November 14, 2022

Jennie M. Easterly
Director
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
245 Murray Lane SW
Washington, DC 20528-0380

Via Federal eRulemkaing Portal: http://www.regulations.gov

Director Easterly:

BSA | The Software Alliance[1] appreciates the opportunity to provide the below comments in response to the Cybersecurity and Infrastructure Security Agency's (CISA) September 12, 2022, Request for Information (Docket ID: CISA-2022-0010). BSA applauds your commitment "to obtaining public input in the development of [CISA's] approach to implementation of the cyber incident and ransom payment reporting requirements of" the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA).

BSA is the leading advocate for the enterprise technology sector. Our members are among the world's most innovative companies and help to drive digital transformation by providing the solutions that make businesses and governments more competitive and effective, including cloud computing, customer relationship management, human resources management, identity and access management, data analytics, manufacturing, and infrastructure tools and services.

BSA shares your concern about the growing number of cyber incidents as well as their impacts on individuals, organizations, and the entire digital ecosystem. We endeavor to address those challenges through public-private collaboration. As we stated in Enhancing

[1] BSA's members include: Adobe, Alteryx, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, CrowdStrike, Databricks, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Intel, Kyndryl, MathWorks, Microsoft, Okta, Oracle, Prokon, PTC, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

Cyber Policy, Advancing Digital Transformation: BSA'S 2023 Global Cyber Agenda, "In a world in which neither industry nor government alone can solve an ever-evolving set of challenges, public-private partnerships have proven to be the most effective approach to improving cybersecurity of both organizations and the digital ecosystem."

In general, BSA suggests CISA begin implementing CIRCIA by focusing the reporting requirements on the most significant incidents and avoiding the noise that can come from an overly broad approach. Erring on the side of requiring reports from fewer entities, on fewer incidents, with fewer reporting requirements would provide CISA the opportunity to build the people, processes, and technology necessary to, as CIRCIA describes, "receive, aggregate, analyze, and secure reports from covered entities," as well as those necessary to share information to help secure US critical infrastructure. Most importantly, such a tailored approach is most likely to lead to the best security outcomes.

Further, CISA should share the actions it intends to take with the information it collects and how it envisions its actions will improve the cybersecurity of organizations and the digital ecosystem with covered entities and other stakeholders.

BSA offers the following responses to specific questions in the RFI.

I. Definitions

The definitions of "covered entity" and "covered cyber incident" are interrelated. As CISA narrows either definition, it can reduce the number of incidents that entities will report and consequently focus resources on those incidents that are most troubling. Consequently, CISA should take a holistic view of these definitions so CISA can achieve an optimal number of incident reports – that is, a number of incident reports it can effectively analyze and share with "Team Cyber." This narrowing of terms and limiting of the number of reports is integral to achieving CIRCIA's goals.

BSA suggests CISA focus on narrowing the definition of "covered cyber incident" because receiving reports of fewer but more impactful incidents has greater potential to improve cybersecurity than does receiving reports from any specific subset of critical infrastructure entities. But having clear definitions of both terms is essential to CISA's effective implementation of the law.

Even though CIRCIA places limits on the definitions of "covered entity" and "covered cyber incident," for example a "covered entity" is an entity in a critical infrastructure sector, given the breadth of the critical infrastructure sectors identified in PPD-21, CISA should further reduce the scope of these terms. Likely the most effective way to narrow these definitions is to establish a public-private process for CISA, its US Government partners, industry, and other stakeholders, to assess the threats, vulnerabilities, and risks, and then identify

covered entities and define covered cyber incidents. Such a process could consider a wide variety of variables, including, for example, those used within the finance sector to determine if an entity is a systemically important financial institution, such as the entity's size, correlation, and concentration.

BSA also suggests CISA consider how it can improve cybersecurity incident reporting through harmonization. CISA should be aware of ongoing cyber incident reporting requirements in countries including Australia (which uses the term "responsible entity"), and the EU (which uses the terms "essential entities" and "important entities") as well as the numerous US federal and state cyber incident reporting laws.

CISA should not harmonize its approach with another agency's solely for the sake of harmonization. Likewise, the US Government should not harmonize its approach with another country's solely for the sake of harmonization. But, to the extent CISA can harmonize definitions, all else being equal, CISA will help the entire digital ecosystem improve cybersecurity.

By working toward harmonized cyber incident reporting laws, CISA can achieve Congress's goal of harmonization, reflected in CIRCIA's Cyber Incident Reporting Council. BSA also suggests, as noted in Enhancing Cyber Policy, Advancing Digital Transformation: BSA'S 2023 Global Cyber Agenda, CISA should "work internationally to harmonize requirements so that vendors are selected based, not on having the largest compliance team, but on the security and functionality of the solutions they offer."

Finally, as directed by CIRCIA, and worth emphasizing, the definitions CISA promulgates, must be clear. This regulatory process is a good forum for discussing the merits of the definitions of "covered entity" and "covered cyber incident." However, once CISA promulgates a final rule, such discussion should cease, and the result should not necessitate further interpretation of defined terms.

A. Covered Entity

CIRCIA defines "covered entity" as "an entity in a critical infrastructure sector . . . that satisfies the definition established by the Director [of CISA]" pursuant to this rule making process. CIRCIA requires the final rule provide:

> *(1) a clear description of the types of entities that constitute covered entities, based on—*
>
> *(A) the consequence that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety;*
>
> *(B) the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country; and*

(C) the extent to which damage, disruption, or unauthorized access to such an entity, including the accessing of sensitive cybersecurity vulnerability information or penetration testing tools or techniques, will likely enable the disruption of the reliable operation of critical infrastructure.

1. CISA should narrow the definition of "covered entity."

If CISA is not going to have a public-private process for identifying covered entities as discussed above, then CISA should define "covered entities" to align with Section 9 of Executive Order 13636, that is critical infrastructure entities for which "a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security." As CISA noted in its April 2019 report to Congress titled, Improving Critical Infrastructure Cybersecurity, "Prioritizing services to Section 9 entities is considered an effective and efficient way to mitigate national risk" which supports the goals of CIRCIA.

By narrowing the definition of "covered entities" CISA will ensure that it is able to "receive, aggregate, analyze, and secure reports from covered entities." Absent such a narrowing, CISA will receive reports from a larger number of entities and may not be positioned to efficiently turn those reports into actionable information it can share to improve the security of individual organizations and the digital ecosystem.

2. CISA should clarify that "covered entity" includes only entities operating within the US or its territories.

To ensure entities are aware of their obligations and that CISA has jurisdiction over the entity in question, CISA should clarify that covered entities include only entities operating within the US or its territories. This approach aligns with CIRCIA's purpose and CISA's mission, contained in the CISA Strategic Plan 2023-2025, to "lead the National effort to understand, manage, and reduce risk to our cyber and physical infrastructure."

3. CISA should clarify that "covered entity" does not include third-party service providers.

CISA should clarify that a covered entity only has the obligation to report a covered incident when it is the entity that is the victim of the covered cyber incident. That is, CISA's regulations should not require a "covered entity" to report when it is acting in its capacity as a third-party service provider. CISA can and should also address this issue in its definition of "covered incident" and "reasonable belief" (discussed below).

For many, if not most, incidents, a third-party service provider is not positioned to determine if an incident is a "covered cyber incident." While "covered cyber incident" remains undefined at this time, the determination of whether a cyber incident is a covered cyber incident will depend on, for example, whether the incident results in "a disruption of

business or industrial operations" or "potential impacts on industrial control systems." The appropriate entity to make those and other similar determinations is the entity that is the victim, not its third-party service providers. Notably, because "covered entity" remains undefined at this time, it is possible that a third-party service provider might similarly not know if its customer is a covered entity.

Additionally, third party service providers are trusted partners for government agencies and businesses alike. Creating a legal obligation to report such speculation will alter the relationship between a third-party service provider and its customer from one of collaboration to one of conflict. This change would undermine trust and degrade cybersecurity.

Of course, a third-party service provider should be responsible for collaborating with a customer before, during, or after an incident, including providing information to that customer which may be helpful in incident response or required by regulations promulgated pursuant to CIRCIA. Customers and service providers typically assign these roles through contracts. Ultimately, it should be the victim entity's responsibility to determine if it is a covered entity, and if it reasonably believes it is the victim of a covered cyber incident, before meeting its reporting obligations.

B. Covered Cyber Incident

CIRCIA defines "covered cyber incident" as "a substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established by the Director" in this rule making process.

CIRCIA requires the final rule provide:

> *(2) A clear description of the types of substantial cyber incidents that constitute covered cyber incidents, which shall—*
>
> *(A) at a minimum, require the occurrence of—(i) a cyber incident that leads to substantial loss of confidentiality, integrity, or availability of such information system or network, or a serious impact on the safety and resiliency of operational systems and processes; (ii) a disruption of business or industrial operations, including due to a denial of service attack, ransomware attack, or exploitation of a zero day vulnerability, against (I) an information system or network; or (II) an operational technology system or process; or (iii) unauthorized access or disruption of business or industrial operations due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise;*
>
> *(B) consider—(i) the sophistication or novelty of the tactics used to perpetrate such a cyber incident, as well as the type, volume, and sensitivity of the data at issue; (ii) the number of individuals directly or indirectly affected or potentially affected by such a cyber incident; and (iii) potential impacts on*

industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers; and

(C) exclude—(i) any event where the cyber incident is perpetrated in good faith by an entity in response to a specific request by the owner or operator of the information system; and (ii) the threat of disruption as extortion, as described in section 2240(14)(A).

1. CISA should narrow and harmonize the definition of "covered cyber incident."

CISA should define "covered cyber incident" as a cyber incident that has caused substantial operational disruption or financial losses for the entity or has caused considerable material or non-material loses. CISA should further provide objective quantitative measures and should consider the work of DHS's National Critical Infrastructure Protection Program, which considers, among other things, fatalities and economic losses.

2. CISA should clarify that a "covered cyber incident" is defined in relation to the victim entity.

CIRCIA's inclusion of the phrase "experienced by a covered entity" appears to limit CIRCIA's reporting requirement to the entity itself, and not to its third-party service providers; but CISA should nonetheless clarify that only a covered entity that has a reasonable belief that it is the victim of a covered cyber incident has the obligation to report. By clarifying "covered cyber incident" to mean a cyber incident suffered by the entity itself, CISA will protect the relationship between a victim entity and its third-party service provider and avoid receiving multiple reports regarding the same incident. For example, absent such a clarification, CISA or covered entities could misunderstand CIRCIA to require a covered entity to report a cyber incident any time it learns of a cyber incident and reasonably believes the cyber incident is a covered cyber incident. That outcome is not the intent of CIRCIA, and clarification would further CISA's implementation of the law.

3. CISA should clarify a "covered cyber incident" is an incident that impacts operations in the US or its territories.

As noted above in relation to "covered entity," CISA should clarify that it does not expect a covered entity to report an incident that does not impact operations in the US or its territories. This limitation aligns with both CIRCIA's purpose and CISA's mission, as well a realistic view of CISA's operational reach.

BSA fully expects and supports CISA engagement outside the US, both with governments and industry. But that engagement should not be based on CISA attempting to require entities to report cyber incidents with impacts outside the US or its territories.

4. CISA should clarify that reporting under CIRCIA has no relation to reporting under other laws or policies.

CISA should clarify that other government agencies should not construe a covered entity's reasonable belief that it is the victim of a covered cyber incident, and subsequent report, as evidence that it has suffered a material cyber incident, or otherwise triggered the reporting requirement of any other law or policy. To achieve CIRCIA's goal of improved cybersecurity, CISA and covered entities need to collaborate, and that collaboration will not be successful if CISA simultaneously incentivizes covered entities to limit the information they share due to other US Government agencies having different missions and insufficient harmonization.

II. Reports Contents and Submission Procedures

During the 72 hours between when a covered entity reasonably believes it is the victim of a covered cyber incident, and its deadline for reporting to CISA, a covered entity will be extremely busy undertaking incident response efforts. Adding detailed reporting requirements will divert incident response resources and add the considerable burden of coordinating its incident response and legal teams, as well as any third-party incident response organizations it brings in to assist (which, notably, could include CISA, FBI, or other government agencies). Therefore, CISA should limit information in the 72-hour report to only the information absolutely needed.

CISA should review its own Federal Government Cybersecurity Incident and Vulnerability Response Playbooks – notably applicable only to US Government agencies, but instructive for this purpose nonetheless – to consider where "reporting a covered cyber incident" would fit, how inserting reporting requirements would impact a covered entity that is the victim of a covered cyber incident, and how CISA can reduce the negative impact through narrow but effective reporting requirements. For example, what information can CISA reasonably expect to receive in the detection and analysis, containment, or eradication and recovery phases that will provide a greater benefit than the reporting will burden the covered entity?

CISA should appreciate that, given the lack of harmonization between the reporting requirements imposed by other agencies, and its own requirements pursuant to this regulatory process, covered entities will likely be responding to multiple, different reporting requirements all while trying to respond to a cyber incident.

A. The Content, or Other Items related to covered Cyber Incident Reporting

Section 2(a) asks for information about the ". . . content, or other items related to covered cyber incident reporting that would be beneficial for CISA to clarify in the regulations."

1. CISA should include minimal, but specific reporting requirements.

CISA should be cautious about what information it requires a covered entity to report. CISA's requirements will directly affect how covered entities use their limited resources while also responding to the cyber incident. CISA reporting requirements could create a perverse incentive for a covered entity to focus on activities that do not advance its response – an outcome CISA and industry should work together to avoid. We understand, respect, and remain optimistic that CIRICA will reduce risk and increase resilience, but, for these reasons, strongly recommend a cautious approach to reporting requirements.

To achieve the goals of CIRCIA, while appreciating both the limited information a covered entity will possess and that information's uncertainty only 72 hours after having a reasonable belief it is the victim of a covered cyber incident, CISA should require a covered entity to report only:

1. Company name
2. Company point of contact information (name, position, telephone, e-mail)
3. Date of incident detection
4. Type of compromise (unauthorized access, unauthorized release, unknown, not applicable)
5. Description of technique or method used in cyber incident
6. Incident narrative (chronological explanation of the incident; threat actor tactics, techniques, and procedures; indicators of compromise; targeting, mitigation strategies)
7. Whether it detected the incident because of information in the National Vulnerability Database, the Known Exploitable Vulnerabilities Catalogue, or a similar repository, or whether the covered entity detected the covered cyber incident because of threat information shared by CISA, for example through a CISA, NSA, FBI joint Cyber Security Advisory

2. CISA should use a portal and verify third-party submitters.

CISA should setup a portal through which a covered entity can report a covered cyber incident. Certain incidents may implicate a covered entity's e-mail systems and having access to a portal would be important to transmit sensitive information securely.

A portal should also provide a third-party submitter, that is, an entity the covered entity is using to transmit reports, the ability to pre-register as a third-party submitter through the portal. By accepting pre-registration, CISA can increase its confidence that a third-party submitter is a reputable organization, prepared to work on behalf of the covered entity.

3. CISA must protect information it receives pursuant to CIRCIA.

A covered entity may include contractor attributional, proprietary, or other sensitive information that it would not customarily share. The unauthorized use or disclosure of such

information could cause substantial harm to the covered entity or its customers. CISA should clarify that it will protect and not share information it receives pursuant to CIRCIA. CISA should also clarify that other government agencies should not rely on either the fact that a covered entity reported information to CISA or the information contained in that report as evidence that a covered entity has suffered a material cyber incident, or otherwise triggered the reporting requirement of any other law or policy.

Of course, CISA should make risk-based decisions about how to protect a report. Given the sensitivity of the information in a report, industry would expect robust protections. CISA should explain the steps it will take to protect these reports, which will help build trust with industry and further incentivize information sharing.

B. Reasonable Belief

Section 2(b) requests information about what constitutes a covered entity's "reasonable belief," that it is the victim of a covered cyber incident, which starts CIRCIA's 72-hour reporting requirement.

CISA should define reasonable belief as a covered entity's belief that, upon investigation, the reliable information it considered at the time provided clear and convincing evidence that it was the victim of a covered cyber incident. This definition will reduce false positives and help CISA focus on the most impactful cyber incidents.

In both courts of law and public opinion, facts appear obvious in hindsight. But in the fog of cyber incident response, multiple teams must ingest and analyze uncertain and evolving information. As CISA notes in its Federal Government Cybersecurity Incident and Vulnerability Response Playbooks, "the most challenging aspect of the incident response process is often accurately detecting and assessing cybersecurity incidents: determining whether an incident has occurred and, if so, the type, extent, and magnitude of the compromise within cloud, operational technology (OT), hybrid, host, and network systems."

CISA should build its understanding of this challenge into its definition of reasonable belief by defining reasonable belief to encapsulate those cyber incidents about which a covered entity's belief, based on the reliable information at the time, creates a high likelihood that it is the victim of a covered cyber incident.

Additionally, CISA should plan for the scenario in which a covered entity reasonably believes it is the victim of a covered cyber incident but subsequently determines that it was not. CISA should provide specific steps an entity can take to inform CISA of its updated determination. In such a circumstance, it would clearly benefit CISA to refocus on more significant covered cyber incidents. It would also benefit an entity to not have to expend resources to develop reports that would not provide the value envisioned by CIRCIA and

these regulations. Amongst other things, an off ramp should clarify how an entity should inform CISA that it no longer has a reasonable belief that it is the victim of a covered cyber incident and that an entity has no additional reporting requirements.

III. Other Incident Reporting Requirements and Security Vulnerability Information Sharing

A. Substantially Similar Reported Information

Section (3)f requests information about how CISA should "determine if a report provided to another federal entity constitutes 'substantially similar reported information.'"

As noted in the Enhancing Cyber Policy, Advancing Digital Transformation: BSA'S 2023 Global Cyber Agenda, BSA prioritizes harmonizing laws and policies within governments, including ensuring "consistency and harmonization across government agencies and sectors."

There should be a rebuttable presumption that a report provided by a covered entity to another federal entity is substantially similar to a report provide pursuant to CIRCIA. CISA should have to justify its determination that a report to another federal entity is not substantially similar reported information. Of course, if CISA rebuts that presumption, it may require a covered entity to make a second report to CISA. Without this rebuttable presumption, CIRCIA will add reporting requirements and complexity to cyber incident reporting, which would undermine CIRCIA's purpose.

Further, such an approach would support the Office of the National Cyber Director in its statutory duty, pursuant to Section 1752 (C)(v) of the National Defense Authorization Act of Fiscal Year 2021, to coordinate with, amongst others, "the Director of the Cybersecurity and Infrastructure Security Agency, on streamlining of Federal policies and guidelines including . . . regulations relating to cybersecurity." Advancing harmonization through a rebuttable presumption would also advance the goals of CIRCIA, specifically found in the report required by Section 107(d) Report on Harmonization of Reporting Regulations.

Absent such a rebuttable presumption, it is unlikely the US Government will confront the large and growing number of federal reporting requirements, which are themselves hurdles to a more secure future.

B. Principles for Vulnerability Disclosure

Section (3)h requests information regarding "principles governing the timing and manner in which information relating to security vulnerabilities may be shared, including any common industry best practices and United States or international standards."

BSA supports organizations developing, maintaining, and using coordinated vulnerability disclosure (CVD) programs based on internationally recognized voluntary consensus standards, not national or regional vulnerability disclosure laws or policies – a priority noted in Enhancing Cyber Policy, Advancing Digital Transformation: BSA'S 2023 Global Cyber Agenda.

On the specific topic of CVD, as BSA, the Cybersecurity Coalition, Cyber Threat Alliance, and Information Technology Industry Council explained in a recent amicus brief in the case *In re: Intel Corporation CPU Marketing, Sales Practices and Products Liability Litigation*:

> *CVD "is a process for reducing adversary advantage while an information security vulnerability is being mitigated" and includes formal internal mechanisms for receiving, assessing, mitigating, and remediating security vulnerabilities submitted by external sources and communicating the outcome to the vulnerability reporter and affected parties. Effective CVD minimizes risk to technology users by establishing processes that increase the likelihood that information about vulnerabilities becomes public simultaneously with patches or other remediations that enable users to protect themselves. CVD principles are of such importance that they are a core practice in the National Institute of Standards and Technology Cybersecurity Framework ("NIST") and are captured in international standards such as ISO/IEC 29147 and ISO/IEC 30111.*

Additionally, pursuant to the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113), subsection (d)(1):

> *"Except as provided in paragraph (3) of this subsection, all Federal agencies and departments shall use technical standards that are developed or adopted by voluntary consensus standards bodies, using such technical standards as a means to carry out policy objectives or activities determined by the agencies and departments . . . (3) EXCEPTION.—If compliance with paragraph (1) of this subsection is inconsistent with applicable law or otherwise impractical, a Federal agency or department may elect to use technical standards that are not developed or adopted by voluntary consensus standards bodies if the head of each such agency or department transmits to the Office of Management and Budget an explanation of the reasons for using such standards.*

Voluntary consensus standards for CVD exist, notably, ISO/IEC 29147 and 30111. These voluntary consensus standards are neither inconsistent with CIRCIA nor otherwise impractical. CISA should simply use these voluntary consensus standards "to carry out policy objectives or activities."

IV. Conclusion

Given the breadth of options that CISA may consider when, amongst other things, defining terms core to the implementation of CIRCIA, like "covered entity" and "covered cyber incident," and the numerous entities that will be impacted by this rulemaking, CISA and

industry alike would be well served by participating in a meaningful dialogue based on proposed regulatory text contained in an NPRM.

BSA applauds CISA's efforts to engage the private sector (including efforts outside the National Capital Area), but notes that CISA designed its listening sessions to be one sided. That is, CISA did not participate in a dialogue or provide any further information. The result of this approach was that these listening sessions did not maximize the potential for industry and CISA to identify the most effective way to implement CIRCIA but only provided the opportunity to provide CISA information in a spoken, rather than written, form.

Moving forward, CISA should publish an analysis of the information it receives (like analyses undertaken by the National Institute of Standards and Technology) and after publishing proposed regulatory text in an NPRM, engage in bi-directional dialogues between CISA and stakeholders. BSA stands ready to assist or participate in such a dialogue.

BSA appreciates the opportunity to provide the above information and looks forward to working with CISA to ensure that CIRCIA delivers concrete cybersecurity improvement for individual organizations and the digital ecosystem.

Henry Young
Director, Policy