Question#:	1
Topic:	State-Affiliated Attacks
Hearing:	America Under Siege: Preventing and Responding to Ransomware Attacks
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: What do you see as our options to best deter and punish state-affiliated ransomware attacks?

Response: Law enforcement agencies, like the United States Secret Service, perform a limited, but important role, in deterring and punishing activities of foreign states. Through our criminal investigations, and international law enforcement cooperation, we detect, investigate, arrest, and prosecute those engaged in transnational cyber crimes and seize their ill-gotten assets. Through these law enforcement actions we directly deter and punish those that engage in the use of ransomware, regardless of a potential affiliation with a state. Law enforcement also develops and shares actionable information that can be used to protect against and mitigate the impact of ransomware.

Law enforcement actions also help to illuminate the conduct of foreign states—for example, are they unwitting of transnational cyber criminals in their jurisdictions or knowingly tolerating such activities. Understanding such distinctions in foreign state conduct can be essential to diplomatic or other efforts to alter the conduct of a foreign state.

Because those responsible for ransomware attacks hide their true identities and physical locations in cyberspace, the State Department has partnered up with federal law enforcement agencies to offer rewards for information leading to the identification and location of key leaders of these transnational criminal organizations under the Transnational Organized Crime Rewards Program pursuant to 22 USC 2708(b)(6). Currently, there are two up to $10 million reward offers for information leading to the identification or location of an individual who holds key leadership positions in the transnational organized crime groups: the DarkSide Ransomware Group and the Sodinokibi Ransomware Group.

For these reasons, law enforcement is an essential component in addressing transnational criminal activity like ransomware.

Question#:	2
Topic:	Payment Mechanisms
Hearing:	America Under Siege: Preventing and Responding to Ransomware Attacks
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: During the hearing you noted that without cryptocurrency that ransomware attacks would still occur but that a different payment mechanism would be utilized. Please describe what other payments structures could or have been utilized by bad actors to facilitate ransomware payments. Are there other payment mechanisms we should focus on in addition to cryptocurrency if we want to disrupt the ability of these criminals to profit from their work?

Response: Cyber extortion schemes, like ransomware, have existed longer than cryptocurrency. For example, cyber extortionists have required payment by mailing a cashier's check (or similar payment order) to a post office box, use of various money transmission services, cash shipments and deliveries, and other payment methods. Such means continue to be utilized, in addition to the use of cryptocurrency. A technology neutral approach to strengthening US enforcement related to money laundering, regardless of the form of money used, could be effective and disrupting the ability of transnational cyber criminals to profit from ransomware and other illicit activity.

Question#:	3
Topic:	Ransomware Guidance
Hearing:	America Under Siege: Preventing and Responding to Ransomware Attacks
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: If victims of ransomware contact either the FBI or USSS, are they given the same or similar guidance? Has federal law enforcement coordinated how reported incidents are investigated? What is the procedure that FBI and USSS use to de-conflict cases?

Response: The Secret Service has closely coordinated with the Federal Bureau of Investigation (FBI), U.S. Department of Justice, the Cybersecurity and Infrastructure Security Agency (CISA), and other agencies in providing information on how organizations should respond to ransomware incidents. We all work closely together to provide consistent and appropriate guidance, to include through the information published on stopransomware.gov.

The Secret Service regularly works with other agencies, to include the FBI and CISA, on deconflicting and jointly investigating incidents as well as identifying tactics, techniques and procedures (TTPs) that can be shared across sectors to limit widespread exploitation. This occurs formally via detailees, joint task forces, and information systems amongst our headquarters offices, as well as directly between our respective field offices. This deconfliction occurs consistent with relevant agency policies, such as DHS Policy directive 045-04 and PPD-41.