Technology Policy Update
13 February 2020
By Michael Kans, Esq.

House Homeland Security Hearing on Facial Recognition

On February 6, the House Homeland Security Committee held its second hearing on facial recognition technology in this Congress titled "About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies, Part II." The House Oversight and Reform Committee also recently held its third hearing on facial recognition technology, with Democrats and Republicans stating they would soon introduce legislation to regulate the use of the technology.

Chair Bennie Thompson (D-MS) said that "[t]he Committee held Part one of this hearing in July of last year—after news that the Department was expanding its use of facial recognition for varying purposes, such as confirming the identities of travelers, including U.S. citizens." He claimed that "[a]s facial recognition technology has advanced, it has become the chosen form of biometric technology used by the government and industry." Thompson stated that "I want to reiterate that I am not wholly opposed to the use of facial recognition technology, as I recognize that it can be valuable to homeland security and serve as a facilitation tool for the Department's varying missions…[b]ut I remain deeply concerned about privacy, transparency, data security, and the accuracy of this technology and want to ensure these concerns are addressed before the Department deploys it further."

Thompson stated that "[l]ast July, I—along with other Members of this Committee—shared these concerns at our hearing and left this room with more questions than answers." He noted that "[i]n December 2019, the National Institute for Standards and Technology (NIST) published a report that confirmed age, gender, and racial bias in some facial recognition algorithms." Thompson explained that "NIST, for example, found that depending on the algorithm, African-American and Asian-American faces were misidentified 10 to 100 times more than white faces." He remarked that "[a]lthough Customs and Border Protection (CBP) touts that the match rate for its facial recognition systems is over 98 percent, it is my understanding that NIST did not test CBP's current algorithm for its December 2019 report." He added that "CBP's figure does not account for images of travelers who could not be captured due a variety of factors such as lighting or skin tone—likely making the actual match rate significantly lower." Thompson said that "[t]hese findings continue to suggest that some of this technology is not ready for "prime time" and requires further testing before widespread deployment."

Thompson stated that "[m]isidentifying even a relatively small percentage of the traveling public could affect thousands of passengers annually, and likely would have a disproportionate effect on certain individuals…[and] [t]his is unacceptable." He said that "[t]ransparency continues to be key…[and] [t]he American people deserve to know how the Department is collecting facial recognition data, and whether the Department is in fact safeguarding their rights when deploying such technology."

Ranking Member Mike Rogers (R-AL) asserted that "[a]fter the tragic events of September 11th, Congress recognized that biometric systems are essential to our homeland security." He stated that "CBP and the Transportation Security Administration have already demonstrated the capability of biometrics to improve security, facilitate travel, and better enforce existing immigration laws." Rogers stated that "[g]overnment and the private sector have made enormous strides in the accuracy, speed, and deployment of biometrics systems."

Rogers stated that "I'm concerned that some of my colleagues have already jumped to misleading conclusions regarding the NIST report on facial recognition." He noted that "[j]ust hours after NIST released over 1,200 pages of technical data, the majority tweeted "This report shows facial recognition is even more unreliable and racially biased than we feared…" Rogers contended that "[i]f the majority had taken the time to read the full report before tweeting, they would have found the real headline: NIST determined that the facial recognition algorithm being adopted by DHS had no statistically detectable race or gender bias." He claimed that "NIST could find no statistical evidence that the facial recognition algorithm DHS is adopting contains racial bias…[and] NIST found measurable and significant errors and bias in other facial recognition algorithms, but not in the algorithm used by DHS." Rogers claimed that "[t]he reality is that facial recognition technologies can improve existing processes by reducing human error…[and yet] [t]hese technologies are tools that cannot and will not replace the final judgement of CBP or TSA officers."

Rogers stated that "[c]oncerns regarding privacy and civil rights are well intentioned…[b]ut these concerns can be fully addressed in how biometric systems are implemented by DHS."

U.S. Customs and Border Protection Deputy Executive Assistant Commissioner John Wagner stated

> CBP has partnered with the National Institute of Standards and Technology (NIST) to explore facial comparison technology capabilities. NIST used CBP data that was contained in the OBIM data in its conclusions issued in a recent demographic differential study. The study supports what CBP has seen in its biometric matching operations – that when a high-quality facial comparison algorithm is used along with high performing cameras, proper lighting and image quality controls, face matching technology can be highly accurate. To ensure higher accuracy rates, as well as efficient traveler processing, CBP compares traveler photos to a very small gallery of high-quality images that those travelers already provided to the U.S. Government to obtain a passport or visa.

Wagner explained

> CBP uses only *one* of the 189 face comparison algorithms evaluated by NIST and produced by NEC Corporation. As the report demonstrates, NIST confirmed that the NEC algorithm that NIST tested is high performing and ranked first or second in most categories evaluated, including match performance in galleries that are much bigger than those used by CBP. The NIST performance metrics described in the report are consistent with CBP operational performance metrics for entry-exit. CBP's operational data continues to show there is no measurable differential performance in matching based on demographic factors. The NIST report shows a wide range in accuracy across algorithm developers, with the most accurate algorithms producing many fewer errors and undetectable false positive differentials. Since many of the performance rates specified in the report would not be acceptable for use in CBP operations, we do not use them.

Wagner stated that "[i]n the upcoming weeks, CBP will directly provide NIST with data for NIST to perform an independent and comprehensive scientific analysis of CBP's operational face matching performance, including impacts due to traveler demographics and image quality…[and] NIST will provide objective recommendations regarding matching algorithms, optimal thresholds, and gallery creation."

Department of Homeland Security Office for Civil Rights and Civil Liberties (CRCL) Deputy Officer for Programs and Compliance Peter Mina stated that "DHS currently uses facial recognition technology to support CBP's Biometric Entry-Exit Program and is researching and testing this technology to see if it can be deployed in other mission areas, such as identity verification in Transportation Security Administration passenger screening." He contended that "[a] key goal of the Department's use of facial recognition technology is identifying and eliminating, to the extent it exists, any impermissible bias based on race and gender." Mina stated that "[i]n addition to the strong civil rights and civil liberties interest in ensuring equality of treatment, the DHS operational Components have a compelling interest in ensuring the accuracy of this or any tool that assists in performing the mission…[and] [i]mproved accuracy and efficiency in the Department's data systems results in better performance of all the DHS missions they support."

Mina said that "DHS partnered with the NIST on the assessment of facial recognition technologies to improve data quality and integrity, and ultimately the accuracy of the technology, as a means of eliminating such impermissible bias:

- Currently, the DHS Office of Biometric Identity Management (OBIM) is partnering with NIST to develop a face image quality standard that will improve the accuracy and reliability of facial recognition as it is employed at DHS.
- CBP is partnering with NIST to analyze performance impacts due to image quality and traveler demographics and providing recommendations regarding match algorithms, optimal thresholds for false positives, and the selection of photographs used for comparison."

Mina stated

- DHS knows that accuracy and reliability, and the resulting operational value of facial recognition technology, varies depending on how the technology is employed. Variables include the nature of the mission supported, variations in the type and quality of the photographs, environmental factors such as lighting, the manner in which the match is made, and the type of computer processing, including the nature of the algorithms, used to make a match.
- Human factors also matter. Users need to be aware of how the technology works, its strengths and weaknesses, and how they can ensure the technology functions in a way that complies with all applicable laws and DHS policy. In addition to being operational considerations, these factors also directly affect the civil rights and civil liberties of those individuals who encounter this DHS technology. In short, the legal and civil rights and civil liberties policy implications of facial recognition technology depend on how the technology is implemented.

Mina added that "CRCL recognizes the potential risks of impermissible bias in facial recognition algorithms, as previously raised by this Committee…[and] supports rigorous testing and evaluation of algorithms used in facial recognition systems to identify and mitigate impermissible bias." Mina asserted that "CRCL will continue to support the collaborative relationship between NIST, the DHS Science & Technology Directorate, OBIM, and DHS Components to that end."

National Institute of Standards and Technology's Information Technology Laboratory Director Dr. Charles Romine stated that "NIST Interagency Report 8280, released on December 19, 2019, quantifies the effect of age, race, and sex on face recognition performance." He stated that "[i]t found empirical evidence for the existence of demographic differentials in face recognition algorithms that NIST evaluated…[and] [t]he report distinguishes between false positive and false negative errors, and notes that the impacts of errors are application dependent."

Romine stated

> I will first address one-to-one verification applications. There, false positive differentials are much larger than for false negatives and exist across many, but not all, algorithms tested. Across demographics, false positives rates often vary by factors of 10 to beyond 100 times. False negatives tend to be more algorithm-specific, and often vary by factors below 3. False positives might present a security concern to the system owner, as they may allow access to impostors. False positives may also present privacy and civil rights and civil liberties concerns such as when matches result in additional questioning, surveillance, errors in benefit adjudication, or loss of liberty. False positives are higher in women than in men and are higher in the elderly and the young compared to middle-aged adults. Regarding race, we measured higher false positive rates in Asian and African American faces relative to those of Caucasians. There are also higher false positive rates in Native American, American Indian, Alaskan Indian and Pacific Islanders. These effects apply to most algorithms, including those developed in Europe and the United States. However, a notable exception was for some algorithms developed in Asian countries. There was no such dramatic difference in false positives in one-to-one matching between Asian and Caucasian faces for algorithms developed in Asia. While the NIST study did not explore the relationship between cause and effect, one possible connection, and area for research, is the relationship between an algorithm's performance and the data used to train the algorithm itself.

Romine stated

> I will now comment on one-to-many search algorithms. Again, the impact of errors is application dependent. False positives in one-to-many search are particularly important because the consequences could include false accusations. For most algorithms, the NIST study measured higher false positives rates in women, African Americans, and particularly in African American women. However, the study found that some one-to- many algorithms gave similar false positive rates across these specific demographics. Some of the most accurate algorithms fell into this group. This last point underscores one overall message of the report: Different algorithms perform differently. Indeed all of our Face Recognition Vendor Testing Program (FRVT) reports note wide variations in recognition accuracy across algorithms, and an important result from the demographics study is that demographic effects are smaller with more accurate algorithms.

Romine said that "[a] general takeaway from these studies is that, there is significant variance between the performance facial recognition algorithms, that is, some produce significantly fewer errors than others." Romine stated that "[c]onsequently, users, policy makers, and the public should not think of facial recognition as either always accurate or always error prone."

Revised CCPA Regulations Released for Comment

California's Office of the Attorney General (OAG) has released revised draft regulations for implementation of the "California Consumer Privacy Act" (CCPA) (AB 375) that alter the draft regulations released in October 2019. OAG claimed "[t]hese changes are in response to comments received regarding the proposed regulations and/or to clarify and conform the proposed regulations to existing law." The OAG released a notice of the new regulations, a redline, and a clean copy. Comments are due on February 25, 2020 at 5:00 p.m. (PST).

In terms of the substance of the changes, in the main, the new language clarifies, illustrates or tightens the language in the first draft of the regulations. Most notably, the revised regulations make clear that businesses subject to the CCPA must draft and publish a privacy policy in accordance with the regulations and must also provide notice at the point of collection before the collection of personal information may occur. The revised regulations also clarify that any business subject to the CCPA that sells personal information must provide people an opportunity to opt-out, and given the very broad definition of sale in the underlying statute, this would cover most transfers of personal information even if no money changes hands. Additionally, any business offering a financial incentive program or a service difference must provide notice to people that explains the program.

The revised regulations provide a number of illustrative examples. Most notably, it provides a picture of an opt-out button a business could use so that people could opt-out of the sale of their personal information. On this topic, the regulations add language specifying that businesses may not make opting out overly difficult or tedious as a means of discouraging people from doing so. Moreover, the revised regulations make clear that browser plug-ins, privacy or device settings signaling a person's desire to opt-out of the sale of their personal information may suffice in most cases.

While the OAG claims the impetus for the revised draft regulations is the input it received during ts comment period and three listening sessions in December, it is also possible that feedback from privacy and consumer advocacy organizations regarding what they see as widely divergent adherence to the CCPA may well have driven the rewrite and clarification of many of these provisions. For example, Uber and Lyft have reportedly not been providing all the information they have on people in response to a request to know such as ratings and customer service calls, which the companies have been quoted as asserting they may do under the CCPA, a claim disputed by privacy and consumer advocacy organizations.

Revised Data Care Act Released

Senator Brian Schatz (D-HI) and his cosponsors have reintroduced a slightly changed version of the "Data Care Act" (S. 2961), a privacy bill that would impose upon many entities that collect and use the personal data of people a fiduciary duty of care. In December 2018, Schatz and his cosponsors introduced the "Data Care Act" (S. 3744) at a time when the Senate Commerce, Science, and Transportation Committee and other committees of jurisdiction had just begun examining the issues related to privacy in light of the recent passage of the "California Consumer Privacy Act" (CCPA)

(A.B. 375). Fourteen other Democratic Senators joined Schatz, including presidential candidates Senators Michael Bennet (D-CO), Amy Klobuchar (D-MN) and Cory Booker (D-NJ). This bill took a novel approach to the issues presented by mass collection and processing ;personal data by extending 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." Most of the original cosponsors are again sponsoring this bill; however, no Republicans cosponsored the first or current iteration of the bill, suggesting the fiduciary framework is not appealing to Senate Republicans.

Of course, Schatz and Klobuchar are also sponsoring the "Consumer Online Privacy Rights Act" (COPRA) (S. 2968) (*see here* for more analysis) along with Senate Commerce, Science, and Transportation Committee Ranking Member Maria Cantwell (D-WA). COPRA that would empower the Federal Trade Commission (FTC) to police privacy and data security violations through augmented authority, not preempt state laws to the extent they provide greater protection, largely leave in place existing federal privacy statutes such as the "Financial Services Modernization Act of 1999" (aka Gramm-Leach-Bliley) and "Health Insurance Portability and Availability Act of 1996" (HIPAA), and allow individuals to sue.

Incidentally, Senator Ed Markey (D-MA) is also sponsoring both bills, and he has his own bill, the "Privacy Bill of Rights Act" (S. 1214), which was one of the only bill to get an A in the Electronic Privacy Information Center's report on privacy bills. (*See here* for more analysis.) Finally, Klobuchar had also released a narrower bill with a Republican cosponsor, the "Social Media Privacy Protection and Consumer Rights Act of 2019" (S. 189), that would require major tech companies to give consumers an opportunity to opt in or opt out of the company's data usage practices after offering enhanced notice of the practices for which the personal data may used. (*See here* for more analysis.)

And, Schatz has been in negotiations with other members of the Senate Commerce, Science, and Transportation Committee with the goal of developing a bipartisan bill to regulate privacy at a federal level. As discussed in past issues of the Technology Policy Update, stakeholders in both the House and Senate continue to negotiate privacy bills but significant disagreements have been reported regarding whether such a bill has a private right of action, preempts the CCPA and other state laws, and whether a new regime is primarily enhanced notice and consent or certain conduct would no longer be allowed amongst other issues.

Turning to the Data Care Act, this legislation was built on a concept fleshed out by law professor Jack Balkin in his article "Information Fiduciaries and the First Amendment" that would place duties on companies collecting and using consumer data similar to those that lawyers and doctors must meet in how they handle client and patient information. Balkin explained that these so-called "information fiduciaries" should "have special duties to act in ways that do not harm the interests of the people whose information they collect, analyze, use, sell, and distribute."

In short, under the "Data Care Act," "online service providers" would be severely be limited on how they collect, share, and sell the personally identifiable information (PII) (known as "individual identifying data" in the bill), 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. What's more, the scope of who is an online service provider would seem to encompass most consumer-facing companies doing business on the internet.

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." This very sweeping definition would cover almost any business or entity doing business in the U.S. even if it is not across state lines as the Supreme Court has often construed the Commerce Clause. However, unlike other bills, the FTC would have the discretionary authority to exclude categories of online service providers from the fiduciary duties the bill would otherwise impose. Normally, the other privacy bills create a threshold below which limited obligations attach for smaller and mid-sized businesses except for data brokers. 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 also 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, the bill would require that 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. The revised bill further tightens this requirement by stipulating that "If an online service provider transfers or otherwise provides access to individual identifying data to another person, the requirements of [the duties of loyalty, care, and confidentiality] shall apply to such person with respect to such data in the same manner that such requirements apply to the online service provider." Note that this additional requirement pertains to the transfer of PII to any *person* and not just other online service providers, meaning virtually any transfer would be captured by this standard and thus a potential loophole in the bill was closed.

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 Administrative Procedure Act (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, some possible exemptions to the duties that would otherwise apply to online service providers (e.g. small companies) but also more broadly . The bill expands the FTC's jurisdiction over non-profit entities and common carriers that may also be online service providers.

There is no private right of action like many of the Democratic bills, which would disappoint many stakeholders on the left but would conversely please many industry and Republican stakeholders. Nor would people have the explicit right to access, correct, delete, or port their information as they would in other bills; and yet, the fiduciary concept would necessarily entail some of these rights. There are no provisions on obtaining a person's consent, for the onus is entirely on how the covered entity handles the information. In short, this seems to be a framework that would sidestep issues related to notice and consent regimes. Additionally, unlike almost all the other bills, there are not detailed exceptions under which a person's consent would not be needed to collect and process information (e.g. for security processes, to protect against fraud, or to develop new products.)

Committee Releases Latest Volume On Its Investigation Into Russian Interference in 2016 Election

The Senate Intelligence Committee released the third volume of its report documenting the results of its investigation "into Russian election interference…[that] examines the Obama Administration's reaction to initial reports of election interference and the steps officials took or did not take to deter Russia's activities."

The Committee made the following unclassified findings:

- The Committee found that the U.S. Government was not well-postured to counter Russian election interference activity with a full range of readily available policy options. One aspect of the administration's response–high-level warnings of potential retaliation–may or may not have tempered Moscow's activity. The Committee found that after the warnings, Russia continued its cyber activity, to include further public dissemination of stolen emails, clandestine social media-based influence operations, and penetration of state voting infrastructure through Election Day 2016.
- (U) The Committee found that the administration was constrained in its response to Russian meddling by (1) the heavily politicized environment; (2) the concern that public warnings would themselves undermine public confidence in the election, thereby inadvertently helping the Russian effort; (3) the unknown extent to which the Russians could target and manipulate election systems; (4) the delay in definitive attribution of some efforts to Russia; (5) the time and resources required to compose policy options prior to execution; and (6) challenges in how to address WikiLeaks. These constraints affected the response options available, as well as the timing and sequencing of their implementation.
- The Committee found that the administration handled the cyber and geopolitical aspects of the Russian active measures campaign as separate issues until August 2016. The Committee believes this bifurcated approach may have prevented the administration from seeing a more complete view of the threat, limiting its ability to respond.
- The Committee found that decisions to limit and delay the information flow regarding the 2016 Russian active measures campaign, while understandable, inadvertently constrained the administration's ability to respond.

The Committee offered the following recommendations:

1. Strengthen Partnerships. The executive branch should bolster partnerships with Russia's "near abroad." Russia uses countries on its periphery as a laboratory for refining its active measures campaigns. The United States should establish and expand partnerships with those countries to identify new Russian active measures and assist these partners' ability to defend

against them. Such partnerships will help to prepare defenses for the eventual expansion ofinte1ference techniques targeting the West.

2. Support Cyber Norms. The United States should lead the way on creating international cyber norms. Russia and China are actively promoting their view of cyber norms to international forums, redefining the cyber battlefield and writing the rules in their favor. Much as with other agreements, U.S. leadership is needed to balance any formalized international agreement on acceptable uses of cyber capabilities.

3. Prepare for the Next Attack. The executive branch should be prepared to face an attack on U.S. elections in a highly politicized environment either from the Russia or from elsewhere. This preparation should include developing a range of standing response options that can be rapidly executed, as appropriate. if a clandestine foreign influence operation is directed at the United States.

4. Integrate Responses to Cyber Incidents. Cyber events, especially those undertaken by a nation state that go beyond traditional intelligence collection, must be assessed within the geopolitical context to identify and understand both the potential intent and impact of an attack. Current and future administrations should align and synchronize cyber as an integral part of foreign policy activity, rather than treating cyber as an isolated domain.

5. Prioritize Collection on Information Warfare. The IC should prioritize resources to better collect on and analyze information warfare and the influence capabilities of hostile nations. The IC should also contextualize cyber events with this information to better understand adversary capability and intent.

6. Increasing Information Sharing on Foreign Influence Efforts. Once credible information is obtained about a foreign influence or active measures operation, that information at the appropriate classification level should be shared as broadly as appropriate within government, including Congress, while still protecting sources and methods. This information should also be shared with relevant state and local authorities, and relevant private sector partners, as appropriate. For operations specifically targeting election infrastructure and systems, federal engagement with state and local election officials, as well as relevant private sector partners, must be substantive and timely.

7. Clarify Roles, Responsibilities, and Authorities. The lack of clear authorities and responsibilities within the IC for detecting and mitigating Russian influence operations conducted via social media inhibited the ability to provide early warning to policymakers, or quickly formulate a complete set of response options. The Committee addresses its findings and recommendations regarding election security and social media in separate volumes of this report.

GAO Finds Mixed Situation Regarding Government-Wide Cybersecurity Directives

The Government Accountability Office (GAO) has found significant problems with how the Department of Homeland Security (DHS) has implemented and utilized its authority to issue Binding Operational Directives (BOD) to civilian agencies to correct enumerated cybersecurity and information security problems. The GAO found that DHS has not always consulted with other federal stakeholders in drafting and issuing BODs nor has the agency effectively followed up to ensure compliance. The GAO did note, however, DHS has gotten better generally in a number of ways but still offered recommendations on how the process could be improved.

The GAO stated that "[a]lthough DHS has designed a process to develop and oversee the implementation of binding operational directives, it is not following all the steps in the draft process...[s]pecifically, the department has not involved key stakeholders, such as NIST and GSA, early in the process." The GAO added that "although guidance from OMB and executive orders emphasize risk-based approaches to information security, CISA did not take such an approach in validating selected agency-reported actions." The GAO stated that "[u]ntil DHS addresses the coordination and validation issues, the likelihood is increased that directives will not fully address key technical considerations and requirements are not fully addressed...[and] [f]ederal civilian agencies have made many significant improvements in cybersecurity by implementing the directives' requirements." The GAO stated that "[h]owever, an important performance metric for addressing vulnerabilities identified by high value asset (HVA) assessments does not align with the process DHS has established." The GAO stated that "[f]urther, DHS has only completed about half of the required assessments for fiscal year 2019...[and] DHS does not plan to issue the guidance, standards, and methodologies on Tier 2 and 3 systems until at least the end of fiscal year 2020." The GAO claimed that "[g]iven these shortcomings, DHS has been reassessing key aspects of the HVA program...[h]owever, there was no schedule or plan for completing the HVA reassessment and for addressing the outstanding issues on completing the required assessments, identifying needed resources, and finalizing guidance for Tier 2 and 3 systems." The GAO cautioned that "[w]ithout such a schedule and plan, agencies may continue to face increased and prolonged cybersecurity threats."

The GAO made "four recommendations to DHS:

- The Secretary of Homeland Security should determine when in the directive development process—for example, during early development and at directive approval—coordination with relevant stakeholders, including NIST and GSA, should occur. (Recommendation 1)
- The Secretary of Homeland Security should develop a strategy to independently validate selected agencies' self-reported actions on meeting binding operational directive requirements, where feasible, using a risk-based approach. (Recommendation 2)
- The Secretary of Homeland Security should ensure that the binding operational directive performance metric for addressing vulnerabilities identified by high value asset assessments aligns with the process DHS has established. (Recommendation 3)
- The Secretary of Homeland Security should develop a schedule and plan for completing the high value asset program reassessment and addressing the outstanding issues on completing the required high value asset assessments, identifying needed resources, and finalizing guidance for Tier 2 and 3 HVA systems. (Recommendation 4)

OMB Launches New Supply Chain Initiative

The Administration has launched yet another effort to better secure the federal supply chain, this one flowing from the White House Summit on Federal Acquisition & Supply Chain Management held late last month. In a blog posting, Deputy Director for Management at the Office of Management and Budget (OMB) Margaret Weichert "announced a call for ideas to help us shape how the government obtains and leverages acquisition and supply chain expertise." OMB is looking to piggyback this effort on the Administration's existing initiative to more widely use category management, a practice started by previous administrations under which agencies across the government look to pool resources to buy products and services together in bulk to maximize savings.

The Administration wants "to hear from private sector organizations, researchers, academic institutions, good government groups, the public, and others on the vision and concept for a mechanism to facilitate curated conversations between the federal government and external supply chain and acquisition experts on a variety of issues and questions that support the government's acquisition modernization efforts." OMB is asking that responses be sent to ideas@omb.eop.gov by 5:00 pm EST on February 17 with the subject line: "Supply Chain Ideas" with the caveat that all submissions may be made public and may be subject to FOIA requests. OMB also explained that it would not respond to all submissions but it may ask for further clarification and for some submitters to participate "in future discussions with other thought leaders."

OMB appears to be trying to address supply chain issues as part of the President's Management Agenda (PMA), specifically through the requirement that agencies utilize category management. OMB noted "[t]his call for ideas supports the President's Management Agenda (PMA) that requires federal agencies to implement category management, an industry best practice where common contracts are leveraged, meaning that contracts are shared in order to buy common goods and services as an enterprise." OMB claimed "Category management has already helped the government eliminate redundancies, increase efficiency, and deliver more value for taxpayers."

In March 2019, Weichert issued an OMB memorandum requiring "agencies to carry out a set of tailored management actions and provide updates on these management actions to evaluate their progress in bringing common spending under management." OMB contended that "[t]he expected result is more effectively managed contract spending through a balance of Government-wide, agency-wide, and local contracts; reduced unnecessary contract duplication and cost avoidance; and continued achievement of small business goals and other socioeconomic requirements." In the December 2019 update to category management Cross-Agency Priority (CAP) goal, the leaders of this initiative reiterated that "[b]y the end of FY 2020, the government will achieve $32 billion in savings for taxpayers by applying category management principles—or smart decision-making where agencies buy the same kinds of goods and services through best value contract solutions—to 60% of common spend." However, it bears noting that three of the four CAP goals for information technology are behind schedule, suggesting problems with following through on this initiative.

Weichert stated at the "summit, we discussed:

- End-to-End Supply Chain Management – How do the best companies plan for and execute large-scale, global supply chain management (e.g., enterprise resource planning, application of emerging technology for more efficient transactions, etc.)?
- Co-creation with Industry/Academia/Consortia – Where can shared business and other interests lead to new models for program delivery (e.g., shared investments, development of supplier consortia, etc.)?
- Continuous Improvement Cycle – How can key business systems become more agile to keep up with the digital age (e.g., rules of engagement, knowledge transfer, dynamic benchmarking) while reducing friction in the acquisition system?

Weichert said that "[t]his call for ideas will help us continue this conversation, as well as discuss mechanisms to answer additional questions like:

- (Benchmarking) How long does it take a comparably-sized organization to develop and deploy a unique technology (or specialized service) so the government can better evaluate its agility and responsiveness?
- (Data/Pricing Sourcing) What external data sources are readily available for real-time access to market trends and pricing data for specific common categories/sectors of spend?

- (Market Research) What is the future of XYZ industry and how should the government prepare for those market changes?
- (Technology) What are the most impactful types of process changes and automation to reduce transaction costs?
- (Continuous Improvement) What are the top 5 inputs that large organizations use to assess their performance, who has access to that data, and how do these organization prioritize change management to become more agile?
- (Human Capital Strategies) There are dozens of private sector credentialing bodies for supply chain management. What is the comprehensive training path for public sector category management professionals across various career paths (i.e. requirement owners, contracting officers, agency leaders) for total lifecycle cost management – including, but not limited to, enterprise buying, implementation of demand and vendor management.

Committee Hears Testimony on Digital Equity

On January 29, the House Energy and Commerce Committee's Communications and Technology Subcommittee held a hearing titled "Empowering and Connecting Communities through Digital Equity and Internet Adoption."

Chair Frank Pallone Jr (D-NJ) said the hearing would focus "on promoting broadband adoption, an issue that affects every one of our districts whether they are urban, suburban, or rural." He said that "[o]n this Committee, we have on many occasions discussed gaps in internet access and how to subsidize and incentivize building the infrastructure necessary to ensure that everyone has access to reliable, high-speed, and resilient internet service." Pallone said that "[b]ut we must also consider the gaps in internet adoption—why people don't, or can't, subscribe to internet service when it is available to them." He contended that "[i]t is increasingly difficult to participate in today's economy without internet service, and yet millions of Americans who are wired for internet access aren't actually connected." He claimed that "[t]he key reason most are not connected is cost."

Pallone stated that "[f]ortunately, there are programs at the state, local and federal level that can provide assistance to people who have trouble affording internet access…[b]ut at the federal level we can and must do more." He said that "[a]s we consider how to spend proceeds of future spectrum auctions, it is important that we invest in solutions to address these adoption issues…[and] Members have introduced legislation to begin closing these adoption gaps." Pallone remarked that "I'm hopeful we can work to find a way to make these proposals—or others that might come as a result of this hearing today—bipartisan…[and] [t]he internet holds incredible promise for the future, but as the technology continues to advance, we must make sure that people are not left behind." He declared that "[t]hat's the concept of digital equity, and it is one I know we will all stand up for."

Ranking Member Greg Walden (R-OR) asserted that "[u]nder a light touch regulatory framework, the internet has thrived, providing Americans access to numerous services, and serving as the single most important driver of economic growth and job creation." He added that "[w]hile the internet has been largely adopted in a relatively short span of time, there are still millions of Americans who do not have access to the internet in their homes." Walden said that "[i]n some cases, it is because high-speed broadband has not been deployed, an issue that this Committee has focused on for many years…[a]nd while we have made progress in promoting broadband deployment, particularly in rural areas, there are many Americans who remain unconnected, even if they do have access to broadband service options."

Walden contended that “[r]ecognizing this issue, companies have made great strides over the last decade to connect millions of low-income households to high-speed broadband.” He said “[f]or example, the Internet Essentials program – developed by one service provider – offers high-speed broadband at an affordable price and has seen great success.” Walden claimed that “[i]t has connected 8 million people in over 2 million households, more than a federal program could likely achieve in the same period of time, and provides opportunity and access for low-income individuals.” He said that “[w]e must make sure that our policies allow for continued experimentation with ways to promote broadband adoption.”

Walden said “[i]t should be noted, that where there are gaps in adoption, state and local governments have done a great job providing support and outreach to their communities.” He stated that “[t]hey have firsthand knowledge of the challenges their communities face, and work with the resources they have to find creative solutions.” Walden conceded that “[i]n many parts of the country, but especially frontier communities like Eastern Oregon, broadband availability remains elusive.” He cautioned that “[i]It’s only been a decade since broadband deployment has exploded into an everyday necessity, and without first addressing the lack of broadband availability, any Federal resources put forward for broadband adoption could further enlarge the digital divide if not done carefully.”

Subcommittee Chair Mike Doyle (D-PA) explained that “[t]oday, we will hear about the challenges of internet adoption that go beyond a lack of access.” He said that “[a]ll too often we talk about how many Americans don’t have access to broadband and discuss the resources necessary to close that gap, but the far more insidious threats are those who have broadband available to them but don’t sign up - and those that don’t have the basic skills to use digital technologies.” Doyle stated that “[a]mong the principal barriers faced by these communities are affordability, digital literacy, and access to devices:

- First off, internet access is expensive, and when cost-constrained consumers are forced to choose between mobile and home internet, they often go mobile-only. Millions though, forgo both. Internet and mobile service can cost hundreds of dollars a month. That’s the equivalent of a car payment. In effect, many of us are essentially buying our ISP a new car every 5 years. This a very serious challenge to adoption, particularly in households making less than thirty-five thousand dollars a year. Adoption numbers are even lower in low-income rural communities.
- Finding ways to close the affordability gap is just one part of closing the digital divide. Another key piece to this puzzle is digital literacy and training - and ensuring that people have the skills, understanding, and confidence to use technology and get connected. Organizations like the National Digital Inclusion Alliance and their partners like Computer Reach, based in Pittsburgh, have long worked to provide digital literacy training and provide access to low cost devices and technology. These programs help engage communities and provide folks with pathways - not just to get connected, but to leverage that connectivity to educate and empower themselves and their family members.
- Whether it’s being able to apply for jobs, enabling kids to do homework, connecting seniors to telehealth services or veterans to support communities, these digital inclusion programs are often essential for opening people’s eyes to the importance of, and opportunities presented by, getting online. Increasingly digital literacy isn’t just the ability to use a computer, but it’s a fluency in technology.

Doyle stated that "[w]e can't afford to let this generation fall behind." He asserted that "[t]hese children are our nation's future, and we need to find ways to close the homework gap for them, and for ourselves." Doyle stated that "[i]t is my hope that we can have a productive discussion about the challenges faced by all of our communities and come to some consensus on solutions that can help close the digital divide…[a]nd as I have said before, I stand ready to work my colleagues on both sides of the aisle to come up with real solutions to address these challenges."

National Digital Inclusion Alliance (NDIA) Executive Director Angela Siefer stated

> Residential internet service in the U.S. is expensive. On the low end, internet service generally runs $65-70 per month. That's a lot of money. Unfortunately, I cannot provide any detail as to the cost of internet service because that data does not exist. We need the [Federal Communications Commission] to begin collecting systematic data on the cost of home internet service and make it publicly available. In the U.S., digital literacy training is under-valued and thus under-funded. One-third of manufacturing workers lack proficient digital skills. Half of all construction, transportation and storage workers lack proficient digital skills. There is no funding for digital literacy training. It has been left up to local governments, libraries, and nonprofits to piece together resources to address the basic digital skills training that millions of Americans need to cross that digital divide. Piecing together funding is the wrong strategy for a strong workforce.

Siefer stated that "[d]igital inclusion solutions in the U.S. have been crafted from the ground up…[and] NDIA's affiliates are providing guidance to low-income parents connecting to their children's teachers, teaching seniors how to use their electronic health records, helping veterans learn digital skills in order to acquire a job, and enabling disabled adults to participate more fully in their communities." Siefer stated that "[w]e know that trust is an important factor…[and] [t]echnology can be quite intimidating." She said that "[t]he most successful digital inclusion programs are rooted in the communities being served." Siefer said that "[d]igital equity planning at the state level" is missing as is "financial support for that planning plus the implementation." Siefer claimed that "[a] good first start would be to pass the [Digital Equity Act of 2019 (S. 1167/ H.R. 4486)]…[and] [w]e are also in need of increased awareness of the problem and the solutions."

Georgetown Law Institute for Technology Law and Policy Distinguished Fellow Gigi Sohn offered a number of policy suggestions on digital equity and broadband adoption, including:

- Require Price Transparency. As we have seen in the E-Rate context, when broadband providers are required to be transparent about their prices, competitive pressures often drive prices down.28 While the FCC has finally changed the type of data broadband providers must submit to demonstrate who does and does not have access to broadband, the carriers are not required to submit pricing information. Congress should mandate that the FCC require broadband providers to submit non-promotional pricing information and should require public disclosure of added fees and equipment costs. In addition, Congress or the FCC should restore the Fixed Broadband Consumer Disclosure Label (reproduced below as Figure 1),29 which was withdrawn by the FCC in 2017. This label will help consumers make informed choices about the price, quality, and value of their broadband service.
- Promote Competition. As discussed above, more competition means lower broadband prices for everyone. There are many things that Congress could do to incentivize more competition, but I will focus on three:

  - First, Congress should prohibit states from blocking communities that wish to build their own broadband networks, be they municipal networks, public-private partnerships or other arrangements. While numerous cities and towns across the nation have successfully built gigabit speed networks at low prices, 19 states still have laws on the books that prohibit either the building or the expansion of such networks. These laws, passed at the urging of the largest incumbent broadband providers, are not only flatly anticompetitive, they prohibit deployment in rural communities that the incumbents have no intention of ever serving. Most destructively, these laws directly raise the price of broadband for the most vulnerable Americans.
  - Second, Congress should give a bidding preference to "open access networks" when allocating broadband deployment subsidies. Open access networks allow any broadband provider to connect to a network and provide last-mile service to a customer. This model has become very popular for community broadband builds. For example, the Utah Telecommunications Open Infrastructure Agency (UTOPIA) network is the largest open-access network in the United States, comprised of a consortium of 15 Utahan cities. UTOPIA owns and operates the fiber middle-mile and last-mile network and permits private service providers to use the infrastructure to offer retail digital services to customers in UTOPIA member cities. Currently there are 10 Internet service providers offering residential service and 30 offering business services on UTOPIA's network. This level of broadband competition is practically unheard of in the United States.
  - Finally, either the FCC or Congress should prohibit exclusive contracts between broadband providers and so-called multi-tenant environments ("MTEs") like apartment buildings and condominiums. Nearly one-third of Americans, including many low-income Americans, live in MTEs and have no choice of broadband provider, leaving them at the mercy of whatever price the provider decides to set. The FCC began a proceeding to examine these exclusive deals last summer but has not yet issued an order.

American Enterprise Institute Visiting Scholar Roslyn Layton offered the following policy recommendations:

- Traditional modes of broadband subsidies, however well-intentioned, are ineffective and unsustainable. The surcharge on the Universal Service Fund, just one component of the many federal broadband subsidy programs, has risen from 3 percent in 1998 to 24.4 percent today. This is a growing tax levied on a declining service that falls hardest on the poorest people. The Lifeline program needs revolutionary, not evolutionary change. Rather than throw more good money after bad, we should improve existing programs. Fortunately, the FCC is reversing this trend and deserves the right to try.
- Under FCC Chairman Ajit Pai's leadership, the FCC is on the right track to close the digital divide, and these efforts should continue. This includes but is not limited to the Connect America Fund (CAF) Phase II reverse auction, the first time use of an innovative model in which operators bid for connect an area by lowest cost. This program attempts to focus funds on areas with little to no network build-out, not displace existing investment. In the EU, providing subsidies to areas with existing networks is a violation of state aid rules. CAF II has allowed $1.5 billion to be distributed to connect more than713,000 homes and businesses nationwide. The auction was also open to all network types and through intermodal, competitive bidding, the FCC reduced $3.5 billion from the $5 billion expected to connect these unserved areas. I also welcome the proposed $20.4 billion Rural Digital

Opportunity Fund in applying the lessons of the reverse auction to expand broadband in unserved rural areas.

- Also laudable are the FCC's efforts to improve wireline and wireless network regulation so that these networks can be built more quickly and with less money and that the transition to modern broadband networks can be accelerated. The FCC is also combatting abuse by franchising authorities, practices which increases the cost of cable to end users and reduce deployment.
- Under then Chairman Upton and Sub-Committee Chairman Walden in 2014, the Energy & Commerce Committee led an effort to modernize the Communications Act in 2014, an important and overdue effort that came to an abrupt halt. Yet this work must still be done as the exigence of regulatory siloes deters competition and innovation in a world in which communications, content, and computing have converged. That we fail to realize individual preferences for internet adoption and inclusion likely reflects that regulatory frameworks from the last century persist. Consider that telephone regulation is 86 years old and still on the books; cable, 36 years; mobile wireless, 25 years. To realize greater digital adoption and inclusion, we must update our outdated laws to reflect the dynamic competition in the marketplace and modernize obsolete regulatory structures. This is the kind of bold work that this Commission should do, not doubling-down on outdated policies written in the age of the rotary phone.
- One area where Congress must act is spectrum, and only Congress has the power to the solve the problem. We connect to the internet increasingly and wirelessly. While the US has made important strides in 5G, we still need major spectrum reform. The US government sits on most of the frequencies, and an audit of federal spectrum is needed to develop a 21st century approach to the resource. Only Congress can authorize auctions, appropriate audit funds, and enable the agency reforms needed so that the US in one the same page to win the global 5G race. While the US has many advantages, it lacks sufficient mid-band spectrum, particularly the C-band, the frequencies which 23 nations have already prioritized for 5G and where standards for devices will be harmonized globally. The window of opportunity for the US is closing on this front, and it is critical that this committee encourage the FCC to conduct a speedy public auction for the C- band. This is also the fastest way to get 5G to rural areas.
- I also encourage this committee to consider the role of satellite broadband. New high throughput satellites offer 100 Mbps, making this technology a contender for rural and urban use. This demands immediate attention as the Chinese are already closing their digital divide for 100 million people via satellite and will export the model globally. Moreover satellite technologies needn't be subsidized.

Targeted Cyber Bills Move Out of Committee

In the last week of January, the House Homeland Security Committee marked up two bills pertaining to the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA):

- The "CISA Director Reform Act" (H.R. 5679)
- The "Cybersecurity Vulnerability Identification and Notification Act of 2020" (H.R. 5680)

The "CISA Director Reform Act" (H.R. 5679) was approved and reported out of committee, as amended, and would limit each CISA Director to a five year term. However, amendments allow for each director to serve two five-year terms and would require that the director have at least five years of experience in cybersecurity, infrastructure security, or security risk management. This bill is sponsored by Cybersecurity, Infrastructure Protection, & Innovation Subcommittee Ranking Member John Katko (R-NY), Chair Cedric Richmond (D-LA) and Representative Jim Langevin (D-RI). To date companion legislation has not been introduced in the Senate.

Broadly speaking, the "Cybersecurity Vulnerability Identification and Notification Act of 2020" (H.R. 5680) would grant CISA the authority to subpoena internet service providers (ISP) so that the agency may obtain contact information for entities at risk regarding their cybersecurity. Both homeland security committees have introduced bills, but House Homeland moved first in marking up its bill, which was approved and reported without amendment.

In December, the Senate Homeland Security Committee has released a long-anticipated bill that would provide CISA the authority to serve subpoenas on ISPs to turn over the contact information of the owners of critical infrastructure with vulnerabilities. Chairman Ron Johnson (R-WI) and Senator Maggie Hassan (D-NH) are cosponsoring the "Cybersecurity Vulnerability Identification and Notification Act of 2019" (S. 3045) a bill that was introduced in response to a legislative proposal submitted by the DHS in mid-2019.

In requesting subpoena authority, DHS allegedly had the operators of industrial systems in mind. Notably, administrative subpoenas can be issued by a number of law enforcement agencies without assent from a court. DHS officials have claimed the power would be used sparingly and only to make the owners and operators of some at risk critical infrastructure "more motivated." At present, ISPs cannot turn over the identity of its customers to a government agency absent a subpoena or a warrant, and law enforcement agencies can typically only issue administrative subpoenas as part of an investigation. Consequently, CISA, which lacks this authority, can seek and obtain the ownership of critical infrastructure that is at risk by piggybacking on a sister agency's authority. For these reasons, CISA is asking for its own standalone authority to clear up these problems.

In 2019, CISA's now departed Assistant Director for Cybersecurity and Communications Jeannette Manfra told reporters '[a] challenge that we have is that we can see a lot of industrial control systems...that have potential vulnerabilities that are accessible from the public internet." Supposedly, CISA can only ask the ISP to pass along its concerns or intelligence to targeted owners or operators. Speaking publicly also this past summer, CISA Director Christopher Krebs remarked that "[w]hat we want to be able to do is if we can't resolve the issue through any other way, then we should be able to go to an ISP and say, 'We're concerned about this, can you provide us your customer contact information so we can go let them know that they have whatever port open or are running a vulnerable system." When asked if DHS might not read and use its authority as expansively as possible as many agencies do, Manfra claimed "[w]e have a long history of collecting similar types of data through voluntary programs and [have] demonstrated ways of protecting that, as well as to ensure that the information is only used for the purposes that it was collected." She contended that CISA would use this authority in "very narrow set of circumstances."

The "Cybersecurity Vulnerability Identification and Notification Act of 2019" would expand the authority of CISA's National Cybersecurity and Communications Integration Center (NCCIC) to issue subpoenas subject to be drafted procedures and limits on how any information collected from subpoena is used and retained. The House and Senate bills are similar except for some key differences. The House Homeland Security bill would tighten the definition of those systems possibly subject to a subpoena from a mere "system" to "information system," a tweak that may have been undertaken to ensure the scope of the bill pertained only to cybersecurity matters. H.R. 5680 would direct CISA to work with the Department of Justice to "develop interagency procedures regarding the issuance of subpoenas" so as to avoid disrupting ongoing investigations and to coordinate with these other agencies to the extent practicable. S. 3045 would not require the agency to take these steps. The House bill further tightens the scope by requiring that subpoenas only be issued for "cybersecurity purposes," a term defined in statute to mean "protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability."

However, in both bills, the scope of the type of systems for which CISA may issue subpoenas is limited to an "enterprise device or system," which rules out consumer devices and systems. The term is defined as

- a device or system commonly used to perform industrial, commercial, scientific, or governmental functions or processes that relate to critical infrastructure, including operational and industrial control systems, distributed control systems, and programmable logic controllers; and
- does not include personal devices and systems, such as consumer mobile devices, home computers, residential wireless routers, or residential Internet enabled consumer devices.

GAO Finds DHS' Election Security Efforts Inadequate

The Government Accountability Office (GAO) issued an assessment of how well the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) "has assisted state and local election officials in securing election infrastructure through regional support and assistance, education, and information sharing." Despite noting progress, GAO found CISA's actions, to date, short of what is needed and cast doubt on the efficacy of DHS to help prepare states and localities for this year's election. The report was required by the "Consolidated Appropriations Act, 2019" (P.L. 116-6).

DHS was the agency with specific jurisdiction over the cybersecurity of U.S. election systems until CISA came into to being in late 2018 and assumed that role. The GAO noted that "[a]s the lead agency for the Election Infrastructure Subsector, CISA is responsible for coordinating partnership activities and information sharing and is the primary federal interface with the subsector's stakeholders with respect to security." The GAO added that "[t]he Election Security Initiative, part of CISA's National Risk Management Center, is responsible for managing the agency's election subsector partnerships."

However, in conclusion, the GAO claimed that "CISA has not developed plans for how it will address challenges, such as concerns about incident response, identified in two reviews—one conducted by CISA and the other done by an external entity under contract—of the agency's 2018 election security assistance…[and] [c]hallenges that the reviews identified include:

- inadequate tailoring of services, which could have made it more difficult for CISA to meet the resource and time constraints of customers such as local election jurisdictions;
- not always providing actionable recommendations in DHS classified threat briefings or making unclassified versions of the briefings available, which may have hindered election officials' ability to effectively communicate with information technology and other personnel in their agencies who did not have clearances;

- the inability of CISA personnel supporting election security operations to access social media websites from situational awareness rooms, which hindered their collection and analysis of threat information;
- few capabilities that CISA field staff could quickly provide on Election Day, which could limit the agency's timeliness in responding to an incident; and
- a lack of clarity regarding CISA's incident response capabilities in the event of a compromise that exhausts state and local resources, which may limit knowledge about agency capabilities that are available."

The GAO found

> With primary elections beginning in February 2020 and culminating in the general election in November 2020, CISA has limited time remaining to help states and local election jurisdictions protect their election infrastructure in advance of these elections. State and local election officials that we contacted have been generally satisfied with CISA's election security efforts. However, CISA's unfinished planning means the agency may be limited in its ability to execute a nationwide strategy for securing election infrastructure. In particular, the #Protect2020 Strategic Plan's higher-level objectives—such as building stakeholder capacity and public awareness—necessarily take time to accomplish. In addition, CISA has not fully assessed and documented how it will address challenges identified in prior assessments, which limits the ability of CISA to address these challenges in its current efforts.

The GAO made three recommendations to the Cybersecurity and Infrastructure Security Agency:

- The CISA Director should urgently finalize the strategic plan and the supporting operations plan for securing election infrastructure for the upcoming elections. (Recommendation 1)
- The CISA Director should ensure that the operations plan fully addresses all lines of effort in the strategic plan for securing election infrastructure for the upcoming elections. (Recommendation 2)
- The CISA Director should document how the agency intends to address challenges identified in its prior election assistance efforts and incorporate appropriate remedial actions into the agency's 2020 planning. (Recommendation 3)

DOD Releases Version 1.0 of Cybersecurity Maturity Model Certification Framework

The Department of Defense (DOD) released version 1.0 of the Cybersecurity Maturity Model Certification (CMMC) framework and its corresponding appendices and will continue efforts to make this the standard against which federal defense contractors will be measured in terms of their fitness for certain procurements. This initiative was launched so that the DOD could better secure the information held by federal contractors, in part, by trying to drive improved cybersecurity throughout the supply chain. The DOD anticipates a rulemaking to amend the Defense Federal Acquisition Regulations (DAFRS) to build the CMMC into the Pentagon's procurement processes by late spring/early summer, a memorandum of understanding to be signed with the new CMMC accreditation body, requests for information (RFIs) in June 2020, and requests for proposals (RFPs) in September 2020 that require use of the CMMC. The DOD added that "[w]hen implementing CMMC, a Defense Industrial Base (DIB) contractor can achieve a specific CMMC level for its entire enterprise network or for particular segment(s) or enclave(s), depending upon where the information to be protected is handled and stored." Depending on how well the CMMC framework is designed and implemented, other agencies may seek to develop similar standards or merely adopt the document.

The DOD explained that it is looking to secure "the following types of unclassified information within the supply chain:

- Federal Contract Information (FCI): FCI is information provided by or generated for the Government under contract not intended for public release.
- Controlled Unclassified Information (CUI): CUI is information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or Atomic Energy Act of 1954, as amended."

Consequently, the DOD explained that "[t]he [CMMC] model encompasses the basic safeguarding requirements for FCI specified in Federal Acquisition Regulation (FAR) Clause 52.204-21 and the security requirements for CUI specified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 per DFARS Clause 252.204- 7012." The DOD also relied on some other cybersecurity standards and benchmarks in formulating the CMMC such as the UK's National Cyber Security Centre's Cyber Essentials and the Australian Cyber Security Centre's Essential Eight. The DOD stated that "[t]he CMMC framework adds a certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level...[and] is designed to provide increased assurance to the DoD that a DIB contractor can adequately protect CUI at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain."

The DOD stated that version 1.0 "focuses on the CMMC model which measures cybersecurity maturity with five levels and aligns a set of processes and practices with the type and sensitivity of information to be protected and the associated range of threats...[and] consists of maturity processes and cybersecurity best practices from multiple cybersecurity standards, frameworks, and other references, as well as inputs from the broader community."

The DOD stated that "[t]he CMMC framework contains five maturity processes and 171 cybersecurity best practices progressing across five maturity levels...[that] institutionalize cybersecurity activities to ensure they are consistent, repeatable, and of high quality." The DOD said that "[t]he CMMC practices provide a range of mitigation across the levels, starting with basic safeguarding at Level 1, moving to the broad protection of Controlled Unclassified Information (CUI) at Level 3, and culminating with reducing the risk from Advanced Persistent Threats (APTs) at Levels 4 and 5." The DOD stressed that "[t]he CMMC framework is coupled with a certification program to verify the implementation of processes and practices."

The DOD stated that "[c]reated in collaboration with a community of DOD stakeholders, University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers (FFRDCs), and the Defense Industrial Base (DIB) sector, the CMMC framework addresses the needs of the DOD to protect its unclassified information (i.e., Federal Contract Information (FCI) and CUI) during the acquisition and sustainment of products and services from the DIB." The DOD said that "[t]his model represents one of multiple lines of effort that the Department and industry are pursuing to enhance the security and resiliency of the DIB sector...[and] [t]hese efforts are instrumental in establishing cybersecurity as a foundation for future DOD acquisitions."

At the press rollout, Under Secretary of Defense for Acquisition and Sustainment Ellen Lord explained future CMMC-related actions:

- Now that we have released the public model today, we are now focusing on the remaining CMMC timeline, selecting third-party vendors, rulemaking and completing a memorandum of understanding with the newly-established CMMC accreditation body. Specifically, we are looking at late spring/early summer timeframe to complete a new defense acquisition regulation, a new Defense Federal Acquisition Regulation, or DFAR.
- Next in the timeline will be the CMMC requirement in selected RFIs [request for information] in the June 2020 timeframe, followed by corresponding RFPs [request for proposals] in September 2020 time frame, where CMMC standards will be required at the time of contract award.
- We continue to work to select third-party certification vendors. There are multiple companies that are interested right now, but we have not officially designated who is qualified. We will keep you updated.
- Earlier this month, the CMMC accreditation body was created. It is made up of unbiased parties that will oversee the training, quality and administration of the CMMC third-party assessment organizations, and of course, we have a new acronym for you.

Further Reading

- "Someone Tried to Hack My Phone. Technology Researchers Accused Saudi Arabia." – *The New York Times*. In June 2018, a reporter who has written extensively about the rise of Saudi Arabia's crown prince, Mohammed bin Salman, was sent a suspicious text he never opened that one group of experts claim is Pegasus spyware developed by an Israeli security firm, the NSO Group. It may be malware similar to that sent to Amazon CEO Jeff Bezos phone that his security experts say was sent by Prince Mohammed. The NSO Group has denied any connection.
- "EXCLUSIVE: The cyber-attack the UN tried to keep under wraps" – *The New Humanitarian*. According to a still secret United Nations report, a sophisticated hacker broke into the servers of three offices, including the UN Office of the High Commissioner for Human Rights, and may have accessed and exfiltrated the information of UN personnel and people with whom they have worked. This report follows years of warnings that UN systems were vulnerable. Nonetheless, the UN has not publicly acknowledged the hack nor need they do so are they are exempt from data security regimes such as the General Data Protection Regulation.
- "Huawei denies German report it colluded with Chinese intelligence" – *Reuters*. The international news agency picked up on an article in a German publication, Handelsblatt, that detailed a classified paper sent by a think tank to the German government detailing the likely risks posed by technical backdoors in Huawei products. These backdoors could be used for surveillance or other practices, and the think tank concluded that considering China's National Intelligence Law, Huawei would be required to use this access to help the Chinese government. Interestingly, Huawei denied that it had ever worked with Chinese intelligence, which was beside the point of the paper. In any event, the German government is said to be considering setting technical requirements high enough for its 5G networks to screen out Huawei without resorting to an out and out ban.
- "Federal Agencies Use Cellphone Location Data for Immigration Enforcement" – *Wall Street Journal*. DHS is buying cellphone location data from at least one private vendor to track,

apprehend, and arrest non-U.S. citizens and residents in the U.S. While the Supreme Court has held that law enforcement agencies must obtain a warrant to directly use location data, it appears going to a private sector third-party may serve as a legal workaround. This may be the first of perhaps more ways law enforcement agencies are using and will use cellphone location data in investigating alleged crimes, and critics argue the potential for abuse is high given the lack of oversight.

- "EU Deepens Antitrust Inquiry Into Facebook's Data Practices" – *Wall Street Journal*. The European Commission (EC) is continuing and deepening its investigation into Facebook's alleged anticompetitive practices of advantaging or disadvantaging its partners with respect to accessing user data on the basis of perceived threat to the social media giant. The EC claims such practices are inherently anticompetitive and in violation of European Union law, while Facebook has denied the allegations and has characterized the EC's efforts to obtain internal communications as unacceptably broad. The EC's examination of Facebook follows other allegations of the company's possibly anticompetitive practices, notably a lawsuit brought by app developer Six4Three and the two troves of Facebook documents that have been released (here and here.)
- "The Billion-Dollar Disinformation Campaign to Reelect the President" – *The Atlantic*. A very deep examination of the playbook the Trump reelection campaign is expanding for this year's election, including disinformation, attacks on the media, and other methods to so muddy the waters that people will have trouble telling truth from fiction.