Operational Technology Cybersecurity Coalition

November 14, 2022

Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
245 Murray Lane
Washington, D.C. 20528-0380
Submitted via Federal eRulemaking Portal, and via email to circia@cisa.dhs.gov

RE: Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022

CISA CIRCIA Team:

The Operational Technology Cybersecurity Coalition (OT Cyber Coalition) appreciates the opportunity to submit feedback to the Cybersecurity and Infrastructure Security Agency's (CISA) Request for Information (RFI)[1] related to the Notice of Proposed Rulemaking (NPRM) required in the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).

The OT Cyber Coalition is a diverse group of leading cybersecurity vendors dedicated to improving the cybersecurity of OT environments. Representing the entire OT lifecycle, we believe that the strongest, most effective approach to securing our nation's critical infrastructure is one that is open, vendor-neutral, and allows for diverse solutions and information sharing without compromising cybersecurity defenses.

We agree that timely reporting of incidents allows for response, remediation, and mitigation to major cybersecurity incidents by fostering public and private partnership in an effort to "render assistance to victims suffering attacks, analyze incoming reporting across sectors to spot trends and understand how malicious cyber actors are perpetrating their attacks, and quickly share that information with network defenders to warn other potential victims."[2] The collaborative effort in the wake of the Colonial Pipeline ransomware attack in May 2021 is just one example of how this approach can work.

Finally, we note that on November 7, 2022, President Biden announced the intent to launch a process to review and revise Presidential Policy Directive 21 (PPD-21),[3] which is the primary

[1] Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, Notice of public listening sessions; Cybersecurity Incentives, 87 FR 55830 (September 12, 2022) https://www.federalregister.gov/documents/2022/09/12/2022-19550/cyber-incident-reporting-for-critical-infrastructure-act-of-2022-listening-sessions
[2] Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, Notice of public listening sessions; Cybersecurity Incentives, 87 FR 55831 (September 12, 2022) https://www.federalregister.gov/documents/2022/09/12/2022-19550/cyber-incident-reporting-for-critical-infrastructure-act-of-2022-listening-sessions
[3] Biden, Joseph R. "Letter from the President to Select Congressional Leadership on the Nation's Critical Infrastructure." *The White House*, 7 November 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/07/letter-from-the-president-to-select-congressional-leadership-on-the-nations-critical-infrastructure/

U.S. policy document on critical infrastructure. This is noteworthy because the CIRCIA definition of covered entity invokes PPD-21 as the foundation for defining a covered entity for purposes of incident reporting (Sec. 2240(5)). We agree that CISA should undertake a thorough prioritization process as it relates to both CIRCIA and PPD-21, and we offer our assistance, insight, and expertise as the review progresses.

As CISA works to develop its NPRM related to CIRCIA, we hope you will keep some key issues in mind.

Third-Party Security Vendors Should Not Be Required to Report Incidents Impacting Covered Entity Customers

The NPRM should make clear that third-party security vendors will not be required to report incidents that are targeted at the customers they have been hired to protect. This could lead to significant duplication in reporting and would significantly damage the relationship that security vendors have with their customers, creating a lack of trust between the parties. As industrial control systems (ICS) and OT cybersecurity vendors, we view Congress's decision not to include that language in its final bill as a clear Congressional intent that third-party security vendors should not be required to report incidents that they are aware are impacting covered entities, if the incident is not impacting the third-party security vendor's network or systems.

However, we do not oppose allowing third-party cybersecurity vendors to report on behalf of their customers so long as that arrangement is agreed to between the vendor and the customer and the NPRM makes clear that CISA 2015 protections also apply to this transmission of data.

Attributes of Effective Government Threat Reporting

Our combined customer base represents the largest and most impactful organizations in critical infrastructure. As a community, we are able to collect asset information, vulnerability data, threats, and security incidents, and share it as part of the collective defense mission. Cybersecurity is a team sport, and we cannot combat cyber threats effectively if we don't have better data about attacks. We support this effort to develop a comprehensive public/private partnership with effective, timely, and bidirectional flows of information.

However, the private sector will only benefit if the information and analysis coming out of CISA help us share protective actions with our clients, including information collected by the United States Intelligence Community. Therefore, we recommend at a minimum that threat reporting coming out of CISA include all available verified details on:

- The specific vulnerabilities that were exploited;
- The assets that were targeted;
- The impact to the safety, reliability, or availability of a critical infrastructure asset or to the confidentiality, integrity, or availability of data;
- Recommendations for capabilities to protect against similar types of attacks; and
- Attack path analysis.

Technology- and Vendor-Neutral Reporting Mechanism

As CISA develops its mechanism for reporting cyber incidents, it is important that CISA ensure that the technology utilized for reporting remains technology- and vendor-neutral. Not only do

proprietary solutions create vendor lock-in, but they also create barriers that could make it challenging for covered entities to report covered incidents in the timeline provided under CIRCIA. Incident reporting to CISA should be as simple as possible and allow covered entities to report incidents efficiently, using any mechanism that is easy for the entity to use and is compliant with CISA's final approach, without having to purchase or contract for third-party solutions.

Real-Time Monitoring

Finally, we encourage CISA to incentivize, but not require, covered entities to adopt cybersecurity solutions that can enable real-time monitoring and analysis. These monitoring solutions should not only be standards-based and interoperable with the diverse infrastructure deployed by covered entities, but also interoperable with CISA's reporting mechanism to ensure that threat information can be shared seamlessly. Real-time solutions can help track network activity, improve network security, and identify anomalous activity. We understand that the costs of real-time monitoring solutions can be prohibitive for smaller entities, but it is the larger entities that often pose the greatest risk to national security if they are breached or taken offline. Incentivizing them to adopt real-time monitoring, as well as prioritizing the most critical factors, will help increase our collective security.

Again, the OT Cyber Coalition thanks CISA for the opportunity to provide feedback that should inform the important work your organization is undertaking to protect all of our nation's ICS and OT environments, not just those involved with critical infrastructure sectors. We welcome questions on our feedback and look forward to continuing to be a part of this discussion as it develops.

Sincerely,

Andrew Howell
Operational Technology Cybersecurity Coalition
andrew@otcybercoalition.org
https://www.otcybercoalition.org