wiley

NEWSLETTER

Homeland Security Focuses on Private Sector Engagement on Emerging Threats to Critical Infrastructure

September 2019

Privacy in Focus®

As next-generation wireless technologies are deployed and adopted, technology and telecommunications companies should be prepared for long-term engagement with the federal government on security issues, especially with the U.S. Department of Homeland Security (DHS). The Department has long recognized that the private sector controls and manages most of the country's critical infrastructure,[1] and it emphasizes the significant importance of public-private partnerships and coordinated risk management across government and the private sector. Within DHS, the Cybersecurity and Infrastructure Security Agency (CISA) leads the federal effort to help safeguard the nation's critical infrastructure from both cyber and physical threats and vulnerabilities. These efforts are largely voluntary, in collaboration with other government and private-sector stakeholders.[2]

At the end of August 2019, CISA released its *Strategic Intent*, which calls for sustained public-private collaboration. According to CISA, "this document lays out the strategic vision and operational priorities of the CISA Director."[3] It outlines the agency's mission to "lead the national effort to understand and manage cyber and physical risk to our critical infrastructure" and overall vision for a more "secure and resilient critical infrastructure for the American people."[4]

The *Strategic Intent*'s first guiding principle outlines that: "Without successful collaboration with our partners, we cannot achieve our mission. Our approach will drive conversation about the problem and

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

potential solutions and will require new models of partnership."[5]

Notably, among the CISA Director's key operational directives, the first stated priority is "China, Supply Chain, and 5G":

China presents the most pressing long-term strategic risk to the United States. The persistent threat posed by China compels CISA's focus on supply chain risk management in the context of national security. CISA is looking to reduce the risks of Chinese supply chain compromise, whether that is through 5G or any other technologies.[6]

The document formalizes and builds upon numerous lines of effort that CISA has launched to secure cyber and communications infrastructures, many of which require and rely upon dynamic participation from the private sector.

Addressing Systemic Risks

CISA's National Risk Management Center (NRMC) is a planning, analysis, and collaboration center working to identify and address the most significant risks to the nation's critical infrastructure. The NRMC works in close coordination with the private sector and other key stakeholders in the critical infrastructure community.[7] In early 2019, the NRMC produced a list of "national critical functions,"[8] which are divided into four different areas: (1) *Supply*, which focuses on providing resources to the public; (2) *Distribute*, which has a heavy focus on the movement of goods and people; (3) *Manage*, which is the largest bucket with a variety of functions; and (4) *Connect*, which focuses on communications and internet services.[9]

CISA maintains close ties with certain critical infrastructure sectors, including the Communications and Information Technology Sectors. CISA established the Tri-Sector Executive Working Group, consisting of senior leaders from the financial services, communications, and electricity communities, working together to manage known and emerging risks. Activities are underway to help direct intelligence collection requirements, build cross-sector risk management playbooks, and better understand and address systemic risk.[10]

Supply Chain, 5G, and Emerging Technologies

CISA "is committed to working with government and industry partners to ensure that supply chain risk management is an integrated component of its cybersecurity efforts."[11] The agency's Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force is a public-private partnership with more than 20 federal partners and over 40 private-sector company representatives focused on four main work streams, including:

- Developing a common framework for the bi-directional sharing of supply chain risk information between government and industry;
- Identification of processes and criteria for threat-based evaluation of ICT supplies, products, and services;

- Identification of market segment(s) and evaluation criteria for Qualified Bidder and Manufacturer List(s); and,
- Producing policy recommendations to incentivize the purchase of ICT from original manufacturers or authorized resellers.[12]

CISA, as noted in its *Strategic Intent*, is preparing to respond to the threats of tomorrow including those in the next generation of wireless technology or "5G." The agency notes that:

[5G] connections will empower a vast array of new and enhanced critical services, from autonomous vehicles and telemedicine, to automated manufacturing and advances to traditional critical infrastructure, such as smart grid electricity distribution. Given 5G's scope, the stakes for safeguarding these vital networks could not be higher. CISA is leading risk mitigation efforts across the federal government and is committed to working with government and industry partners to ensure the security and integrity of 5G technology in our nation.[13]

As part of these mitigation efforts, CISA collaborated with industry representatives to develop an *Overview of Risks Introduced by 5G Adoption in the United States* and related *5G Infographic*.[14] This document states that the U.S. government can manage vulnerabilities by "encouraging the continued development of trusted 5G technologies, services, and products" and "continued engagement with the private sector on risk identification and mitigation efforts," among other things.[15]

In May, the President issued the *Executive Order on Securing the Information and Communications Technology and Services Supply Chain*. DHS, through CISA and other collaborating offices, was required to "assess and identify entities, hardware, software, and services that present vulnerabilities in the United States and that pose the greatest potential consequences to the national security of the United States."[16] This assessment was developed "in coordination with sector-specific agencies and coordinating councils as appropriate."[17] The risk assessment is being used to inform the U.S. Department of Commerce as it develops rules called for by the *Executive Order*.

Looking Ahead

On September 18 – 20, CISA hosted the second annual National Cybersecurity Summit, to "bring together critical infrastructure stakeholders from around the world to a forum with presentations focused on emerging technologies, vulnerability management, incident response, risk mitigation, and other current cybersecurity."[18] Like the first Summit held in 2018, this event underscores the Department's view that cybersecurity, and national security more broadly, is a shared responsibility – one in which critical infrastructure operators, including technology and communications companies, play a central role. As DHS states, the Summit provided the opportunity for [government] agencies, private sector organizations, and international partners to highlight successes and opportunities for collective action.[19]

For CISA, now and into the future, collaborative and iterative risk assessments will need to leverage private-sector knowledge and expertise. The private-sector companies providing innovative technologies and communications products and services should expect and be prepared to engage with the Department, as it wrestles with ever-evolving security challenges.

For additional information, please contact:

Megan L. Brown
202.719.7579 / mbrown@wiley.law

Michael L. Diakiwski
202.719.4081 / mdiakiwski@wiley.law

[1] *See* DHS, *Critical Infrastructure Sectors* ("There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."), available at: https://www.dhs.gov/cisa/critical-infrastructure-sectors.

[2] DHS, CISA, *Supporting Policy and Doctrine*, available at: https://www.dhs.gov/cisa/supporting-policy-and-doctrine.

[3] DHS, *CISA Strategic Intent – Defend Today, Secure Tomorrow* (August 2019), available at: https://www.dhs.gov/publication/cisa-strategic-intent. ("*CISA Strategic Intent*").

[4] *CISA Strategic Intent* at 5.

[5] *Id.*

[6] *CISA Strategic Intent* at 8.

[7] *See* DHS, CISA, *National Risk Management Center*, available at: https://www.dhs.gov/cisa/national-risk-management.

[8] *See* DHS, *National Critical Functions: An Evolved Lens For Critical Infrastructure Security and Resilience*, available at: https://www.dhs.gov/sites/default/files/publications/national-critical-functions-overview-508.pdf (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 effect on security, national economic security, national public health or safety, or any combination thereof.").

[9] *See* DHS, CISA, *National Critical Functions Set*, available at: https://www.dhs.gov/cisa/national-critical-functions-set.

[10] *See CISA Strategic Intent* at 12; *see also* DHS, CISA, *Tri-Sector Executive Working Group*, available at: https://www.dhs.gov/cisa/tri-sector-executive-working-group.

[11] DHS, CISA, *Supply Chain Risk Management* available at: https://www.dhs.gov/cisa/supply-chain-risk-management.

[12] DHS, CISA, *Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force*, available at: https://www.dhs.gov/cisa/information-and-communications-technology-ict-supply-chain-risk-management-scrm-task-force.

[13] DHS, CISA, *5G Adoption in the United States*, available at: https://www.dhs.gov/cisa/5g.

[14] DHS, CISA, *Overview of Risks Introduced by 5G Adoption in the United States*, available at: https://www.dhs.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf.; *see also* DHS, CISA, *5G Infographic*: *5G Wireless Networks Market Penetration and Risk Factors* (July 2019), available at: https://www.dhs.gov/sites/default/files/publications/pdm19028_5g_risk_characterizationc_v14_05july2019.pdf.

[15] *See id* at 1.

[16] President Donald J. Trump, *Executive Order on Securing the Information and Communications Technology and Services Supply Chain* (May 15, 2019), available at: https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

[17] *Id.*

[18] DHS, CISA, *a 2019 CISA Cybersecurity Summit*, available at: https://www.us-cert.gov/event/2019-cisa-cybersecurity-summit.

[19] *Id.*