Question#:	1
Topic:	Prioritizing Cybersecurity
Hearing:	Election Interference: Ensuring Law Enforcement Is Equipped to Target Those Seeking to Do Harm
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: What is DHS doing to prioritize cybersecurity operations inside the agency and what can Congress do to help?

Response: Safeguarding and securing cyberspace is a core homeland security mission. On May 15, 2018, the Department of Homeland Security (DHS) released its current Cybersecurity Strategy, providing DHS with a framework to execute our cybersecurity responsibilities during the next five years to keep pace with the evolving cyber risk landscape by reducing vulnerabilities and building resilience; countering malicious actors in cyberspace; responding to incidents; and making the cyber ecosystem more secure and resilient. DHS is actively developing an accompanying implementation plan which will identify ongoing and planned cybersecurity efforts across the Department. The implementation plan will enable greater connectivity between the Department's strategic cybersecurity objectives and resourcing, budgetary, and prioritization processes.

DHS provides entities with information, technical assistance, and guidance they can use to secure their networks, systems, assets, information, and data, by reducing vulnerabilities, ensuring resilience to cyber incidents, and supporting their holistic risk management priorities. These efforts are carried out by DHS's National Protection and Programs Directorate, which includes the National Cybersecurity and Communications Integration Center (NCCIC). The NCCIC operates at the intersection of the private sector, state and local governments, federal departments and agencies, international partners, law enforcement, intelligence, and defense communities.

DHS will continue to work with Congress on creating a new Cybersecurity and Infrastructure Security Agency. Transforming the National Protection and Programs Directorate (NPPD) into a new agency is the logical next move for the cybersecurity and infrastructure security mission within DHS. This new agency would continue NPPD's mission of leading the national effort to improve infrastructure security, enhancing the protection of the Federal Government's networks and critical infrastructure, and helping entities in the public and private sectors manage risk. In addition to the important step of providing this new organization with a name that better reflects its central mission, legislation would streamline and focus the critical operations of the new agency by removing current responsibilities that are not well aligned to the cyber and infrastructure security mission. This change reflects the important work the men and women at DHS carry out every day on behalf of the American people to safeguard and secure our homeland.

Question#:	2
Topic:	Discouraging Minority Voters
Hearing:	Election Interference: Ensuring Law Enforcement Is Equipped to Target Those Seeking to Do Harm
Primary:	The Honorable Mazie Hirono
Committee:	JUDICIARY (SENATE)

Question: Special Counsel Mueller's indictment against several Russian entities noted that one way they interfered in the 2016 elections was by encouraging minority voters not to vote. In fact, the Pew Research Center found that in 2016, turnout of African-American voters in a presidential election dropped for the first time in 20 years - even though a record number of people voted in 2016. At the hearing, Nina Jankowicz testified about the complex strategies Russia used to target the African-American community and discourage African Americans from voting.

What steps are you taking to combat interference efforts to discourage minority groups from voting?

Do you believe these steps are sufficient to ensure that the votes of minorities are not suppressed in future elections?

How you seen foreign efforts similar to that used in 2016 to discourage minority groups from voting in the 2018 elections?

Response: The Department of Homeland Security (DHS) is focused on enhancing awareness of the threat of foreign influence, sharing information with federal, state, local, and private sector partners, and increasing stakeholder resilience. But our efforts are in support of the Federal Bureau of Investigation (FBI), which leads federal efforts to counter foreign influence. We defer to the FBI to provide additional details on their work in this area.

Question#:	3
Topic:	Information Sharing
Hearing:	Election Interference: Ensuring Law Enforcement Is Equipped to Target Those Seeking to Do Harm
Primary:	The Honorable Mazie Hirono
Committee:	JUDICIARY (SENATE)

Question: Timely coordination by the federal government with state and local officials is important to ensure that cyber threats are promptly addressed. Hawaii, for example, has the Hawaii State Fusion Center, which shares information with its partners on cyber threats that affect Hawaii.

What are the Justice Department and the Department of Homeland Security (DHS) doing to help ensure that states, like Hawaii, receive timely information about cyber threats and have adequate resources to counteract such threats?

How quickly are you identifying, notifying, and neutralizing these cyber threats?

What additional tools do you need to improve the timeliness and effectiveness of this process?

Response: The Department of Homeland Security (DHS) engages with non-federal entities, such as the State of Hawaii, to share cybersecurity information and provide technical assistance on a voluntary basis. This information sharing partnership includes leveraging the Hawaii State Fusion Center to share intelligence. Additionally, DHS participates in the bi-directional sharing of cyber threat indicators and analysis through various methods, including through automated, machine-speed capabilities to enhance collective cybersecurity in Hawaii. The automated indicator sharing (AIS) capability enables the exchange of cyber threat indicators between the Federal Government and Hawaii at machine speed. AIS is a part of DHS's effort to create an ecosystem where as soon as an entity observes an attempted compromise, the indicator will be shared in real time with all of our partners, protecting them from that particular threat.

Additionally, the State of Hawaii participates in the Multi-State Information Sharing and Analysis Center (MS-ISAC), an information sharing organization funded by DHS. MS-ISAC includes membership of state, local, tribal, and territorial governments, enabling members to share cybersecurity information and collaborate with each other. DHS funds provided to MS-ISAC have also supported an intrusion detection system that protects government networks in states, such as Hawaii. This system is similar to the intrusion detection system operated by DHS that protects Federal Government networks.

Question#:	4
Topic:	Protecting Election Systems
Hearing:	Election Interference: Ensuring Law Enforcement Is Equipped to Target Those Seeking to Do Harm
Primary:	The Honorable Mazie Hirono
Committee:	JUDICIARY (SENATE)

Question: Since the Department of Homeland Security has designated election systems as part of the nation's "critical infrastructure," what guidance and resources have you provided to state and local officials to support their efforts to protect election systems? What steps have DHS taken to foster an effective federal partnership with state and local election systems?

Response: Threats to our elections are a national security issue and of the utmost importance to the Department of Homeland Security (DHS). As Secretary Nielsen recently said, "The President has been clear, and DHS and our interagency partners have been clear. We will not allow any foreign adversary to change the outcome of our elections. Every American must have confidence in the integrity of the system and that their votes are counted, and counted correctly." DHS has moved quickly to prioritize existing resources to establish and support the Election Infrastructure Subsector (EIS), by increasing our engagements with election stakeholders, and deploying a range of cybersecurity services to state and local partners.

DHS has made tremendous strides and has been committed to working collaboratively with those on the front lines of administering our elections—state and local election officials and the vendor community—to secure election infrastructure from risks. The establishment by DHS of election infrastructure as a critical infrastructure subsector has formalized the prioritization of assistance from the Federal Government for state, local, tribal, and territorial governments and private sector entities in their efforts to reduce cyber and physical risks to election infrastructure.

In 2017, DHS created an Election Task Force to improve coordination with and support to election stakeholders. The Task Force is focused on enhancing coordination between election officials, the intelligence community, and law enforcement partners to secure their systems. The Department has worked with federal, state, and local partners to establish the EIS Government Coordinating Council (GCC), which focuses on issues such as developing information sharing protocols and key working groups. Additionally, DHS has worked with a range of relevant private sector companies to establish a Sector Coordinating Council (SCC), which is focused on security issues relevant to private sector companies that support the operations of our election process. The EIS GCC and SCC work together to address the needs of the Election Infrastructure Subsector.

DHS has authority to make available the process and application for security clearance to state, local, tribal, and territorial government officials. As such, the Department has been

Question#:	4
Topic:	Protecting Election Systems
Hearing:	Election Interference: Ensuring Law Enforcement Is Equipped to Target Those Seeking to Do Harm
Primary:	The Honorable Mazie Hirono
Committee:	JUDICIARY (SENATE)

working with state chief election officials to help them obtain security clearances in an expedited manner and has expanded the offer of security clearances to two additional officials in each state. Furthermore, DHS is assisting members of the more recently established Sector Coordinating Council with obtaining security clearances to ensure adequate information sharing with the private sector. In partnership with the Office of the Director of National Intelligence and the Federal Bureau of Investigation, in February we gathered all state chief election officials at an intelligence community facility and provided one-time read-ins to a classified threat briefing. This was the first such gathering in our history.

DHS has supported election officials with automated cyber hygiene scans, providing election officials with weekly scans for vulnerabilities and recommended mitigations. We also offer Risk and Vulnerability Assessments, a more in-depth service, during which DHS cyber operators attempt to penetrate networks to identify vulnerabilities that can be mitigated before an adversary exploits them. Other services and support include incident detection and response, cybersecurity exercises, and vulnerability analysis. Additionally, although some state and local entities have chosen not to use our services, we are aware that some have procured similar services from third-party vendors. We continue to urge election officials to seek assistance from DHS to enhance the security of election infrastructure. Additional information on available resources can be found at: https://www.dhs.gov/topic/election-security.

Question#:	5
Topic:	Social Media Platforms
Hearing:	Election Interference: Ensuring Law Enforcement Is Equipped to Target Those Seeking to Do Harm
Primary:	The Honorable Mazie Hirono
Committee:	JUDICIARY (SENATE)

Question: Last year, the Senate Judiciary Subcommittee on Crime and Terrorism held a hearing with Facebook, Google, and Twitter to address ways Russians used social media platforms to interfere in our elections. I asked these social media companies about their commitment to prevent abuse on their platforms.

What law enforcement tools do you think would be effective to prevent efforts by foreign actors to interfere in our elections using social media platforms?

Response: Intelligence and information sharing is the most important law enforcement tool to effectively prevent foreign actors from using social media platforms to interfere in our elections. Social media companies have the capability to stop or slow down foreign interference campaigns if they understand the tactics, techniques and procedures of the adversary, or if they are provided specific accounts that are conducting interference activities.