Technology Policy Update
20 April 2020
By Michael Kans, Esq.

GAO on DOD Cyber Hygiene

The Government Accountability Office (GAO) found that the Department of Defense (DOD) has failed to fully implement three separate initiatives to instill better cyber hygiene across the Pentagon and its component agencies. This report necessarily throws into question how well the DOD can ride herd on its component agencies and service branches to force the use of basic processes to ensure cybersecurity.

The Pentagon's efforts to police cyber hygiene in the DOD and its component agencies have been incomplete, and most likely ineffective, raising questions about other initiatives.

The GAO explained the policy background for ensuring the highest levels of cyber hygiene:

> As DOD has become increasingly reliant on information technology (IT) systems and networks to conduct military operations and perform critical functions, risks to these systems and networks have also increased because IT systems are often riddled with cybersecurity vulnerabilities—both known and unknown. These vulnerabilities and human error can facilitate security incidents and cyberattacks that disrupt critical operations; lead to inappropriate access to and disclosure, modification, or destruction of sensitive information; and threaten national security.

The GAO worked from Carnegie-Mellon University's definition of cyber hygiene because "[a]ccording to DOD officials, there is not a commonly-used definition for cyber hygiene in DOD doctrine." Consequently, the GAO worked from Carnegie Mellon University's Software Engineering Institute's definition of the term to mean "a set of practices for managing the most common and pervasive cybersecurity risks faced by organizations today."

The GAO noted "DOD officials identified three department-wide cyber hygiene initiatives: the 2015 DOD Cybersecurity Culture and Compliance Initiative (DC3I), the 2015 DOD Cyber Discipline Implementation Plan (CDIP), and DOD's Cyber Awareness Challenge training." The GAO found incomplete implementation:

- The Culture and Compliance Initiative set forth 11 overall tasks expected to be completed in fiscal year 2016. It includes cyber education and training, integration of cyber into operational exercises, and needed recommendations on changes to cyber capabilities and authorities. However, seven of these tasks have not been fully implemented.
- The Cyber Discipline plan has 17 tasks focused on removing preventable vulnerabilities from DOD's networks that could otherwise enable adversaries to compromise information and systems. Of these 17, the DOD Chief Information Officer is responsible for overseeing implementation of 10 tasks. While the Deputy Secretary set a goal of achieving 90 percent implementation of the 10 CIO tasks by the end of fiscal year 2018, four of the tasks have not been implemented. Further, the completion of the other seven tasks was unknown because no DOD entity has been designated to report on the progress.

- The Cyber Awareness training is intended to help the DOD workforce maintain awareness of known and emerging cyber threats, and reinforce best practices to keep information and systems secure. However, selected components in the department do not know the extent to which users of its systems have completed this required training. GAO's review of 16 selected components identified six without information on system users that had not completed the required training, and eight without information on users whose network access had been revoked for not completing training.

Moreover, the GAO stated beyond those initiatives "DOD has

> (1) developed lists of the techniques that adversaries use most frequently and pose significant risk to the department, and
> (2) identified practices to protect DOD networks and systems against these techniques.

And yet, the GAO found the DOD "does not know the extent to which these practices have been implemented…[and] [t]he absence of this knowledge is due in part to no DOD component monitoring implementation, according to DOD officials." The GAO concluded that "until DOD completes its cyber hygiene initiatives and ensures that cyber practices are implemented, the department will face an enhanced risk of successful attack."

Overall, the GAO determined

> …the department faces challenges implementing the DC3I and CDIP because the DOD CIO has not taken appropriate steps to ensure that the DC3I tasks are implemented, DOD components have not developed plans with scheduled completion dates to implement the remaining four CDIP tasks overseen by DOD CIO, and the Deputy Secretary of Defense has not identified a DOD component to oversee the implementation of the seven other CDIP tasks and report on progress implementing them.

The GAO asserted that "[b]y improving oversight through implementing the DC3I tasks, DOD components developing plans with scheduled completion dates to implement the remaining four CDIP tasks that the DOD CIO oversees, and identifying a DOD component to oversee implementation of the seven other CDIP tasks and report on progress implementing them, the department can be better positioned to safeguard DOD's network by removing preventable, well-known vulnerabilities."

The GAO made seven recommendations to the DOD:

- The Secretary of Defense should ensure that the DOD CIO takes appropriate steps to ensure implementation of the DC3I tasks. (Recommendation 1)
- The Secretary of Defense should ensure that DOD components develop plans with scheduled completion dates to implement the four remaining CDIP tasks overseen by DOD CIO. (Recommendation 2)
- The Secretary of Defense should ensure that the Deputy Secretary of Defense identifies a DOD component to oversee the implementation of the seven CDIP tasks not overseen by DOD CIO and report on progress implementing them. (Recommendation 3)
- The Secretary of Defense should ensure that DOD components accurately monitor and report information on the extent that users have completed the Cyber Awareness Challenge training as well as the number of users whose access to the network was revoked because they have not completed the training. (Recommendation 4)

- The Secretary of Defense should ensure that the DOD CIO ensures all DOD components, including DARPA, require their users to take the Cyber Awareness Challenge training developed by DISA. (Recommendation 5)
- The Secretary of Defense should direct a component to monitor the extent to which practices are implemented to protect the department's network from key cyberattack techniques. (Recommendation 6)
- The Secretary of Defense should ensure that the DOD CIO assesses the extent to which senior leaders' have more complete information to make risk-based decisions—and revise the recurring reports (or develop a new report) accordingly. Such information could include DOD's progress on implementing (a) cybersecurity practices identified in cyber hygiene initiatives and (b) cyber hygiene practices to protect DOD networks from key cyberattack techniques. (Recommendation 7)

Becerra on CCPA

California's attorney general reminds residents of their rights under the now effective CCPA, contrary to calls to delay implementation.

Through the issuance of a press release, California Attorney General Xavier Becerra answered the calls for delaying enforcement of the "California Consumer Privacy Act" (CCPA) (AB 375), by "reminding consumers of their data privacy rights amidst the COVID-19 public health emergency." Last month, some industry stakeholders pressured Becerra to delay enforcement of the CCPA because companies were trying to cope with the onslaught of COVID-19, which is siphoning off resources that would otherwise be used to comply with California's newly effective privacy law. More than 30 groups asked Becerra to not enforce the CCPA until January 2, 2021.

Regarding the CCPA, Becerra stated that "[a]s the health emergency leads more people to look online to work, shop, connect with family and friends, and be entertained, it is more important than ever for consumers to know their rights under the CCPA." He noted that "CCPA went into effect on January 1, 2020 and offers new rights to consumers that can be used both during the emergency and afterwards.

- Websites that collect and sell your personal information should have a "Do Not Sell My Information" link, which you can click on to opt-out of the sale of your personal information.
- If you want to minimize or reduce the data collected by businesses during or after the emergency, you can request that the business delete personal data that it has collected from you.
- You can also request that a business disclose to you what personal information the business collects, uses, shares, or sells. You may exercise this right twice during a 12-month period.

Becerra also offered tips on how to avoid email scams, protecting virtual meetings and home networks, and means to ensure children are safe and protected online.

Singapore's DPA Cautions On Apple and Google App

Singapore's Government Technology Agency (GTA) explained in a blog posting titled "Automated contact tracing is not a coronavirus panacea" that an app paired with artificial intelligence and machine learning is not enough to combat and track COVID-19. Director of Government Digital Services Jason Bay addressed the recent announcement of Google and Apple working together through the prism of Singapore's experiences. Bay stated

> If you ask me whether any Bluetooth contact tracing system deployed or under development, anywhere in the world, is ready to replace manual contact tracing, I will say without qualification that the answer is, No. Not now and, even with the benefit of AI/ML and — God forbid — blockchain (throw whatever buzzword you want), not for the foreseeable future.

There are critical factors (like ventilation — see below; *update: or singing!*) that a purely automated system will not have access to. You cannot "big data" your way out of a "no data" situation. Period. Any attempt to believe otherwise, is an exercise in hubris, and technology triumphalism. There are lives at stake. False positives and false negatives have real-life (and death) consequences. We use TraceTogether to supplement contact tracing — not replace it. - Director of Government Digital Services Jason Bay

Bay stated "[t]here are critical factors (like ventilation — see below; *update: or singing!*) that a purely automated system will not have access to." He stressed, "[y]ou cannot "big data" your way out of a "no data" situation…Period."

Bay asserted

> Any attempt to believe otherwise, is an exercise in hubris, and technology triumphalism. There are lives at stake. False positives and false negatives have real-life (and death) consequences. We use TraceTogether to supplement contact tracing — not replace it.

Bay stated

- A human-out-of-the-loop system will certainly yield better results than having no system at all, but where a competent human-in-the-loop system with sufficient capacity exists, we caution against an over-reliance on technology.
- Finally, the experience of Singapore's contact tracers suggest that contact tracing should remain a human-fronted process. Contact tracing involves an intensive sequence of difficult and anxiety-laden conversations, and it is the role of a contact tracer to explain how a close contact might have been exposed — while respecting patient privacy — and provide assurance and guidance on next steps.
- Singapore's contact tracers are on the frontline of the fight against COVID-19; they are able to do this because they incorporate multiple sources of information, demonstrate sensitivity in their conversations with Singaporeans who have had probable exposure to SARS-CoV-2, and help to minimise unnecessary anxiety and unproductive panic. These are considerations that an automated algorithm may have difficulty explaining to worried users.

Team Telecom Returns Negative Recommendation On China Telecom

The "Team Telecom" agencies recommended that the Federal Communications Commission (FCC) "revoke and terminate China Telecom (Americas) Corp.'s authorizations to provide international telecommunications services to and from the United States." This action comes a week after the White House issued an executive order, reorganizing the process by which the U.S. government will review foreign investment in the telecommunications. In this case, the executive branch agencies that form Team Telecom called on the FCC to terminate and revoke the application of a company from the People's Republic of China (PRC) to operate in the U.S.

Executive branch agencies veto a Chinese telecom operating in the U.S. because of "identified substantial and unacceptable national security and law enforcement risks associated with China Telecom's operations, which render the FCC authorizations inconsistent with the public interest."

The Department of Commerce's National Telecommunications and Information Administration (NTIA) "filed on behalf of the Executive Branch of the United States Government a recommendation that the FCC terminate and revoke the Section 214 international authorizations of China Telecom (Americas) Corporation (China Telecom) to provide international voice traffic between the United States and foreign countries" per the agency's press release. The NTIA continued, "[f]or purposes of this recommendation, the Executive Branch represents agreement among the Departments of Justice (DOJ), Homeland Security (DHS), Defense (DOD), State, Commerce, and the U.S. Trade Representative (USTR)."

The DOJ's press release provided additional details on Team Telecom's recommendation, and the agencies "identified substantial and unacceptable national security and law enforcement risks associated with China Telecom's operations, which render the FCC authorizations inconsistent with the public interest." DOJ explained, "[m]ore specifically the recommendation was based on:

- the evolving national security environment since 2007 and increased knowledge of the PRC's role in malicious cyber activity targeting the United States;
- concerns that China Telecom is vulnerable to exploitation, influence, and control by the PRC government;
- inaccurate statements by China Telecom to U.S. government authorities about where China Telecom stored its U.S. records, raising questions about who has access to those records;
- inaccurate public representations by China Telecom concerning its cybersecurity practices, which raise questions about China Telecom's compliance with federal and state cybersecurity and privacy laws; and
- the nature of China Telecom's U.S. operations, which provide opportunities for PRC state-actors to engage in malicious cyber activity enabling economic espionage and disruption and misrouting of U.S. communications.

DOJ added

> Some of the foregoing relate to China Telecom's failure to comply with a 2007 Letter of Assurance, which was a basis for the existing FCC authorizations. The Department's National Security Division, Foreign Investment Review Section, identified those compliance issues through its mitigation monitoring program. As a result, the Executive Branch agencies concluded that the national security and law enforcement risks associated with China

Telecom's international Section 214 authorizations could not be mitigated by additional mitigation terms.

Earlier this month, President Donald Trump has issued an executive order creating an inter-agency review body to determine whether foreign investment in U.S. telecommunications companies presents national security issues. However, the executive order merely formalizes and change the longstanding "Team Telecom" process through which proposed foreign investment in the U.S. telecommunications industry have been evaluated. Like the previous body, the new body will consist of representatives from the Departments of Defense, Homeland Security, and Justice and other agencies in an advisory role.

EDPB Responds To EC's Request For Advice On Using Technology To Track COVID-19

> **"The EDPB welcomes the Commission's initiative to develop a pan-European and coordinated approach as this will help to ensure the same level of data protection for every European citizen, regardless of where he or she lives." –** EDPB Chair Andrea Jelinek

The European Data Protection Board (EDPB or Board) responded to the European Commission's recommendation on the European Commission's (EC) proposed unified approach throughout the European Union (EU) on how smartphones and data are used to fight the spread of COVID-19. The EDPB was only able to provide general guidance on what contact tracing and the use of an app would ideally be since a system has not yet been put in place. Nonetheless, the EDPB's recommendations are aligned with its previous pronouncements on the issues presented by using the smartphones of people in the EU to stem the spread of COVID-19. Moreover, many of these recommendations are similar to those detailed by European Data Protection Supervisor (EDPS) Wojciech Wiewiórowski in a speech earlier this month. And yet, it is not certain whether the EU or its member states will develop apps themselves, contract out for these services, or use and/or modify functionality already being deployed.

The EDPB stressed "that the implementation of data protection principles and the respect of fundamental rights and freedoms is not only a legal obligation, but also a requirement to reinforce the effectiveness of any data-based initiatives for combating the spread of the COVID-19 virus and for informing de-escalation strategies."

The EDPB stated that it "is aware that no one-size-fits-all solution applies to the matter at stake, and that the available options require many factors to be considered, including the fact that individuals' health may be impacted." The Board stated that "[t]his is why envisaged technical solutions need to be examined in detail, on a case-by- case basis." Additionally, the EDPB expressed its belief "that it is a step in the right direction to highlight the essential need to consult with data protection authorities to ensure that personal data is processed lawfully, respecting the rights of the individuals, in accordance with data protection law." The EDPB claimed "[t]he development of the apps should be made in an accountable way, documenting with a data protection impact assessment all the implemented privacy by design and privacy by default mechanisms, and the source code should be made publicly available for the widest possible scrutiny by the scientific community."

Moving beyond generalities, the EDPB "address[ed] specifically the use of apps for the contact tracing and warning functionality, because this is where increased attention must be paid in order to minimise interferences with private life while still allowing data processing with the goal of preserving public health."

The EDPB offered the following guidance to the EC:

- In the case where such applications would prove relevant in the implementation of some public health policy, they may only achieve their maximum efficiency if used by the largest possible share of the population, in a collective effort to fight the virus. Any functional heterogeneity, lack of interoperability or even individual difference in the use of the app may create negative externalities on others, resulting in a reduced sanitary effect. The EDPB strongly supports the Commission's proposal for a voluntary adoption of such apps, a choice that should be made by individuals as a token of collective responsibility. It should be pointed out that voluntary adoption is associated with individual trust, thus further illustrating the importance of data protection principles.
- The EDPB notes that the mere fact that the use of the contact tracing takes place on a voluntary basis, does not mean that the processing of personal data by public authorities necessarily be based on the consent. When public authorities provide a service, based on a mandate assigned by and in line with requirements laid down in law, it appears that the most relevant legal basis for the processing is the necessity for the performance of a task for public interest. The enactment of national laws, promoting the voluntary use of the app without any negative consequence for the individuals not using it, could be a legal basis for the use of the apps.
- Contact tracing apps do not require location tracking of individuals users. Their goal is not to follow the movements of individuals or to enforce prescriptions. The main function of such apps is to discover events (contacts with positive persons), which are only likely and for the majority of users may not even happen, especially in the de-escalation phase. Collecting an individual's movements in the context of contact tracing apps would violate the principle of data minimisation. In addition, doing so would create major security and privacy risks.
- Health authorities and scientists are well placed to identify what constitutes an event to be shared if, where and when it happens, under a strict necessity test as required by the law, and they should define some of the functional requirements of the app. Another debated issue is the storage of such events. Two main options are envisaged: local data storage within individuals' devices, or centralised storage. The EDPB is of the opinion that both can be valid alternatives, provided that adequate security measures are in place, and that different entities may also be considered as controllers depending on the ultimate objective of the app (e.g. the controller and data processed may be different if the objective is to provide in-app information or to contact the person on the phone, for instance). In any case, the EDPB wants to underline that the decentralised solution is more in line with the minimisation principle.
- Finally, these apps are not social platforms for spreading social alarm or giving rise to any sort of stigmatisation. In fact, they should be tools for empowering people to do their part. Quoting the draft Guidance, their sole objective is "*for public health authorities to identify the persons that have been in contact with a person infected by COVID-19 and ask him/her to self-quarantine, rapidly test them, as well as to provide advice on next steps, if relevant, including what to do if developing symptoms*". The quality of the processed data is of paramount importance in this effort.
- Algorithms used in contact tracing apps should work under the strict supervision of qualified personnel in order to limit the occurrence of any false positives and negatives, and by no

means the task "*to provide advice on next steps*" should be fully automated. It is advisable that a call-back mechanism is put in place where the person is given a telephone number or a contact channel to get more information from a human agent. Also, in order to avoid stigmatisation, no potential identifying element of any other data subject should be part of this "*advice*", nor should the use of the app, or part of it (like dashboards, configuration settings etc.), allow the re-identification of any other persons, infected by COVID-19 or not. The EDPB strongly suggests not to store any directly identifying data in users' device and that such data be in any case deleted as soon as possible.

- The EDPB strongly supports the concept in the Recommendations that once this crisis is over, such emergency system should not remain in use, and as a general rule, the collected data should be erased or anonymised.

FCC Asks How To Implement Program To Replace Chinese Telecom Equipment

The FCC wants to know if a current rulemaking to pay smaller telecoms to remove and replace Huawei and ZTE equipment comports with a subsequently enacted statute.

The Federal Communications Commission's (FCC) Wireline Competition Bureau (Bureau) released a notice, asking for comment on how to implement "Section 4 of the recently enacted" "Secure and Trusted Communications Networks Act of 2019" (P.L. 116-124). This bill is aimed at addressing national security risks presented by Huawei, ZTE, and other Chinese companies that already have sold or may sell telecommunications equipment and services to the U.S. and other countries for building 5G networks. The bill would authorize appropriations of $1 billion to help smaller telecommunications systems remove Huawei equipment and use technology the U.S. government claims is safer and more secure. And so, Section 4 of the bill requires the FCC to develop and establish a program to help smaller telecommunications providers remove and replace equipment from Huawei and related companies. The FCC is tying implementation of this legislation to a rulemaking started last fall to address the presence of Huawei, ZTE, and other Chinese companies throughout the supply chain, and the agency is asking what, if any, changes should be made to its proposed rulemaking to align that process with the new statute.

The FCC noted

> On November 26, 2019, the Commission adopted the Report and Order, which prohibits the use of Universal Service Fund support to purchase equipment or services from any company identified as posing a national security risk to communications networks or the communications supply chain. In the Report and Order, the Commission also initially designated Huawei Technologies Company (Huawei) and ZTE Corporation (ZTE), and their subsidiaries, parents, or affiliates, as companies that may pose such a risk to the communications networks and supply chain, and established a process for future designations of other companies posing such a risk. In the Further Notice of Proposed Rulemaking, the Commission sought comment on a reimbursement program proposal that would require eligible telecommunications carriers (ETCs) to remove and replace communications equipment and services from finally designated companies in their networks and would reimburse ETCs for the cost of doing so. Finally, in the Information Collection Order, the Commission required ETCs, and their subsidiaries or affiliates, to report whether

> they had Huawei or ZTE equipment in their networks and to estimate the cost to replace such equipment.

The FCC asserted that "Section 4 of the Secure Networks Act is largely consistent with the Commission's proposals in the Further Notice of Proposed Rulemaking, which proposed a reimbursement program for ETCs to replace potentially prohibited equipment and services." The FCC added that this provision "directs the Commission to establish a reimbursement program for "providers of advanced communications service" replacing covered communications equipment or services." The FCC cautioned that "[t]he legislation, inter alia, limits program eligibility to providers with two million or fewer customers and restricts funding to the permanent replacement of covered equipment and services obtained before August 14, 2018 so long as the equipment and services replaced are identified as "covered" on the initial list issued by the [FCC] pursuant to Section 2 of the Secure Networks Act." The FCC stated that "[i]f equipment or services are subsequently added to the initial list, then providers may use the funds to replace equipment and services obtained no more than 60 days after the date the equipment or services were added to the list." The FCC is seeking "comment on whether the Commission should modify the reimbursement program proposed in the Further Notice of Proposed Rulemaking to implement these new statutory requirements…[c]ommenters should also specifically address how the Commission should interpret "providers of advanced communications service."

The FCC explained its responsibilities under the bill

> The Secure Networks Act directs the Commission on how to structure the reimbursement program application filing and review process, and describes a process that largely resembles the application process proposed in the Further Notice of Proposed Rulemaking. Specifically, under the statute, the Commission must: (1) require applicants to provide initial reimbursement cost estimates; (2) act on applications within 90 days of submission unless a 45 day extension is warranted; (3) provide applicants an opportunity to cure a deficiency; (4) require certifications as to the applicant's plan and timeline; and (4) "make reasonable efforts to ensure that reimbursement funds are distributed equitably among all applicants."

In terms of the bill's larger purpose, according to the Committee Report, H.R. 4998 would:

- require the Federal Communications Commission (FCC or Commission) to develop and maintain a list of communications equipment and services that pose an unacceptable risk to national security and prohibit the use of Federal funds administered by the FCC to purchase, rent, lease, or otherwise obtain such equipment and services.
- establish the Secure and Trusted Communications Reimbursement Program to assist small communications providers with the costs of removing prohibited equipment and services from their networks and replacing prohibited equipment with more secure communications equipment and services.

The Committee explained that "[t]he United States identified individual Chinese telecommunications firms, including Huawei Technologies Co. Ltd (Huawei) and its affiliates, as posing significant threats to U.S. commercial and security interests." The Committee claimed

> Large communications companies with sophisticated network security operations and significant capital generally have avoided installing and using Huawei and other suspect foreign equipment in their networks. Moreover, Federal agencies have actively reached out to large carriers to express concerns when carriers have considered purchasing suspect

equipment. In contrast, some smaller carriers with more limited resources and less sophisticated security operations have purchased and installed Huawei, and other suspect foreign equipment, in their networks either because the equipment was less expensive or they were unaware of the security risk, or both.

U.S. Releases Guidance on the North Korean Cyber Threat

The Departments of State, the Treasury, and Homeland Security (State, Treasury, and DHS), and the Federal Bureau of Investigation (FBI) issued "Guidance on the North Korean Cyber Threat" "as a comprehensive resource…for the international community, network defenders, and the public." The guidance was likely released to counter increased North Korean hacking or new attacks hitting the U.S. and its partners. However, according to experts who have long tracked North Korean cyber activities, the only new information in the guidance is that North Korean "cyber actors have also been paid to hack websites and extort targets for third-party clients." This guidance follows another recent United States government warning on North Korea's cyber activities. In mid-February, the Cybersecurity and Infrastructure Security Agency (CISA), the FBI, and the Department of Defense (DOD) identified " malware variants used by the North Korean government."

The Democratic People's Republic of Korea's (DPRK) malicious cyber activities threaten the United States and the broader international community and, in particular, pose a significant threat to the integrity and stability of the international financial system. Under the pressure of robust U.S. and UN sanctions, the DPRK has increasingly relied on illicit activities – including cybercrime – to generate revenue for its weapons of mass destruction and ballistic missile programs.

In this most recent guidance, the agencies stated

> The Democratic People's Republic of Korea's (DPRK) malicious cyber activities threaten the United States and the broader international community and, in particular, pose a significant threat to the integrity and stability of the international financial system. Under the pressure of robust U.S. and UN sanctions, the DPRK has increasingly relied on illicit activities – including cybercrime – to generate revenue for its weapons of mass destruction and ballistic missile programs. In particular, the United States is deeply concerned about North Korea's malicious cyber activities, which the U.S. government refers to as HIDDEN COBRA. The DPRK has the capability to conduct disruptive or destructive cyber activities affecting U.S. critical infrastructure. The DPRK also uses cyber capabilities to steal from financial institutions, and has demonstrated a pattern of disruptive and harmful cyber activity that is wholly inconsistent with the growing international consensus on what constitutes responsible State behavior in cyberspace.

The agencies declared that "[i]t is vital for the international community, network defenders, and the public to stay vigilant and to work together to mitigate the cyber threat posed by North Korea."

In the section titled "DPRK's Malicious Cyber Activities Targeting the Financial Sector," the agencies explained

> Many DPRK cyber actors are subordinate to UN- and U.S.-designated entities, such as the Reconnaissance General Bureau. DPRK state-sponsored cyber actors primarily consist of hackers, cryptologists, and software developers who conduct espionage, cyber-enabled theft targeting financial institutions and digital currency exchanges, and politically-motivated operations against foreign media companies. They develop and deploy a wide range of malware tools around the world to enable these activities and have grown increasingly sophisticated. Common tactics to raise revenue illicitly by DPRK state-sponsored cyber actors include, but are not limited to:
>
> - Cyber-Enabled Financial Theft and Money Laundering.
> - Extortion Campaigns.
> - Cryptojacking.

The agencies added that "[t]hese activities highlight the DPRK's use of cyber-enabled means to generate revenue while mitigating the impact of sanctions and show that any country can be exposed to and exploited by the DPRK….[and] [a]ccording to the UN Security Council 1718 Committee Panel of Experts' 2019 mid-term report (2019 POE mid-term report), the POE is also investigating such activities as attempted violations of UN Security Council sanctions on the DPRK."

In the section titled "Cyber Operations Publicly Attributed to DPRK by U.S. Government," the agencies stated

> The DPRK has repeatedly targeted U.S. and other government and military networks, as well as networks related to private entities and critical infrastructure, to steal data and conduct disruptive and destructive cyber activities. To date, the U.S. government has publicly attributed the following cyber incidents to DPRK state-sponsored cyber actors and co-conspirators:
>
> - Sony Pictures.
> - Bangladesh Bank Heist.
> - WannaCry 2.0.
> - FASTCash Campaign.
> - Digital Currency Exchange Hack.

Apple Responds To Concerns Raised By Democratic Senators On COVID-19 App

Earlier this month, Senators Robert Menendez (D-NJ), Kamala Harris (D-CA), Richard Blumenthal (D-CT), and Cory Booker (D-NJ) sent Apple a letter "raising concerns about the company's COVID-19 screening tools and the safety and security of private health data that will potentially be collected from users." This letter follows a pair of mid-March "letters to the Trump Administration and the tech giant Google raising concerns over privacy and cybersecurity vulnerabilities involving a third-party coronavirus (COVID-19) testing website announced last week by President Trump and coronavirus response coordinator Dr. Deborah Birx."

Apple explained that its app and website are not subject to health information security and privacy regulations, that it will minimize data, allow people to access the information Apple collects on them, and will not sell the information to third parties.

The Senators stated that "[i]n their March 27 announcement, Apple maintained it will collect "some information" to help improve the site but failed to identify what that information would include." Menendez, Harris, Blumenthal, and Booker posed a list of questions to the company regarding its security and privacy practices regarding the new app and website.

Menendez, Harris, Blumenthal, and Booker stated

> on March, 27, 2020, the Centers for Disease Control and Prevention (CDC) announced the release of an app and website created by Apple in partnership with the White House Coronavirus Task Force and the U.S. Department of Health and Human Services. The app and website are designed for individuals to complete a questionnaire about their health and exposure to determine if they should seek care for COVID-19 symptoms. Both the website and app guide users through a diagnostic questionnaire, and once completed, provide CDC recommendations on next steps including guidance on social distancing and self-isolating, how to closely monitor symptoms, recommendations on testing, and when to contact a medical provider.

Apple answered the Senators in a letter last week. Apple contended

> At the request of HHS, Apple also drew upon its engineering and clinical resources to help develop a new COVID-19 website and COVID-19 app, in partnership with the CDC, the White House Coronavirus Task Force, and FEMA, to make it easy for people across the country to get trusted information and guidance at a time when the US is feeling the heavy burden of COVID-19.

Apple stated "[c]onsistent with Apple's strong dedication to user privacy, the COVID-19 app and website were built to protect the privacy and security of users' data."

Apple asserted that the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act regulations that bind healthcare providers and others regarding security and privacy do not apply to the company's screening site and app. Apple claimed

> HIPAA applies when a covered entity (health care provider, health insurance company or health care clearinghouse) or business associate (on behalf of a covered entity) is using, disclosing, creating, receiving, maintaining or transmitting certain health information (known as "protected health information"). Here, data are entered into the website and app directly by users, and no covered entities are involved in or otherwise required for that interaction. Therefore neither the site nor app are covered by HIPAA.

In response to a question from the Senators, "[c]an individuals who use the website and app access and monitor the data that Apple collects about them," Apple asserted it "is a strong proponent of fundamental privacy rights, including the right for an individual to access personal information that a company maintains on them." The company continued, "[i]n support of these rights, Apple has developed a global privacy portal, through which individuals can access and download a copy of their personal information." However, it bears note that Apple did not say it was following a certain statute or standard in allowing people to access their information, so it is unclear how fulsome or robust this disclosure may be. Apple added that "an important component of a comprehensive privacy program is data minimization — to only collect

personal information where it makes sense to do so." Apple stated that "[w]ith respect to the COVID-19 website and app, Apple does not collect or retain identifiable information about individuals. As such, there is no identifiable information for individuals to access and monitor."

While Apple said it would not *sell* personal information collected through the app, it did allow that it may *share* the information at some point in the future subject to legal requirements. The company claimed "[i]f in the future we do share any of the data collected through the app and website with third parties, any such sharing will be limited and subject to strong privacy and security requirements."

Further Reading

- "Burning Cell Towers, Out of Baseless Fear They Spread the Virus" – *The New York Times*.
- "Big tech is more essential than ever. That won't stop antitrust hawks." – *Protocol*.
- "The ancient computers in the Boeing 737 Max are holding up a fix" – *The Verge*.
- "The internet is surviving the pandemic — let the feuding begin" – *Politico*.
- "Apple, Google debut major effort to help people track if they've come in contact with coronavirus" – *The Washington Post*.
- "'Blind to the data': Behind the effort to anonymously track COVID-19 carriers" – *Protocol*.
- "To fight Covid-19, cyberattacks worldwide must stop immediately" – *Vox*.
- "Everything must go: Cybercriminal forums offer discounts during pandemic" – *cyberscoop*.
- "Zoom will let paying customers pick which data center their calls are routed from" – *The Verge*.
- "Will Google's and Apple's COVID Tracking Plan Protect Privacy?" – The Markup
- "A company's challenge: Anonymity in tracking COVID-19 carriers" – Protocol