to monitor, track, and investigate cyber incidents; incident response; international stakeholder coordination; and the creation and dissemination of threat briefings, security bulletins, and notices related to emerging threats and vulnerabilities impacting these technologies.

National Risk Management

Our adversaries' capabilities online are outpacing our stove-piped defenses. Specifically, there has been a critical gap in cross-sector, cross-government coordination on critical infrastructure security and resilience. Working together with the private sector and other government partners, we are taking collective action to strengthen cross-sector, cross-government coordination against malicious cyber actors.

Through the NRMC within CISA, we have stepped up our efforts to provide a comprehensive risk management approach to cyber and physical security. The NRMC is a core component of DHS's efforts to take a holistic cross-sector approach to managing risks to the critical functions that drive our economy and are necessary to our national security. Through the NRMC, government and industry are coming together to create a more complete understanding of the complex perils that threaten the Nation's critical infrastructure.

Risk is increasingly cross-sector in nature. A silo-ed approach to risk identification and management simply will not work. By the nature of the threat, and infrastructure design, risk transcends infrastructure sectors, is shared across state and national lines, and is held by both government and industry. As an example, we recently briefed industry on cyber activities that have been attributed to China. Attempts to steal intellectual property do not discriminate between sectors of our economy. From biotechnology, to aircraft components, to advanced rail equipment, and electrical generation equipment – information is at risk, and it can be weaponized. Similarly, the cascading nature of cyber incidents across sectors is very real. We need to look no further than NotPetya, the most costly cyber-attack in history - which we have attributed to Russia - to see how risk easily jumps across sectors and continents and how it can hit private sector organizations particularly hard.

National Critical Functions

Historically, the U.S. Government has focused on prioritizing critical infrastructure from the perspective of assets and organizations. A different approach for prioritization is needed to better address system-wide and cross-sector risks and dependencies. CISA, through the NRMC, is leading an effort to develop a set of National Critical Functions to guide critical infrastructure risk management.

National Critical Functions are defined as "the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on national security, economic security, national public health or safety." This construct forces a risk management conversation that is less about whether an entity is a business or government, and more about what an entity does to manage risk and what risk it enables. This framework allows us to look at issue sets in the risk management space not in isolation, but with a more holistic context.

We are partnering with SSAs and all 16 critical infrastructure sectors, including the Transportation Systems, Communications, Financial Services, and Energy sectors to identify and validate National Critical Functions. This list will be finalized in the coming months and will form the basis for subsequent analysis – including consequence modeling and dependency analysis – in order to develop a Risk Register of the most pressing threats facing the critical infrastructure community. Such a Risk Register will guide collective action between government and industry on how to best address risk management.

In doing the critical functions work, we have already identified aspects associated with surface transportation, such as pipeline operations, that need to be prioritized in terms of security. Although we are in our early stages of that work, we agree with the Committee on the pressing need to address risks associated with nation-state exploitation of vulnerabilities that link information to infrastructure operations and which could have significant consequences on community and economic security.

Surface Transportation Cybersecurity

The Pipeline Security Initiative is a partnership between CISA, TSA, the Department of Energy, and industry. Bad actors have shown interest in infiltrating systems in sectors with less mature cyber hygiene, and using that access to better understand ways to manipulate equipment in sectors with more advanced security protocols. This can lead to critical pipeline systems, including water, natural gas, and liquid fuels, being at risk.

By leveraging the TSA's SSA expertise and CISA's technical cybersecurity capabilities, the Pipeline Security Initiative is working to improve our ability to identify and mitigate vulnerabilities to the pipeline ecosystem. This initiative uses different voluntary assessments—ranging from single and multi-day inspections to self-assessments—to help our industry partners identify and mitigate potential vulnerabilities and provide the government with a broader view of pipeline security risk.

In December 2018, we completed our first comprehensive assessment under this new initiative. This initial assessment served as a successful test-bed to ensure that tools and other techniques offer the detail and data necessary to conduct the comprehensive analysis needed to ensure critical services and product flow through the pipeline systems. We anticipate nine more assessments in 2019.

Supply Chain Risks

Information and communications technology (ICT) is critical to every business and government agency's ability to carry out its mission efficiently and effectively. Vulnerabilities in ICT can be exploited intentionally or unintentionally through a variety of means, including deliberate mislabeling and counterfeits, unauthorized production, tampering, theft, and insertion of malicious software or hardware. If these risks are not detected and mitigated, the impact to the ICT could be a fundamental degradation of its confidentiality, integrity, or availability and potentially create adverse impacts to essential government or critical infrastructure systems.

Increasingly sophisticated adversaries seek to steal, compromise, alter, or destroy sensitive information on systems and networks, and risks associated with ICT may be used to facilitate these activities. The Office of the Director of National Intelligence (ODNI) acknowledges that "the U.S. is under systemic assault by foreign intelligence entities who target the equipment, systems, and information used every day by government, business, and individual citizens." The globalization of our supply chain can result in component parts, services, and manufacturing from sources distributed around the world. ODNI further states, "Our most capable adversaries can access this supply chain at multiple points, establishing advanced, persistent, and multifaceted subversion. Our adversaries are also able to use this complexity to obfuscate their efforts to penetrate sensitive research and development programs, steal intellectual property and personally identifiable information, insert malware into critical components, and mask foreign ownership, control, and/or influence of key providers of components and services."

CISA has launched the ICT Supply Chain Risk Management (SCRM) Task Force as a public-private partnership to mitigate emerging supply chain threats. The Task Force is the main private sector point of entry for our SCRM efforts and is jointly chaired by DHS and the chairs of IT and Communications Sector Coordinating Councils. The Task Force is focused on supply chain threat information sharing, supply chain threat mapping and assessment, establishing criteria for qualified bidder and manufacturer lists, and incentivizing the purchase of ICT from original manufacturers and authorized resellers.

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. The coming revolution of autonomous operations of infrastructure and other core functions, which combines data, machine learning, algorithms, and computing power and which is associated with massive new markets in artificial intelligence, smart cities, and quantum computing is going to radically change the nature of national security. The underpinning systems enabling functioning infrastructure have become more complex, and design considerations have created new vulnerabilities. Combine the reality of adversaries who are seeking to achieve strategic gain in the global marketplace and there is an essential imperative to have security remain a first order consideration for key infrastructure deployments and in the establishment of supply chains.

CISA is working with partners to meet this century's risks. Doing so requires being vigilant about security risk today and playing the long game – which will require continued collaboration between the executive and legislative branches. As the Committee considers these issues, we are committed to working with Congress to ensure that this effort is done 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.