wiley

ALERT

DHS Releases Its Cybersecurity Strategy

May 16, 2018

On May 15, 2018, the U.S. Department of Homeland Security (DHS or Department) released its Cybersecurity Strategy and an associated Fact Sheet. According to DHS, "the strategy outlines a guiding framework for the Department and the homeland security enterprise to manage growing national cybersecurity risks." The DHS Cyber Strategy document was mandated by the 2017 National Defense Authorization Act (NDAA). In April, the White House submitted a classified cyber policy report to select congressional committees, outlining aspects of a broader U.S. government approach to cyber. This broader document has yet to be released.

DHS Secretary Nielsen stated that "DHS is rethinking its approach by adopting a more comprehensive cybersecurity strategy. In an age of brand-name breaches, we must think beyond the defense of specific assets—and confront systemic risks that affect everyone from tech giants to homeowners." To address these risks, "a core guiding principle underlying the DHS strategy approach is collaboration across the cybersecurity community, including with our partners in the federal government, state and local governments, industry, and the international community."

DHS's role in national cybersecurity policy is becoming increasingly important. Likewise, the Department is increasing its engagement with and expectations for the private sector. At a Department level, DHS interfaces with most (and regulates some) U.S.-based "Critical Infrastructure" owners and operators,[1] facilitates information sharing programs, publishes vulnerability alerts, and assists with incident response. Various DHS divisions and agencies are closely involved in digital forensics, domestic and international law enforcement investigations, and cybersecurity policy more broadly.[2]

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

DHS Cybersecurity Strategy

The DHS Strategy sets out five foundational "pillars" and seven cybersecurity "goals." These are:

- Pillar I – Risk Identification
  - Goal 1: *Assess Evolving Cybersecurity Risks*. We will understand the evolving national cybersecurity risk posture to inform and prioritize risk management activities.
- Pillar II – Vulnerability Reduction
  - Goal 2: *Protect Federal Government Information Systems*. We will reduce vulnerabilities of federal agencies to ensure they achieve an adequate level of cybersecurity.
  - Goal 3: *Protect Critical Infrastructure*. We will partner with key stakeholders to ensure that national cybersecurity risks are adequately managed.
- Pillar III – Threat Reduction
  - Goal 4: *Prevent and Disrupt Criminal Use of Cyberspace*. We will reduce cyber threats by countering transnational criminal organizations and sophisticated cyber criminals.
- Pillar IV – Consequence Mitigation
  - Goal 5: *Respond Effectively to Cyber Incidents*. We will minimize consequences from potentially significant cyber incidents through coordinated community-wide response efforts.
- Pillar V – Enable Cybersecurity Outcomes
  - Goal 6: *Strengthen the Security and Reliability of the Cyber Ecosystem*. We will support policies and activities that enable improved global cybersecurity risk management.
  - Goal 7: *Improve Management of DHS Cybersecurity Activities*. We will execute our departmental cybersecurity efforts in an integrated and prioritized way.

Key Takeaways for the Private Sector

Increased Private Sector Engagement and Expectations. In its vision statement, the Strategy outlines broader engagement with the private sector. By 2023, DHS will "foster[] a more secure and reliable cyber ecosystem through a unified departmental approach, strong leadership, and close partnership with other federal and nonfederal entities." One of the Department's core "guiding principles" is collaboration with key stakeholders. "The growth and development of the Internet has been primarily driven by the private sector and the security of cyberspace is an inherently cross-cutting challenge. To accomplish our cybersecurity goals, we must work in a collaborative manner across our Components and with other federal and nonfederal partners."

Under Pillar II Goal 3, the Department cites its authority to "engage broadly with federal and nonfederal entities to collaboratively address cybersecurity risks."[3] "DHS must partner with key stakeholders, including … the private sector, to drive better cybersecurity by promoting the development and adoption of best practices and international standards,[4] by providing services like risk assessments and other technical offerings, and

by improving engagement efforts to advance cybersecurity risk management efforts." And DHS "must deepen technical collaboration across all the sectors and with other key nonfederal entities on risk mitigation efforts."

DHS may also rely on its regulatory authorities in some sectors. In order to prevent the disruption of essential services from cyber incidents, "DHS must ... smartly leverage its regulatory authorities in tailored ways, and engage with other agencies to ensure that their policies and efforts are informed by cybersecurity risks and aligned to national objectives to address critical cybersecurity gaps." The Department also aims to improve its "outreach to critical infrastructure owners and operators, service providers, and other key enablers of risk management activity."

Connected Devices and IoT. The document outlines the cyber threat environment underscoring that technological advances have increased the risk surface, specifically addressing Internet-connected devices and the Internet of Things (IoT). "Substantial growth in Internet access, use of Internet-enabled devices, and the availability of high speed information technology systems and large datasets have facilitated productivity, efficiencies, and capabilities across all major industries. The proliferation of technology also presents new cybersecurity challenges and leads to significant national risks. More than 20 billion devices are expected to be connected to the Internet by 2020. The risks introduced by the growing number and variety of such devices are substantial." DHS emphasizes the need to mitigate potential risks of connected devices' software and hardware components and seeks to expand its work mitigating supply chain risks, as discussed in more detail below.

Enhanced Information Sharing. A primary objective of the Strategy is for DHS to "build on and expand automated mechanisms to receive, analyze, and share cyber threat indicators, defensive measures, and other cybersecurity information with critical infrastructure and other key stakeholders." The Department recognizes the need to improve its analytic capabilities and enhance the quantity and quality of information shared to increase the value of information sharing programs. "We must identify and address barriers to sharing information with the U.S. Government."[5] DHS also acknowledges the need "to rapidly declassify cyber threat [s] and associated contextual information" to enhance its information sharing efforts.

A More Global Approach. DHS recognizes that no one entity or nation can address cybersecurity on its own, noting that, "[r]obust international engagement and collaboration is required to accomplish our national cybersecurity goals. DHS must engage internationally to manage global cyber risks, respond to worldwide incidents, and disrupt growing transnational cyber threats as well as encourage other nations and foreign entities to adopt the policies necessary to create an open, interoperable, secure, and reliable Internet."

Closer Sector Relationships and Heightened Incident Reporting. DHS states that it "plays a unique role" in responding to "significant cyber incidents in close coordination with the Department of Justice and other federal agencies. In our role as asset responder, DHS must enhance capabilities to protect entities from additional harm following an incident, reduce the risk to others, safeguard sensitive personal and business information, and coordinate responses to significant incidents. As part of the law enforcement community, DHS must investigate incidents and be prepared to identify and counteract immediate cyber threats."

With this role in mind, the Department seeks to increase voluntary incident reporting and victim notification by building trusted relationships. "DHS must encourage the reporting of incidents, and work with other incident responders to develop consistent processes for notifying potential victims of cyber incidents." According to DHS, "[e]ncouraging a culture of reporting, notification, and information sharing will increase the security and resilience of critical infrastructure, help prevent, counter, and disrupt illicit cyber actors, and enable the government to assess and potentially manage responses to incidents of unknown severity."

Fostering More Resilient Networks and Securing the Supply Chain. DHS seeks to shift the "status quo" to improve security and resiliency. Noting that nearly all cyber incidents "involve exploitation of vulnerabilities or misconfigurations in software or hardware," DHS notes that "network operators are also increasingly dependent on vendors of commercial off-the-shelf products or integrators of commercially available products, and lack the capability to effectively manage supply chain risks." DHS states that "continued globalization of the information technology supply chain and shifting of information and services to cloud or other shared infrastructure introduces additional risks. As Internet-connected and other new technologies rapidly proliferate, the number of attack vectors also increases. Developers and manufacturers of many internet-of-things and other consumer devices are frequently motivated by speed to market rather than strong security. Even specialized technologies, like medical devices and industrial control systems, remain susceptible to compromise."

To foster greater security, "DHS must partner with information technology, communications, cybersecurity services, and other communities to incentivize security and enable cybersecurity outcomes such as minimizing vulnerabilities and addressing supply chain risks ... and encourage improved security for cloud infrastructure and throughout the life-cycle of internet-of-things devices and emerging technologies." To do this, DHS plans to leverage its security expertise and support relevant standards-setting efforts.

Conclusion

The DHS Cybersecurity Strategy presents a vision for an expanding role of the Department in cyberspace. Core objectives include increased engagement and collaboration with and from critical infrastructure operators. There is a particular emphasis on partnering with network operators and connected-device manufacturers and developers to minimize vulnerabilities and address risk.

---

[1] The Critical Infrastructure sectors are: 1) Chemical; 2) Commercial Facilities; 3) Communications; 4) Critical Manufacturing; 5) Dams; 6) Defense Industrial Base; 7) Emergency Services; 8) Energy; 9) Financial Services; 10) Food and Agriculture; 11) Government Facilities; 12) Healthcare and Public Health; 13) Information Technology; 14) Nuclear Reactors, Materials, and Waste; 15) Transportation Systems; and 16) Water and Wastewater. (https://www.dhs.gov/critical-infrastructure-sectors)

[2] *E.g.,* DHS agencies involved in cyber include: the National Protection and Programs Directorate (NPPD) which manages the National Cybersecurity and Communications Integration Center (NCCIC) and U.S. Computer Emergency Readiness Team (US-CERT); Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI), which investigates computer related fraud and crimes; the United States Secret

Service which investigates cyber crimes with a financial nexus; and the U.S. Coast Guard which has expanded its operational role in cyberspace to protect maritime transportation.

[3] *See* 6 U.S.C. § 148(c)(9) ("The cybersecurity functions of the [National Cybersecurity and Communications Integration] Center shall include: sharing cyber threat indicators, defensive measures, and other information related to cybersecurity risks and incidents with Federal and non-Federal entities, including across sectors of critical infrastructure and with State and major urban area fusion centers, as appropriate."); *see also* 6 U.S.C. § 143 (authorizes NPPD to provide "analysis and warnings related to threats to, and vulnerabilities of, critical information systems" to state and local government entities, and upon request to owners and operators of critical information systems. Also authorizing NPPD to provide "crisis management support" and "technical assistance," including recovery assistance, to the private sector and governmental entities.).

[4] Including NIST's *Framework for Improving Critical Infrastructure Cybersecurity*. We discuss the recently released Version 1.1 of the *Framework* here.

[5] *See also* DHS Office of the Inspector General, Press Release: *DHS Can Improve Cyber Threat Information Sharing* (Nov. 6, 2017) (https://www.oig.dhs.gov/news/press-releases/2017/11062017/dhs-can-improve-cyber-threat-information-sharing).