Question#:	1
Topic:	Huawei Equipment
Hearing:	Defending the U.S. Electric Grid Against Cyber Threats
Primary:	The Honorable Peter Welch
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: After our intelligence community issued repeated warnings about the threat of using Huawei equipment, the Federal Communications Commission moved to block Huawei products from being used on our communications network. Congress later prohibited U.S. government communications systems from using Huawei equipment.

Does the Department of Homeland Security (DHS) have the same concerns about Huawei equipment (e.g. solar inverters, electric vehicle charging stations, etc.) being used on our electric grid? Is there any ongoing review or rulemaking at DHS regarding the use of Huawei equipment in the energy sector?

Response: The Cybersecurity and Infrastructure Security Agency (CISA) fully supports the decisions and policies prohibiting U.S. government communications systems from using Huawei equipment. CISA shares concerns over allowing any product or company that is subject to risk of coercion and compromise from a foreign power to have a presence in our energy infrastructure.

The use of Huawei equipment raises the remote access potential, which could facilitate surveillance, collection and exploitation of data, and compromise electric grid industrial control systems devices and software applications. This potential could also be exploited by nation-states and other sophisticated actors to place our infrastructure at risk.

CISA's unique role at the intersection of cybersecurity and critical infrastructure provides a perspective on issues surrounding supply chain security and the energy sector and positions CISA to reduce the risks of supply chain compromise. CISA has taken the lead to convene industry and federal partners to discuss supply chain security, to include compromises linked to specific products such as those produced by Huawei. CISA's supply chain risk management work includes engagement through the Information and Communications Technology Supply Chain Risk Management Task Force, which is composed of representatives from large and small private sector organizations and federal agencies, as well as subject matter experts, infrastructure owners and operators, and other key stakeholders who provide recommendations and guidance to help shape trusted supply chain practices. In addition, specific to supply chain risks facing the federal government, CISA is a member of the Federal Acquisition Security Council, which is responsible for issuing exclusion and removal orders across the federal government to ensure that potential vulnerabilities will not compromise the integrity of federal information systems.

Question#:	2
Topic:	Ransomware Attack
Hearing:	Defending the U.S. Electric Grid Against Cyber Threats
Primary:	The Honorable Nancy Mace
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: Any network-connected device can be used as a vector for a ransomware attack, including mobile devices, like smartphones. How can we ensure that mobile devices connected to the networks of critical infrastructure providers aren't a soft target for ransomware criminals, and what options can critical infrastructure operators pursue to secure not just the device's connection to the network, but the device itself?

Response: There are many actions that CISA recommends that critical infrastructure providers take actions to reduce the risk of cyber-attacks, including ransomware attacks. A good place to start is CISA's Cyber Essentials, a guide for leaders of small businesses as well as leaders of small and local government agencies to develop an actionable understanding of where to start in implementing organizational cybersecurity practices. In addition, critical infrastructure operators can take advantage of no-cost CISA Cyber Assessment Services, like Vulnerability Scanning and Web Application Scanning.

In response to the rising number of ransomware attacks, CISA and the Multi-State Information Sharing and Analysis Center also released the Joint Ransomware Guide. This resource provides critical infrastructure operators concrete steps to prepare for, mitigate against, and respond to a ransomware attack and includes best practices as well as a ransomware response checklist.

More specifically, there are several steps that critical infrastructure providers can take, including:

- **Mobile Device Management**:
    - Use of an enterprise mobility management/unified endpoint management solution to manage devices, enforce security policies such as device unlock passcode policies, and ensure that operating system, firmware, and mobile app versions are up to date to prevent compromised devices from accessing critical infrastructure resources.
    - Enforce user and device authentication and device security posture check before allowing any access to the Operational Technology (OT) network. Guidance for securing mobile devices on the network include the National Institute of Standards and Technology's: Mobile Threat Catalogue and practice guides for Mobile Device Security: Corporate-Owned Personally-Enabled and Bring Your Own Device.
- **Least Privilege Access Control**:

Question#:	2
Topic:	Ransomware Attack
Hearing:	Defending the U.S. Electric Grid Against Cyber Threats
Primary:	The Honorable Nancy Mace
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

- Ensure that access to any OT networks or systems that control critical infrastructure functionality is limited to only those with an identified need and that privileges are limited to only those necessary to perform their function.

- Enforce multi-factor authentication for access to OT components, networks and assets.

- Limit remote access to authorized, enterprise-managed devices. Ideally, do not allow mobile devices to connect to the critical infrastructure's network segment. This includes prohibiting users from plugging a mobile device into an OT system for charging, which has been demonstrated to be a vector for attack.

· **Operational Technology Network Protections:**

- A first step in protecting the OT networks from attack is securing the network. Recognizing that some critical infrastructure components may not be running the latest versions of operating systems, operators should follow best practices for configuring and securing the OT network to limit access vectors (such as a mobile phone or a rogue laptop) that could compromise the OT network.

- Where possible, segment the network. This serves to limit exposure from compromise of any single device or group of devices compromise.

- Employ traditional network protections such as a deny list or firewalls.

- Use a robust monitoring strategy on the network to detect known bad actors or behaviors associated with bad actors. Log and monitor all access to critical components to detect suspicious or anomalous activity.

· **Ransomware Defenses:**

- Use Stopransomware.gov, which provides no-cost resources such as ransomware prevention best practices, cyber hygiene services including free scanning and testing services, and a ransomware response checklist if one has been hit by ransomware along with numerous other resources from across the Federal government.

- Have a backup of data in secure storage with protections such as write once.

- Identify and backup data on all devices and monitor those assets.

Question#:	2
Topic:	Ransomware Attack
Hearing:	Defending the U.S. Electric Grid Against Cyber Threats
Primary:	The Honorable Nancy Mace
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

- Establish a mitigation and containment capability on the network, which could include stopping execution of associated programs, disabling user accounts, and disconnecting a system from the network.

· **User Training:** Conduct regular user security awareness training on phishing and other social engineering attacks as well as restrictions on using mobile devices to access OT systems or charge mobile devices.