Cyber Update
13 March 2019
By Michael Kans

House Passes Package of Election Reforms, Including Election Cybersecurity Provisions

Last week, the House passed the "For the People Act" (H.R. 1), a House Democratic priority bill, a package of electoral reforms that would seek to bolster the cybersecurity of election systems across the country. The House Rules Committee posted an amended version of the bill that would be considered by the House and the 72 amendments made in order under the rule governing debate. Last week, the House Administration Committee marked up the bill and reported out a bill with an amendment in the nature of a substitute. The Committee provided a summary of the changes made to the underlying bill.

And, yet, if this bill were enacted as written, there would be significant changes to current regulation. However, it is unlikely the Senate will take up this bill as written, and any measure in the Senate regarding election security would be more circumscribed.

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. For example, "qualified election infrastructure vendors" must agree "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 $1.7 billion in funding for 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

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

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 package requires "qualified election infrastructure vendors" (i.e. "any person who provides, supports, or maintains, or who seeks to provide, support, or maintain, election infrastructure on behalf of a State, unit of local government, or election agency") to meet these requirements:

- [T]o 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.
- [T]o maintain its information technology infrastructure in a manner that is consistent with the cybersecurity best practices issued by the Technical Guidelines Development Committee.
- Reporting cybersecurity incidents "involving any of the goods and services provided by the vendor" to the EAC and DHS within three days of discovery
- "[T]o permit independent security testing by the [EAC]...and by the Secretary of the goods and services provided by the vendor pursuant to a grant"

Last week, the EAC's Technical Guidelines Development Committee released for comment "Proposed Voluntary Voting System Guidelines 2.0 Principles and Guidelines" that would serve as a basis for rewriting the current voluntary standards in place. If the provisions in H.R. 1 pertaining to the Technical Guidelines Development Committee

These draft Principles and Guidelines direct that voting systems should be interoperable, protect voter privacy, provide robust safety, restricts access to appropriate parties, safeguards data from unauthorized access, modification, or deletion, maintains system integrity, and furnish the means to detect anomalous or malicious behavior. Once these Principles and Guidelines are finalized, the Technical

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

Guidelines Development Committee will issue Requirements that contain more detailed voluntary standards.

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 of state and local elections systems to the Government Facilities sector.

The Committee Report provides an overview of the cybersecurity and technology related provisions in H.R. 1:

> *Bolstering the Resilience of Election Infrastructure*
> There are serious challenges with aging election equipment and the machinery of democracy. Ineffective, aging voting equipment can cause lengthy lines at polling places, discourage participation, and chip away at confidence in election outcomes. A 2014 report by the bipartisan Presidential Commission on Election Administration found that aging systems purchased with federal money pursuant to the Help America Vote Act in 2002 were "reaching the end of their operational life."
> Foreign threats to interfere in American elections are also of paramount concern, including the threats that cyberattacks pose to voting systems. The Department of Homeland Security confirmed that "election-related networks, including websites, in 21 states were potentially targeted by Russian government cyber actors" during the 2016 election. Nonstate and state actors alike have targeted voter registration systems and Election Night reporting websites. These tactics could sow confusion and undermine confidence in election outcomes should they occur again on a larger scale due to the vulnerabilities in our systems.
> There is a need to bolster the resilience of the machinery of democracy that H.R. 1 fulfills. Thirteen states use voting machines that do not have paper back-ups, for example, including five that use them statewide.
>
> *Promoting Cybersecurity Through Improvements in Election Administration*
> Given the threat of interference in our elections from state and nonstate actors alike, H.R. 1 provides guardrails to further rein- force cybersecurity. It requires, for example, voting systems (including electronic pollbooks) to be tested nine months before general Federal elections. The Election Assistance Commission would be required to issue election cybersecurity guidelines, including

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

standards and best practices for procuring, maintaining, testing, operating, and updating election systems to prevent and deter cybersecurity incidents.
Another innovative element of the bill is the establishment of an Election Security Bug Bounty program to encourage independent assessments of election systems by technical experts.

Honest Ads Act
The Honest Ads Act updates the rules that apply to online political advertising by incorporating disclosure and disclaimer concepts that apply to traditional media, while providing regulatory flexibility for new forms of digital advertising. This will help ensure that voters make informed decisions at the ballot box and to know who is spending money on digital political advertisements that they view.
It also expands the definition of public communication to include paid internet or paid digital communications, and amends the definition of electioneering communication to include certain digital or internet communications placed or promoted for a fee online.
Finally, the bill requires that large online platforms (defined to include those with 50,000,000 or more unique monthly United States visitors) maintain public databases of political ad purchases. This is a concept that already applies to broadcasters, who must maintain public files of political advertisements. The online data- bases maintained by the platforms will provide the public with in- formation about the purchasers of online political ads, including how the audience is targeted. Political advertisements are defined to include those that communicate messages relating to political matters of national importance, including about candidates, elections, and national legislative issues of public importance.
Finally, the Honest Ads Act requires all broadcasters, cable or satellite television and online platforms to take reasonable efforts to ensure that political advertising is not purchased by foreign nationals, directly or indirectly.

FISA Reauthorization

Sparing has begun over the December expiration of Foreign Intelligence Surveillance Act (FISA) authorities used by U.S. intelligence agencies for surveillance of electronic communications. To the extent that Members want to see cybersecurity, data security, or privacy legislation enacted, this pending deadline to reauthorize what a number of stakeholders consider vital national security authorities may function to block consideration of such bills. Enactment of the "USA Freedom Act" (P.L. 114-23), a PATRIOT Act reauthorization, in mid-2015 cleared the path for consideration of cybersecurity information sharing legislation ultimately enacted in the "Cybersecurity Act of 2015" (P.L. 114-113).

This week, 30 progressive civil liberties and privacy groups sent a letter to House Democratic Leadership, asking them not to reauthorize three provisions in the "USA PATRIOT Act" (P.L. 107-56) that expire on December 15, 2019, including Section 215 the National Security Agency (NSA) has used to collect bulk telephone metadata among other communications. They stated "[w]e implore you to use the sunset of Section 215 as an opportunity to diminish rather than expand or extend the ability of Donald Trump and subsequent administrations to conduct mass surveillance of innocent people."

They stated

> More than five years have passed since the public became aware of the damning extent of mass surveillance that is conducted against innocent people in the United States pursuant to Section 215. Despite broad public outrage and several Congressional attempts to meaningfully reform Section 215, mass surveillance of innocent people continues. Indeed, one sub-provision of Section 215 created when the USA FREEDOM Act last extended this provision's sunset produced over 534 million call detail records in 2017, pursuant to only 40 orders. There are an additional 77 Section 215 orders from 2017, which have produced an unknown volume of additional records.

The letter comes a week after the *New York Times* quoted a top aide to House Minority Leader Kevin McCarthy (R-CA) in an article, claiming that the NSA is no longer using authority under the FISA that was exposed by former NSA contractor Edward Snowden. McCarthy's national security adviser Luke Murry made these claims during a *Lawfare* podcast.

In January 2018, Congress extended for six years Title VII of FISA that allows U.S. intelligence agencies to surveil non-U.S. persons outside the U.S. without a warrant and for non-intentional surveillance of U.S. persons reasonably believed to be outside the U.S. According to critics, the bill also allowed federal law enforcement and intelligence agencies to continue to conduct warrantless searches of communications acquired by the NSA in all cases except criminal investigations and authorized so-called "about" searches that would expand the scope of communications that could be examined.

Data Breach Hearing

On March 7 the Senate Homeland Security and Governmental Affairs Committee's Permanent Subcommittee on Investigations held a hearing entitled "Examining Private Sector Data Breaches."

The following witnesses appeared before the subcommittee:

Panel I

- Equifax, Inc. Chief Executive Officer Mark W. Begor
- Marriott International, Inc. President and Chief Executive Officer Arne M. Sorenson

Panel II

- Government Accountability Office Financial Markets and Community Investment Director Alicia Puente Cackley
- Federal Trade Commission Bureau of Consumer Protection Director Andrew Smith
- Center for Internet Security President and Chief Executive Officer John M. Gilligan

In concert with the hearing, Republican and Democratic Subcommittee staff released a report titled "How Equifax Neglected Cybersecurity And Suffered A Devastating Data Breach" that "investigated the causes of this breach to identify ways to prevent future incidents of this scope."

Staff made the following recommendations that would entail legislation:

> (1) Congress should pass legislation that establishes a national uniform standard requiring private entities that collect and store PII to take reasonable and appropriate steps to prevent cyberattacks and data breaches.
> (2) Congress should pass legislation requiring private entities that suffer a data breach to notify affected consumers, law enforcement, and the appropriate federal regulatory agency without unreasonable delay
> (3) Congress should explore the need for additional federal efforts to share information with private companies about cybersecurity threats and disseminate cybersecurity best practices that IT asset owners can adopt.
> (4) Federal agencies with a role in ensuring private entities take steps to prevent cyberattacks and data breaches and protect PII should examine their authorities and report to Congress with any recommendations to improve the effectiveness of their efforts.
> (5) Private entities should re-examine their data retention policies to ensure these policies properly preserve relevant documents in the event of a cyberattack.

Chairman Rob Portman (R-OH) remarked that "[i]t seems no industry is immune from data breaches that expose sensitive consumer information:

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

- Some of the biggest recent breaches have included Google+, Uber, Facebook, and the department store Saks Fifth Avenue.
- Government agencies have also suffered breaches, including over 20 million security clearance background files held by the Office of Personnel Management.

He said that the subcommittee's report "documents how Equifax failed to follow basic cyber security practices, which prevented the company from identifying and patching an exploitable vulnerability on its system." Portman said "Marriott's investigation determined that the hacker had access to guest information related to 383 million guest records since 2014.

- As part of the database, the hackers also gained access to over 23 million passport numbers and 9.1 million credit card numbers, most of which were expired.
- Marriott learned of the breach on September 8, 2018, but waited almost 12 weeks to notify the public on November 30, 2018.

Portman said that "[t]he goal of today's hearing and the Subcommittee's report is to fully understand these breaches; but also to find solutions:

- Companies and government agencies, alike, must take steps to protect the data consumers entrust to them.
- And when that data is compromised, we deserve to know as soon as possible so we can do everything we can to ensure criminals are not taking advantage of us.
- I look forward to working with my Ranking Member, Senator Carper, on legislation to ensure both the protection of consumer data and prompt notification when data is compromised.

Ranking Member Tom Carper (D-DE) stated that "[w]hen hackers are able to obtain someone's personal information, the consequences are real." He stated that "more than 40 percent of the individuals polled had discovered fraudulent charges on their credit cards…[and] [o]thers reported that someone had attempted to take out loans in their name, file tax returns in their name, or steal their identity." Carper claimed that "[h]ere in Congress, I think it's long past time for us to come to agreement on a federal data security law that lays out for private industry what we expect from them, both in data protection and data breach notification." He asserted that "[w]e also need to ensure that the system we've established for sharing information on cyber threats and cybersecurity best practices is as effective as it could be." Carper added that "[i]f a company as large and sophisticated as Equifax can fail so badly at implementing basic cybersecurity practices, we can certainly do a better job making clear what will and won't work when it comes to blocking hackers and preventing data breaches."

Puente Cackley asserted that "[r]ecent data breaches and developments regarding Internet privacy suggest that this is an appropriate time for Congress to consider what additional actions are needed to protect consumer privacy, including comprehensive Internet privacy legislation." She stated that "[a]lthough FTC has been addressing Internet privacy through its unfair and deceptive practices authority and FTC and other agencies have been addressing this issue using statutes that target specific industries or consumer segments, the lack of a comprehensive federal privacy statute leaves consumers' privacy at risk." Puente Cackley contended that "[c]omprehensive legislation addressing Internet privacy that establishes specific standards and includes APA notice-and-comment rulemaking and first-time violation civil penalty authorities could enhance the federal government's ability to protect consumer privacy, provide more certainty in the marketplace as companies innovate and develop new products using consumer data, and provide better assurance to consumers that their privacy will be protected." She stated that "[i]n our January 2019 report, we recommended that Congress consider developing comprehensive legislation on Internet privacy that would enhance consumer protections and provide flexibility to address a rapidly evolving Internet environment. Issues that should be considered include:

- which agency or agencies should oversee Internet privacy;
- what authorities an agency or agencies should have to oversee Internet privacy, including notice-and-comment rulemaking authority and first-time violation civil penalty authority; and
- how to balance consumers' need for Internet privacy with industry's ability to provide services and innovate."

Smith said the FTC "reiterates its longstanding bipartisan call for enactment of a comprehensive federal data security law." He noted that "[i]n particular, the FTC supports data security legislation that would provide the agency with three essential additional authorities:

(1) the ability to seek civil penalties to effectively deter unlawful conduct,
(2) jurisdiction over non-profits and common carriers, and
(3) the authority to issue implementing rules under the Administrative Procedure Act (APA), as appropriate.

Smith added that "[u]nder current laws, the FTC only has the authority to seek civil penalties for data security violations related to children's online information (under COPPA) or credit report information (under the FCRA)."

Hearing on Diversity and Inclusion in the Technology Sector

The Consumer Protection and Commerce Subcommittee of the House Energy and Commerce Committee held a hearing titled "Inclusion in Tech: How Diversity Benefits

All Americans." Democrats released this background memorandum before the hearing.

The witnesses were:

- Brookings Institution Fellow Nicol Turner Lee, Ph.D.
- Digital Media Strategist Mark Luckie
- Asian Americans Advancing Justice Vice President Jiny Kim
  Rutgers Law School Co-Dean David Lopez
- Disability:IN President & CEO Jill Houghton
- University of Maine President Joan Ferrini-Mundy, PhD
- Military Talent Partners Natalie Oliverio CEO

Chair Jan Schakowsky (D-IL) remarked that whereas technology continues to play a bigger and bigger role in the lives of Americans, technology's workforce remains largely homogeneous. She said that women, people of color, and older Americans have all been noticeably absent from the tech workforce. Schakowsky said that the corresponding problem for this lack of diversity is that the technology itself reflects this lack of diversity. She said there are real world implications. For example, some algorithms show bias in recommending sentencing guidelines and some soap dispensers do not recognize the hands of African Americans and Latinos. Schakowsky suggested that unfair practices and extreme market concentration in the tech sector may accentuate the bias in the "young boys club we're examining today."

Ranking Member Cathy McMorris Rodgers (R-WA) said that "[t]oday we are focused on an issue I have led on for quite some time: diversity in the tech industry." She said that "we will have an opportunity to give credit where credit is due, while also exploring how we continue to do better...especially where we can continue to improve where we recruit, retain, and promote a more diverse workforce." McMorris Rodgers said that "[a]s the *Wall Street Journal* just reported, women are driving the labor- force comeback...[and] a record number of African Americans, Hispanics, and people with disabilities are coming off the sidelines and finding work." She said that "[i]t means that more people are finding opportunities for a better life in healthcare, energy, construction, the service industry and more...[and] [t]oday's hearing is about ensuring more individuals have opportunities to pursue and advance careers in the tech industry too." McMorris Rodgers said that "[w]e need to continue to do more to address the pipeline, whether it's young people of every background and girls in elementary and middle school... and exceptional people with disabilities...[and] [w]e also need to focus on how we retain those individuals once they are recruited and do more to encourage their promotion to leadership positions."

Turner Lee asserted that "that the absence of diversity among the people that make the decisions around products and services for the tech sector, along with the markets

that these companies serve will ultimately doom the United States to abysmal failure." She recommended the following:

- Companies that are disrupting societal norms through the sharing economy, social media and the internet of things must do better to address the less than remarkable representation of people of color as creators, influencers and decision makers. As in the case of Historically Black Colleges and Universities (HBCUs) and Hispanic-Serving Institutions (HSIs), the tech sector should work to strengthen those relationships and programs, which target these students for future employment. Congress and federal agencies, including the U.S. Department of Education, need to also do more to ensure that minority-serving institutions are establishing premiere programs that include both technology access and cutting-edge career development in fields where the nation will soon face massive shortages.
- The tech sector must be more proactive in developing solutions that reduce, or better yet, eliminate bias from newer and emerging technologies. Transitioning to a more of a "white-box" construct for designing and evaluating algorithms, the tech sector can employ better practices that pre-identify potential unintended consequences of algorithms, while minimizing the effects of digital inequalities. Further, tech companies must recognize that data scientists, engineers and other innovators bring their own set of explicit, implicit, and unconscious biases to the design of computer systems and computational procedures.
- Congress should consider a review and the potential modernization of civil rights laws and apply them to certain online use cases. In 1964, Congress passed Public Law 88-52 that "forbade discrimination on the basis of sex as well as race in hiring, promoting, and firing." The Civil Rights Act of 1968 was amended to include the Fair Housing Act, which further prohibits discrimination in the sale, rental and financing of dwellings, and in other housing-related transactions to federally mandated protected classes. The Equal Credit Opportunity Act (ECOA) in 1974 prohibits any creditor from discriminating against any applicant from any type of credit transaction based on protected characteristics. Without question, many of these legislative and regulatory frameworks should be applied to digital and other-related activities which seek to harm online users, especially individuals from protected classes.

Luckie stated that "The concern surrounding the lack of diversity at U.S. technology companies is not just about the fair treatment of their employees...[and] [w]hat is even more alarming is the inequalities in consumer technology that the deficiency is creating." He stated that "[u]nfortunately, there is no shortage of examples of discrimination built into the products emerging from Silicon Valley companies:

- COMPAS, the artificial intelligence software used across the country by judges to determine if a convicted criminal is likely to commit more crimes, was found

to be biased against minorities. The formula built into the product was particularly likely to falsely flag black defendants as future criminals, wrongly labeling them this way at almost twice the rate as white defendants, according to *ProPublica*.

- When Amazon's Prime same-day delivery service rolled out nationally in 27 metropolitan areas, it excluded ZIP codes that have predominantly black populations, according to an analysis by Bloomberg.
- Upon its release in 2014, Apple's HealthKit app enabled users to track a wide range of vital functions like sleep, blood pressure, calorie intake, respiratory rate, blood-alcohol level, and even copper intake. But it did not track menstrual cycles, one of the most fundamental parts of women's lives, until one year later.
- A widely circulated video on YouTube shows a "smart" soap dispenser that automatically detects when a hand is waved beneath its nozzle but appears to not work on black skin.
- The website for The Princeton Review's online SAT prep course listed prices that varied depending on the ZIP code of the user, according to another *ProPublica* investigation. Asians were nearly twice as likely to be charged a higher price, even if the income in their area was below average.

FTC Seeks Comments on Potential Changes to Financial Services Data Security Regulations

Last week, the Federal Trade Commission (FTC) released notices of proposed rulemaking (NPRM) for two of the data security regulations with which some financial services companies must comply:

- Standards for Safeguarding Customer Information (Safeguards Rule)
- Privacy of Consumer Financial Information Rule (Privacy Rule)

The reassessment of the Safeguards Rule began in 2016 when the FTC asked for comments. The proposed Safeguards Rule demonstrates the agency's thinking on what data security regulations should look like, which is important because the FTC is the agency most likely to become the enforcer and writer of any new data security or privacy regulations. Notably, the new Safeguards regulation would require the use of certain best practices such as encrypting data in transit or at rest or requiring the use of multi-factor authentication "for any individual accessing customer information." Moreover, the other financial services agencies charged with implementing the section of Gramm-Leach-Bliley (GLB) that requires financial services companies to safeguard customers' information may follow suit (e.g. the Federal Reserve Board or the Comptroller of the Currency.)

In the proposed rule, the FTC noted that its changes to the Safeguards Rule would "include more detailed requirements for the development and establishment of the information security program required under the Rule…[and] [t]hese amendments are based primarily on the cybersecurity regulations issued by the New York Department of Financial Services, 23 NYCRR 500 ("Cybersecurity Regulations"), and the insurance data security model law issued by the National Association of Insurance Commissioners ("Model Law")."

The FTC's authority to regulate the security and privacy of consumers' information held by some financial services companies was provided under the "Gramm-Leach-Bliley Act" and later significantly narrowed under the "Dodd-Frank Act," which transferred much of the rulemaking authority for the Privacy Rule to the Consumer Financial Protection Bureau (CFPB), which is now titled Regulation P. The FTC retained rulemaking authority under the Privacy Rule only over "motor vehicle dealers that are predominantly engaged in the sale and servicing or the leasing and servicing of motor vehicles, excluding those dealers that directly extend credit to consumers and do not routinely assign the extensions of credit to an unaffiliated third party." Moreover, and perhaps more importantly, the FTC retained enforcement authority for its portion of the Privacy Rule.

The FTC noted

> In light of this history, the Commission is issuing this notice of proposed rulemaking. The Commission now proposes to make three types of changes to the Privacy Rule: (1) technical changes to the Rule to correspond to the reduced scope of the Rule due to Dodd-Frank Act changes, which primarily consist of removing references that do not apply to motor vehicle dealers; (2) modifications to the annual privacy notice requirements to reflect the changes made to the GLBA by the FAST Act; and (3) a modification to the scope and definition of "financial institution" to include entities engaged in activities that are incidental to financial activities, which would bring the Rule into accord with the CFPB's Regulation P.

In the Safeguards Rule proposal, the FTC explained

> The proposal contains five main modifications to the existing Rule.
>
> - First, it adds provisions designed to provide covered financial institutions with more guidance on how to develop and implement specific aspects of an overall information security program, such as access controls, authentication, and encryption.

- Second, it adds provisions designed to improve the accountability of financial institutions' information security programs, such as by requiring periodic reports to boards of directors or governing bodies.
- Third, it exempts small businesses from certain requirements.
- Fourth, it expands the definition of "financial institution" to include entities engaged in activities that the Federal Reserve Board determines to be incidental to financial activities. Such a change would add "finders"–companies that bring together buyers and sellers of a product or service–within the scope of the Rule.
- Finally, the Commission proposes to include the definition of "financial institution" and related examples in the Rule itself rather than incorporate them by reference from a related FTC rule, the Privacy of Consumer Financial Information Rule.

The FTC's Safeguards Rule applies to the following and other entities:

> [M]ortgage lenders, "pay day" lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors and other financial advisors, tax preparation firms, non- federally insured credit unions, investment advisors that are not required to register with the Securities and Exchange Commission, and entities acting as finders.

The FTC explained that it "is proposing to expand the definition of "financial institution" in both the Privacy Rule and the Safeguards Rule to specifically include so-called "finders," those who charge a fee to connect consumers who are looking for a loan to a lender...[because] [t]his proposed change would bring the Commission's Rule in line with other agencies' interpretation of the Gramm Leach Bliley Act."

GAO's High-Risk List Continues To Flag Technology Items

The Government Accountability Office (GAO) has released its biennial High-Risk List, and to no great surprise, the GAO flagged a number of cybersecurity, data security, information technology (IT), and acquisitions problems still plaguing federal agencies. However, of note, the GAO removed the DOD's supply chain management from the High-Risk List because of the Pentagon made "made progress on seven actions and outcomes related to monitoring and demonstrated progress that GAO recommended for improving supply chain management." However, on the negative side of the ledger, the GAO again takes the federal government, particularly the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS), to task for failing to implement the GAO's many recommendations on IT acquisition and cybersecurity. Additionally, the GAO is calling for Congress to update the

Privacy Act of 1974 and the e-Government Act of 2002, and to address privacy and data security at the federal level.

Overall, the GAO noted:

> Since GAO's last update in 2017, seven areas improved, three regressed, and two showed mixed progress by improving in some criteria but declining in others. Where there has been improvement in high-risk areas, congressional actions have been critical in spurring progress in addition to actions by executive agencies.

Here are the technology-related items the GAO considers high-risk and their recommendations:

> **Ensuring the Cybersecurity of the Nation**
> We have identified four major cybersecurity challenges facing the nation: (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data. To address the four major cybersecurity challenges, we identified 10 critical actions the federal government and other entities need to take. These critical actions include, for example, developing and executing a more comprehensive federal strategy for national cybersecurity and global cyberspace; addressing cybersecurity workforce management challenges; and strengthening the federal role in protecting the cybersecurity of critical infrastructure.
>
> We also have previously suggested that Congress consider amending laws, such as the Privacy Act of 1974 and the E-Government Act of 2002, because they may not consistently protect PII. Specifically, we found that while these laws and guidance set minimum requirements for agencies, they may not consistently protect PII in all circumstances of its collection and use throughout the federal government, and may not fully adhere to key privacy principles. However, the relevant revisions to the Privacy Act and the E-Government Act had not yet been enacted as of the date of this report.
>
> Further, we suggested that Congress consider strengthening the consumer privacy framework and review issues such as the adequacy of consumers' ability to access, correct, and control their personal information; and privacy controls related to new technologies such as web tracking and mobile devices. However, these suggested changes had not yet been enacted as of the date of this report.

Strengthening Department of Homeland Security Management Functions

Over the years, we have made hundreds of recommendations related to DHS management functions and many have been implemented. Continued progress for this high-risk area depends primarily on addressing the remaining outcomes. In the coming years, DHS needs to continue implementing its Integrated Strategy for High-Risk Management to show measurable, sustainable progress in implementing corrective actions and achieving outcomes. In doing so, it remains important for DHS to

- maintain its current level of top leadership support and sustained commitment to ensure continued progress in executing its corrective actions through completion;
- continue to identify the people and resources necessary to make progress towards achieving outcomes, work to mitigate shortfalls and prioritize initiatives as needed, and communicate to senior leadership critical resource gaps;
- continue to implement its plan for addressing this high-risk area and periodically provide assessments of its progress to us and Congress;
- closely track and independently validate the effectiveness and sustainability of its corrective actions, and make midcourse adjustments as needed; and
- make continued progress in achieving the 13 outcomes it has not fully addressed and demonstrate that systems, personnel, and policies are in place to ensure that progress can be sustained over time.

Improving the Management of IT Acquisitions and Operations

As we have recommended, OMB and covered federal agencies should further implement the requirements of FITARA. OMB will need to provide sustained oversight to ensure that agency actions are completed and the desired results are achieved.

Beyond implementing FITARA and OMB's guidance to improve the capacity to address our high-risk area, agencies need to implement our recent recommendations related to improving CIO authorities, as well as past recommendations on improving IT workforce planning practices.

Agencies must establish action plans to modernize or replace obsolete IT investments.

Agencies need to implement our recommendations to address weaknesses in their IT Dashboard reporting of investment risk and incremental development implementation.

OMB and agencies should work toward implementing our remaining 456 open recommendations related to this high-risk area. These remaining recommendations include 12 priority recommendations for agencies to, among other things, report all data center consolidation cost savings to OMB, plan to modernize or replace obsolete systems as needed, and improve their implementation of PortfolioStat. OMB and agencies need to take additional actions to (1) implement at least 80 percent of our open recommendations related to the management of IT acquisitions and operations, (2) ensure that a minimum of 80 percent of the government's major IT acquisitions deliver functionality every 12 months, and (3) achieve at least 80 percent of the over $6 billion in planned PortfolioStat savings.

Ensuring the Effective Protection of Technologies Critical to U.S. National Security Interests

The need for action remains in addressing Capacity, Monitoring, and Demonstrated Progress. The Export Enforcement Coordination Center (E2C2) is performing a critical role in coordinating export control enforcement activities, with participation across a wide breadth of federal agencies. However, according to Homeland Security officials, the E2C2 and the intelligence community's lack of formal coordination limits E2C2's effectiveness, stalling its efforts to develop standard operating procedures. Until this coordination occurs, the E2C2 is limited in its ability to realize its full potential to facilitate enhanced coordination and intelligence sharing.

Key agencies have taken necessary steps to reconcile various definitions, regulations, and policies for export controls. If the agencies choose to proceed with consolidation activities initially planned under the 2010 Export Control Reform Initiative, Congressional action will be required. For example, because there are currently separate statutory bases for the Departments of State and Commerce to review and issue export licenses, legislation would be required to consolidate the current system into a single licensing agency.

ECPA Court Ruling

The United States Court of Appeals for the Fourth Circuit (Fourth Circuit) handed down a ruling finding that previously opened and delivered email is protected under the Electronic and Communications Privacy Act (ECPA), specifically Title II of ECPA, the Stored Communications Act (SCA). The question before the court on appeal was whether opened and undeleted email stored by an online service like Gmail or Outlook was subject to the protections of ECPA and SCA against searches by the government and third parties in most circumstances. However, while the Fourth

Circuit's ruling aligns the court with other Circuits, at least one Circuit has ruled the ECPA and SCA do not protect opened, delivered email, setting up the possibility that the Supreme Court of the United States and/or the Congress will need to address this difference in construing ECPA and the SCA.

This case arose from the unauthorized access of the email account offered by Blue Ridge Community College in Virginia and used by a graduate (i.e. Hately). The graduate's estranged wife convinced her new boyfriend (i.e. Watts) that the graduate was dating the boyfriend's estranged wife, leading the boyfriend to access the graduate's email, using the password the graduate had given his estranged wife. The graduate sued under a Virginia statute and ECPA and SCA. The U.S. District Court ruled in Watt's favor, and Hately appealed to the Fourth Circuit, which reversed and ruled in his favor on the ECPA and SCA claims and sent the case back to the trial court for further proceedings.

Specifically, the Fourth Circuit found that the plain language of 18 U.S.C. § 2510(17)(B) and Congress' intent in enacting ECPA was that "electronic storage" for "backup protection" should include opened email. The U.S. District Court found the email were not in "electronic storage" stored for the purpose of "backup protection" in a way that would trigger the protections of ECPA and SCA. The Fourth Circuit noted

> Under the district court's reading, the [SCA] renders unlawful unauthorized access of *unopened* messages stored by web-based email services, whereas unauthorized access of *opened and saved* messages stored by such services would not violate the [SCA].

The Fourth Circuit held that:

> We conclude that previously delivered and opened emails stored by an electronic communication service are stored for "purposes of backup protection," under the plain and ordinary meaning of those terms. And because such emails amount to "wire or electronic communications" in "storage" by an "electronic communication service," such emails are in "electronic storage"

Because of cases like these, stakeholders in Congress have worked to update ECPA which was first passed in 1986, with a bill often clearing the House but dying in the Senate. In the last Congress, the "Email Privacy Act" (H.R. 387/S. 1654) was passed by the House by itself on a voice vote and attached to must-pass legislation. However, the Senate stripped these provisions out of those bills and never took up the bill by itself. Notably, in a 2016 Senate Judiciary Committee markup, amendments were offered that would have expanded the government's use of National Security Letters,

an administrative subpoena used to obtain electronic communications and financial records. Consequently, the bill's sponsors removed it from consideration.

Broadly speaking, the "Email Privacy Act" would regularize the varied treatment of electronic communications such as email that depends largely on the status and location of the communications. For example, under ECPA, email in transit or stored locally on a home computer can only be accessed by the government with a warrant. However, opened email or email older than 180 days can be accessed by the same government agency with only a subpoena. The Email Privacy Act would institute a warrant requirement for all electronic communications.

As noted, the legal backdrop against which service providers and companies work when the government wants electronic communications is varied. In *Warshak v. United States*, the United States Court of Appeals for the Sixth Circuit held that a warrant showing probable cause is required before such companies may hand over electronic communications to government entities. Agencies like the Securities and Exchange Commission (SEC) claim that this warrant requirement has or will impeded their ability to go to electronics communications providers to obtain communications the targets of investigations may destroy.

Other Hearings and Events

"Electronic Health Record Modernization and Information Technology Oversight" – House Appropriations/Military Construction, Veterans Affairs, and Related Agencies
"China: Challenges for U.S. Commerce" – Senate Commerce, Science, and Transportation

Further Reading

"Stalkers and Debt Collectors Impersonate Cops to Trick Big Telecom Into Giving Them Cell Phone Location Data" – *Motherboard*
"Facebook's Mark Zuckerberg Says He'll Shift Focus to Users' Privacy"
"Zuckerberg's So-Called Shift Toward Privacy"– *The New York Times* and "Don't Trust Facebook's New Privacy Play" – *The Atlantic*
"NSA-Cyber Command Chief Recommends No Split Until 2020" – *Nextgov*
"Researcher: The West Isn't Ready for the Coming Wave of Chinese Misinformation" – *Nextgov*
"No 'smoking gun' evidence coming on Huawei, NSA official says" – *cyberscoop*
"Iranian Hackers Have Hit Hundreds of Companies in Past Two Years" – *The Wall Street Journal*

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