MAYER | BROWN

January 8, 2021

Legal Update

The U.S. National Defense Authorization Act for Fiscal Year 2021: Cybersecurity Provisions

The William (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 ("NDAA," the "Act") was enacted into law on New Year's Day when the U.S. Congress overrode President Trump's veto of the legislation. It is, in the words of Senator Angus King (I-ME), "the most comprehensive piece of national cybersecurity legislation ever passed in U.S. history."[1] The bill enacts major changes to America's cyber defenses, reshaping how the private sector can combat growing cyber threats, as well as realigning roles and responsibilities of federal government agencies.[2]

The NDAA includes some 26 provisions among dozens of recommendations to combat such threats, proposals put forth this spring by the bipartisan, bicameral, public-private initiative known as the Cyberspace Solarium Commission ("CSC").[3] The Commission, created by the 2019 NDAA, set out to recommend a strategic approach to protect the United States against a cyber incident of significant consequence and recently put out a white paper focusing on frameworks for dealing with a cybersecurity supply-chain attack.[4]

This Legal Update discusses select cyber provisions in the NDAA and highlights key takeaways for private companies and the federal government, as stakeholders strengthen resources and heighten cooperation to combat new cyber threats and supply-chain risks.

National Cyber Director (Sec. 1752)

One of the key cyber provisions in the bill is the reestablishment of cybersecurity leadership at the White House by creating a Senate-confirmed National Cyber Director ("NCD") position within the Executive Office of the President (sec. 1752). One of the main objectives of the NCD would be to serve as the nexus within the White House and act as the key intermediary with the private sector on all cyber issues.

Under the NDAA, the newly empowered NCD would be Senate-confirmed,[5] a principal of the National Security Council,[6] and authorized to have a staff of up to 75 persons.[7] The NCD would be "the principal advisor to the President on cybersecurity policy and strategy relating to the *coordination*" of policy (emphasis added) on "information security and data protection" and "efforts to understand and deter malicious cyber activity," as well as "diplomatic and other efforts to develop norms and international consensus around responsible state behavior in cyberspace."[8] While these policy areas

will no doubt implicate activities by US Cyber Command, the State Department, and other major agencies, the role of the NCD stresses coordination of and not origination of or directive authority over the implementation of those policies. The NCD is beneficial for coherence not just in the federal government but also in the private sector, providing a central resource for information and policy guidance. In this regard, subpart (c)(1)(F) specifically calls on the NCD to "coordinate and consult with private sector leaders on cybersecurity and emerging technology issues" to better assist with preparing for and preventing cyberattacks.[9] As a key White House adviser, the NCD would also coordinate with his or her counterparts abroad to share intelligence and align potential responses or countermeasures, as well as help inform policies by allies and partners with respect to their domestic private sectors.

CISA Subpoena Power (Sec. 1716); DHS Joint Cyber Planning Office (Sec. 1715)

Section 1716 of the NDAA for FYI 2021 would authorize the Department of Homeland Security's (DHS) Cybersecurity & Infrastructure Agency ("CISA") to issue administrative subpoenas to, for example, internet service providers that would compel them to provide "information necessary to identify and notify such entity at risk"[10] from cyber vulnerabilities detected within networks "commonly used to perform industrial, commercial, scientific, or governmental functions or processes that relate to critical infrastructure."[11] Such subpoena power is intended to streamline the information-sharing process between the government and private sector regarding known or unknown cyber vulnerabilities, patching advancements, and emerging threats. Current subpoena authorities are mostly limited to the criminal context in the form of grand jury subpoenas that usually deal with systems already compromised, rather than with systems that might merely be vulnerable, which could assist private companies on a preventive basis. This kind of tailored administrative subpoena power, centered in CISA, would expand the federal government's authority to receive and put out information on identified vulnerabilities.

Section 1715 establishes a Joint Cyber Planning Office at DHS under CISA[12] to facilitate across federal departments and agencies and the private sector "plans for cyber defense operations . . . to protect, detect, respond to, and recover from cybersecurity risks or incidents . . . that pose a potential risk to critical infrastructure or national interests."[13] Contingency planning efforts to date have not adequately included the private sector; a central planning cell would significant enhance information-sharing at the planning and operational level across the US economy and pre-position resources and playbooks to streamline a coordinated response in lockstep with the federal government and private sector. The cell would also oversee the "development of additional plans" for "offensive and intelligence activities in support of cyber defense operations," bringing the Department of Defense ("DoD") together with the private sector to collaborate on intelligence development and defensive measures. The cell would also pre-position "agreements necessary for the rapid execution of plans for cyber defense operations"[14] so that joint, public-private campaigns are ready to be executed once a significant malicious cyber threat is identified. The office would create resources and long-term planning architecture to support public-private initiatives and enhance collaboration with ICT partners such as internet service providers, cloud service providers, and software and hardware companies, as well as cybersecurity forensics analysts.

CISA Strengthening Federal Networks/Active Threat Hunting (Sec. 1705)

Section 1705 authorizes CISA to engage in "hunting for and identifying, with or without advance notice to or authorization from agencies, threats and vulnerabilities within Federal information systems," as well as "deploying, operating, and maintaining secure technology platforms and tools . . . [for] collecting, maintaining, storing, processing, disseminating, and analyzing information."[15] While only authorizing threat-hunting on federal government networks, this provision would better equip CISA to collect real-time threat information to share more expeditiously with private-sector partners, as well as better secure federal networks from emerging or nascent threats.

Cyber Reserve Force (Sec. 1730)

Section 1730 provides that DoD is to conduct an assessment regarding the need and potential models/requirements for "a uniformed, civilian, or mixed cyber reserve force to remedy shortfalls in expertise and capacity"[16] in the event of a major national cyber emergency, including evaluating "the ability of the Department to attract the personnel with the desired expertise"[17] from the private sector. The assessment would focus on a variety of models, including one where DoD could call up volunteers from the private sector to serve in the event of a national emergency. A potential model for assessment might also include retaining active-duty talent in a reserve status if service members were to join the private sector, facilitating easy return of talent if needed to surge capacity. The assessment also calls for evaluating the impact such a reserve force would have on the private sector during and immediately after a major cyber incident.[18]

Cybersecurity State Coordinator (Sec. 1717)

Section 1717 provides for the Director of CISA to appoint a CISA employee in each state as a "Cybersecurity State Coordinator." The provision would provide a federally funded cybersecurity coordinator, responsible for preventing and responding to cyber threats, as well as advising on cyber risks, at the state level—including attacks on and threats to K-12 schools,[19] hospitals,[20] state governments,[21] and police departments,[22] all of which have fallen victim in recent months, especially amid the COVID-19 pandemic.[23] The coordinator would help fill gaps at the state level where the federal government may be less able to assist, including regarding cyber information-sharing with state and local entities, as well as assisting private companies or institutions with developing vulnerability disclosure programs in line with federal standards.[24] The coordinator would also build private sector relationships, "including by advising on establishing governance structures to facilitate the development and maintenance of secure and resilient infrastructure."[25]

GAO Report on Cyber Insurance Industry (Sec. 9005); DHS Strategy to Secure Email (Sec. 9006)

Additional cyber provisions in the bill have some particular consequences for private industry. Section 9005 calls upon the Government Accountability Office to issue a report studying ways to improve the overall market for cybersecurity insurance—recently valued globally at $5.95 billion in 2019 and projected to reach $32.47 billion worldwide by 2027.[26] The study would focus on "(1) identifying the number and dollar volume of cyber insurance policies currently in force and the percentage of businesses, and specifically small businesses, that have cyber insurance coverage; (2) assessing the

extent to which States have established minimum standards for the scope of cyber insurance policies; and (3) identifying any barriers to modeling and underwriting cybersecurity risks."[27] Moreover, the bill directs DHS to develop a strategy to standardize all US-based email providers across our economy on the same "Domain-based Message Authentication, Reporting, and Conformance" standard to secure emails from spam, phishing attacks, and ransomware that have wreaked havoc in recent months.[28]

For more information about the topics raised in this Legal Update, please contact any of the following lawyers.

Rajesh De
+1 202 263 3366
rde@mayerbrown.com

David A. Simon
+1 202 263 3388
dsimon@mayerbrown.com

Marcus A. Christian
+1 202 263 3731
mchristian@mayerbrown.com

Stephen Lilley
+1 202 263 3865
slilley@mayerbrown.com

Marcia G. Madsen
+1 202 263 3274
mgmadsen@mayerbrown.com

Gabriel Perlman
+1 202 263 3348
gperlman@mayerbrown.com

Endnotes

[1] https://columbiauniversity.zoom.us/webinar/register/WN_UmeGGJEATKOvoozBgzbTXQ

[2] The Act also contains a broad range of policy reforms that will impact the financial services industry and a significant number of new measures that will have an enduring effect on government contracting and contractors. These are discussed in our Legal Updates The US National Defense Authorization Act for Fiscal Year 2021: What Financial Services Companies Need to Know and The US National Defense Authorization Act for Fiscal Year 2021: Procurement Policy and Requirements.

[3] https://www.solarium.gov/report. Mayer Brown partner David Simon has served as Chief Counsel for Cybersecurity & National Security to the CSC, as well as partner Veronica Glick and senior associate Joshua Silverstein having served as deputies. https://www.mayerbrown.com/en/news/2019/10/mayer-brown-to-serve-as-cyberspace-solarium-commissions-pro-bono-cybersecurity-and-national-security-counsel

[4] https://www.solarium.gov/public-communications/supply-chain-white-paper

[5] NDAA Section 1752(b)(1).

[6] NDAA Section 1752(d).

[7] NDAA Section 1752(e).

[8] NDAA Section 1752(c).

[9] NDAA Section 1752(c)(1)(F).

[10] NDAA Section 1716(a)(3)(2)(A).

[11] NDAA Section 1716(a)(3)(1)(A).

[12] The Joint Office would include representatives from U.S. Cyber Command, the NSA, FBI, DOJ, and ODNI, as well. NDAA Section 1715(c).

[13] NDAA Section 1715(a).

[14] NDAA Section 1715(b)(6).

[15] NDAA Section 1705(1)(C).

[16] NDAA Section 1730(b)(2).

[17] NDAA Section 1730(b)(3).

[18] NDAA Section 1730(b)(8).

[19] https://us-cert.cisa.gov/ncas/alerts/aa20-345a

[20] https://www.wired.com/story/ransomware-hospitals-ryuk-trickbot/

[21] https://statescoop.com/cozybear-solarwinds-three-states/

[22] https://www.govtech.com/security/Texas-County-Sheriffs-Office-Suffers-Ransomware-Attack.html

[23] https://www.securitymagazine.com/articles/92886-covid-19-pandemic-sparks-72-ransomware-growth-mobile-vulnerabilities-grow-50

[24] NDAA Section 1717(a)(1)(B).

[25] NDAA Section 1717(a)(1)(B)(b)(1).

[26] https://www.prnewswire.com/news-releases/cyber-insurance-market-worth--32-47-billion-globally-by-2027-at-23-76-cagr-verified-market-research-301181491.html

[27] NDAA Section 9005(a).

[28] NDAA Section 9006. The provision defines the relevant standard as "an email authentication, policy, and reporting protocol that verifies the authenticity of the sender of an email and blocks and reports to the sender fraudulent accounts." *Id*. subpart (d).