



U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency
Washington, DC 20528

June 7, 2024

The Honorable Charles E. Grassley
Ranking Member
Committee on the Budget
United States Senate
Washington, DC 20510

Dear Ranking Member Grassley:

Thank you for your April 5, 2024, letter to the Department of Homeland Security (DHS) concerning the security of critical infrastructure and the threat of ransomware. I am responding on behalf of the Department.

As the Nation's cyber defense agency, the Cybersecurity and Infrastructure Security Agency (CISA) is charged with leading the national effort to understand, manage, and reduce risk to cyber and physical infrastructure. Securing our Nation's critical infrastructure is a shared responsibility requiring a whole-of-nation approach. CISA is only able to accomplish its mission by building collaborative, trusted partnerships across all levels of government, the private sector, and the international community.

CISA serves as the National Coordinator for critical infrastructure security and resilience, which includes coordinating activities across Sector Risk Management Agencies (SRMAs) that have specialized expertise within their critical infrastructure sectors. Further, CISA provides numerous voluntary cybersecurity services and capabilities support to non-federal entities, including all sectors of critical infrastructure. This includes sharing intelligence and information such as cyber threat indicators, analysis, mitigation guidance, and best practices; maintaining cross-sector situational awareness of malicious cyber activity; providing, upon request, operational technical assistance and incident response capabilities, which may include continuous monitoring and detection of cybersecurity risks to critical infrastructure; and providing training and exercises.

CISA's understanding of cybersecurity incidents and ransomware events is partly reliant on the voluntary reporting of cyber incidents by private sector and state and local entities. CISA will gain greater visibility into the cyber threat landscape through the implementation of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), which will require covered critical infrastructure entities to report to CISA covered cyber incidents and ransom payments. The enactment of CIRCIA marked an important milestone toward improving America's cybersecurity. Once implemented, CISA will have a much-improved understanding of cyber threats to U.S. critical infrastructure, which will allow CISA to rapidly deploy resources and render assistance to victims suffering attacks, analyze incoming reporting across sectors to spot trends, and quickly share that information with network defenders to reduce the number of additional victims and enable risk mitigation at scale across critical infrastructure. On April 4, 2024, CISA published the CIRCIA Notice of Proposed Rulemaking. The comment period ends

on July 3, 2024. Independent of CIRCIA, CISA encourages all organizations to voluntarily share with CISA information on cyber incidents.

CIRCIA also established the Joint Ransomware Task Force co-chaired by CISA and the Federal Bureau of Investigation (FBI). It serves as a central body for coordinating an ongoing nationwide campaign against ransomware attacks in addition to pursuing opportunities for international cooperation. CISA launched StopRansomware.gov to serve as a one-stop location for critical infrastructure entities and the public to access resources to address ransomware threats more effectively.

At an operational level, CISA routinely notifies and works with organizations to mitigate the impact of ransomware incidents before harm occurs. Through our Pre-Ransomware Notification Initiative, we use tips from researchers and industry to identify organizations that have already been compromised by a ransomware actor but where the actor has not yet encrypted or stolen data. By notifying these entities, they can often implement a remediation before damage occurs. Through our Ransomware Vulnerability Warning Pilot, we proactively identify information technology (IT) systems across critical infrastructure that contain security vulnerabilities commonly associated with ransomware attacks. Once CISA identifies these affected systems, our cybersecurity personnel notify system owners of their vulnerabilities and the connection of those vulnerabilities to ransomware attacks, enabling timely mitigation. In 2023, we conducted over 1,700 notifications to organizations, including hospitals, water utilities, K-12 school districts, and state, local, tribal, and territorial government entities about open vulnerabilities on their networks so they could protect themselves prior to a successful ransomware incident.

Aside from the ransomware threats raised in your letter, there are several factors that help CISA prioritize cyber threats to critical infrastructure, including those informed by the U.S. Intelligence Community. For example, in January, I testified publicly alongside, FBI Director Chris Wray, National Security Agency Director Paul Nakasone, and National Cyber Director Harry Coker. Our testimony conveyed the real and urgent threat posed by the People's Republic of China (PRC). We noted that in recent years, we have observed a deeply concerning evolution in PRC targeting of U.S. critical infrastructure that has little to no intelligence value. This threat is driving targeted mitigation activities across multiple critical infrastructure sectors by CISA and our interagency partners.

Securing the Nation's critical infrastructure requires a whole-of-nation approach, and CISA's engagement with the private sector is essential. There are many ways CISA engages the private sector, including through formal councils—to include Sector Coordinating Councils, Cross-Sector Coordinating Councils, CISA's Cybersecurity Advisory Committee, the Critical Infrastructure Partnership Advisory Council, and the Joint Cyber Defense Collaborative. CISA also has Cybersecurity Advisors (CSAs) across the country who offer cybersecurity assistance in communities in every state and territory. CSAs increase awareness of and provide CISA cybersecurity products and services directly to critical infrastructure entities. They can provide cyber preparedness assessments and protective resources, guidance on best practices, and support during cyber incidents. In addition, CISA coordinates with SRMAs to distribute alerts, services, and products that CISA produces for critical infrastructure entities.

With respect to exercises, CISA consults and plans with government and private sector stakeholders to conduct preparedness exercises for resilience disciplines, including cybersecurity and physical security. These range from small-scale, discussion-based exercises to large-scale, operations-based exercises. This April, CISA hosted Cyber Storm IX, a biennial exercise that is the largest, most comprehensive government-led, full-scale cyber incident exercise. The biennial exercise includes participants from across the federal government, state and local governments, private sector, and international partners to simulate a response to a large-scale, coordinated, significant cyber incident impacting the Nation's critical infrastructure. Lessons learned from this year's exercise will help inform CISA's next update to the National Cyber Incident Response Plan. CISA also significantly expands the reach of its exercise resources by offering a wide portfolio of downloadable tabletop exercise packages that serve as an off-the-shelf solution for stakeholders' exercise needs.

To obtain even greater awareness of cyber threats targeting critical infrastructure, CISA receives cyber reports, including from other federal agencies. For example, through security directives and regulations, the Transportation Security Administration and the U.S. Coast Guard have implemented mandatory cyber incident reporting requirements for certain critical infrastructure entities, which either direct or encourage incident reporting through CISA. For incidents potentially compromising the confidentiality, integrity, or availability of an information system of a federal agency, those agencies are required to report it to CISA within one hour.

CISA has cyber hunt and incident response teams and other capabilities to respond to cyber incidents impacting federal and non-federal entities upon request. Under *Presidential Policy Directive-41, United States Cyber Incident Coordination*, CISA is the lead federal agency for asset response activities during a significant cyber incident. Asset response includes furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents; identifying other entities that may be at risk and assessing their risk to the same or similar vulnerabilities; assessing potential risks to the sector or region, including potential cascading effects, and developing courses of action to mitigate these risks; facilitating information sharing and operational coordination with threat response; and providing guidance on how best to utilize federal resources and capabilities in a timely, effective manner to speed recovery.

Further, upon declaration by the Secretary of Homeland Security of a significant cyber incident under the Cyber Response and Recovery Act (CRRRA), CISA has access to additional resources that can be used for surging incident response and evicting adversaries from U.S. critical infrastructure via the Cyber Response and Recovery Fund (CRRF).

To assist with the security and modernization of legacy IT systems, CISA helps coordinate the disclosure of vulnerabilities, and distributes advisories and guidance to help critical infrastructure entities mitigate risks related to legacy IT systems. CISA is aware of legacy IT systems in critical infrastructure sectors, particularly those sectors that are resource poor but target rich, such as the education, water and wastewater management, and healthcare sectors. We have worked closely with our partners in the Department of Education, Environmental Protection Agency, and the Department of Health and Human Services to provide


a variety of resources and toolkits to improve those respective sectors' cybersecurity.¹ Congress also provided funding for the State and Local Cybersecurity Grant Program, which those governments can use to improve the cybersecurity of publicly owned critical infrastructure.

Regarding your interest in the January 30, 2024, Government Accountability Office (GAO) report,² the Department concurred with the four recommendations directed to it. CISA provides ransomware support to all sectors and is also working proactively to identify, notify, and help mitigate vulnerabilities related to ransomware attacks. CISA is working to expand the use of its cross-sector Cybersecurity Performance Goals (CPGs) by measuring cross-sector implementation and improving products and services based on stakeholder feedback.

The CPGs, which were released in October 2022, are voluntary practices that outline the highest-priority baseline measures business and critical infrastructure owners of all sizes can take to protect themselves against cyber threats, including ransomware. CISA is measuring implementation of two CPGs across participating entities and will utilize both internal and commercially sourced data to measure an additional fifteen CPGs, including those that reduce the risk of ransomware. These measures will identify the extent to which sectors, including the critical manufacturing and transportation systems sectors, are adopting the CPGs. Since the release of the CPGs, CISA has remained committed to receiving stakeholder feedback and updating the CPGs as appropriate. Presently, CISA obtains feedback through a stakeholder engagement survey and the public CPG Discussions webpage. CISA also plans to track and measure effectiveness of CISA products in helping reduce the risk of ransomware to the critical manufacturing and transportation systems sectors. CISA will formally update Congressional requesters and the Office of Management and Budget on the response to each recommendation within 180 days of the final report's issuance as required.

Thank you again for your letter. Should you have any additional questions, please have your staff contact CISA's Office of Legislative Affairs at CISA_OLA@cisa.dhs.gov.

Sincerely,

A handwritten signature in black ink, appearing to read 'Jen Easterly', with a stylized, cursive script.

Jen Easterly
Director

¹ <https://www.cisa.gov/K12Cybersecurity>; <https://www.hhs.gov/about/news/2023/10/25/cisa-hhs-release-collaborative-cybersecurity-healthcare-toolkit.html>; <https://www.cisa.gov/news-events/news/cisa-fbi-and-epa-release-incident-response-guide-water-and-wastewater-systems-sector>.

² GAO, GAO-24-106220, *Critical Infrastructure Protection: Agencies Need to Enhance Oversight of Ransomware Practices and Assess Federal Support* (Jan. 30, 2024), <https://www.gao.gov/assets/d24106221.pdf>.