Cyber Update
7 January 2019
By Michael Kans

Shutdown Shutters Some Federal Cyber and Data Security Operations

The continuing, partial government shutdown has shuttered or limited a number of key agencies with cybersecurity and data security oversight and responsibilities. Aside from deadlines for responding to rulemakings and other regulatory matters (e.g. the National Institute of Standards and Technology's (NIST) Privacy Framework), it remains unclear what the ultimate impact will be on the operations of these agencies. However, it is quite likely to delay investigations by the Federal Trade Commission (FTC) into Facebook and other data security matters, to name one agency's operations. Also, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) is reportedly operating with only 40% of its staff as those have been deemed essential and therefore required to work during the shutdown. Consequently, the standing up of this new agency may be delayed until after DHS receives FY 2019 appropriations.

Last week, the House passed a package of appropriations bills, and a continuing resolution (CR) for DHS on largely party line votes. However, despite the bills being virtually identical to those reported out of the Senate Appropriations Committee last year, Senate Majority Leader Mitch McConnell (R-KY) said the Senate would not take up bills to reopen closed agencies without President Donald Trump's support.

This week, the House will take up four of these appropriations bills, some of which fund agencies with cybersecurity and data security responsibilities:

- Financial Services and General Government
- Agriculture, Rural Development, Food and Drug Administration, and Related Agencies
- Interior, Environment, and Related Agencies
- Transportation, and Housing and Urban Development, and Related Agencies

The House Appropriations Committee claimed that the FY 2019 Financial Services and General Government Appropriations Act would provide these funds:

- Commodity Futures Trading Commission (CFTC) – $281.5 million, an increase of $32.5 million above the FY2018 enacted level and equal to the President's budget request.
- Federal Trade Commission (FTC) – $309.7 million, an increase of $3.4 million above the FY2018 enacted level and equal to the President's budget request.

Michael Kans, Esq. | mdk@michaelkanslaw.com | @michael_kans

- Federal Communications Commission (FCC) – $333.1 million, an increase of $11.1 million above the FY2018 enacted level and equal to the President's budget request.
- Securities and Exchanges Commission (SEC) – $1.69 billion, an increase of $6.3 million above the FY 2018 enacted level and equal to the President's budget request. The amount also includes $37 million to cover relocation costs for the New York Regional Office.

House Democrats Unveil Election Bill

Late last week, House Democrats released the "For the People Act of 2019" (H.R. 1), a package of electoral reforms that would seek to bolster the cybersecurity of election systems across the country. However, it is unlikely the Senate will take up this bill, and any measure in the Senate regarding election security would be more circumscribed. Nonetheless, this bill is shaping up to be a centerpiece of the House Democrats' early policy push.

Regarding the cybersecurity of election systems, the bill includes a process by which cybersecurity standards would be established for election infrastructure vendors and would also authorize grants for states and localities to upgrade and secure their election systems. Last year, House Democrats released the "Election Security Act" (H.R. 5011), the source for many of the cybersecurity provisions in H.R. 1.

"Qualified election infrastructure vendors" must agrees "to ensure that the election infrastructure will be developed and maintained in a manner that is consistent with the cybersecurity best practices issued by the Technical Guidelines Development Committee" and to promptly report cybersecurity incidents to the Department of Homeland Security (DHS) and the Election Assistance Commission (EAC).

The bill would authorize the EAC to make grants to states for a number of purposes, including "to carry out voting system security improvements" to undertake the following

> (1) The acquisition of goods and services from qualified election infrastructure vendors by purchase, lease, or such other arrangements as may be appropriate.
> (2) Cyber and risk mitigation training.
> (3) A security risk and vulnerability assessment of the State's election infrastructure which is carried out by a provider of cybersecurity services under a contract entered into between the chief State election official and the provider.
> (4) The maintenance of election infrastructure, including addressing risks and vulnerabilities which are identified under either of the security risk and vulnerability assessments described in paragraph (3), except that none of the

> funds provided under this part may be used to renovate or replace a building or facility which is used primarily for purposes other than the administration of elections for public office.
> (5) Providing increased technical support for any information technology infrastructure that the chief State election official deems to be part of the State's election infrastructure or designates as critical to the operation of the State's election infrastructure.
> (6) Enhancing the cybersecurity and operations of the information technology infrastructure described in paragraph (4).
> (7) Enhancing the cybersecurity of voter registration systems.

The bill would authorize appropriations of $1.7 billion for these grants.

H.R. 1 would also change the Department of Homeland Security's organic statute to make "election infrastructure" a critical infrastructure sector. In January 2017, then Secretary of Homeland Security Jeh Johnson expanded the Government Facilities Sector to include an Election Infrastructure Subsector. However, if H.R. 1 were enacted, then the election sector would be the 17th critical infrastructure sector and a future Secretary could not rescind this designation as one may with Johnson's addition to state and local elections systems to the Government Facilities sector.

The Director of National Intelligence would be required to "submit an assessment of the full scope of threats to election infrastructure, including cybersecurity threats posed by State actors and terrorist groups, and recommendations to address or mitigate the threats" at least 180 days before any regularly scheduled federal election.

Within a year of enactment, the Secretary of Homeland Security must "issue a national strategy to protect against cyber attacks, influence operations, disinformation campaigns, and other activities that could undermine the security and integrity of United States democratic institutions." And, within 90 days, the Secretary must also release "an implementation plan for Federal efforts to implement such strategy." A National Commission To Protect United States Democratic Institutions would be established to develop findings, conclusions, and recommendations on how to protect the U.S. from interference with democratic processes.

Last August, the Senate Rules Committee postponed indefinitely a markup on a compromise bill to provide states additional assistance in securing elections from interference, the "The Secure Elections Act" (S.2593). Reportedly, there was concern among state officials that a provision requiring audits of election results would be in effect an unfunded mandate even though this provision was softened at the insistence of Senate Republican leadership. However, a White House spokesperson indicated in a statement that the Administration opposed the bill, which may have posed an

additional obstacle to Committee action. However, even if the Senate had passed its bill, it seemed unlikely the House would consider companion legislation (H.R.6663).

Warner and Rubio Bill Would Target China's Technology Push

Last week, Senators Mark Warner (D-VA) and Marco Rubio (R-FL) introduced a bill to establish the Office of Critical Technologies and Security, a new entity that would be housed within the Executive Office of the President to craft a whole-of-government approach to maintaining U.S. technological superiority over adversaries. However, the sponsors of the bill made clear in their press release that the bill is aimed at the threat China poses to U.S. technological dominance. Warner and Rubio asserted their bill will "help combat tech-specific threats to national security posed by foreign actors like China and ensure U.S. technological supremacy by improving interagency coordination across the U.S. government."

The bill would task the new Office of Critical Technologies and Security would:

- coordinate a whole-of-government response to protect critical emerging, foundational, and dual-use technologies and to effectively enlist the support of regulators, the private sector, and other scientific and technical hubs, including academia, to support and assist with such response; and
- develop a long-term strategy to achieve and maintain United States technological supremacy with respect to critical emerging, foundational, and dual-use technologies and ensure supply chain integrity and security for such technologies.

The Director of Office of Critical Technology and Security would also serve as a Deputy National Security Advisor and Deputy Director for the National Economic Council. The Director would also chair the Council on Critical Technologies and Security, which will "advise the President on matters relating to challenges posed by foreign powers with respect to technology acquisition and transfer."

This bill follows the enactment of a number of measures in the last Congress to reform the process by which the federal government reviews proposed foreign acquisitions of U.S. companies, how the federal government identifies and excludes information technology supply chain threats, and legislation aimed at Chinese technology firms Huawei and ZTE. This bill is also introduced amidst the imposition of tariffs by both the U.S. and China.

New OSTP Head

In the waning days of the 115th Congress, the Senate confirmed a number of Trump Administration nominees before their nominations expired. The nominee for the Office

of Science and Technology Policy (OSTP), Kelvin Droegemeier, was among the confirmed appointees, meaning the OSTP will have its first head under the Trump Administration. The OSTP is the office within the Executive Office of the President that helps determine technology policy for cybersecurity, data security, artificial intelligence, and other related policy matters.

Healthcare Cybersecurity Guidance

Last week, the Department of Health and Human Services (HHS) released Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP), in response to a requirement in Section 405(d) of the "Cybersecurity Act of 2015" (P.L. 114-113). Shortly after enactment, HHS convened a Task Group to address cybersecurity in the realm of healthcare, and this guidance document along with supporting materials represent the agency's response to Congress' intent. In June 2017, HHS submitted a report to Congress titled "Improving Cybersecurity In The Health Care Industry."

HHS makes clear, however, that these guidance materials are meant to foster best practices, raise awareness, and bring about greater cyber hygiene. Yet, these materials *do not* displace or add to the statutory and regulatory standards healthcare providers must meet under the "Health Insurance Portability and Accountability Act of 1996" (HIPAA). Nonetheless, the Task Group "felt that the best approach to "moving the cybersecurity needle" was to leverage the NIST Cybersecurity Framework… introducing the Framework's terms to start educating health sector professionals on an important and generally accepted language of cybersecurity and answering the prevailing ques on, "Where do I start and how do I adopt certain cybersecurity practices?"

HHS framed the document as "a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes to achieve three core goals:

1. Cost-effectively reduce cybersecurity risks for a range of health care organizations;
2. Support the voluntary adoption and implementation of its recommendations; and
3. Ensure, on an ongoing basis that content is actionable, practical, and relevant to health care stakeholders of every size and resource level.

HHS also released these guidance documents:

- Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations: Technical Volume 1 discusses the ten Cybersecurity Practices along with Sub-Practices for small health care organizations.

- Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations: Technical Volume 2 discusses the ten Cybersecurity Practices along with Sub-Practices for medium and large health care organizations.
- Resources and Templates: The Resources and Templates portion includes a variety of cybersecurity resources and templates for end users to reference.

Michael Kans, Esq. | mdk@michaelkanslaw.com | @michael_kans