Before the
Cybersecurity and Infrastructure Security Agency
Washington, D.C.

In the Matter of	)	
	)	
Request for Information on	)	CISA-2022-0010
the Cyber Incident Reporting for	)	
Critical Infrastructure Act of 2022	)	
	)	

COMMENTS OF USTELECOM—THE BROADBAND ASSOCIATION

/s/ Paul Eisler

Paul Eisler
Senior Director, Cybersecurity

USTelecom – The Broadband Association
601 New Jersey Avenue, NW, Suite 600
Washington, DC 20001
(202) 326-7300

November 14, 2022

TABLE OF CONTENTS

I. INTRODUCTION

USTelecom – The Broadband Association ("USTelecom")[1] submits these comments in response to the Cybersecurity and Infrastructure Security Agency ("CISA") Request for Information ("RFI") in the above-captioned proceeding. USTelecom shares CISA's commitment to reducing risk to our nation's cyber and physical infrastructure, and the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA") is an important milestone in ensuring the U.S. government has the information it needs. As a leading partner of the U.S. government in cybersecurity, USTelecom offers recommendations to help CISA develop effective rules that will maximize the benefits of our collaboration and partnership.

USTelecom's long history of collaboration with U.S. government partners informs our comments in these proceedings. USTelecom presently chairs the Communications Sector Coordinating Council ("CSCC") and co-chairs the DHS ICT Supply Chain Risk Management Task Force ("SCRM Task Force"), the two principal organizations that serve as the government's industry partners for developing cybersecurity and supply chain security policies. USTelecom also helped the National Institute of Standards and Technology ("NIST") develop the Cybersecurity Framework, and we led the Federal Communications Commission's ("FCC") Communications Security, Reliability, and Interoperability Council's ("CSRIC") landmark effort to implement the Framework in the communications sector.

USTelecom founded, and presently co-leads with the Consumer Technology Association, the Council to Secure the Digital Economy ("CSDE"), a group of fifteen large international ICT companies dedicated to preserving the security of our communications infrastructure and

[1] USTelecom is the premier trade association representing service providers and suppliers for the telecom industry. Its diverse member base ranges from large publicly traded communications corporations to small companies and cooperatives—all providing advanced communications services to both urban and rural markets.

connected digital ecosystem. CSDE is recognized by the U.S. government as a leading industry partnership in coordinating efforts to respond to cyber crises, and also promote cybersecurity of critical infrastructure through development of best practices that influence U.S. and global security standards.

As our leadership in these efforts makes clear, USTelecom fully recognizes the significant security challenges facing our nation's critical infrastructure as a result of cybersecurity and supply chain risks. USTelecom is committed to finding proactive solutions that help the U.S. government achieve its goals and offers these comments in the spirit of partnership and collaboration.

II. DEFINITIONS, CRITERIA, AND SCOPE OF REGULATORY COVERAGE

In this section, USTelecom provides analyses of key definitions that will be essential to meeting the goals of CIRCIA.

A. The meaning of "covered entity," consistent with the definition provided in section 2240(5) of the Homeland Security Act of 2002 (as amended), taking into consideration the factors listed in section 2242(c)(1).

CIRCIA prescribes that a "covered entity" must be understood as "an entity in a critical infrastructure sector" as defined by Presidential Policy Directive 21 ("PPD 21").[2] Additionally, CIRCIA calls for "a clear description" of covered entities based on the following elements:[3]

- The consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety;

[2] 6 U.S. Code § 681(4).
[3] 6 U.S. Code § 681b(c)(1).

- The likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country; and
- 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.

PPD21 derives its definition of "critical infrastructure" from section 1016(e) of the USA Patriot Act of 2001, which applies to "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[4] PPD 21 specifically identifies 16 critical infrastructure sectors, including the communications sector, and designates the Department of Homeland Security as the sector-specific agency for the communications sector.[5]

Therefore, an entity in the communications sector with systems and assets that meet the definition of "critical infrastructure" under section 1016(e), and also meets the three elements identified by CIRCIA, would be a covered entity.

[4] 42 U.S.C. 5195c(e).
[5] Presidential Policy Directive 21, Critical Infrastructure Security and Resilience, Feb. 12, 2013, *available at* https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

B. The meaning of "covered cyber incident," consistent with the definition provided in section 2240(4), taking into account the requirements, considerations, and exclusions in section 2242(c)(2)(A), (B), and (C), respectively. Additionally, the extent to which the definition of "covered cyber incident" under CIRCIA is similar to or different from the definition used to describe cyber incidents that must be reported under other existing federal regulatory programs.

The criteria for what constitutes a "covered cyber incident" should be set high enough to avoid overreporting, consistent with the intent of Congress. Additionally, covered cyber incidents should only be those pertaining directly to the mission of CISA. Non-covered cyber incidents may be reportable to other agencies for purposes outside the scope of CISA's unique mission, and CISA should not seek to duplicate these reporting requirements.

CIRCIA prescribes that a covered cyber incident must include at least one of the elements in 2242(c)(2)(A) "at a minimum".[6] Which is to say that not every situation where one of these elements is met has to rise to the level of a covered incident. When appropriate mitigations are in place, communications providers are able to manage a broad variety of cyber risks as part of their routine business operations.

Further, it is important to acknowledge the vast differences between covered entities, even within the same sector, and avoid imposing the assumptions of one entity upon another. The same type of attack may be a substantial incident for one entity, but far less substantial for another entity with greater maturity, resources, and capabilities to mitigate against the real-world consequences of cyber incidents. For example, a denial of service attack of certain volume may overwhelm some providers but not others.

Finally, but importantly, the definition of a covered cyber incident should make clear that reporting obligations reside with the entities whose information systems or data are targeted for attack by malicious actors, and not any intermediary transport or retransmitting entities or

[6] 6 U.S. Code § 681b(c)(2)(A).

contractors. This understanding is embedded within CIRICIA itself, which prescribes that a covered cyber incident is a "substantial cyber incident" that is "*experienced* by a covered entity".[7]

While intermediaries should be covered when their own information systems are attacked in a manner that triggers a reporting obligation, they should not have a duty to report their customers' or other compromised entities' incidents to the government, as such a policy would implicate privacy concerns, disrupt business relationships and operations, and create potential legal issues associated with compelled disclosures of incidents affecting third parties.

C. The number of covered cyber incidents likely to occur on an annual basis either in total or within a specific industry or sector.

The number of covered cyber incidents likely to occur on an annual basis will be a product of how key terms in this proceeding are defined. It is essential to ensure that definitions are not overbroad to avoid detracting resources from cyber defense for sake of regulatory compliance.

It is critical for government partners to note that significant cyber resources will be dedicated to determining whether a given event rises to the level of being reportable. Below are examples of routine incident types that would need to be analyzed to determine if they rise to the criteria as outlined.

- A significant incident that is higher in terms of significant risk to the business (current or imminent).
- A critical vulnerability that exists on a significant portion of the provider network, and/or on perimeter facing systems, for which exploit code exists in the wild.

[7] 6 U.S. Code § 681(4) (emphasis added).

- Any potential administrative level compromise on a system that is connected to an untrusted network, and/or contains sensitive data.
- A major virus, ransomware, or worm outbreak on the provider enterprise that is not contained.
- A backbone impacting DDoS, Fraud or other newsworthy security event.
- Any incident involving a potential data breach of the provider's proprietary or otherwise critical information.
- Any incident involving a potential data breach of provider's customer CPNI, PII or other sensitive data (SOX, UK) that is potentially reportable.
- Any security incident that may cause significant financial loss for the provider.
- Any security incident that may cause loss of reputation for the provider.

D. The meaning of "substantial cyber incident."

Congress has been clear that the definition for "substantial cyber incident" should be set at a level to not flood CISA with reporting. Day to day observations of malicious cyber activity should not be reported.

A rational definition of "incident" in the cybersecurity context is found in 6 U.S. Code § 659, which defines an incident as an "occurrence" – not merely a hypothetical event – and said occurrence must "actually or imminently" cause one of the enumerated jeopardies (to information or information systems) without lawful authority.[8] As a threshold matter, any cyber

[8] 6 U.S. Code § 659(a)(5) ("[T]he term 'incident' means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system").

event that fails to meet this basic definition of "incident" should not be considered a substantial cyber incident.

To avoid confusion and inconsistent interpretations by policymakers and stakeholders more broadly, the term "substantial cyber incident" should address the same areas of concern as "significant cyber incident", as defined by Presidential Policy Directive 41 ("PPD41"). Namely, harm to "national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people."[9]

The definition of "substantial cyber incident" does not preclude voluntary communications to be shared with the U.S. government and other providers. Even though a given event may not rise to a reportable event, for instance if no data loss is experienced, providers may certainly voluntarily share information informally with U.S. government or industry partners on event observations that the provider may find worrisome and worthy of further collaboration. However, such further voluntary self-reporting and collaboration should not be made mandatory though any definition.

E. The meaning of "supply chain compromise," consistent with the definition in section 2240(17).

The term supply chain compromise should be limited to static goods and services. Data supply chains, in contrast, are dynamic and constantly changing. Importantly, communications providers should not be understood as part of the supply chain compromise merely because data is transiting their networks.

[9] Presidential Policy Directive 41, United States Cyber Incident Coordination, July 26, 2016, *available at* https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

Not all supply chain risks rise to the level of compromises. A supply chain compromise, according to CIRCIA, means "an incident within the supply chain of an information system that an adversary can leverage or does leverage to jeopardize the confidentiality, integrity, or availability of the information system or the information the system processes, stores, or transmits, and can occur at any point during the life cycle."

The term "incident" as defined by 6 U.S. Code § 659 refers to an "occurrence" – not merely a hypothetical event – and said occurrence must "actually or imminently" cause the jeopardy in question. Pursuant to this carefully considered definition, the mere possibility of jeopardy that is not actual or imminent would not satisfy the definition of supply chain compromise, even if such jeopardy were conceivable.

III. REPORT CONTENTS AND SUBMISSION PROCEDURES

In this section, USTelecom provides recommendations on report contents and submission procedures to efficiently achieve the goals of CIRCIA.

A. How covered entities should submit reports on covered cyber incidents, the specific information that should be required to be included in the reports (taking into consideration the requirements in section 2242(c)(4)), any specific format or manner in which information should be submitted (taking into consideration the requirements in section 2242(c)(8)(A)), any specific information that should be included in reports to facilitate appropriate sharing of reports among federal partners, and any other aspects of the process, manner, form, content, or other items related to covered cyber incident reporting that would be beneficial for CISA to clarify in the regulations.

USTelecom represents telecom service providers and suppliers of every size. Our diverse member base ranges from large publicly traded communications corporations to small companies and cooperatives, all providing advanced communications services to both urban and rural

markets. Our members, from the smallest to the largest, have expressed concern about the substantial resources they will need to dedicate to complying with a rapidly growing patchwork of cybersecurity reporting requirements.

Providers need to be able to submit reports to a single agency. It will be essential to streamline the contents of reports as much as possible – by developing a common format – while allowing a variety of flexible reporting mechanisms that could ideally be tailored to the unique needs of organizations. Because of the variety of covered entities that will submit reports to CISA and their vastly different sizes, processes, and experience working with federal government partners, it will be important to consider entities' unique needs and constraints, and identify strategies to increase efficiency for both industry and government.

B. What constitutes "reasonable belief" that a covered cyber incident has occurred, which would initiate the time for the 72-hour deadline for reporting covered cyber incidents under section 2242(a)(1).

The 72-hour reporting window should only start to toll after the covered entity has confirmed an incident meets the reporting criteria—this confirmation should be what constitutes "reasonable belief" that a covered cyber incident has occurred. No reporting obligation should be triggered unless and until the affected entity has had the opportunity to assess and confirm an incident has met applicable criteria and thresholds.

Otherwise, out of an abundance of caution, industry would likely have to report many events that do not meet reporting criteria because of the remote possibility of escalation. This overreporting could strain government resources and be counterproductive for both sides of the public-private partnership.

C. When should the time for the 24-hour deadline for reporting ransom payments begin (i.e., when a ransom payment is considered to have been "made").

A ransom payment should be considered "made" for purposes of CIRCIA when it clears the covered entity's bank account or the bank account of the third party (usually a law firm) that is executing the payment. This would ensure only actual payments count, rather than unaccepted offers or statements made in the course of negotiations.

D. How covered entities should submit supplemental reports, what specific information should be included in supplemental reports, any specific format or manner in which supplemental report information should be submitted, the criteria by which a covered entity determines "that the covered cyber incident at issue has concluded and has been fully mitigated and resolved," and any other aspects of the process, manner, form, content, or other items related to supplemental reports that would be beneficial for CISA to clarify in the regulations.

After a covered entity confirms that a covered cyber incident has occurred, the 72-hour deadline to submit a report should be initiated. By the end of this reporting window, a covered entity may still be investigating key details about the confirmed incident. Indeed, "substantial new or different information" may become known after the reporting window has already closed. In such cases, supplemental reports should include information that would allow critical infrastructure organizations to defend themselves, as well as whether the covered cyber incident has been "fully mitigated and resolved".

To determine when a covered cyber incident should be considered fully mitigated and resolved, it is instructive to consider the definition of an "incident" under 6 U.S. Code § 659 - National Cybersecurity and Communications Integration Center. An incident there is defined as an "occurrence" (not a continuous state of affairs) that "*actually or imminently jeopardizes*… the

integrity, confidentiality, or availability of information on an information system, or *actually or imminently jeopardizes*… an information system."[10]

Focusing on jeopardy that is actual or imminent is essential to ensure an organization's limited resources can be allocated rationally. As such, a reported incident where an investigation by the covered entity or a third party hired by the covered entity does not yield clear evidence of actual or imminent jeopardy should be considered fully mitigated and resolved.

E. The timing for submission of supplemental reports and what constitutes "substantial new or different information," taking into account the considerations in section 2242(c)(7)(B) and (C).

Multiple federal agencies require or propose that reports be made on cyber incidents, including *inter alia* DHS, FCC, and the Securities and Exchange Commission ("SEC"). While agencies may require reports, the reported information needs to be made consistent between the agencies and providers need to be able to submit reports to a single agency. As well, a report to one should be a report to all versus requiring duplicative reports to several agencies.

Cyber incident reports to states should be consistent with the federal incident reporting and provided to the single federal agency.

For reasons discussed previously, after a covered entity confirms that a covered cyber incident has occurred, the 72-hour deadline to submit a report should be initiated. A supplemental report may be required after the initial report if "substantial new or different information" surfaces as a result of investigations.[11] However, pursuant to Section 2242(a)(1)(B), CISA may not require reporting of the initial report "any earlier than 72 hours after the covered entity reasonably believes that a covered cyber incident has occurred." It stands to reason that

[10] 6 U.S. Code § 659(a)(5) (emphasis added).
[11] 6 U.S. Code § 681b(a)(3).

CISA should not require a supplemental report during the period of time when it cannot require the initial report. Otherwise, covered entities would be penalized for submitting reports in a timely manner.

Security experts and researchers at covered entities should be allowed to exercise their professional judgment as to when new findings deserve a supplementary report. At a minimum, however, a new 72-hour reporting window (that initiates immediately after "substantial new or different information" is confirmed) should be afforded to providers. This is the minimum necessary amount of time to properly respect the balance of government partners' need for situational awareness and cybersecurity practitioners' time-sensitive responsibilities that CIRCIA struck. Nothing should prevent covered entities from submitting supplemental reports sooner if they are prepared to do so.

F. What CISA should consider when "balanc[ing] the need for situational awareness with the ability of the covered entity to conduct cyber incident response and investigations" when establishing deadlines and criteria for supplemental reports.

Before submitting a supplementary report, covered entities should be afforded sufficient time to confirm new findings, as well as investigate potential leads that may yield additional information of relevance to government partners, which should be included in the same report. Therefore, a new 72-hour reporting window should start immediately after "substantial new or different information" is confirmed by the covered entity.

G. Covered entity information preservation requirements, such as the types of data to be preserved, how covered entities should be required to preserve information, how long information must be preserved, allowable uses of information preserved by covered entities, and any specific processes or procedures governing covered entity information preservation.

Covered entities should follow their legal obligations for data retention. The costs and burdens associated with retention of data can be considerable, especially when the data itself must be kept secure. Instead of creating additional requirements, it makes more sense to allow entities to allocate finite resources to proactive security measures.

IV. OTHER INCIDENT REPORTING REQUIREMENTS AND SECURITY VULNERABILITY INFORMATION SHARING

In this section, USTelecom provides recommendations on other incident reporting requirements and security vulnerability information sharing to efficiently achieve the goals of CIRCIA.

A. Other existing or proposed federal or state regulations, directives, or similar policies that require reporting of cyber incidents or ransom payments, and any areas of actual, likely, or potential overlap, duplication, or conflict between those regulations, directives, or policies and CIRCIA's reporting requirements.

In addition to CIRCIA regulations, the communications sector is subject to a host of other reporting requirements at the federal level (e.g., SEC disclosures, FCC breach, outage and disaster, and new EAS reporting) and state level (e.g., data breach and incident reporting notifications), and international level. Considerations at the international level include, for example:

- Proposed European Commission Proposed Directive on Security of Network and Information Systems (NIS2 Directive)

- Australia Security of Critical Infrastructure Act 2018 (SOCI Act)
- India Cert-In Cyber Security Regulation

B. What federal departments, agencies, commissions, or other federal entities receive reports of cyber incidents or ransom payments from critical infrastructure owners and operators.

At the federal level, USTelecom members participate in FCC programs such as the Disaster Information Reporting System (DIRS), FCC Network Outage Reporting System (NORS) and CPNI breach notification portal. The sector has long-established, voluntary cyber incident reporting relationships with the FBI and the Secret Service. Communications providers are also subject to the SEC requirement for publicly traded companies to disclose cyber incidents.

C. Criteria or guidance CISA should use to determine if a report provided to another federal entity constitutes "substantially similar reported information."

If the report already submitted covers the same incident and there is no "substantial new or different information" (that would require a supplementary report) then the already-submitted report's contents should constitute "substantially similar reported information".

D. What constitutes a "substantially similar timeframe" for submission of a report to another federal entity.

A substantially similar timeframe should be any timeframe where no "substantial new or different information" (that would require a supplementary report) has been discovered by the covered entity's investigations. Otherwise, covered entities would need to duplicate efforts by reporting the same or substantially similar information to multiple agencies.

E. 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.

In 2019, CSDE published its initial *Cyber Crisis Report*[12] with key insights for incident response, including how to handle disclosure of security vulnerabilities. CSDE's membership, which has since grown, included at the time thirteen global companies including USTelecom's members AT&T, Ericsson, Lumen, NTT, Oracle, Telefónica, and Verizon. The guidance was developed in consultation with experts and sources from industry, government, and civil society.

The report specifically notes widely-adopted international standards focusing on Coordinated Vulnerability Handling and Disclosure, ISO/IEC 30111 (2019) and ISO/IEC 29147 (2018). As CSDE states, the Coordinated Vulnerability Disclosure (CVD) process "guides vendors, security researchers, and other stakeholders in the digital economy to cooperate on the development of mitigations addressing a given vulnerability while simultaneously limiting disclosure of information concerning that vulnerability until such time as mitigations and information can be made available to the public in a coordinated manner. The CVD process is consistent with NIST's Cybersecurity Framework, which recommends the establishment of processes to 'receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers).' The National Telecommunications and Information Administration (NTIA) has collaborated with industry and global stakeholders represented in the Forum of Incident Response and Security Teams (FIRST) to develop guidelines and practices for multi-party vulnerability coordination and disclosure."

[12] CSDE, Cyber Crisis: Foundations of Multi-Stakeholder Coordination (2019), https://csde.org/wp-content/uploads/2019/09/CSDE_CyberCrisis-Report_2019-FINAL.pdf.

V. CONCLUSION

USTelecom appreciates this opportunity to provide recommendations on how to approach the CIRCIA rulemaking. USTelecom welcomes the continuation of these critical dialogues and these comments should be understood in the context of our firm support for the federal government's crucial role in advancing the cybersecurity of critical infrastructure.

Respectfully submitted,

/s/ Paul Eisler

Paul Eisler
Senior Director, Cybersecurity

USTelecom – The Broadband Association
601 New Jersey Avenue, NW, Suite 600
Washington, DC 20001
(202) 326-7300

November 14, 2022