

United States Senate  
WASHINGTON, DC 20510

March 4, 2024

**VIA ELECTRONIC TRANSMISSION**

The Honorable Jen Easterly  
Director  
U.S. Department of Homeland Security  
Cybersecurity and Infrastructure Security Agency

Dear Director Easterly:

The cybersecurity of U.S. critical infrastructure systems is vital to our national security. Cyberattacks targeting critical infrastructure have occurred more frequently, highlighting “industrial control systems that are known to be easy targets for cyber attackers.”<sup>1</sup> On January 31, 2024, FBI Director Christopher Wray sounded the alarm over China, stating that “China’s hackers are positioning on American infrastructure in preparation to wreak havoc and cause real-world harm to American citizens and communities, if and when China decides the time has come to strike.”<sup>2</sup> These types of attacks put our national security at risk, placing “energy, finance, food and agriculture, healthcare, municipal services, transportation, water” and other sectors in vulnerable positions.<sup>3</sup>

In 2022, the Government Accountability Office (GAO) released a report with six recommendations for the Cybersecurity & Infrastructure Security Agency (CISA) to improve prioritizing the protection of our critical infrastructure through the National Critical Infrastructure Prioritization Program.<sup>4</sup> Two of these recommendations have not been implemented and remain open.

CISA’s stated mission is to lead the national effort to understand, manage, and reduce risk to U.S. cyber and physical infrastructure.<sup>5</sup> GAO’s first open recommendation focuses on

---

<sup>1</sup> Gordon G. Chang, *Terrifying Hacks on Critical Infrastructure Have Arrived. America Isn’t Ready*, THE HILL (Dec. 12, 2023, 11:00 AM), <https://thehill.com/opinion/cybersecurity/4353922-terrifying-hacks-on-critical-infrastructure-have-arrived-america-isnt-ready/>.

<sup>2</sup> *The CCP Cyber Threat to the American Homeland and National Security: Hearing Before the H. Select Comm. on the Chinese Communist Party*, 118th Cong. 12 (2024) (statement of Christopher Wray, Director, Federal Bureau of Investigation).

<sup>3</sup> Stephen Webber, *Threats to America’s Critical Infrastructure are now a Terrifying Reality*, THE HILL (Feb. 11, 2024, 1:00 PM), <https://thehill.com/opinion/technology/4458692-threats-to-americas-critical-infrastructure-are-now-a-terrifying-reality/>.

<sup>4</sup> U.S. GOV’T ACCOUNTABILITY OFF., GAO-22-104279, CRITICAL INFRASTRUCTURE PROTECTION: CISA SHOULD IMPROVE PRIORITY SETTING, STAKEHOLDER INVOLVEMENT, AND THREAT INFORMATION SHARING 42-43 (2022) <https://www.gao.gov/products/gao-22-104279>.

<sup>5</sup> About CISA, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, <https://www.cisa.gov/about>

your role in ensuring that CISA's process for selecting critical infrastructure priorities reflects current threats.<sup>6</sup> The second open recommendation advises you to document the goals and strategies for the National Critical Functions framework.<sup>7</sup> Two years after the GAO report was published, according to GAO, CISA has yet to close the recommendations.<sup>8</sup>

While CISA is tasked with protecting critical infrastructure, current and former CISA employees claim that it has dramatically faltered in abiding by that mission.<sup>9</sup> Instead of prioritizing securing our critical infrastructure from targeted attacks, CISA has reportedly "metastasized into the nerve center of the federal government's domestic surveillance and censorship operations on social media."<sup>10</sup> The U.S. Court of Appeals for the 5th Circuit recently found that CISA "likely violated the First Amendment," when it became "significantly entangled" in social media platforms' moderation decisions regarding Covid-19 origin information.<sup>11</sup>

In an internal November 2020 email from CISA employee Robert Schaul to the Alliance for Securing Democracy, Mr. Schaul stated that "Mail voting fraud disinfo is in-bound for us this time, domestic or foreign; so if you see something you're worried about let us know – especially if our messaging can help counter."<sup>12</sup> Further, in a May 2020 pamphlet, CISA outlined Covid-19 disinformation activities and provided contact information for American citizens to report on disinformation.<sup>13</sup> It appears that CISA has broadened its jurisdiction from physical critical infrastructure to include elections and public health campaigns.

While speaking at a conference in 2021, you discussed your plans to strengthen CISA's misinformation, disinformation, or malinformation (MDM) team and stated, "[o]ne could argue we're in the business of critical infrastructure, and the most critical infrastructure is our cognitive infrastructure, so building that resilience to misinformation and disinformation, I think, is incredibly important."<sup>14</sup>

Based on a 2022 CISA pamphlet titled *Planning and Incident Response Guide for Election Officials*, "MDM also may originate from domestic sources aiming to sow divisions and

---

<sup>6</sup> *Supra* note 4 at 42.

<sup>7</sup> *Id.*

<sup>8</sup> *Id.*

<sup>9</sup> Suzanne Smalley, Nihal Krishan, & AJ Vicens, *Insiders Worry CISA is too Distracted from Critical Cyber Mission*, CYBERSCOOP (Dec. 22, 2022), <https://cyberscoop.com/cisa-dhs-easterly-cyber-mission/>.

<sup>10</sup> STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T OF THE H. COMM. ON THE JUDICIARY, 118<sup>TH</sup> CONG., REP. ON THE WEAPONIZATION OF CISA: HOW A "CYBERSECURITY" AGENCY COLLUDED WITH BIG TECH AND "DISINFORMATION" PARTNERS TO CENSOR AMERICANS 1 (Comm. Print 2023), <https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/cisa-staff-report6-26-23.pdf>.

<sup>11</sup> *Missouri v. Biden*, 83 F.4th 350, 391 (5th Cir. 2023).

<sup>12</sup> *Supra* note 10 at 11.

<sup>13</sup> American Hospital Association, *CISA Insights: Covid-19 Disinformation Activity*, (May 2022), <https://www.aha.org/other-cybersecurity-reports/2020-05-11-cisa-insights-covid-19-disinformation-activity>.

<sup>14</sup> Maggie Miller, *Cyber Agency Beefing Up Disinformation, Misinformation Team*, THE HILL (Nov. 10, 2021, 2:52 PM), <https://thehill.com/policy/cybersecurity/580990-cyber-agency-beefing-up-disinformation-misinformation-team/>.

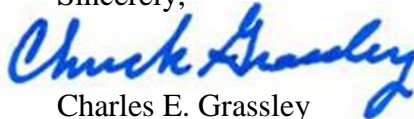
reduce national cohesion.”<sup>15</sup> According to the DHS Inspector General, in 2021 CISA swapped its Countering Foreign Influence Task Force for an MDM team “to be responsive to current events” and “promote more flexibility to focus on general MDM.”<sup>16</sup> A CISA official stated that the CFITF established a 15 member MDM staff in January 2021 to focus on disinformation activities related to elections and critical infrastructure.<sup>17</sup>

Accordingly, so Congress may conduct objective and independent oversight concerning CISA’s efforts to prioritize the protection of our critical infrastructure, please provide answers to the following no later than March 18, 2024.

1. When does CISA plan to finalize updates to the National Critical Infrastructure Prioritization Program nomination thresholds against current threats?
2. When does CISA plan to finalize the documentation of the goals and strategies of the National Critical Functions framework?
3. What steps has CISA taken to improve its process for identifying critical infrastructure priorities to better reflect current threats? How does CISA determine which threats to our critical infrastructure take priority? Please provide all documents.
4. Does CISA acknowledge and agree that cyberattacks originating from foreign actors should be considered one of the most prevalent threats against U.S. critical infrastructure? If not, why not?
5. In light of recent attacks on hospitals, water systems, and financial institutions, does CISA continue to adopt the position that “cognitive infrastructure” is the most critical infrastructure?
6. Describe CISA relationship with the FBI’s Foreign Influence Task Force

Thank you for your prompt review and responses. If you have any questions, please contact Tucker Akin on my Committee staff at (202) 224-0642.

Sincerely,



Charles E. Grassley  
Ranking Member  
Committee on the Budget

---

<sup>15</sup> *Supra* note 10 at 10.

<sup>16</sup> U.S. DEP’T OF HOMELAND SEC. OFFICE OF THE INSPECTOR GENERAL, OIG-22-59, DHS NEEDS A UNIFIED STRATEGY TO COUNTER DISINFORMATION CAMPAIGNS (Aug. 10, 2022), at 7, <https://www.oig.dhs.gov/sites/default/files/assets/2022-08/OIG-22-58-Aug22.pdf>.

<sup>17</sup> *Id.*