Question#:	1
Topic:	Supply Chain Task Force
Hearing:	China's Non-Traditional Espionage Against the United States: The Threat and Potential Policy Responses
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: Bloomberg recently reported a troubling story on alleged supply chain hacking. Tiny chips were allegedly inserted into servers manufactured in China which were shipped to the U.S. and incorporated into networks used by over 30 American companies. The Chinese government was reportedly able to gain access to the computers' networks through the chip. Some computers were alleged to have gone to Department of Defense data centers and the onboard networks of Navy warships. DHS has vehemently denied the report. However, DHS established a new task force in October focused on supply chain threats to information and communications technology. The task force's objectives would include partnerships with the private sector and recommendations for industry to protect itself.

Does DHS still stand by its denial?

Response: The Department of Homeland Security (DHS) does not have any evidence to support the claims asserted in the article published by Bloomberg Businessweek, *The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies.* Information and communications technology supply chain security is at the core of DHS's cybersecurity mission, and we are committed to the security and integrity of the technology on which Americans and others around the world increasingly rely. DHS recently launched several government-industry initiatives to develop near- and long-term solutions to manage risk posed by the complex challenges of increasingly global supply chains. These initiatives are building on existing partnerships with a wide range of technology companies to strengthen our Nation's collective cybersecurity and risk management efforts.

Question: What specific work is the task force doing to address these issues?

Response: ICT Supply Chain Risk Management (SCRM) Task Force, a public-private partnership between the Cybersecurity and Infrastructure Security Agency (CISA) and ICT companies, has five key work streams that are guiding efforts to develop consensus recommendations to identify and manage risk to the global ICT supply chain. These work streams are the following:

1. Generating an inventory of ongoing and planned Federal and private sector SCRM activities, best practices, and guidance.
2. Developing a common framework for the bi-directional sharing of supply chain risk information between government and industry.

Question#:	1
Topic:	Supply Chain Task Force
Hearing:	China's Non-Traditional Espionage Against the United States: The Threat and Potential Policy Responses
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

3. Identification of processes and criteria for threat-based evaluation of ICT supplies, products, and services.
4. Identification of market segment(s) and evaluation criteria for Qualified Bidder and Manufacturer List(s).
5. Producing policy recommendations to incentivize the purchase of ICT from original manufacturers or authorized resellers.

The Task Force will assist with private sector engagement for the newly created Federal Acquisition Security Council (FASC). Every entity represented on the FASC also participates, by design, in the Task Force.

Question: How can the private sector protect itself? What can law enforcement do to help private companies?

Response: All purchasers and users of ICT should demand transparency and security from manufacturers and sellers. Following the SCRM practices for approving products used in the DHS Continuous Diagnostics and Mitigation (CDM) program[1] is a good start and increased adoption of these practices will send a signal to manufacturers and sellers of ICT that improved security is important to consumers. While the Department of Homeland Security does not endorse non-federal entities, products or services, numerous private sector organizations have developed guidance that can be used to enable increased security in ICT products and services. Some examples include:

- SAFECode publication "*Managing Security Risks Inherent in the Use of Third-party Components*," available at: https://www.safecode.org/wp-content/uploads/2017/05/SAFECode_TPC_Whitepaper.pdf
- East West Institute publication "*Purchasing Secure ICT Products and Services: A Buyers Guide*," available at: https://www.eastwest.ngo/sites/default/files/EWI_BuyersGuide.pdf
- The Open Trusted Technology Provider Standard, available at: https://ottps-cert.opengroup.org/ottps-standard

[1] Available at: https://gsa.gov/portal/getMediaData?mediaId=167746.

Question#:	2
Topic:	Chinese Threat
Hearing:	China's Non-Traditional Espionage Against the United States: The Threat and Potential Policy Responses
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: A report issued by a private cyber security firm claims that China is the most prolific cyber attacker of Western nations. The report explained that biotechnology companies, pharmaceuticals, defense, mining and transport were all targets. The report noted that very sophisticated techniques were used to hide Chinese hackers' attacks on universities, which have valuable research, as well as financial and personal data.

Is China our biggest threat in terms of recent and potential near term cyber attacks?

Response: In understanding the cyber capabilities of our adversaries and strategic competitors, we generally consider three separate areas of most concern: cyber espionage, cyber attack, and cyber influence. Each of our major cyber adversaries—China, Russia, Iran, and North Korea— presents a unique threat and engages in a different array of malicious activity to seek political, economic, and military advantage.

At present, China and Russia pose the greatest espionage and cyber attack threats. China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on US critical infrastructure. Additionally, Chinese actors, as reflected in multiple Department of Justice indictments since 2014, are historically the most significant cyber economic espionage threat to US corporations.

Question: What targets is DHS observing that China is interested in, including anything the general public might not expect?

Response: For years, China and others have conducted cyber espionage to collect intelligence and targeted our critical infrastructure to hold it at risk. China remains the most active strategic competitor responsible for cyber espionage against the US Government, corporations, and allies. We are also concerned about the potential for Beijing to use Chinese information technology firms as espionage platforms against the United States and allies. Chinese economic espionage targets are closely aligned with planning priorities as outlined in such documents as the Chinese Communist Party's Five-Year Plans and the Made in China 2025 Plan.

Industries targeted by indicted Chinese cyber actors include aerospace, financial services, manufacturing, pharmaceuticals, oil and gas, communications, information technology, and maritime industries. Activity related to the Chinese Ministry of State Security-affiliated cyber actors indicted in 2018 was particularly broad reaching. In addition to the activity covered in the indictment, DHS and private sector cyber security firms identified

Question#:	2
Topic:	Chinese Threat
Hearing:	China's Non-Traditional Espionage Against the United States: The Threat and Potential Policy Responses
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

a great amount of significant additional activity by the organization affiliated with the indicted persons. These actors compromised managed service providers (MSPs) in several countries, and, when successful, used the trusted connections to navigate across and through the computer networks of their numerous customers in several countries, potentially placing thousands of companies at risk.

Question: Are government targets or private sector targets more likely to be cyberattacked by the Chinese?

Response: Beijing will authorize cyber targeting against the US government or key US technology sectors when doing so addresses a significant national security or economic goal not achievable through other means, so the target is more dependent on whether it provides value rather than whether it is public or private sector.

Question: What is DHS doing to assist the private sector to prevent and respond to cyber attacks?

Response: DHS Cybersecurity and Infrastructure Security Agency (CISA) conducts a wide range of activities to enable and enhance cybersecurity. Most recently, CISA conducted a robust private-sector engagement program in response to China's managed service provider (MSP) compromises and published an alert with mitigation strategies and techniques. DHS' Office of Intelligence and Analysis (I&A) provides classified and unclassified cyber intelligence products and briefings to the private sector. I&A also works closely with the fusion centers around the country to support their information sharing activities with the public and private sector.

Question#:	3
Topic:	Existing Laws
Hearing:	China's Non-Traditional Espionage Against the United States: The Threat and Potential Policy Responses
Primary:	The Honorable Christopher Coons
Committee:	JUDICIARY (SENATE)

Question: I am concerned that we are not doing enough to combat persistent cyber intrusions from our adversaries, including China. There are many laws, such as the Computer Fraud and Abuse Act, that would allow law enforcement to identify, charge, and prosecute cyber criminals. Although it may be difficult to successfully extradite and prosecute individuals located in countries like China, there have been a number of cases where the U.S. has had success in arresting and extraditing cyber attackers from foreign countries.

Do you agree that we should be more aggressive in using existing laws against cyber criminals located abroad, such as in China?

Does law enforcement have sufficient resources to prioritize investigation and prosecution of these cyber-crimes? Where would additional resources have the most impact?

What is your assessment of federal law enforcement's ability to attribute specific cyber-crimes to the individual actors who committed the attacks?

Response: The Cybersecurity and Infrastructure Security Agency defers this response to the Department of Justice (DOJ), as the investigation and prosecution of cyber-crimes fall within the scope of DOJ’s mission area

Question#:	4
Topic:	Meng Wanzhou Case
Hearing:	China's Non-Traditional Espionage Against the United States: The Threat and Potential Policy Responses
Primary:	The Honorable Richard Blumenthal
Committee:	JUDICIARY (SENATE)

Question: Following the arrest of Meng Wanzhou, the Chief Financial Officer of Huawei, the president suggested that he would intervene in her case. His suggestion that he would intervene to block action by the Department of Justice either in that extradition proceeding or in the underlying criminal action is extremely disturbing to me and may be to others in the law enforcement community. Acknowledging that you cannot comment on a pending criminal proceeding, I ask:

Were you consulted before President Trump said he might intervene in Ms. Meng's case?

Response: Department of Homeland Security defers to DOJ regarding the pending legal matters.