Question#:	1
Topic:	Designation Protections
Hearing:	Protecting Democracy's Frontline Workers
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: You testified that election infrastructure was designated as a critical infrastructure subsector by the Department of Homeland Security in 2017. What extra protections, oversight, or prioritization does this designation entitle election infrastructure to?

Response: In January 2017, the U.S. Department of Homeland Security (DHS) designated the Election Infrastructure Subsector under the Government Facilities Sector. This designation enables DHS to prioritize cybersecurity and physical security assistance to state and local election officials and their private sector partners. Collectively, this designation makes clear that election infrastructure enjoys the associated benefits offered by the U.S. government, including voluntary services and resources, information sharing, and incident response assistance. Further, this designation makes it easier for the federal government to have full and direct discussions with key stakeholders regarding vital information. Since 2017, both the Election Infrastructure Government Coordinating Council (EI-GCC) and Election Infrastructure Sector Coordinating Council (EI-SCC) have been established to interface with the Department and help inform initiatives and services to further critical election infrastructure. The GCC and SCC have served as mechanisms for collaboration between DHS, law enforcement, the intelligence community, and private sector partners to enhance information sharing about risks to the Nation's election infrastructure, identify resources to help mitigate such risks, communicate best practices, address identified vulnerabilities, and enable election officials' access to threat information and intelligence. This designation does nothing to change the role state and local governments have in administering elections.

Question#:	2
Topic:	Expanding Resources
Hearing:	Protecting Democracy's Frontline Workers
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: Your opening statement referenced CISA's five priorities to ensure election integrity for this year's midterm elections. As the final prong of CISA's approach, you stated that CISA is "expanding resources and services that help keep election officials and their voters safe." What specific resources and services will you be expanding?

Response: In addition to expanded promotion of existing resources like physical security assessments of election facilities provided by our Protective Security Advisors, CISA continues to develop and evolve its current offerings and develop new offerings to meet the evolving needs of this subsector. In coordination with the Intelligence Community, including the DHS Office of Intelligence & Analysis and federal law enforcement partners, CISA continues to facilitate threat briefings to the election community. These briefings are tailored to reflect the current risk landscape and have recently included increased focus on physical security threats. CISA also continues to host tabletop exercises at the state and national levels. The scenarios for CISA's tabletop exercises for election officials, including the annual national Tabletop the Vote exercise, are scoped with input from the election community to ensure they reflect current priorities. For example, "Tabletop the Vote 2022" included expanded focus on physical security issues.

CISA has developed factsheets, trainings, and other resources to help election officials improve the physical security of their infrastructure and keep their voters safe. For example, the Election Infrastructure Insider Threat Mitigation Guide highlights risks associated with insider threats and offers guidance for establishing a mitigation program. The Election Personnel Threat Response Guide is a resource to effectively document and report threats made against election officials and workers to law enforcement.

In addition to developing new products, CISA also works to contextualize existing resources for use by election infrastructure stakeholders. Examples include:

- De-escalation Series for Critical Infrastructure Owners and Operators offers guidance on recognizing the warning signs of someone on a path to violence to enable assessment and management of an evolving threat.
- CISA Insight – Mitigating the Impacts of Doxing defines and provides examples of doxing; explains its potential impacts and mitigations; offers protective and preventative measures, and resources for individuals and organizations.
- Personal Security Considerations Fact Sheet encourages vigilance and reporting of suspicious behaviors and contains best practices that can mitigate threats to personal safety.

Question#:	2
Topic:	Expanding Resources
Hearing:	Protecting Democracy's Frontline Workers
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

- Physical Security Considerations for Temporary Facilities Fact Sheet provides security considerations for operators of temporary facilities to mitigate the impacts of a potential attack.

CISA also conducts active shooter preparedness webinars that focus on behavioral indicators, actions that may be taken to increase the probability of survival, and how to recover from an incident. Election officials often participate in these trainings and the Agency will dedicate webinars specifically for the subsector upon request.

Question#:	3
Topic:	CISA Authority
Hearing:	Protecting Democracy's Frontline Workers
Primary:	The Honorable Mike Lee
Committee:	JUDICIARY (SENATE)

Question: Ms. Wyman, The Cybersecurity and Infrastructure Security Agency has a "MDM" Team "charged with building national resilience to [Mis, Dis-, and Malinformation] and foreign influence activities."

Ms Wyman, is CISA's statutory directive to analyze and disseminate information to prevent terrorist attacks limited to actions and "rumors" directly traceable to malicious foreign actors?

Does this authority extend to analyzing information propagated by domestic actors? Is CISA authorized, for example, to direct social media companies to remove posts from citizens when CISA believes the posts contain "misinformation"?

Is this authority limited to Mis, Dis-, and Malinformation about the infrastructures identified in the Cybersecurity and Infrastructure Security Agency Act, or does it include all Mis, Dis-, and Malinformation on subjects outside of the scope of identified infrastructure? Does it include misinformation on Covid-19?

Response: CISA helps the American people understand the scope and scale of MDM activities targeting election infrastructure and critical infrastructure and enables them to take actions to mitigate associated risks.

Through its support to the election community through voluntary partnerships, CISA works closely with state and local election officials to enhance the security and resilience of election infrastructure. One of the ways CISA has done this historically is by transmitting information identified by state and local election officials as potential disinformation concerning the administration or security of election infrastructures —for example, posts suggesting falsely that election-related deadlines have changed—to social media platforms for any action the platform deems appropriate. CISA does not direct social media companies to remove posts that may contain misinformation. CISA provided this service for state and local officials during the 2018 and 2020 election cycles.

Maintaining functioning critical infrastructure has been imperative during the response to the COVID-19 emergency for both public health and safety. Consistent with the authorities described above, the MDM team has supported the interagency and private sector partners' COVID-19 response as appropriate in support of the security and resilience of critical infrastructure that support the response to COVID-19.

Question#:	4
Topic:	Collaborating with Social Media
Hearing:	Protecting Democracy's Frontline Workers
Primary:	The Honorable Mike Lee
Committee:	JUDICIARY (SENATE)

Question: What efforts has CISA made to collaborate with social media companies in censoring unpopular opinions voiced by actual Americans?

Response: CISA does not censor speech or opinions. CISA supports the election community through voluntary partnerships and works closely with state and local election officials to enhance the security and resilience of election infrastructure. One of the ways CISA has done this historically is by transmitting information identified by state and local election officials as potential election security-related disinformation—for example, posts suggesting that election-related deadlines have changed—to social media platforms for any action the platform deems appropriate. CISA does not direct social media companies to remove posts that may contain misinformation. CISA provided this service for state and local officials during the 2018 and 2020 election cycles.

Question#:	5
Topic:	Transparency Requests
Hearing:	Protecting Democracy's Frontline Workers
Primary:	The Honorable Mike Lee
Committee:	JUDICIARY (SENATE)

Question: In a Reuter's article published the morning of the hearing, you were quoted as complaining about American's submitting requests for transparency from their local election offices. You were quoted saying, these requests were "voluminous and daunting" and "You still have a group of people in each state that believe that the election was stolen." Ms. Wyman, isn't transparency-not censorship-the best way to combat falsehoods?

Response: CISA is committed to transparency. To that end, CISA shares accurate information about election infrastructure and its underlying processes on our website, in materials we produce, and through partnerships with state, local, tribal, and territorial election officials. For example, CISA's election security rumor vs. reality webpage debunks common misinformation and disinformation narratives and themes that relate broadly to the security of election infrastructure and related processes. This resource addresses false election security rumors by describing common and generally applicable protective processes, security measures, and legal requirements designed to protect against or detect large-scale security issues related to election infrastructure and processes.