Cyber Update
31 December 2018
By Michael Kans

IT Supply Chain Risk Bill Goes To White House

Earlier this month, Congress sent a revised version of the "Federal Acquisition Supply Chain Security Act of 2018" (S. 3085), which was presented to the President on December 21. This bill was added to other Department of Homeland Security (DHS) related provisions. The ''Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act'' (SECURE Technology Act) (H.R. 7327) contains the revised S. 3085. However, it is unclear if the President will sign the legislation.

Broadly speaking, the revised language IT supply chain softens some of the language in the bill as reported out of committee. Notably, for entities for whom there are recommendations or orders to remove or exclude them from the IT supply chain, they now have the right to file for judicial review by the D. C. Circuit Court of Appeals "claiming that the issuance of the exclusion or removal order or covered procurement action is unlawful." The previous version of the bill did not allow for any judicial review. However, excluded or removed entities may still not file a bid protest with the Government Accountability Office (GAO). Likewise, the powers of the Federal Acquisition Security Council have been softened visa vis agencies, notably by allowing this new body to make recommendations on excluding or removing risky IT from the supply chain that would be reviewed by other agencies. Also, of note, the bill would make many of the new responsibilities part of the agency's FISMA responsibilities.

The "Federal Acquisition Supply Chain Security Act of 2018" would establish a Federal Acquisition Security Council that will be chaired by a "senior-level official" from the Office of Management and Budget (OMB) and have IT and supply chain specialists from a number of agencies including DHS, DOD, DOJ, DNI, and others. This Council would:

- Identify existing NIST standards for agencies to use to mitigate and address IT supply chain risks or recommend that NIST develop new ones
- Develop an information sharing process for agencies to circulate decisions throughout the federal government made to exclude entities determined to be IT supply chain risks
- Designate an agency to serve as a clearinghouse for such shared information
- Identify agencies that can offer shared services or "common contract solutions" to help agencies manage IT supply chain risk

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

- Establish a process by which entities determined to be IT supply chain risks may excluded from procurement government-wide (exclusion orders) or suspect IT must be removed from government systems (removal orders)
- Create an exception process under which IT from an entity subject to a removal or exclusion order may be used if warranted by national interest or national security
- Issue recommendations for agencies on excluding entities and IT from the IT supply chain and "consent for a contractor to subcontract" and mitigation steps entities would need to take in order for the Council to rescind a removal or exclusion order

The Council's recommendations for removal and exclusion orders would be reviewed by DHS for civilian agencies, DOD for national security systems, and DNI for "sensitive comparted systems." If each of these agencies concur in the Council's recommendations and issue these orders, then GSA would implement government-wide orders to exclude IT sources or remove IT from specified sources. The Council must also develop "a strategic plan for addressing supply chain risks posed by the acquisition of covered articles and for managing such risks."

The bill makes each agency head responsible to managing and mitigating IT supply chain risks, including "developing an overall supply chain risk management strategy and implementation plan and policies and processes to guide and govern supply chain risk management activities." Agency heads may carry out a "covered procurement action" (i.e. excluding sources posing IT supply chain risks, a source that fails to meet an acceptable rating, or withholding consent for a contractor to subcontract with a certain source) after receipt of a joint determination from the agency's CIO and chief acquisition officer. Entities subject to a covered procurement action must be informed of this action and have the opportunity to produce evidence arguing against this determination. This process may be expedited if national security calls for it, and effected entities would have a delayed opportunity to respond.

Title I of the bill contains provisions requiring DHS to establish a policy on how entities may report vulnerabilities in DHS IT to the agency and how the agency may use these vulnerabilities, including possible public disclosure. This policy must be made publicly available, and the agency must annually brief relevant committees in Congress on the policy for three years. DHS must also establish "a bug bounty pilot program to minimize vulnerabilities of appropriate information systems of the Department."

Five Eyes and Others Attribute Hacks To China; DOJ Indicts Hackers

On December 20, the United States, United Kingdom, Canada, Australia, and New Zealand (the Five Eyes nations) identified and condemned a Chinese campaign dating back to 2014 to hack into unnamed managed service providers (MSP) spanning at least 12 countries designed "to gain unauthorized access to the computers and computer networks of the MSP's clients and steal, among other data, intellectual property and confidential business data on a global scale" according to a U.S. indictment. What is being called the "MSP Theft Campaign" allegedly targeted the MSPs' of "companies that were involved in a diverse array of commercial activity, industries, and technologies, including banking and finance, telecommunications and consumer electronics, medical equipment, packaging, manufacturing, consulting, healthcare, biotechnology, automotive, oil and gas exploration, and mining." The U.S. also pinned the blame for a campaign targeting U.S. companies on these hackers, that included a breach of the Navy's systems. It is unlikely that the two suspects named in the indictment will be tried in U.S. courts.

In a statement, Secretary of State Mike Pompeo and Secretary of Homeland Security Kirstjen Nielsen asserted that "[s]ince at least 2014, Chinese cyber actors associated with the Chinese Ministry of State Security have hacked multiple U.S. and global managed service and cloud providers." They claimed that "[t]hese Chinese actors used this access to compromise the networks of the providers' clients, including global companies located in at least 12 countries." Pompeo and Nielsen stated that "[t]he United States is concerned that this activity violates the 2015 U.S.-China cyber commitments made by President Xi Jinping to refrain from conducting or knowingly supporting 'cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.'" They called on China "to abide by its commitment to act responsibly in cyberspace" and reiterated "that the United States will take appropriate measures to defend our interests."

In his remarks, Deputy Attorney General Rod Rosenstein claimed

> More than 90 percent of the Department's cases alleging economic espionage over the past seven years involve China. More than two-thirds of the Department's cases involving thefts of trade secrets are connected to China. In the last few months of this year, our Department has announced charges in three cases alleging crimes committed at the behest of a branch of the Chinese Ministry of State Security.

Rosenstein added

> Today's charges mark an important step in revealing to the world China's continued practice of stealing commercial data. Responding to that conduct requires a strategic approach to the threats that China poses. That is why the

> Department of Justice recently announced an initiative to address the full range of threats. One tactic is to increase our enforcement efforts. Another is to conduct foreign investment reviews to protect against China improperly acquiring sensitive information. A third is to find ways to better protect our telecommunications networks.

In a press release, the Department of Justice (DOJ) announced indictments of two members "of a hacking group operating in China known within the cyber security community as Advanced Persistent Threat 10 (the APT10 Group)." DOJ claimed that "[t]he defendants worked for a company in China called Huaying Haitai Science and Technology Development Company (Huaying Haitai) and acted in association with the Chinese Ministry of State Security's Tianjin State Security Bureau." It is unlikely that the two suspects named in the indictment will be tried in U.S. courts.

The DOJ stated

> Through their involvement with the APT10 Group, from at least in or about 2006 up to and including in or about 2018, Zhu [Hua] and Zhang [Shilong] conducted global campaigns of computer intrusions targeting, among other data, intellectual property and confidential business and technological information at managed service providers (MSPs), which are companies that remotely manage the information technology infrastructure of businesses and governments around the world, more than 45 technology companies in at least a dozen U.S. states, and U.S. government agencies. The APT10 Group targeted a diverse array of commercial activity, industries and technologies, including aviation, satellite and maritime technology, industrial factory automation, automotive supplies, laboratory instruments, banking and finance, telecommunications and consumer electronics, computer processor technology, information technology services, packaging, consulting, medical equipment, healthcare, biotechnology, pharmaceutical manufacturing, mining, and oil and gas exploration and production. Among other things, Zhu and Zhang registered IT infrastructure that the APT10 Group used for its intrusions and engaged in illegal hacking operations.

The press release and indictment also revealed that the two defendants had engaged in a Technology Theft Campaign starting in 2006 described as "an intrusion campaign to obtain unauthorized access to the computers and computer networks of commercial and defense technology companies and U.S. government agencies in order to steal information and data concerning a number of technologies." APT 10 allegedly accessed the computers and systems of 45 entities in 12 states and "stole hundreds of gigabytes of sensitive data." These hackers also "compromised more than 40 computers in order to steal confidential data from those systems belonging to

the United States Department of the Navy, including the personally identifiable information of more than 100,000 Navy personnel."

Senate Intelligence Committee Releases Two Third-Party Reports On 2016 Election

The Senate Intelligence Committee released "two independent analyses of social media tactics used by Russia's Internet Research Agency (IRA) in their attempts to influence U.S. political discourse" according to the Committee's press release. The Committee claimed that "[t]he reports are the first comprehensive analyses of their kind conducted by entities other than social media companies themselves, and are based in part on data provided by the [Committee]." The Committee added that "[t]he reports, titled "*The Tactics and Tropes of the Internet Research Agency*" and "*The IRA and Political Polarization in the United States, 2015-2017*," were authored by New Knowledge, and University of Oxford and Graphika, respectively." The Committee cautioned that "[t]he findings, interpretations, and conclusions presented within are those of the authors and do not necessarily represent the views of the Senate Intelligence Committee or its Membership." The Committee added that it "will release its own report on social media with its findings as an installment of its investigation."

New Knowledge concluded

> There remains much to be done. With regard to the Internet Research Agency specifically, further investigation of subscription and engagement pathways is needed; and only the platforms currently have that data. Understanding the reactions of targeted Americans, and attempting to gauge the impact that the repeated exposure to this propaganda had, is also a key area for ongoing investigation; only the platforms have the comment data. We hope that platforms will provide more data that can speak to the impact and uptake among targeted communities.
>
> More broadly, we must promote a multi-stakeholder model in which researchers, tech platforms, and government work together to detect foreign influence operations that attempt to undercut public discourse and democracy. The United States government has departments with decades of experience managing foreign propaganda and espionage. But because these influence operations are happening on private social platforms, there has been minimal information sharing. Robust collaboration between government agencies, platforms, and private companies is key to combatting this threat.

University of Oxford and Graphika stated that

Finally, this process of investigating IRA activities has also allowed us—as researchers—to develop some recommended best practices for social media firms that want to hold the public trust. First, all social media platforms should provide an open and consistent API that allows researchers to analyze important trends in public life. For example, Twitter used to provide researchers at major universities with access to several APIs, but has withdrawn this and provides so little information on the sampling of existing APIs that researchers increasingly question its utility for even basic social science. Facebook provides an extremely limited API for the analysis of public pages, but no API for Instagram. Facebook provided the US Senate with information on the organic post data of 81 Facebook pages, and the data on Facebook ads bought by 76 accounts. Twitter's data contribution covered activity in multiple languages, but Facebook's data contribution focuses on activity only in English. Facebook chose not to disclose data from IRA *Profiles* or *Groups* and only shared organic post data from a small number of *Pages* with the Committee. Google chose to supply the Senate committee with data in a non-machine-readable format. The evidence that the IRA had bought ads on Google was provided as images of ad text and in PDF format whose pages displayed copies of information previously organized in spreadsheets. This means that Google could have provided the useable ad text and spreadsheets—in a standard machine- readable file format, such as CSV or JSON, that would be useful to data scientists—but chose to turn them into images and PDFs as if the material would all be printed out on paper.

Even in times of crisis, social media firms need to co-operate with public agencies in a way that respects users' privacy. However, sharing data about public problems should be more than performative, it should be meaningful and constructive. And it should be matched with responsive support and communication channels so that researchers can make progress understanding problems that the social media firms themselves seem to have difficulty investigating.

Equifax Investigation Yields Differing Remedies

The Republican and Democratic staffs of the House Oversight and Government Reform Committee have released a report that "explains the circumstances of the cyberattack against Equifax, one of the largest consumer reporting agencies (CRA) in the world," that ultimately effected 148 million Americans. However, the Democratic staff of the House Oversight and Government Reform and House Science Committees released recommendations aside and apart from Republican recommendations in the report.

Not surprisingly, the broad remedies called for by Republicans and Democrats differ and align closely with previously proposed policies to address cyber and data security generally and how well CRAs are storing and safeguarding consumer information specifically. Although, there is some shared ground arising from both staffs recommending that CRAs be more tightly regulated and that federal contractors be subject to a NIST standard currently applicable only to DOD contractors that requires safeguarding parts of their systems that are being not used for performance of the federal contract.

In its press release, Republican staff summarized the "Key Findings," with which Democrats did not explicitly disagree:

- Entirely preventable. Equifax failed to fully appreciate and mitigate its cybersecurity risks. Had the company taken action to address its observable security issues, the data breach could have been prevented.
- Lack of accountability and management structure. Equifax failed to implement clear lines of authority within their internal IT management structure, leading to an execution gap between IT policy development and operation. Ultimately, the gap restricted the company's ability to implement security initiatives in a comprehensive and timely manner.
- Complex and outdated IT systems. Equifax's aggressive growth strategy and accumulation of data resulted in a complex IT environment. Both the complexity and antiquated nature of Equifax's custom-built legacy systems made IT security especially challenging.
- Failure to implement responsible security measurements. Equifax allowed over 300 security certificates to expire, including 79 certificates for monitoring business critical domains. Failure to renew an expired digital certificate for 19 months left Equifax without visibility on the exfiltration of data during the time of the cyberattack.
- Unprepared to support affected consumers. After Equifax informed the public of the data breach, they were unprepared to identify, alert and support affected consumers. The breach website and call centers were immediately overwhelmed, resulting in affected consumers being unable to access information necessary to protect their identity.

The Republican recommendations point to possible legislation focused on expanding the FTC's powers to regulate only the CRAs. Currently, the FTC uses Section 5 of the FTC Act and Gramm-Leach-Bliley to regulate the data security of CRAs. This approach would be in line with the response to the Equifax breach many Republicans preferred (i.e. a bill tightly focused on CRAs and not a larger data security bill.) Otherwise, the recommendations place the onus on action by the private sector and consumers that is ideally guided and encouraged by the federal government:

- Recommendation 1: Empower Consumers through Transparency

- Recommendation 2: Review Sufficiency of FTC Oversight and Enforcement Authorities
- Recommendation 3: Review Effectiveness of Identity Monitoring and Protection Services Offered to Breach Victims
- Recommendation 4: Increase Transparency of Cyber Risk in Private Sector
- Recommendation 5: Hold Federal Contractors Accountable for Cybersecurity with Clear Requirements
- Recommendation 6: Reduce Use of Social Security Numbers as Personal Identifiers
- Recommendation 7: Implement Modernized IT Solutions

As is to be expected, Democrats formulated different recommendations based on a more aggressive regulatory regime directed by new federal legislation:

- hold federal financial regulatory agencies accountable for their consumer protection oversight responsibilities;
- require federal contractors to comply with established cybersecurity standards and guidance from the NIST
- establish high standards for how data breach victims should be notified; and
- strengthen the ability of the FTC to levy civil penalties for private sector violations of consumer data security requirements.

OMB Revises Program To Protect Federal Crown Jewels

The Office of Management and Budget (OMB) has released a memorandum that revamps the federal government's program to identify and protect High Value Assets (HVA), which was started by the Obama Administration in 2015 in response to the breach at the Office of Personnel Management (OPM.) The program has undergone a few different iterations, and this most recent iteration rescinds the previous OMB memoranda and changes the program.

This memorandum "outlines expectations for the following areas:"

- Establishing Enterprise HVA Governance;
- Improving the Designation of HVAs;
- Implementing Data-Driven HVA Prioritization; Increasing the Trustworthiness of HVAs;
- Protecting Privacy and HVAs; and
- Defining HVA Reporting, Assessment, and Remediation Requirements.

OMB explained that "the HVA program is expanding to support all agencies, including both CFO Act and non-CFO Act agencies (i.e. more than two dozen federal agencies such as the FTC, CFTC, and EEOC), in HVA identification, assessment, remediation, and response to incidents." The definition of what is an HVA is expanded to include "the establishment of multiple categories under which an agency

may designate an HVA." Agencies themselves are responsible for identifying HVAs except with respect to "national security" HVAs which OMB and/or DHS can designate. However, this authority reserved for OMB and DHS does not apply to "national security systems" (NSS) (i.e. those systems critical to the execution of military, intelligence, and cryptologic operations).

In order to increase the trustworthiness of information systems, agencies must take the following actions that would likely have downstream effects in how IT is developed for the federal government:

- Implement the systems security engineering principles, concepts, techniques, and System Development / Engineering Lifecycle (SDLC / SELC) in NIST SP 800-160, Volume 1, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems for all HVAs
- Ensure that security and privacy requirements for HVAs reflect the systems security engineering principles, concepts, and techniques that have been incorporated into their enterprise architecture and procurements; and,
- Ensure that the procurement of information systems, system components, applications, or services designated as HVAs or that are intended to support HVAs, include requirements for developers, manufacturers, and vendors to employ systems security and privacy engineering concepts and methods, security and privacy design principles, secure coding techniques, and trusted computing methods in the system development life cycle.

OMB noted that "[t]he HVA program does not supersede, but rather compliments the responsibilities of agencies as required by the Federal Information Security Modernization Act of 2014." OMB added that "[t]his memorandum consolidates and updates previous requirements from OMB memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government,* and OMB memorandum M-17-09, *Management of Federal High Value Assets,* and rescinds these memoranda in accordance with burden reduction guidance in OMB memorandum M-17-26, *Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memorandum.*"

Senate Democrats Unveil Privacy Bill

Senator Brian Schatz (D-HI) and 14 other Senate Democrats introduced the "Data Care Act" (S. 3744) which would extend the concept of fiduciary responsibility currently binding on health care professionals and attorneys with respect to the patients and clients' information to "online service providers" such as Facebook, Google, Apple, etc. In short, these online service providers would be severely be limited on how they collect, share, and sell the personally identifiable information (PII), for these companies would need to treat their customers' PII as privileged and

deserving of a greater level of protection, much like the HIPAA regulations impose this standard on health care providers or bar associations' rules on attorneys. However, the scope of who is an online service provider would seem to encompass most consumer-oriented companies doing business on the internet. Yet, like most other privacy and data security bills, the Federal Trade Commission (FTC) would enforce the new regime.

An "online service provider" is defined as an entity "engaged in interstate commerce over the internet or any other digital network; and in the course of business, collects individual identifying data about end users, including in a manner that is incidental to the business conducted." However, the FTC would have the discretionary authority to exclude categories of online service providers from the fiduciary duties the bill would otherwise impose. The FTC is directed to consider the privacy risks posed by the category of online service provider.

The bill requires that "[a]n online service provider shall fulfill the duties of care, loyalty, and confidentiality" towards consumers' personal information, which is broadly defined in the bill. The duty of care requires online service providers to "reasonably" safeguard "individual identifying data" from unauthorized access and notify consumers of any breach of this duty, subject to FTC regulations that would be promulgated. The duty of loyalty would require online service providers to not use the information in a way that benefits them to the detriment of consumers, including uses that would result in reasonably foreseeable material physical or financial harm to the consumer. Finally, the duty of confidentiality limits the disclosure or sale of consumers' information to instances where the duties of care and loyalty are observed (i.e. when the information must be safeguarded and not used to the detriment of consumers). Moreover, under this duty, should an online service provider wish to share or sell consumers' information with a third party, they would need to enter into a contract with the other party that requires them to meet the same duties of care, loyalty, and confidentiality.

As noted, the FTC would enforce the act and would have the authority to levy fines in the first instance for violations, but state attorneys general would also be able to bring actions for violations in the event the FTC does not act or after FTC action. This latter power has long been a Democratic priority in the realm of data security and may be a non-starter with Republicans. Moreover, the bill does not preempt state laws, meaning the FTC could investigate a violation under this act and states could investigate under their laws. The FTC would be given authority under the APA to promulgate regulations regarding data breach notification instead of the much more onerous Moss-Magnuson rulemaking procedures the FTC must otherwise use. These regulations include the aforementioned regulations on breach notification and some possible exemptions to the duties that would otherwise apply to online service

providers (e.g. small companies). The bill expands the FTC's jurisdiction over non-profit entities and common carriers that may also be online service providers.

This bill is much more narrowly focused than Senator Ron Wyden's (D-OR) bill, the "Consumer Data Protection Act" (S. 2188) that would vastly expand the power of the FTC to police both the security and privacy practices off many U.S. and international multinational companies, largely regardless of sector. The Data Care Act is a more mainstream Democratic bill. However, as of yet, a companion bill has not yet been introduced in the House, and the Democrat's ultimate position on how to regulate the privacy practices of companies may come down to what House Democrats produce. Moreover, the HIPAA/attorney model may be seen as worth extending to all entities collecting, disclosing, or selling PII as one means of addressing data security standards.

HHS Begins Review of HIPAA Regulations

This month, the Department of Health and Human Services' Office for Civil Rights (OCR) released a Request for Information (RFI) that could result in the most significant amendment to the HIPAA regulations since the HITECH Act. OCR is at the very beginning of the process, and there is no sense as to when there may be draft regulations available for comment or review. Nonetheless, OCR is accepting comments on its RFI until February 12, 2019.

OCR stated that the purpose of the RFI is "to assist OCR in identifying provisions of the Health Insurance Portability and Accountability Act (HIPAA) privacy and security regulations that may impede the transformation to value-based health care or that limit or discourage coordinated care among individuals and covered entities (including hospitals, physicians, and other providers, payors, and insurers), without meaningfully contributing to the protection of the privacy or security of individuals' protected health information." OCR explained that "[t]his RFI requests information on whether and how the rules could be revised to promote these goals, while preserving and protecting the privacy and security of such information and individuals' rights with respect to it."

OCR explained that it

> seeks public input on ways to modify the HIPAA Rules to remove regulatory obstacles and decrease regulatory burdens in order to facilitate efficient care coordination and/or case management and to promote the transformation to value-based health care, while preserving the privacy and security of protected health information (PHI). Specifically, OCR seeks information on the provisions of the HIPAA Rules that may present obstacles to, or place unnecessary burdens on, the ability of covered entities and business associates to conduct

care coordination and/or case management, or that may inhibit the transformation of the health care system to a value-based health care system. Correspondingly, OCR seeks comment on modifications to the HIPAA Rules that would facilitate efficient care coordination and/or case management, and/or promote the transformation to value-based health care. OCR also broadly requests information and perspectives from regulated entities and the public about covered entities' and business associates' technical capabilities, individuals' interests, and ways to achieve these goals.

Additionally, OCR wants "comment on aspects of the Privacy Rule that OCR has identified for potential modification to further these goals, specifically:

- Promoting information sharing for treatment and care coordination and/or case management by amending the Privacy Rule to encourage, incentivize, or require covered entities to disclose PHI to other covered entities.
- Encouraging covered entities, particularly providers, to share treatment information with parents, loved ones, and caregivers of adults facing health emergencies, with a particular focus on the opioid crisis.
- Implementing the HITECH Act requirement to include, in an accounting of disclosures, disclosures for treatment, payment, and health care operations (TPO) from an electronic health record (EHR) in a manner that provides helpful information to individuals, while minimizing regulatory burdens and disincentives to the adoption and use of interoperable EHRs.
- Eliminating or modifying the requirement for covered health care providers to make a good faith effort to obtain individuals' written acknowledgment of receipt of providers' Notice of Privacy Practices, to reduce burden and free up resources for covered entities to devote to coordinated care without compromising transparency or an individual's awareness of his or her rights.

Senate Passes Energy Cyber Security Bill

Earlier this month, the Senate sent a bill to the House that would task the Department of Energy with setting up a pilot program to identify security vulnerabilities and possible technological solutions for critical cyber infrastructure in the energy sector, including "analog and nondigital control systems." The "Securing Energy Infrastructure Act" (S. 79) would also require the Department to "develop a national cyber-informed engineering strategy to isolate and defend covered entities from security vulnerabilities and exploits in the most critical systems" of the energy sector. However, it is unlikely this bill becomes law in the current Congress, but it is likely the bill's sponsors will try again in the next Congress.