November 14, 2022

Director Jen M. Easterly
Cybersecurity and Infrastructure Security Agency (CISA)
U.S. Department of Homeland Security

RE: Comments in response to CISA Request for Information on the "Cyber Incident Reporting for Critical Infrastructure Act of 2022" (Docket Id.: CISA 2022-0010)

Palo Alto Networks appreciates the opportunity to provide comments in response to the Cybersecurity and Infrastructure Agency's (CISA) Request for Information (RFI), *Cyber Incident Reporting for Critical Infrastructure Act of 2022*.

Palo Alto Networks is the global cybersecurity leader, securing the networks and information of more than 85,000 enterprise and government customers in 150+ countries to protect billions of people globally. 95% of the Fortune 100 and more than 71% of the Global 2000 rely on us to improve their cybersecurity posture. We work with some of the world's largest organizations across all industry verticals, including U.S. critical infrastructure (CI) sectors.

Palo Alto Networks has long valued our partnerships with CISA, and takes pride in our various initiatives to facilitate timely and efficient cybersecurity threat information sharing with our Federal Government partners. Palo Alto Networks is one of nine founding members of the Joint Cyber Defense Collaborative (JCDC), the U.S. government's primary forum for bringing together the public and private sectors to coordinate defensive actions and drive down risk in advance of cyber incidents occurring. Through the JCDC and other collaborative forums, we assisted with the public-private planning and response to significant national cyber incidents such as SolarWinds, Microsoft Exchange and Log4j. In February of 2022, a Palo Alto Networks executive and Senior Vice President was appointed an inaugural member of the Cyber Safety Review Board (CSRB), one of the U.S. government's primary forums for recommending proposals that drive improvements to incident response across the public and private sector to advance national cybersecurity. Additionally, we are founding members of the Cyber Threat Alliance, the cybersecurity community's first automated cyber threat information sharing organization, now comprised of over 30 of the world's leading cybersecurity providers.

Palo Alto Networks supports CISA's efforts in implementing the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), and we welcome the opportunity to contribute ideas and principles to the final rule. As demonstrated by the bipartisan consensus in passing CIRCIA into law, there is recognition that the dynamic nature of the cyber threat environment is best addressed through close collaboration between the public and private sectors, including in areas like incident reporting. As we move towards implementation, we recognize CIRCIA and other reporting regimes' aim to increase cybersecurity resilience, but urge that the rules be crafted in a manner that both enhances operational efficacy while considering implementation feasibility for the entities they cover. Entities' incident response (IR) teams must be able to dedicate the requisite time and resources to identifying and containing incidents as quickly as possible to prevent and/or minimize damage. Further, industry-leading IR plans and procedures require proper identification and analysis of incidents prior to communicating externally in order to provide relevant stakeholders and users with actionable information.

GENERAL COMMENTS

At the outset and at a strategic level, there are three central principles we believe should be considered in working towards a final rule.

1. Ensure the rule's outcome focuses on demonstrably improving security: The impact of this law, and implementing rule, should ultimately be assessed by how information from these reported cyber incidents is analyzed, enriched, and disseminated - ideally in a de-identified or anonymized manner - to bolster the security of the broader cyber ecosystem. To this end, we suggest the final rule include two things: 1) uniform and consistent reporting forms, supported by programmatic reporting capabilities, that enable CISA to quickly and efficiently operationalize data and re-disseminate to industry in unattributed reporting; and 2) selecting reporting elements that would give CISA the ability to provide some reciprocal benefit to the impacted party or broader cyber ecosystem, for example by requesting specific threat actor identifiers, tactics, techniques or procedures, while scoping out victim identifiers/observables. Both elements would help ensure that reported incident information is used to develop actionable intelligence that is rapidly pushed out to protect entities in real-time and not simply compiled in periodic retroactive threat reports. The notional objective of this reporting requirement should be directed toward supplying critical information, in real-time, to empower frontline cyber defenders to stop attacks, and clarifying that notional goal will help address many tactical aspects of the final rule.

2. Address Protections for Reported Data: Language in CIRCIA rightfully includes digital security requirements for the collection, storage, and protection of reports submitted to CISA, in accordance with the requirements of moderate impact federal information systems as defined by FIPS 199. However, we are still less than two years removed from SolarWinds - where Russian intelligence had at least nine months of persistent access to the information systems of nine federal agencies. While substantial federal network security progress has been made since then, buoyed by the Executive Order on Improving the Nation's Cybersecurity, the inherent sensitivity of cyber incident reports demands maximum vigilance, for at least two reasons. First, a repository of incident reports from critical infrastructure companies across the United States may itself be a valuable target for cyber adversaries. Second, without adequate protections, the unintended publication of these reports could cause additional security, reputational, regulatory and potentially financial damage to reporting organizations which had expected this information to remain confidential. CISA should include in its final rule information about what protections are applied to reports that come from covered entities.

3. Harmonize with Similar Reporting Regimes Globally: In addition to the implementation of this law, many private sector companies are, or will concurrently be covered by other cyber incident reporting regimes, both domestically and internationally.[1] As a result, varying breach

[1] For example, in March 2022, the United States Securities and Exchange Commission (SEC) published a proposed rule that would update reporting requirements for cyber incidents, and the Federal Acquisition Regulatory Council is expected to move forward with rulemaking for the reporting of cyber incidents by federal contractors.

determination procedures and the accompanying compliance activities are becoming resource intensive for many organizations, and consuming critical bandwidth from essential incident responders. Without clarity on how these distinct, but thematically similar regimes logically interact, and an effort by CISA to minimize any differences between these regimes and CIRCIA, compliance could continue to spiral into a truly undue burden for cybersecurity's first responders - the Information Security teams that focus on incident prevention, response and remediation. Recognizing that shared cybersecurity goals are ultimately undermined if entity-level incident response procedures are unduly disruptive, incident reporting regimes should strive for reciprocity, avoiding duplicative reports to multiple agencies or governments, and complementary with existing incident response best practices utilized by industry. Further, this harmonization should be scoped broadly to help multinational companies and organizations navigate concurrent regulatory obligations, especially with respect to data privacy and the protection of personal information.

In response to some areas of questions contained in the CIRCIA RFI, Palo Alto Networks offers the following proposals and recommendations.

THRESHOLD DEFINITIONS

Definition of a 'Covered Cyber Incident' to Be Reported

CIRCIA currently defines reportable incidents as those "that lead to the substantial loss or compromise of the confidentiality, integrity, or availability of the data or business operations, or an impact on the safety or resiliency of operational systems or processes." We would suggest CISA's rule further refine the scope to exclude unintentional disruptions and/or accidental outages, and focus on incidents where there is an actual loss of confidentiality, integrity or availability of networks or systems. Here again, such scoping would help ensure the reporting requirement is geared toward providing reciprocal benefits to the reporting entity or broader cyber ecosystem.

The threshold for reporting requirements should be mapped to specific criteria and specific incident severity levels related to identifiable harms. Many incidents may end up being benign and there is little to no value in reporting unless there are attributes of the incident that further national security or the security of the private sector. Reporting requirements should only focus on severe and significant attacks that cause actual disruption or loss of confidentiality, integrity or availability, and should include specific parameters to facilitate reciprocal benefits of the reporting requirement to the entity or broader ecosystem. Focused reporting that is limited to significant incidents reduces the burden on information security teams and frees resources for the essential tasks of examining and remediating incidents and securing the organization's systems. Moreover, it reduces the likelihood of information overload for government partners that would undermine their ability to prioritize responses and divert limited agency resources from critical risk mitigation activities.

Internationally, Australia and the EU both finalized new incident reporting requirements in the past year, and the UK is in the process of updating its own requirements.

Clearly Limit Covered Cyber Incident Threshold to Confirmed Incidents
Incident reporting requirements should be limited to confirmed incidents with a tangible national security impact. CIRCIA's language concurrently scopes cyber incidents to exclude incidents that "imminently, but not actually, jeopardize[] information or information systems" while asking industry to report when they "reasonably believe[]" an incident has occurred. CISA's final rule should clarify that reporting is limited to incidents that *have been confirmed* to lead to the substantial loss or compromise of the confidentiality, integrity, or availability of the data or business operations. It is essential the rule gives organizations the ability to rely on evidence of an *actual* loss or compromise of confidentiality, integrity or availability, for reasons we explain below.

Without further clarification, subjective standards like "reasonably believes," without evidentiary thresholds, can be difficult for an entity to operationalize and could lead to disparate reporting standards across sectors and organizations. In addition, today's leading cybersecurity capabilities leverage machine learning and automation to block cyberattacks in real-time; given the frequency of automated cyberattacks, a somewhat subjective definition could potentially translate to innumerable "near misses" for entities each day. A requirement to report incidents where there is evidence of an actual loss to system functionality would avoid the reporting of near misses, and would do more to improve the security of the whole ecosystem by allowing CISA to triage and address the most substantial incidents. Further, subjective or ambiguous thresholds will unnecessarily burden covered entities who will likely err on the side of overreporting, diverting information security teams' attention and limited security resources away from the essential tasks of actually examining and remediating incidents and securing their systems. It also will likely result in CISA being overwhelmed by receiving thousands of reports (if not more) per day, particularly if there is uncertainty among covered entities of their obligations to report something that ultimately has no suspected or actual impact on an organization's network or systems. This information overload will 1) prevent CISA from prioritizing actual, confirmed incidents, and undertaking appropriate responses and 2) undermine CISA's ability to provide timely and actionable information and advice to entities that are facing real incidents. In contrast, reporting incidents where organizations have evidence of compromise will help to avoid unnecessary overreporting that will strain limited incident response capacity and capabilities inside and outside the government. It will also help ensure that information received is both useful and actionable.

Guidelines or Procedures for Third-Party Submitters
CIRCIA envisions a scenario where third-party incident response firms can assist with submissions of reports for covered cyber incidents on behalf of covered entities. This allowance is sensible, and in many cases preferable, for covered entities as third-party incident response firms are often best positioned to compile the requisite analysis that underpins elements of cyber incident reporting. However, CIRCIA rulemaking would benefit from clarifying that third-party firms will never be *required* to submit reports on behalf of clients, and would only be able to do so when that client has expressly enlisted them to submit such a report. It should be further clarified that the ultimate responsibility to submit cyber incident reports rests with the covered entity, whether that entity choses to do so on its own or via a third-party.

HOW INCIDENT INFORMATION SHOULD BE REPORTED

The protocols and mechanisms of reporting an incident should avoid duplicative reporting obligations and be consistent with existing frameworks, recognized sectoral, international, and industry best practices, much like the Incident Reporting System already used by CISA. Here again, the inclusion of reporting elements, like threat actor identifiers or tactics, techniques or procedures–without victim identifiers/observables–would allow CISA to provide reciprocal benefit to the impacted party or broader cyber ecosystem. Two specific recommendations on this topic are below.

Develop an Appropriate and Flexible Reporting Template

Incident reports should follow a standardized template to ensure consistent reporting. In developing a standard template, CISA should ensure consistency with existing frameworks, like MITRE ATT&CK[2] and/or VERIS[3]. The rule should also consider international industry best practices, and ensure that the template fits the needs and existing practices of a particular sector. Reporting entities can use such a template to report the most relevant information where available. By way of example, the template should include appropriate and reasonably obtained information (if known) on 1) the attack vector or vectors that led to the compromise; 2) tactics or techniques used by threat actor; 3) the indicators of compromise; 4) information on the affected systems, devices, or networks; 5) information relevant to the identification of the threat actor or actors involved (such as IP addresses or domain names associated with a threat actor); 6) a point of contact from the affected entity; and 7) impact, earliest known time, and duration of compromise. Entities should have the option to report additional types of information on cybersecurity incidents to help to identify emerging trends or otherwise preempt attacks.

Entities should not be penalized for or precluded from reporting an incident if all information, including the information proposed in this list, is not available. This is particularly important, as often it takes weeks for a security team to determine the attack vector and all the IOCs for an incident; security teams should have a mechanism to flexibly update their initial report with additional details as those aspects are confirmed. While CIRCIA provides that supplemental reports should be furnished "promptly" as "new or different information becomes available," the final rule should recognize common security team processes and the continued contextualization of incident information as investigations progress by providing flexibility on the timing and substance of any supplemental reports. Again, where reportable covered cyber incidents are focused on actual loss of confidentiality, integrity or availability of networks or systems, the flexibility to update reports with subsequent information will operationally keep the focus of incident responders on mitigation and remediation actions rather than compliance obligations.

Allow for Bi-Directional Information Sharing

CISA's final rule should ensure that there are processes or mechanisms in place that streamline and allow for bi-directional sharing of incident information to help CISA better assist entities throughout the U.S.

---

[2] MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. See https://attack.mitre.org/

[3] Vocabulary for Event Recording and Incident Sharing (VERIS) is a set of metrics designed to provide a common language for describing security incidents in a structured and repeatable manner. See http://veriscommunity.net/

economy (ensuring that CISA has first anonymized the identification of the reporting entity appropriately).

Designate a Single Point of Contact in the U.S. Government for Covered Entities to Report Security Incidents

Incident response and recovery resources are in short supply. To effectuate the efficient use of limited resources, the U.S. government should designate, and adequately fund, a single point of contact for all organizations that need to report an incident under any U.S. federal statute. Impacted organizations should not be required to report an incident multiple times to multiple different government entities.

In addition, a single point of contact in the government for questions about reporting obligations would be desired. If companies are required to report on incidents, they should also be able to ask questions regarding their potential obligations.

CONCLUSION

Palo Alto Networks supports CISA's work and diligence in moving forward with the implementation of the Cyber Incident Reporting for Critical Infrastructure Act of 2022. Palo Alto Networks has a deep, long-standing commitment to partnering with responsible governments around the globe – providing innovative security technologies, lending our expertise on cybersecurity best practices and policies and sharing cyber threat intelligence. Organizations across the country and in every sector can be subject, and in most cases likely have been subject to cyber incidents which information security teams diligently work to prevent, respond to, and remediate. We understand that providing certain cyber incident information to appropriate entities can potentially contribute to improving cybersecurity for individual entities as well as across sectors and economies, but only when appropriately scoped, handled, and ultimately leveraged. As such, any government mandate to report incident information must be effectively crafted. We hope that our experiences and insight will be helpful to CISA's efforts so that the end result will meet the goals of the law–to improve cybersecurity in the United States. For more information please contact Coleman Mehta, Senior Director, U.S. Public Policy at cmehta@paloaltonetworks.com.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before.