



IT-ISAC Comments in Response to CISA Cyber Incident Reporting RFI

November 14, 2022

The Information Technology-Information Sharing and Analysis Center appreciates the opportunity to provide the following comments in response to the [Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022](#), which was issued on September 12, 2022. With over 20 years' experience in facilitating information sharing, the IT-ISAC understands the value of collaboration, partnership and cyber threat intelligence sharing to help manage the ever-expanding range of cyber threats.

To begin, we would like to emphasize the importance of developing and implementing regulations that do not further strain security resources. Private enterprise operates in an environment of finite resources such as talent and money. Resources that are devoted to ensuring compliance with mandatory reporting requirements are resources that are not available to actively mitigate or respond to an incident.

Because of this reality, it is important that victim companies understand the final regulations so they can easily comply with them. To enable this compliance, the final regulation must be clear on who needs to report an incident, when a victim company needs to report an incident, and what they need to report. As such, we plan to focus our comments on the following topics:

- Defining a Covered Entity
- Defining a Covered Cyber Incident
- How Submissions are made

Defining a “Covered Entity”

For obvious reasons, it is not practical to require every critical infrastructure company to report every cyber incident. Therefore, it is important to provide clarity to both industry and government as to who is required to report an incident and under what circumstances. However, defining these requirements and obligations are difficult without a clearer understanding as to what the purpose of the reporting requirements are and how CISA will use the information that is reported to it.

For example, if the purpose of reporting an incident to CISA is to help it understand threats to the National Critical Functions, then reporting requirements could be limited to companies, or a subset of companies, who provide those functions. However, if the goal is different, then this would change who would be required to report.

There remains much confusion in the community as to the actual purpose of the reporting requirements, how the information will be used, and how and when it will be shared across agencies. Once this is better understood, it could be easier to define covered entities. The use case will help inform the requirements. CISA should establish clearly defined objectives for the program to better define the reporting requirements aligned to those objectives.

Defining Covered Cyber Incident

Collectively, critical infrastructure owners and operators block countless attacks daily. They also investigate a substantial number of anomalies that turn out to not be successful attacks. Not every cyber event is a cyber incident. But even requiring every cyber incident be reported to CISA will likely overwhelm CISA and result in noise. This will quickly drain resources and make substantive analysis difficult.

Therefore, we suggest that covered cyber incidents should be limited to those that have a substantive, severe, or meaningful impact on a victim entities' operations, or its ability to provide critical services to critical infrastructure customers. A covered cyber incident should be limited to those that cause disruptions in operations or services. Such incidents are most relevant to CISA's role as the National Risk Manager and would be of significant interest to other critical infrastructure owners and operators.

Focusing on the incident's impact on critical infrastructure might also provide a path to defining the term "covered entity." For example, if the goal of the program is to manage risks and disruptions to critical infrastructure, CISA could define "covered entities" based on the products or services companies provide to critical infrastructure. In this way, a covered entity is not determined by its size, but by the criticality of the products or services it provides to other critical infrastructure.

Additionally, we caution against categorizing known vulnerabilities as a cyber incident. A vulnerability that is exploited can lead to a cyber incident, but the mere existence of a vulnerability should not be considered a cyber incident. We also encourage the continued use of coordinated disclosure of vulnerabilities. To the extent possible, a vulnerability disclosure should be limited to widely accepted best practices around responsible disclosure.

How Submissions are Made

To balance the requirements to report with the need to resolve an incident, the process of submitting reports should be as simple as possible. There should be multiple options for submitting the information such as a secure web interface, secure email, and use of STIX/TAXII and other automation tools. It is important that organizations have the option to automate submissions through an API. The information required for the incident submission should be detailed enough to provide CISA with situational awareness without providing an undue burden to the submitting organization.

In the first 72 hours of an incident, information gained from the early stages of an investigation may not always be technically accurate. Incident analysis changes as more information about an incident is discovered. Further, it will take multiple hours for an incident report to be developed and reviewed internally before being submitted to CISA. By the time the report is submitted, it is possible that the victim company may have additional or conflicting information. As such, CISA should provide a process for victim companies to update their initial report with updated information without penalty. This should also be available via API or some automatable mechanism.

The most important elements of incident reporting include:

- How the organization identified the attack
- What weakness or vulnerabilities the attacker exploited
- The indicators of impact
- How the attack can be mitigated
- What are the impacts of the attack

The above information should provide CISA with enough information to understand the potential severity of a reported incident, as well as technical indicators it can use to help protect others. However, since not all information may be available when organizations are required to report an incident, organizations should only be required to submit what is known to them at the time they prepare the report.


We also encourage CISA to establish a flexible reporting framework. For example, CISA could:

- Minimize reporting burdens by mapping to existing mandatory, existing national, or international reporting requirements
- Create a framework for intra-governmental reporting so that submitting a required incident report to one government agency is shared with CISA, so a victim company does not need to submit multiple reports to multiple government organizations on the same incident
- Establish rules that declare that reporting a cyber incident to the FBI fulfills the victim organization's reporting requirements and institutes methods for sharing between the FBI and CISA
- Engage with Information Sharing and Analysis Centers to ensure a timely dissemination of attack Tactics Techniques and Procedures (TTPs) from CISA to support prevention and detection activities across the industry
- Limit the number of mandatory reporting elements to only what is necessary to achieve program objectives

In terms of third-party reporting, the company that experienced the incident is the proper authority to report the incident. Third parties who manage networks or who provide incident response and investigation services should not be responsible for reporting incidents on client networks. Instead, the victim company should be the party responsible for reporting. However, the victim company should have the option to leverage a third party, such as a service provider, to report an incident.

We very much appreciate the opportunity to provide these comments. We understand that this is the first step in creating the regulations and look forward to working with CISA throughout this process.

Sincerely,



Scott C. Algeier

Executive Director, IT-ISAC