Question#:	1
Topic:	Election Vulnerability
Hearing:	Dangerous Partners: Big Tech and Beijing
Primary:	The Honorable Cory A. Booker
Committee:	JUDICIARY (SENATE)

Question: From your vantage point, what is the single greatest vulnerability in the U.S. election security infrastructure for 2020?

What actions is your office (and/or related offices at the Department of Homeland Security) taking to address that vulnerability?

Response: The exploitation of vulnerabilities on internet-connected Election Infrastructure presents significant risk to the integrity, availability, and confidentiality of systems and information critical to administering an election.

The Cybersecurity and Infrastructure Security Agency (CISA) has taken a variety of actions to address this risk:

- CISA continues to encourage state and local governments to use auditable voting systems and implement efficient and effective post-election audits. CISA has funded the development of an open-source post-election auditing tool, which is now available to state and local governments. A version of this tool was used in counties in Pennsylvania, Michigan, Georgia and other states in the November 2019 election.
- CISA, through the EI-ISAC, has supported the voluntary deployment of intrusion detection systems – known as Albert sensors – for the protection of election infrastructure in all 50 states, 208 localities, and five territories. Not only are targeted attacks on election systems now more likely to be detected and quickly responded to, but we also have greater visibility into threats than previously..
- CISA provides weekly vulnerability scans of internet-connected election infrastructure systems for 39 states, 193 local partners, one territory, and 21 private sector partners.
- CISA, through the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), now shares alerts with all 50 states and more than 2,500 local and territorial election offices.
- CISA has published informational products on threats to election infrastructure, such as ransomware and phishing, and provides voluntary guidance and recommendations to election infrastructure stakeholders that they can implement to address associated vulnerabilities. These products can be found at https://www.cisa.gov/protect2020.

Question#:	2
Topic:	Election Security Act
Hearing:	Dangerous Partners: Big Tech and Beijing
Primary:	The Honorable Cory A. Booker
Committee:	JUDICIARY (SENATE)

Question: Please review, if you have not done so already, S. 1540, the Election Security Act of 2019. What would this legislation do to address the vulnerability you identified?

In your assessment, would our election infrastructure be more secure if the Election Security Act were enacted into law?

Response: CISA has appreciated the opportunity to engage with you and your staff on a range of election security efforts, including providing technical drafting assistance to provisions in legislative proposals that impact our agency. We are always willing to provide additional feedback on proposed legislation. The legislation also includes provisions that fall outside CISA equities.

It's important to note that CISA already has broad authorities to assist state and local election officials. We are already offering support, products, and services, such as classified and unclassified briefings, vulnerability scanning, threat information and indicator sharing, risk assessments, and remote penetration testing, at no cost, to all states, more than 6,000 local election officials, political organizations and Presidential campaigns, 8 election associations, and 21 election technology providers.

Question#:	3
Topic:	Handling China
Hearing:	Dangerous Partners: Big Tech and Beijing
Primary:	The Honorable John Kennedy
Committee:	JUDICIARY (SENATE)

Question: As of January 2020, Chinese law requires all companies, including foreign owned companies, to allow the Chinese government access to their computer networks and all the data that is stored on, transits over, or in any other way touches Chinese information infrastructure.

From a U.S. security standpoint, what is your agency's recommendation for how American tech companies should handle themselves with regard to China?

Response: We encourage extreme vigilance and deliberate, risk-based scrutiny for all Information and Communications Technology (ICT) activity that involves a Chinese supply chain nexus. There are a broad range of supply chain attack vectors that could be compromised or leveraged for malicious intent that are outlined in the ICT Supply Chain Risk Management Task Force report on threat scenarios. Companies should have awareness of their exposure across these threat categories and formulate risk management strategies accordingly.

CISA encourages all companies to adopt a risk-based security framework, to include risk-based assessments of its ICT supply chain. We urge companies to conduct a holistic, careful evaluation of potential hardware and software equipment, vendors and the supply chain. CISA works with its private sector partners to encourage industry to incentivize security, including supply chain risk management, in the marketplace and ensure it is a primary consideration in product development, manufacture, acquisition, and procurement. CISA's ICT Supply Chain Risk Management Task Force is a key tool for public-private coordination in this area. If vulnerabilities are discovered, then companies must give serious consideration to procurement of ICT made domestically or by trusted allies that do not expose those companies to supply chain attack vectors.

Our adversaries, China in particular, are ambitiously investing not only to close the technological gap with the United States, but also to invert it. When it comes to addressing products that pose real and potential threats, especially from foreign entities, we are working hard and constructively to be more proactive by stopping potentially harmful products from being deployed in the first place. Establishing such international cybersecurity norms must be an ongoing, collaborative effort with our private industry partners. We must, and will, continue to encourage responsible behavior and oppose those who would seek to disrupt networks and systems.

Question#:	4
Topic:	Complicit Practices
Hearing:	Dangerous Partners: Big Tech and Beijing
Primary:	The Honorable John Kennedy
Committee:	JUDICIARY (SENATE)

Question: In November, a cybersecurity expert from the Heritage Foundation testified to this subcommittee that Big Tech companies like Google, Apple, and Amazon were "complicit" in the persecution of religious minorities and dissidents in China.

Apple recently removed the Taiwan flag emoji for its users in Hong Kong, and earlier this year Apple warned some creators of Apple TV programming not to portray China in a negative light.

How do we get these companies to end their complicit practices with the Chinese Communist Party in order to maintain access to its market of 1.4 billion people?

Response: Companies have corporate, moral, ethical, and legal responsibilities that they must uphold. Complicit practices with the Chinese Communist Party could expose companies to reputational, and in certain instances, legal risks under U.S. sanctions and enforcement actions including withhold release orders, criminal investigations, and with respect to export controls. Companies should understand the reputational, material, and legal risks of complicity in forced labor and human rights abuses if they determine proper due diligence in their supply chain is not possible and they still choose to conduct business. Companies are also encouraged to collaborate with industry groups to share information, develop the capacity to research potential indicators of forced labor or labor abuses in Chinese languages, and build relationships with Chinese suppliers and recipients of U.S. goods and services.

Pertaining to goods that may be produced wholly or in part with forced labor in China and imported or destined for import into the United States, on January 15, 2020, DHS released its first ever *Strategy to Combat Human Trafficking, the Importation of Goods Produced with Forced Labor, and Child Sexual Exploitation* (Strategy). As noted in the Strategy, industry's support for and collaboration on the prohibition on the importation of goods produced with forced labor is essential to compliance so that forced labor is prevented, not simply a cost of doing business. DHS supports industry in taking proactive measures to prevent and eliminate human trafficking in their supply chains. For example, U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) partner with companies to promote awareness and proactive Corporate Social Responsibility initiatives.

CBP and ICE also enforce the prohibition against importing goods produced with forced, indentured, or convict labor through administrative, civil, and criminal enforcement actions, respectively. Where evidence reasonably indicates that goods are produced with forced, indentured, or convict labor and likely to be imported into the United States, CBP will deny entry to those goods, which could lead to the goods being seized and forfeited, or even to the issuance

Question#:	4
Topic:	Complicit Practices
Hearing:	Dangerous Partners: Big Tech and Beijing
Primary:	The Honorable John Kennedy
Committee:	JUDICIARY (SENATE)

of civil penalties against the importer and other parties, as appropriate. HSI may initiate criminal investigations relating to the importation of forced labor-made goods in violation of U.S. law. HSI's criminal enforcement authorities may lead to the criminal prosecution of individuals and/or corporations for their roles in the importation of goods into the United States in violation of U.S. law, potentially resulting in incarceration, fines, seizure, and forfeiture of the goods. In addition, businesses that contract with the Federal Government may be subject to suspension and debarment and other penalties pursuant to the Federal Acquisition Regulation prohibitions on human trafficking outlined in clauses 52.222-19 and 52.222-50.

Question#:	5
Topic:	Supporting Forced Labor
Hearing:	Dangerous Partners: Big Tech and Beijing
Primary:	The Honorable John Kennedy
Committee:	JUDICIARY (SENATE)

Question: A report published Monday by the Australian Strategic Policy Institute claims that a large number of global companies including Microsoft, Apple, Amazon, Google, and Huawei are benefiting from the forced labor of Uyghurs (Chinese Muslims) and other minorities.

Should Americans continue to support these companies and buy their products knowing they are benefiting from forced labor practices?

Response: As stated in the DHS *Strategy to Combat Human Trafficking, the Importation of Goods Produced with Forced Labor, and Child Sexual Exploitation* (Strategy), forced labor is antithetical to American values and undermines legitimate trade and competition. U.S. law prohibits the importation of goods mined, produced, or manufactured wholly or in part from forced labor and violators may face criminal and civil consequences. Therefore, it is incumbent upon U.S. importers to ensure their supply chains are free from forced labor. The United States continues to institute this prohibition and DHS is the primary federal department tasked with enforcing this ban. In addition to harming laborers, consumers, and corporations, importing such goods undermines the ability of similar American-made goods to be sold at a competitive price.

CBP is responsible for enforcing the prohibition on the entry of goods produced with forced labor into U.S commerce. When information reasonably but not conclusively indicates that merchandise within the purview of this provision is being or likely to be imported, the Commissioner may issue a Withhold Release Order (WRO) in accordance with 19 C.F.R. § 12.42(e). Evidence that merchandise is being made with forced labor does not suffice to issue a WRO. Rather, goods must also be, or likely to be, imported to the United States. CBP pursues information from various sources to investigate the entities involved, their production practices, supply chains, and nexus to U.S. imports.

Since 1991, CBP has issued 33 WROs and 6 Findings on merchandise from China produced or harvested with forced labor and imported to the United States. The most recent WRO related to China CBP issued was on May 1, 2020 on products made by the Hetian Haolin Hair Accessories Co. Ltd.. These China-related WROs and Findings are published and publicly available on CBP's website, and in the CBP Bulletin and the Federal Register pursuant to 19 C.F.R. § 12.42(f).

Question#:	5
Topic:	Supporting Forced Labor
Hearing:	Dangerous Partners: Big Tech and Beijing
Primary:	The Honorable John Kennedy
Committee:	JUDICIARY (SENATE)

Question#:	6
Topic:	Aiding Censorship
Hearing:	Dangerous Partners: Big Tech and Beijing
Primary:	The Honorable John Kennedy
Committee:	JUDICIARY (SENATE)

Question: Do you believe it is appropriate for American technology firms to aid censorship efforts by the Chinese government?

How will your agencies weigh in on the appropriateness of American technology companies abetting censorship efforts of the Chinese government, and what consequences should tech company's face if they do help facilitate censorship efforts of the Chinese government?

Response: Aiding in or complicity with censorship efforts by the Chinese government could expose companies to reputational harm or carry potential legal risks under U.S. sanctions and export controls and related enforcement actions. Companies must implement due diligence policies, procedures, and internal controls to ensure compliance with applicable legal requirements and align with international best practice across the upstream and downstream supply chain.

The *National Security Strategy* demands that the United States "rethink the policies of the past two decades – policies based on the assumption that engagement with rivals and their inclusion in international institutions and global commerce would turn them into benign actors and trustworthy partners." The *Strategy* further notes: "For the most part, this premise turned out to be false. Rival actors use propaganda and other means to try to discredit democracy. They advance anti-Western views and spread false information to create divisions among ourselves, our allies, and our partners."

Question#:	7
Topic:	Google Exemption
Hearing:	Dangerous Partners: Big Tech and Beijing
Primary:	The Honorable John Kennedy
Committee:	JUDICIARY (SENATE)

Question: Huawei is a demonstrable threat to U.S. cybersecurity. Google is lobbying for an exemption from U.S. policies to continue to work with them.

From the perspective of your agency, is it a security risk for Google to continue to work with a company which knowingly presents a cybersecurity threat to the U.S.?

Response: DHS Team Telecom and CISA, along with the other Interagency Team Telecom partners carefully weighed numerous factors before their recommendation to restrict Google from providing a direct subsea cable connection between the U.S. and Hong Kong and mainland China. Our assessment concluded that submarine cables are a fundamental element of global communications critical infrastructure, carrying most of the world's internet, voice, and data traffic between continents. The PRC has demonstrated the intent to steal or acquire U.S. persons' sensitive personal data through both digital infrastructure investments and new PRC intelligence and cybersecurity laws. With its increasingly data rich environment, driven by global market changes, subsea cable infrastructure is vulnerable to exploitation. DHS, from a national security perspective, did not believe it to be in the best interest of the U.S. to approve commercial operation of cables landing directly in Chinese territory. It is a security risk for American companies to work with foreign companies that knowingly present cybersecurity threats to the U.S. China has shown both intent and capability to put U.S. companies at risk by stealing intellectual property, pursuing technically sophisticated campaigns (e.g., Cloudhopper and Equifax), and leveraging Chinese companies' market presence and technological reach to negatively affect the competitive market. Chinese laws and policies can be used to force companies to comply with intelligence activities and pursue national security interests that may affect company operations. Furthermore, the Chinese government may also hold a financial stake in a Chinese company, which would increase the Chinese government's ability to influence and coerce company operations.

We encourage extreme vigilance and deliberate, risk-based scrutiny for all Information and Communication Technology (ICT) activity that involves a Chinese supply chain nexus. There are a broad range of supply chain attack vectors that could be compromised or leveraged for malicious intent that are outlined in this report out of the ICT Supply Chain Risk Management Task Force. Companies should have awareness of their exposure across these threat categories and formulate risk management strategies accordingly.

CISA encourages all companies to adopt a risk-based security framework, to include risk-based assessments of its ICT supply chain. We urge companies to conduct a holistic, careful evaluation of potential hardware and software equipment, vendors and the supply chain. CISA works with its private sector partners to encourage industry to incentivize security, including supply chain

Question#:	7
Topic:	Google Exemption
Hearing:	Dangerous Partners: Big Tech and Beijing
Primary:	The Honorable John Kennedy
Committee:	JUDICIARY (SENATE)

risk management, in the marketplace and ensure it is a primary consideration in product development, manufacture, acquisition, and procurement. CISA's ICT Supply Chain Risk Management Task Force is a key tool for public-private coordination in this area.

In his 2018 Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974, the United States Trade Representative (USTR) determined that numerous acts, policies, and practices of the People's Republic of China (PRC) government were unreasonable or discriminatory, and burden or restrict United States commerce. Based on a rigorous investigation, USTR found that the PRC: (1) requires or pressures United States companies to transfer their technology to Chinese entities; (2) places substantial restrictions on United States companies' ability to license their technology on market terms; (3) directs and unfairly facilitates acquisition of United States companies and assets by domestic firms to obtain cutting edge technologies; and (4) conducts and supports unauthorized cyber intrusions into United States companies' networks to access sensitive information and trade secrets.

As outlined in the recently released *United States Strategic Approach to The People's Republic of China*, the PRC's attempts to dominate the global information and communications technology industry through unfair practices is reflected in discriminatory regulations like the PRC National Cyber Security Law, which requires companies to comply with Chinese data localization measures that enable Chinese Communist Party (CCP) access to foreign data. Other PRC laws compel companies like Huawei and ZTE to cooperate with Chinese security services, even when they do business abroad, creating security vulnerabilities for foreign countries and enterprises utilizing Chinese vendors' equipment and services.

The United States will continue to restrict U.S. exports to Huawei and its non-U.S. affiliates on the Entity List, as Huawei remains engaged in behavior that threatens U.S. national security. Licenses for Huawei are reviewed with a "presumption of denial", but each license is examined individually and approved or denied based on national security considerations.