September 12, 2022

**RE: Request for Information (RFI) on the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), Docket ID: CISA-2022-0010, Sept. 12, 2022.**

To whom it may concern: In response to the RFI issued by CISA about CIRCIA rulemaking, I write to make the following suggestions:

- **Define 'covered entity' with reference to National Critical Functions developed by CISA/DHS**: CIRCIA cyber incident and ransomware reporting requirements apply to covered entities in 16 key critical infrastructure sectors. However, rulemaking must more specifically define these entities for the purposes of these reporting requirements. CISA and DHS previously have noted key dependencies and interdependencies among critical infrastructure sectors. For instance in a 2014 report, DHS identified significant dependencies of the health care and public health sector on "Chemical, Communications, Energy, Information Technology, Nuclear, Transportation Systems, and Water & Wastewater" sectors and interdependencies with Emergency Services, Food and Agriculture.[1] The importance of these other sectors to health care has been reflected recently in Jackson, MS, where past water problems impacted hospital functioning and one major hospital recently was impacted by loss of water pressure as part of a water outage affecting much of the city.[2] Likewise, two hospitals in California lost backup power during the recent 'record breaking' heat wave, showing the importance of continued attention to utilities and backup power.[3]

  One way to define covered entity for CIRCIA purposes is to reference these 55 National Critical Functions developed by CISA.[4] Critical functions include activities "so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." These critical functions are divided by CISA into four categories: connect; distribute; manage; supply. Supply functions include providing housing and supplying water. Manage functions include providing medical care and supporting community health. Distribute functions include transporting passengers and cargo by air or vessel. Connect functions include providing wireless and radio. GAO states that CISA is updating this list and using it to identify systems in each area.[5] CISA is committed according to its 2021 status letter to aligning "broader CISA programs" with this framework and has developed some materials on cyber risks (see wastewater and supply water infographics). Specifically referencing the NCFs or these functions in the definition of covered entity for the 16 key infrastructure sectors would help achieve this goal.

- **Develop a reporting template and sample reports (including a PDF/Word version for offline use) and note in rulemaking specific elements required for reporting**: CIRCIA specifies elements that should be reporting when a covered cyber incident occurs such as the date(s) of the event, its impact, the actor believed to be responsible, security defenses that were in place and

[1] Sector Risk Snapshots - Homeland Security Digital Library, 2014, https://www.hsdl.org/?abstract&did=754033

[2] https://www.clarionledger.com/story/news/2022/08/31/2010-water-crisis-sparked-jackson-hospitals-to-take-action/65466395007/; https://mississippitoday.org/2022/08/30/jackson-water-failure-impacts-ability-of-states-largest-hospital-to-fight-fires/; https://www.washingtonpost.com/nation/2022/09/03/jackson-mississippi-water-crisis/; https://www.modernhealthcare.com/providers/water-shortages-threatening-patient-safety

[3] https://www.fiercehealthcare.com/providers/backup-generators-fail-northern-california-hospital-during-record-breaking-heatwave

[4] https://www.cisa.gov/national-critical-functions

[5] CISA Should Improve Priority Setting, Stakeholder Involvement, and Threat Information Sharing GAO March 2022, https://www.gao.gov/products/gao-22-104279; Status Update on the National Critical Functions, CISA, Dec. 2021

contact information for the covered entity. Additional information is required for ransomware payment events. However, more specific details will be included in this forthcoming rule and have been noted in recent CISA guidance.[6] As part of this rulemaking or in subsequent guidance or materials, CISA should develop a specific form for reporting to facilitate compliance by covered entities (however that term is defined). Ideally, this form can be standardized with processes and requirements of other federal or private/nonprofit entities so that common elements are being reported across various critical infrastructure sectors. CISA already has strong programs for reporting cyber incidents and information-sharing.[7] However, as the law requires cooperation between CISA and other federal agencies, the form developed should meet their needs as well. CIRCIA is intended to avoid duplicative reporting and a wide range of overlapping reporting requirements apply to various sectors (health care, chemical, etc.).[8] Developing a template form and consolidating CIRCIA reporting requirements with those of other federal agencies and private/nonprofit organizations that may collect similar reports (e.g., internet service vendors, software manufacturers) would be helpful. Additionally, it may be helpful to have a fictionalized/sample report as an example that contains the elements and narrative CISA would like other reporters to submit.

- **Elements for reporting on template/form:** It would be helpful to include on this form or in the regulation a list of critical infrastructure sectors; CISA has asked in its April 2022 guidance for reporters to identify the critical infrastructure sector(s) affected if known. Including a list of the 16 key sectors, 55 national critical functions or similar items with boxes to check could help at least preliminarily to identify key sectors impacted, which will help with follow up and response.
- **Require reporting of past cyber incidents when detected:** Covered cyber incidents under CERCIA must be reported "not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred" or 24 hours after a ransom payment is made. However, in practice it may take months for an organization to recognize that a covered cyber incident has occurred.[9] By that time, though an organization still may be at risk, but the substantial loss of confidentiality, integrity or other damage may already have occurred. A company investigating a data breach or potential hacking, for instance, may realize that a cyber incident occurred in the past, but this attack may no longer be ongoing. The timeline of some high-profile cyber attacks spans up to two years between the attack and eventual recognition and response by affected entities. Accordingly, the CIRCIA regulations should require or at least strongly encourage reporting of past as well as ongoing cyber incidents with 72 hours once they have been detected and recognized as by the covered entity.
- **Emphasize international cooperation**: Though not mentioned by the law, it is also important to note that some level of international cooperation also will be needed; the European Union (EU) and other non-US entities have their own reporting requirements that may impact US companies operating outside the US and foreign companies that own critical US infrastructure. [10]A more standardized and harmonized domestic incident reporting approach can help facilitate such cooperation. Input from the new Cyber Incident Reporting Council also will be helpful.[11] CISA also should consult with the European Union for lessons learned and challenges with its reporting

[6] https://www.cisa.gov/uscert/ncas/current-activity/2022/04/07/guidance-sharing-cyber-incident-information
[7] https://www.cisa.gov/ciscp
[8] By the Numbers: Parsing Cybersecurity Incident and Breach Reporting Requirements, R Street, Sept. 1, 2022, https://www.rstreet.org/2022/09/01/by-the-numbers-parsing-cybersecurity-incident-and-breach-reporting-requirements/; https://www.rapid7.com/blog/post/2022/08/10/navigating-the-evolving-patchwork-of-incident-reporting-requirements/
[9] https://www.semtechit.com/blog/how-long-does-it-take-to-detect-a-cyber-attack/; March 3, 2022 - Health Sector Cyber Security: 2021 Retrospective and 2022 Look Ahead, https://www.hhs.gov/about/agencies/asa/ocio/hc3/products/index.html#sector-alerts; https://www.lepide.com/blog/the-danger-of-delayed-threat-detection-and-how-to-prevent-it/
[10] Committee on Foreign Investment in the United States, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-reports-and-tables
[11] https://www.dhs.gov/news/2022/07/25/readout-inaugural-cyber-incident-reporting-council-meeting

process for cyber incidents and ransomware.[12] For instance, one key gap identified in the EU is technical information in reports as to how attackers breached an entity's systems.[13]

- **Collaborate with FEMA and states**: The Federal Emergency Management Agency (FEMA) and CISA have complementary missions within DHS. As explained by the DHS Office of Inspector General in a recent report on the energy sector, "CISA identifies and prioritizes critical infrastructure, provides technical assistance to critical infrastructure partners, conducts risk assessments of all 16 sectors, and coordinates the Federal response to security-related incidents. FEMA manages and oversees disaster response efforts and provides technical assistance and grant funding opportunities to improve preparedness, response, recovery, and mitigation efforts."[14] FEMA and CISA have collaborated on recent cyber security grant funding opportunities. FEMA can be a key partner with CISA in the education and outreach required by CERCIA, as in some cases cyber incidents and impacts will be related to its mission as well as CISA's. Similarly, some state governments are adopting reporting laws analogous to CERCIA and other government agencies may operate critical infrastructure (e.g. emergency systems, health care institutions, utilities), highlighting the value and importance of federal, state, local, tribal and territorial government collaboration.[15]
- **Include third-party supply chain vendors in reporting requirements**: As highlighted during COVID-19, smaller organizations and other entities perhaps not thought of as being vulnerable to cyberattacks may comprise key nodes in the supply chain for important goods and services.[16] Such vendors and suppliers may be targets for cyber incidents that ultimately paralyze key critical infrastructure services, providers and owners.[17] Accordingly, third-party suppliers and vendors to covered entities and owners/operators of critical infrastructure, even if not themselves covered entities, should be required to report either covered entities or CISA when hey have experienced a significant cyber incident or made a ransomware payment. This will help ensure the downstream supply chain and covered entities can more efficiently adapt to impacts on critical infrastructure.

Thank you for your consideration of these suggestions.

Sincerely,

Mitchell Berger

Note/disclaimer: I am a federal employee. However, the views expressed above are my own and should not be imputed to other individuals or to any public or private entity.

---

[12] https://industrialcyber.co/ransomware/enisa-reports-shortcomings-of-current-reporting-mechanisms-across-eu-in-latest-ransomware-threat-analysis/

[13] https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks

[14] CISA and FEMA Can Improve Coordination Efforts to Ensure Energy Sector Resilience, Sept. 2022, https://www.oig.dhs.gov/; https://www.nga.org/news/commentary/opportunities-for-cybersecurity-investment-in-the-bipartisan-infrastructure-investment-and-jobs-act/; CISA-FEMA Tribal Cybersecurity Grant Program
Framing Paper for Tribal Consultation August 2022

[15] https://www.govtech.com/security/faster-faster-trends-in-u-s-cyber-incident-notification-laws

[16] National Academies of Sciences, Engineering, and Medicine 2022. Building Resilience into the Nation's Medical Product Supply Chains. Washington, DC: The National Academies Press. https://doi.org/10.17226/26420; National Strategy for a Resilient Public Health Supply Chain, July 2021; https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/08/fact-sheet-biden-harris-administration-announces-supply-chain-disruptions-task-force-to-address-short-term-supply-chain-discontinuities/; Enabling a More Resilient and Shared Supply Chain Strategy for the Nation: Lessons Learned from COVID-19, IBM Center for the Business of Government, 2022, https://www.businessofgovernment.org/report/supply-chain-strategy-covid-19; Public Health Supply Chain and Industrial Base One-Year Report In Response to Executive Order 14017 (February 2022) [PDF]
Feb 2022, ASPR, HHS, https://aspr.hhs.gov/MCM/IBx/2022Report/Pages/default.aspx

[17] https://www.mynewsdesk.com/nccgroup/pressreleases/supply-chain-security-risks-are-providing-a-back-door-for-hackers-3174531