The MITRE Corporation appreciates the opportunity to comment on the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), and its associated incident response and ransomware reporting requirements. The below comments are informed by MITRE's history developing cybersecurity standards and tools, directly addressing advanced persistent threats, and serving as a trusted cybersecurity advisor to many government and industry partners as an operator of federally funded research and development centers (FFRDCs). They are also informed by MITRE's experience managing the security of our internal networks as a member of the Defense Industrial Base (DIB) critical infrastructure sector. Below please find responses to six areas of interest in the RFI with associated general observations and implications for consideration. These observations and implications are not intended to cover all areas of interest in the Request for Information (RFI).

- **Area of RFI Interest: Conditions That Lead to Reasonable Belief That a Covered Incident Has Occurred**
  - **Observation**: There is often high variability between the time an adversary begins exploiting a network to the time when that exploitation is detected. Additionally, there is often a great deal of uncertainty in the early stages of observed anomalous behavior about whether such behavior rises to the level of an incident. This early stage, when analysts are determining and confirming an incident, is one of the most challenging times for security operations, especially when the activity has not been seen before. Yet, it is often less supported and discussed across security operations than post-detection activity.
  - **Implication:** CIRCIA reporting requirements should be focused on, and triggered by, determination that a covered incident has occurred. However, the ability to determine that a covered incident has occurred in the first place could be enhanced with support for operational approaches that enable cross-organizational "pre-CIRCIA" early-stage incident discovery. Such approaches create a "safe place" for on-line collaboration, where:
    - analysts can work in trusted environments that are easy to access and use, yet secure
    - analysts are trusted and vetted
    - Rules are in place to separate reporting from collaborating to protect collaborator and data within the environment. This provides confidence that data will not be used for official reporting.

    This is analogous to working "in the trenches" together, where analysts across security operations centers can compare notes and determine the nature of an event, and when it rises to an incident. This can promote earlier warning, as analysts become confident of an incident sooner than in current conditions. Also, operators working together are more likely to find the widespread activity when comparing notes. Whether or not government agencies, support, contribute to, or participate in these types of arrangements, requirements should clarify that "pre-

CIRCIA" collaboration mechanisms are not part of the mandatory reporting requirements under CIRCA. This would minimize any potential legal or other reporting implications resulting from this type of collaboration. CISA may want to consider a model similar to the FAA's Aviation Safety Reporting System (ASRS) where early voluntary reporting can count toward compliance requirements should they become necessary.

- **Area of RFI Interest: General Uses of Information Reported (Additional Policies, Procedures, and Requirements)**
  - **General Observation:** There are several possible uses for cyber incident information. Such uses include:
    - Aiding asset response, and preventing imminent harm, associated with impact to a specific organization
    - Supporting the early identification of systemic adversary activity or campaigns of activity against US interests impacting multiple parties
    - Information sharing with other federal, industry, and state, local, tribal, and territorial (SLTT) partners to inform cyber defenses
    - Law enforcement investigation/prosecution
    - Informing other actions by the United States Government

    Regardless of purpose, if reporting results in certain forms of public disclosure before an incident is contained, mitigation(s) to an exploited vulnerability are identified, and/or a ransomware negotiation and recovery hasn't been completed, it could prompt attackers to take more aggressive or destructive actions.

  - **Implications:** Given CISA's mandates, information requirements that support asset response, early identification of adversary activity, and information sharing priorities should be prioritized and the required information focused on that which supports those use cases. This will ease the burden both on the submitting organization and on CISA and will help to focus activity key elements that provide the most utility. One way to strengthen the overall effectiveness of this effort is to describe how CISA will utilize information that is received (i.e., an operational model). This would communicate and demonstrate to the community the benefits and value of this effort as well as help to explain why the information is being requested. Some areas that an operational model could address include:
    - How analysts could collaborate in an earlier discovery phase outside of the CIRICA requirements (see above)
    - How information shared with the government will be publicly shared in a way that would allow other potentially impacted entities to act, without compromising information that should not yet be publicly disclosed
    - The types of support or services that a victim organization could expect to receive from federal organizations

- Delineating how information will be shared and used by different federal organizations with different missions (e.g., CISA and the FBI)
- How organizations will receive an acknowledgement that their information was received; and
- How shared information will be protected

An operational model that addressed these types of issues could help stakeholders understand how specific situations might be handled. For example, if a victim organization is in negotiations with cyber criminals during a ransomware incident, what will be the implications of information being shared with law enforcement?

Recognizing that entities may have other federal reporting requirements, it will be important to deconflict new reporting requirements with complementary channels/processes for reporting information that inform other federal reporting requirements. And, as it takes resources to support reporting and those same resources are likely to be helping address the response itself, the U.S. government should pursue the goal of having victim organizations share information with one government agency, which can then share with other government agencies as appropriate.

- **Areas of RFI Interest: Timing Around Information Reporting During First 72 hours and Post-72 hours After Reasonable Belief Has Been Established and Specific Information Types Required**
  - **General observation**: For a variety of reasons what is known and knowable about any potential incident will vary and evolve over time. And, based on organizational capabilities, not all potentially impacted organizations will have the ability to consistently gather and report on all desired information elements (e.g., specific vulnerability exploited, adversary tactics, techniques, and procedures).
  - **Implications.** Most information will not be available within 72 hours of incident identification and, based on the nature of the incident and capabilities of the impacted organization, some may never be known. Regarding the first 72-hours, initial reporting requirements should focus on a minimal set of data points that reflects a victim organization's reasonable understanding at the time, for example:
    - Organizational contact information,
    - General description of what occurred
    - Initial description of the harm/damage that resulted and
    - Associated efforts to contain/eradicate/recover from the incident.

    This type of initial reporting could help inform alerts to other potentially impacted organizations and trigger other response activities such as the stand-up of stand-up of a Unified Command Group (UCG). Initial reporting can also help clarify and prioritize what other information would be relevant. Additional reporting can then be tailored to the specific circumstances of the incident. Past the first 72 hours, information will be reported in an ongoing and evolving manner, and depending on how novel the attack is, it could take weeks or months for some information to be known and reported. To these ends, final requirements can clarify the expectation about what is reasonable to expect when, and how reporting can be tailored to the specifics of the incident. Requirements could also encourage victim organizations to also share indicators of compromise (IOC), if known. If shared more broadly, these IOCs could help other potentially impacted organizations determine if they have been affected.

- **Area of RFI Interest: Applications and Tools to Support Information Sharing**
  - **General Observation:** Depending on the nature of the incident, different organizations will use different applications, naming conventions, and tools to support information sharing. It is also possible that the underlying systems that organizations use to share that information may themselves be compromised.

  - **Implication:** Especially in the early stages of information reporting, it should be as easy as possible to report information, recognizing that reporting systems may be compromised, and/or some organizations have more limited capabilities to report information. Capabilities that enable comparative ease of reporting include: the ability to phone directly, a basic web application, and an instant messaging application. Requirements should clarify how these types of capabilities will be provided/accessed. To the extent that applications and tools are used, they should be informed by common taxonomies and definitions (e.g., STIX/TAXII, NIEM for cyber incidents, Vocabulary for Event Recording and Incident Sharing (VERIS), MITRE Adversarial Tactics, Techniques, and Common Knowledge ATT&CK®, and CVE for publicly disclosed vulnerabilities.) The use of widely-accepted taxonomies will enhance the ability to effectively share across organizations.

- **Area of RFI Interest: Timing, Manner, Standards for Sharing Vulnerability Information**
  - **General Observation:** A common standard (i.e., CVE) exists for identifying, defining, and cataloguing publicly disclosed cybersecurity vulnerabilities. However, a specific incident may involve the exploitation of a previously unknown or undisclosed vulnerability, where patches or mitigations haven't been identified.

  - **Implication:** Understanding whether a vulnerability has been previously known/publicly disclosed will drive the timing, manner, and standards for how information should be shared. In situations where a vulnerability has been previously published with a CVE record, the victim organization should use the associated CVE ID number to communicate the vulnerability, as well as communicating this to CISA. In cases, where a vulnerability that hasn't been previously identified or disclosed, the victim organization should engage the vendor about the vulnerability and CISA to communicate what is known, as part of CISA's coordinated vulnerability disclosure process. That process should dictate when responsible public disclosure of the vulnerability should take place. Common Weakness Enumeration (CWE) is an enumerated list of community identified software and hardware weaknesses. To the extent that victim organizations, government agencies, and/or vendors identify hardware and/or software weaknesses as part of the incident response process, CWE can be used to communicate weaknesses.

- **Area of Interest: Information Retention and Preservation Requirements**
    - **General Observation:** There is a large amount of potential information that could be retained and preserved after any incident. Depending on specific reporting requirements, it could be time consuming for victims to provide this information. To the extent that forensic images are preserved and shared, they could also include sensitive data that is not relevant to the incident itself.
    - **Implication:** Retention and preservation requirements should be focused on provision of the information that is directly relevant for supporting incident response and information sharing missions, and, similar to responses above, should be tailored based on the specifics of the incident. Additionally, requirements should clarify how this retained information would be shared, protected, and handled in cases where preserved information is held by multiple potential information recipients.