wiley

ALERT

National Cyber Strategy Emphasizes Private Sector's Shared Responsibility for Cyberspace

September 21, 2018

On September 20, 2018, the White House released the long-awaited National Cyber Strategy (Strategy). The Strategy builds off of Executive Order 13800 "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" and the National Security Strategy, which was heavily focused on cyber issues.

While a major policy shift includes enabling offensive cyber measures as a means of deterrence, the private sector should take note of the emphasis on shared responsibilities and rising expectations for government contractors, technology companies, the transportation and telecommunications sectors, and others.

The Strategy notes that America's adversaries have taken advantage of American innovation, using our openness and reliance on connected networks as an asymmetric equalizer. This environment of "new threats and a new era of strategic competition," the Administration contends, demands "a new cyber strategy that responds to [these] new realities, reduces vulnerabilities, deters adversaries, and safeguards opportunities for the American people to thrive."

The Strategy confirms trends that we have observed in recent years: the government is putting more responsibility on the private sector. The National Cyber Strategy outlines rising expectations for government and non-government actors, including contractors, information and communications technology developers, telecommunications providers, and satellite system operators, among others.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas

Telecom, Media & Technology

Objectives and Actions

Organized into four key pillars, each with objectives and priority actions, the Strategy is ambitious:

"The Strategy's success will be realized when cybersecurity vulnerabilities are effectively managed through identification and protection of networks, systems, functions, and data as well as detection of, resilience against, response to, and recovery from incidents; destructive, disruptive, or otherwise destabilizing malicious cyber activities directed against United States interests are reduced or prevented; activity that is contrary to responsible behavior in cyberspace is deterred through the imposition of costs through cyber and non-cyber means; and the United States is positioned to use cyber capabilities to achieve national security objectives."

Pillar I: Protect the American People, the Homeland, and the American Way of Life

The Strategy calls for "a series of coordinated actions focused on protecting government networks, protecting critical infrastructure, and combating cybercrime. The United States Government, private industry, and the public must each take immediate and decisive actions to strengthen cybersecurity, with each working on securing the networks under their control and supporting each other as appropriate." Many of the actions build off recent developments, including the 2019 National Defense Authorization Act. They envision active collaboration with the private sector and an expanded role for government.

Securing Federal Networks. Among its first objectives is securing Federal networks. "[T]he Administration will centralize some authorities within the Federal Government, enable greater cross-agency visibility, improve management of our Federal supply chain, and strengthen the security of United States Government contractor systems."

The Department of Defense has long required increased cybersecurity from its contractors. Indeed, Deputy Defense Secretary Patrick Shanahan said earlier this week that cybersecurity would likely join quality, cost and schedule, as one of the critical measurements the DOD uses when assessing contract bids. "It's just like we wouldn't pay extra for quality, we shouldn't pay extra for security," he said. "So part of this is just to recognize that we're in a new world, and security is the standard; it's the expectation; it's not something that's above and beyond what we've done before."

The Strategy, however, focuses heavily on government contractors across the board, and not just those in the defense industrial base. It envisions a muscular approach to managing contractors' technology. Notably it says, "[g]oing forward, the Federal Government will be able to assess the security of its data by reviewing contractor risk management practices and adequately testing, hunting, sensoring, and responding to incidents on contractor systems. Contracts with Federal departments and agencies will be drafted to authorize such activities for the purpose of improving cybersecurity."

- Supply chain risk will be integrated into agency procurement and risk management processes, "in accordance with federal requirements that are consistent with industry best practices[.]" Better information sharing related to supply chain threats will be a priority and a "supply chain risk assessment shared service" will be created. The government will also provide streamlined authorities to

"exclude risky vendors, products, and services, when justified."

- The Strategy wants to "consolidate[] acquisition strategies to improve cybersecurity and reduce overhead costs associated with using inconsistent contract provisions across the Federal Government."
- Federal Chief Information Officers will be given greater authority to assure "IT procurement decisions assign the proper priority to securing networks and data."
- Using federal procurement to bolster security, the government wants to "use its purchasing power to drive sector-wide improvement in products and services. The Federal Government will also be a leader in developing and implementing standards and best practices in new and emerging areas."
- The Strategy also points to the Department of Commerce's National Institute of Standards and Technology (NIST). Identifying NIST's work evaluating "quantum-resistant, public key cryptographic algorithms[,] the United States must be at the forefront of protecting communications by supporting rapid adoption of these forthcoming NIST standards across government infrastructure and by encouraging the Nation to do the same."

The Strategy empowers DHS to take a more active approach in the security of federal networks.

- The Department of Homeland Security (DHS) will be empowered to secure federal networks. "This will likely require new policies and architectures that enable the government to better leverage innovation."
- The Department of Defense (DOD) and Intelligence Community (IC) "will consider these activities as they work to better secure national security systems, DOD systems, and IC systems, as appropriate."

Securing Critical Infrastructure. The Strategy highlights the shared responsibility of the private sector and government to secure critical infrastructure. This has been an area of intense focus at DHS, underscored at the recent National Cybersecurity Summit and with the establishment of the National Risk Management Center.

- "The Administration will clarify the roles and responsibilities of Federal agencies and the expectations on the private sector related to cybersecurity risk management and incident response."
- It plans to address national risks by working with the private sector to understand and identify "national critical functions." A focus will be on communications and information technology, energy and power, banking and finance, health and safety, and transportation (maritime cybersecurity is identified specifically).
- The government wants to work with information and communication technology (ICT) providers "to devise cross-sector solutions to challenges at the network, device, and gateway layers, and we will encourage industry-driven certification regimes that ensure solutions can adapt in a rapidly evolving market and threat landscape."
- To incentivize cyber investments, government "will work with private and public sector entities to promote understanding of cybersecurity risk so [all stakeholders] make more informed risk-management decisions, invest in appropriate security measures, and realize benefits from those investments."

- Additionally, the "Administration is concerned about the growing cyber-related threats to space assets and supporting infrastructure," including satellite communications and networks. The government will work with industry and international partners to strengthen the resilience of these systems.
- The government will also provide technical and risk management support to strengthen democratic processes.

Combat Cybercrime and Improve Incident Reporting. "The Administration will push to ensure that our Federal departments and agencies have the necessary legal authorities and resources to combat transnational cybercriminal activity, including identifying and dismantling botnets, dark markets, and other infrastructure used to enable cybercrime, and combatting economic espionage." This effort seems to contemplate increased information flow from the private sector.

- Targeting, investigating, and prosecuting transnational cybercriminal groups and enhancing cooperation with international law enforcement partners will be a priority.
- The Strategy includes Department of Justice and other agency calls for workarounds to encrypted devices. "[L]aw enforcement will work with private industry to confront challenges presented by technological barriers, such as anonymization and encryption technologies[.]"
- To improve incident reporting and response, the government "will continue to encourage reporting of intrusions and theft of data by all victims, especially critical infrastructure partners. The prompt reporting of cyber incidents to the Federal Government is essential to an effective response, linking of related incidents, identification of the perpetrators, and prevention of future incidents."
- The Strategy calls for "updat[ing] electronic surveillance and computer crime statutes to enhance law enforcement's capabilities to lawfully gather necessary evidence of criminal activity, disrupt criminal infrastructure through civil injunctions, and impose appropriate consequences upon malicious cyber actors."
- The Strategy calls for international norms and standards development by "expand[ing] the international consensus favoring the Convention on Cybercrime of the Council of Europe (Budapest Convention)."

Pillar II. Promote American Prosperity

Aiming to preserve the "United States influence in the technological ecosystem and the development of cyberspace as an open engine of economic growth, innovation, and efficiency," the Strategy notes that innovation and advancement of the Internet economy has also presented challenges for security.

Foster a Vibrant and Resilient Digital Economy. The "United States Government will model and promote standards that protect our economic security and reinforce the vitality of the American marketplace and American innovation." This section lauds the importance of third party standards and global collaboration.

- Working across stakeholder groups, including with the private sector and civil society, the government will "promote best practices and develop strategies to overcome market barriers to the adoption of secure technologies" and "improve awareness and transparency of cybersecurity practices to build

market demand for more secure products and services."

- The Strategy pushes back against data localization regimes and other regulatory segmentation that are "unjustifiable barriers to the free flow of data and digital trade."
- Federal officials will "[c]ollaborate with international partners to promote open, industry-driven standards with government support, as appropriate, and risk-based approaches to address cybersecurity challenges."

The Strategy calls hints at increased government scrutiny of emerging technology and aims to influence market forces, including in the deployment of next-generation communications networks.

- The Strategy promotes the "implementation and continuous updating of standards and best practices that deter and prevent current and evolving threats and hazards in all domains of the cyber ecosystem."
- Focusing on telecommunications network innovation and infrastructure, "[t]he United States Government will work with the private sector to facilitate the evolution and security of 5G, examine technological and spectrum-based solutions, and lay the groundwork for innovation beyond next-generation advancements."
- It calls on government to "[e]xamine the use of emerging technologies, such as artificial intelligence and quantum computing, while addressing risks inherent in their use and application. We will collaborate with the private sector and civil society to understand trends in technology advancement to maintain the United States' technological edge in connected technologies and to ensure secure practices are adopted from the outset."
- The Strategy also seeks to "promote full-lifecycle cybersecurity, pressing for strong, default security settings, adaptable, upgradeable products, and other best practices built in at the time of product delivery." This should include "regular testing and exercising of the cybersecurity and resilience of products and systems during development using best practices from forward-leaning industries."

Foster and Protect United States Ingenuity. "The United States Government will nurture innovation by promoting institutions and programs that drive United States competitiveness. The United States Government will counter predatory mergers and acquisitions and counter intellectual property theft." This builds on recent legislative action on foreign investment review and concern about IP issues.

- The government will update mechanisms to review foreign investment and operation in the United States telecommunications networks. The Strategy aims to "safeguard the telecommunications networks we depend on in our everyday lives so they cannot be used or compromised by a foreign adversary," and "formaliz[e] and streamlin[e] the review of Federal Communications Commission referrals for telecommunications licenses. The United States Government will facilitate a transparent process to increase the efficiency of this review."
- Recognizing that digital theft has had a profound impact on the economy, the government will "work against the illicit appropriation of public and private sector technology and technical knowledge by

foreign competitors, while maintaining an investor-friendly climate."

Develop a Superior Cybersecurity Workforce. Aligning several pushes across government, the Strategy includes cyber workforce development, aiming to build a pipeline of cyber talent with educational and training opportunities.

Pillar III: Preserve Peace through Strength

Asserting that "[c]yberspace will no longer be treated as a separate category of policy or activity disjointed from other elements of national power. The United States will integrate the employment of cyber options across every element of national power." The government will "[i]dentify, counter, disrupt, degrade, and deter behavior in cyberspace that is destabilizing and contrary to national interests."

Enhancing Cyber Stability Through Norms of Responsible State Behavior. The U.S. will encourage universal adherence to cyber norms and "promote a framework of responsible state behavior in cyberspace built upon international law, adherence to voluntary non-binding norms of responsible state behavior that apply during peacetime, and the consideration of practical confidence building measures to reduce the risk of conflict stemming from malicious cyber activity." Adopting standards that define acceptable behavior will "promote greater predictability and stability in cyberspace."

Attribute and Deter Unacceptable Behavior in Cyberspace. The United States government will "ensure that there are consequences for irresponsible behavior that harms the United States and our partners. All instruments of national power are available to prevent, respond to, and deter malicious cyber activity against the United States. This includes diplomatic, information, military (both kinetic and cyber), financial, intelligence, public attribution, and law enforcement capabilities."

- The Federal government will identify and attribute malicious cyber activity that threatens United States national interests.
- Impose consequences, including with like-minded allies, "[t]he United States will launch an international Cyber Deterrence Initiative to build such a coalition and develop tailored strategies to ensure adversaries understand the consequences of their malicious cyber behavior."
- "Expose and counter the flood of online malign influence and information campaigns and non-state propaganda and disinformation."

Pillar IV: Advance American Influence

With a goal of preserving the openness, interoperability, security, and reliability of the Internet, "[t]he United States will maintain an active international leadership posture to advance American influence and to address an expanding array of threats and challenges to its interests in cyberspace."

Promote an Open, Interoperable, Reliable, and Secure Internet. The government will "work to ensure that our approach to an open Internet is the international standard. We will also work to prevent authoritarian states that view the open Internet as a political threat from transforming the free and open Internet into an

authoritarian web under their control, under the guise of security or countering terrorism."

- This approach will be done through a "multi-stakeholder model of Internet governance ... characterized by transparent, bottom-up, consensus-driven processes [which] enables governments, the private sector, civil society, academia, and the technical community to participate on equal footing."
- The U.S. will continue "active engagement in key organizations, such as the Internet Corporation for Assigned Names and Numbers, the Internet Governance Forum, the United Nations, and the International Telecommunication Union."
- The government will promote communications infrastructure and Internet connectivity through investment, and "provide greater opportunities for American firms to compete." This will "protect America's security and commercial interests by strengthening United States industry's competitive position in the global digital economy. The Administration will also support and promote open, industry-led standards activities based on sound technological principles."
- "The United States will continue to promote markets for American ingenuity overseas, including for emerging technologies that can lower the cost of security."

Build International Cyber Capacity. Looking at the big picture, the U.S will leverage "strategic partnerships that promote cybersecurity best practices through a common vision of an open, interoperable, reliable, and secure Internet that encourages investment and opens new economic markets." Enhancing international cyber capacity, the Strategy notes, "allows for additional opportunities to share cyber threat information, enabling the United States Government and our partners to better defend domestic critical infrastructure and global supply chains, as well as focus whole-of-government cyber engagements. Our leadership in building partner cybersecurity capacity is critical to maintaining American influence against global competitors."