MARK E. GREEN, MD, TENNESSEE
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Eighteenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

July 3, 2024

Mr. Todd Klessman
CIRCIA Rulemaking Team Lead
Cybersecurity Infrastructure and Security Agency
circia@cisa.dhs.gov

Re: Comments on the Notice of Proposed Rulemaking (NPRM) on Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements

Dear Mr. Klessman:

We appreciate the opportunity to comment on the NPRM for CIRCIA. A strategically scoped incident reporting framework will improve the security and resilience of the digital ecosystem. We look forward to working with you to ensure that CIRCIA implementation has that effect.

We began drafting CIRCIA just over three years ago. At the time, a provision included in the House-passed version of H.R. 6395, the *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*, which would have established a cyber incident reporting requirement for critical infrastructure owners and operators, had been dropped from the final bill,[1] and the SolarWinds supply chain compromise had demonstrated such reporting was a security imperative.[2] Because victims of the SolarWinds supply chain attack were not required to report

[1] H.R. Rep. 116-617, at 1929 (2020)(Conf. Rep).

[2] *See Weathering the Storm: The Role of Private Tech in the SolarWinds Breach and Ongoing Campaign* before the H. Comm. on Oversight and Reform and H. Comm. on Homeland Security, 117th Cong. (Feb.26, 2021) (Chairman Bennie G. Thompson describing potential solutions to better identifying and disrupting cyber attacks, observing: "In recent days, I have been encouraged to learn of growing interest in enacting a cyber incident reporting law. Former chairman of the Cybersecurity Subcommittee, Cedric Richmond, authored an amendment included in the House-passed National Defense Authorization Act that would have established a cyber incident notification requirement. Unfortunately, we were unable to reach agreement with our Senate counterparts, but we look forward to trying again this year and hope we can enact cyber incident notification legislation in short order."). In response to a question from Rep. Yvette Clarke about the value of mandating cyber incident reporting for critical infrastructure entities, Microsoft President and Vice Chairman Brad Smith responded: "[T]he reason that we should want companies in the private sector, companies that, as you mentioned, are in the area of critical infrastructure, it is to provide information about threats so that one entity is in a position to scan the entire horizon and connect the dots between all of the attacks or hacks that are taking place." *Id.* In response to the same question, SolarWinds President and Chief Executive Officer Sudhakar Ramakrishna responded: "Having a single entity to which all of us can refer to will serve the fundamental purpose of building speed and agility in this process. Too much time is wasted in communicating across agencies where information is very fragmented, and oftentimes the dots are not connected

that they had been compromised, efforts to understand the full scope, impact, and motives of the incident were frustrated. A series of additional high-profile cyber attacks – including ransomware attacks against Colonial Pipeline, Kaseya,[3] and JBS, along with the 2021 Microsoft Exchange Server zero-day compromise[4] – further underscored that the Federal government's limited visibility into malicious activity on critical infrastructure networks posed an unacceptable obstacle to preventing, detecting, and mitigating cyber attacks.

Recognizing that a mandatory cyber incident reporting framework could serve any number of purposes, we focused on two primary goals: (1) enabling the Federal government to work with its private sector partners to detect and disrupt malicious cyber campaigns sooner and (2) identifying evolving threat trends and tactics used by our adversaries to enable more strategic investments in security.[5]

Three considerations drove our approach to CIRCIA. First, we understood that a cyber incident reporting framework designed to benefit both the government and the private sector would require ample involvement and input from the private sector. We chose CISA as the centralized hub for critical infrastructure cyber incident reports because it has strong history of productive collaboration with the private sector and existing authorities and capabilities to contextualize and action the information.[6]

Second, we anticipated that cyber incident reporting would be one of many new actions the Federal government would be asking the private sector to undertake to improve the Nation's cybersecurity. The final CIRCIA text reflected our best effort to balance ensuring CISA had sufficient information to achieve the bill's objectives against the burdens associated with the private sector's existing and future cybersecurity obligations.

Third, we had observed past efforts to facilitate and operationalize cyber threat information fail to achieve their objectives - most notably the Automated Indicator Sharing (AIS) program – and we sought to apply the lessons learned in the CIRCIA framework.[7] Notably, AIS suffered from poor

---

because they are separate. That is the fundamental reason why I think having a singular agency to which all of us can communicate to and have two-way communication with them is fundamental to improving our speed and agility around these topics." *Id.*

[3] *See Kaseya Ransomware Attack: Guidance for Affected MSPs and their Customers,* Cybersecurity and Infrastructure Security Agency (Jul. 12, 2021), https://www.cisa.gov/news-events/news/kaseya-ransomware-attack-guidance-affected-msps-and-their-customers.

[4] *See ED 21-02: Mitigate Microsoft Exchange On-Premises Product Vulnerabilities,* Cybersecurity and Infrastructure Security Agency (Mar. 3, 2021), https://www.cisa.gov/news-events/directives/ed-21-02-mitigate-microsoft-exchange-premises-product-vulnerabilities.

[5] H. Comm. on Homeland Security, The Cyber Incident Reporting for Critical Infrastructure Act, at 1 (Aug. 2021) ("To be a more effective security partner to CI, the Federal government needs to better understand the techniques adversaries are using to carry out cyberattacks so that it is in the best possible position to identify malicious cyber campaigns early and help CI owners and operators defend against future incidents."), *available at* https://democrats-homeland.house.gov/download/incident-reporting-bill-draft-fact-sheet.

[6] *See id.* ("CISA has . . . established mechanisms for public- information sharing and interagency collaboration").

[7] *Stakeholder Perspectives on the Cyber Incident Reporting for Critical Infrastructure Act of 2021*, Subcomm. on Cybersecurity, Infrastructure Protection, and Innovation of the H. Comm. on Homeland Security, 117th Cong. (Sept. 2, 2021)(statement of Chairman Bennie G. Thompson)(" As you know, this might be our 2.0 initiative, because we

participation and stakeholders complained that AIS threat information was untimely, lacked context, and focused too much on the quantity of information shared and not the quality.[8] In 2020, the Department of Homeland Security's Office of the Inspector General attributed some of these challenges to insufficient staffing.[9] With that in mind, we aimed to scope the requirements of CIRCIA in a manner that would yield reporting for CISA sufficient to identify and action information on malicious cyber campaigns and threat trends without overwhelming its resources.

We appreciate that implementing CIRCIA is an enormous undertaking, and we commend CISA for achieving the important milestone of issuing the NPRM. Early in the implementation process, we were encouraged that CISA solicited stakeholder feedback through listening sessions and a Request for Information.[10] Since then, we are concerned that engagement with stakeholders has diminished and that CISA drafted the NPRM without the benefit of ongoing stakeholder input. Relatedly, we are concerned that the NPRM appears to, at times, mischaracterize or dismiss Congressional intent. We offer further, more detailed comment on the NPRM below.

I. Scope

At the outset, we observe the NPRM's definition of "covered entity" and "covered cyber incident" are broad, and the some of the information required in incident reports goes beyond what is required by statute.[11] We anticipate incident reporting requirements to evolve over time and to adjust as the threat landscape and the maturity of stakeholders changes.[12] That is why we expressly authorized subsequent rulemakings.[13] We very deliberately approached CIRCIA in a manner that would reduce overreporting of incidents to avoid the previous pitfalls of AIS. Indeed, we established a 72-hour CIRCIA reporting deadline to give covered entities time to better assess whether an incident is actually subject to reporting. Given the demands the initial implementation of CIRCIA will exact upon CISA and its workforce, as well as covered entities, we encourage CISA to scope the NPRM in a manner that does not overtax its resources or overburden the private sector and will best position CISA to demonstrate the unique value cyber incident reporting can generate.

---

tried a similar effort in our Cyber Act of 2015 to incentivize volunteer public, private information sharing and, unfortunately, no one has gotten out of what they bargained for.").

[8] *See* Office of the Inspector General, U.S. Dept. of Homeland Security, DHS Made Limited Progress to Improve Information Sharing under the Cybersecurity Act in Calendar Years 2017 and 2018, 9-10 (Sept. 2020), https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-74-Sep20.pdf.

[9] *Id.* at 11.

[10] Cyber Incident Reporting for Critical Infrastructure Act of 2022 Listening Sessions, 87 Fed. Reg. 55830 (Sept. 12, 2022); Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022, 87 Fed. Reg. 55833 (Sept. 12, 2022). We are aware that PPD-21 has been replaced by National Security Memorandum-22. That change does not affect the definition of critical infrastructure for purposes of CIRCIA.

[11] *See* Proposed Rule §§ 226.1, 226.2, and 226.8.

[12] *See Stakeholder Perspectives on the Cyber Incident Reporting for Critical Infrastructure Act of 2021*, Subcomm. on Cybersecurity, Infrastructure Protection, and Innovation of the H. Comm. on Homeland Security, 117th Cong. (Sept. 2, 2021)(statement of Robert Mayer, Senior Vice President of Technology and Innovation, U.S. Telecom) ("So what you want to look for is the Goldilocks solution here. It can be too narrow or it could be too broad, and you really have to find that right balance in terms of, you know, laser on that kind of consideration. So the fact that there is a process of engagement, that there is going to be a continuous dialog, I believe, there will be opportunities to say, we didn't do enough, we did too much, or it was too narrow, too broad, and to refine that.").

[13] 6 U.S.C. 681b(b)(3).

A. Covered Entity

CIRCIA defines "covered entity" as "an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21 ["PPD-21"], that satisfies the definition established by the Director in the final rule."[14] Congress directed CISA to further clarify the definition of "covered entity" and provided specific considerations for CISA to employ to determine which entities within critical infrastructure would be subject to mandatory cyber incident reporting:

> (A) the consequences 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.[15]

The NPRM includes a definition of "covered entity" broader than contemplated by CIRCIA.[16] Following a protracted discussion about the statutory definition of covered entity and whether such an entity "must own or operate systems or assets that meet the definition of critical infrastructure in PPD–21," CISA determined it did not.[17] The NPRM expressly rejects limiting the definition of "covered entity" to "critical infrastructure or a subset thereof," asserting that doing so would be inconsistent with Congressional intent and undermine the goals of CIRCIA.[18] Instead, the NPRM expands the already broad definition of critical infrastructure, as it is defined by PPD-21, to include those entities that "are active participants in critical infrastructure sectors and communities," but do not own or operate systems or assets that are critical infrastructure.[19] The NPRM thus proposes to define "covered entity" as an "entity in a critical infrastructure sector that either: (a) Exceeds the small business size standard . . . or (b) Meets a sector-based criterion."[20] CISA estimates that over 316,000 entities will be subject to CIRCIA.[21]

We were surprised. Initially, we would point out that the statute authorizing the NPRM is titled the "Cyber Incident Reporting *for Critical Infrastructure* Act of 2022" [emphasis added]. In our view, that alone would make clear Congress intended to limit the definition of "covered entity" to critical infrastructure owners and operators. But if the title of the legislation was not sufficient, certainly the comments of its author should have been. At a hearing on CIRCIA, Representative Clarke said: "I want to be clear that we do not expect all critical infrastructure owners and operators

---

[14] 6 U.S.C. 681(4).
[15] 6 U.S.C. 681b(c)(1).
[16] *See* Proposed Rule § 226.2.
[17] Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 Fed. Reg. 23644, at 23676.
[18] *Id.* at 23677.
[19] *Id.* at 23676-77.
[20] Proposed Rule § 226.2.
[21] 89 Fed. Reg. at 23648.

to be subject to this reporting requirement. Rather, we expect it to apply only to a subset."[22] Contrary to what the NPRM asserts, Congress *did* intend for covered entities to be a subset of critical infrastructure owners and operators.

We are also concerned that the discussion of whether an entity is an owner or operator of critical infrastructure or "in a critical infrastructure sector" is, by and large, a tortured distinction without a sufficiently meaningful difference to justify the confusion among stakeholders it might cause about whether CIRCIA applies to them.[23] Additionally, we ask CISA to consider the compliance costs that may ultimately be imposed on small businesses and make a determination whether the information those entities are likely to have will meaningfully advance the objectives of CIRCIA.

Finally, we take issue with how the NPRM interprets the considerations described in 6 U.S.C. 681b(c)(1) as a lens rather than a limit.[24] The NPRM is correct that covered entities need not meet all three criteria in 6 U.S.C. 681b(c)(1), but certainly the considerations were intended to refine the scope of the entities subject to incident reporting to ensure that only those most likely to have information valuable to the broader ecosystem were subject to reporting requirements.

As we have indicated, our goal is to ensure that CISA has the information necessary to achieve the goals we established for CIRCIA. We deliberately established a broad definition of covered entity and gave CISA authority to further refine it. We did so because we were concerned that reporting from too many entities would result in overreporting of incidents that do not have any bearing on CIRCIA's goals. Accordingly, we are concerned that the overly broad definition of covered entity in section 226.2 of the Proposed Rule could result in CISA being inundated with incident reports that do not contain information that will reduce systemic risk and, instead, overburden CISA's analytical capabilities. CIRCIA and stakeholders have suggested various approaches to refine the definition of "covered entity," and we urge CISA to consider them.

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 the final rule."[25] It directs CISA to provide a definition of "substantial cyber incidents" that:

> (A) at a minimum, require the occurrence of—

---

[22] *Stakeholder Perspectives on the Cyber Incident Reporting for Critical Infrastructure Act of 2021*, Subcomm. on Cybersecurity, Infrastructure Protection, and Innovation of the H. Comm. on Homeland Security, 117th Cong. (Sept. 2, 2021)(statement of Rep. Yvette Clarke). *See also Surveying CIRCIA: Stakeholder Perspectives on the Notice of Proposed Rule Making*, Subcomm. on Cybersecurity, Infrastructure Protection, and Innovation of the H. Comm. on Homeland Security, 118th Cong. (May 1, 2024) (statement of Rep. Yvette Clarke) ("[O]ur intent was that reporting requirements would be appropriately tailored to limit overreporting and ensure that CIRCIA ultimately yields the security benefits we intended. In short, we wanted reporting from more than the one twenty -- 120 entities, the Solarium Commission recommended and a greater range of incidents than just those that would trigger a unified coordination group.").

[23] 89 Fed. Reg. at 23677.

[24] *Id.* at 23678.

[25] 6 U.S.C. 681(3).

> (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;[26]

The statute further directs CISA to consider the following as it defines "substantial cyber incidents:"

> (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;[27]

With these provisions, Congress expressly intended to limit the scope of cyber incidents subject to reporting to ensure that only those incidents demonstrating a potential to reveal evolving adversary tactics, help detect and disrupt a malicious cyber campaign, or curtail the impact of a broader incident would be reported. Congress's goal was to reduce overreporting to ensure efficient intake and analysis of cyber incident reports and minimize the burden on covered entities.

The NPRM proposes to require covered entities to report all substantial cyber incidents, arguing doing so is more straightforward for both CISA and covered entities, so the scope of covered incidents turns on the definition of that term.[28] The NPRM largely adopts that statutory definition of "substantial cyber incidents," and the changes that are included appear to expand the scope of covered incidents, not narrow it.[29] Stakeholders have justifiably raised concerns that the NPRM is so broad in its description of "substantial cyber incident" that it will lead to overreporting.

Once again, we were surprised. Congress's intent was clear. CIRCIA provided CISA broad authority to define "substantial cyber incident," for purposes of defining "covered cyber incident," by working with stakeholders. At a September 2021 hearing on CIRCIA, Rep. Clarke stated: "One of the goals in drafting this legislation was to provide CISA with enough information to analyze and understand threats . . . without inundating CISA with false positives or inaccurate . . . unhelpful

---

[26] 6 U.S.C. 681b(c)(2).
[27] 6 U.S.C. 681b(c)(2)(B).
[28] 89 Fed. Reg. at 23661.
[29] *Id.*

reports . . . . Toward that end, we have directed CISA to consider a number of factors when defining covered cyber incidents."[30] Rep. Clarke followed up with a question about the impact of an overly broad rule, and witnesses responded such a rule would undermine the goals of CIRCIA but expressed confidence that an appropriate balance would be struck during the rulemaking process.[31]

CIRCIA expressly directed CISA to provide "a clear description of the types of substantial cyber incidents that constitute covered cyber incidents" based on the parameters the statute described,[32] but the NPRM does not adequately do so. The has led to widespread concern among stakeholders that de minimis incidents will need to be reported – an outcome Congress deliberately tried to avoid.[33] The NPRM dismisses concerns that overreporting will frustrate Congress's objectives for CIRCIA, arguing that there have been "advances in technology and strategies for managing large data sets, [and] the potential challenges associated with receiving large volumes of reports can be mitigated through technological and procedural strategies."[34] We are not convinced.

While we appreciate CISA's concern that narrowing or clarifying the definition of "substantial cyber incident" will interfere with access to the information necessary to achieve CIRCIA's goals, we do not agree that the additional refinements Congress directed CISA to make in CIRCIA and that stakeholders seek will have that affect. Accordingly, we urge CISA to refine the definition of "substantial cyber incident" in a manner that will raise the threshold for "covered cyber incidents."

C. Cyber Incident Reports

Section 2242(c)(4) of CIRCIA directs CISA to provide a "clear description of the specific required contents" of a cyber incident report and sets forth a range of data the Director may request. Notably, the data points described in section 2242(c)(4) of CIRCIA are tethered to the underlying goals of the incident reporting program: (1) detecting and disrupting malicious cyber campaigns

---

[30] *Stakeholder Perspectives on the Cyber Incident Reporting for Critical Infrastructure Act of 2021*, Subcomm. on Cybersecurity, Infrastructure Protection, and Innovation of the H. Comm. on Homeland Security, 117th Cong. (Sept. 2, 2021)(statement of Rep. Yvette Clarke).

[31] *Id.* (statements of Heather Hogsett, Senior Vice President of Technology and Risk Strategy for BITS, Banking Policy Institute and Robert Mayer, Senior Vice President of Technology and Innovation, U.S. Telecom).

[32] 6 U.S.C. 681b(c)(2).

[33] *See Surveying CIRCIA: Stakeholder Perspectives on the Notice of Proposed Rule Making*, Subcomm. on Cybersecurity, Infrastructure Protection, and Innovation of the H. Comm. on Homeland Security, 118th Cong. (May 1, 2024)(statement of Scott Aaronson, Senior Vice President for Security and Preparedness at the Edison Electric Institute (EEI))("The inclusion of 'any nonpublic information' and 'third-party data hosting provider or a supply chain compromise' in this definition is very broad, which may result in CISA receiving far more incident reports than it is capable of triaging."); *id.* (statement of Heather Hogsett, Senior Vice President of Technology and Risk Strategy for BITS, Banking Policy Institute)("CISA should revise the definition of 'substantial cyber incident' to ensure a higher threshold for reporting and avoid over-reporting of incidents that cause minimal harm or impact. For instance, the requirement to report a 'disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services' lacks an impact threshold and could lead to a large number of immaterial or less significant incidents being reported."); *id.* (statement of Robert Mayer, Senior Vice President of Technology and Innovation, U.S. Telecom)("The proposed scope of "covered entities" and "covered cyber incident" are expansive and currently lack key guidance that cybersecurity practitioners will need, as they seek to provide CISA with information that is responsive to the agency's mission."); *id.* (statement of Amit Elazari, CEO and Co-Founder, Openpolicy)("Concerns related to the definition of "covered cyber incident" capturing 'too much' and in a manner that does not advance CISA's situational awareness, but rather overwhelms CISA.").

[34] 89 Fed. Reg. at 23652.

earlier; and (2) identifying evolving threat trends and tactics used by our adversaries to enable more strategic investments in security.

The NPRM expands the type of data covered entities must submit in cyber incident reports. For example, section 226.8(a)(4) of the Proposed Rule requests information on "direct economic impact to operations." Section 226.8(i) of the Proposed Rule requests detailed information related to "mitigation and response activities taken by the covered entity." Although it may be that this data would advance the goals of CIRCIA, the NPRM does not sufficiently make that case. If CISA plans to request information from covered entities beyond what CIRCIA provides, it must make the case that such information directly advances the goals of CIRCIA. Moreover, we ask that CISA, to the extent practicable, distinguish between the information that must be reported within the 72-hour window to detect and disrupt malicious cyber attacks and the information necessary to identify evolving trends and tactics, which may not be as urgently required.

II. Regulatory Harmonization

In order to reduce the burden on reporting entities, it is important that cyber incident reporting requirements across the Federal government be harmonized to the greatest extent possible. A major priority for Congress when enacting CIRCIA was to facilitate greater harmonization in light of the rapid growth of cyber incident reporting requirements across Federal agencies. While we understand that harmonization requires the cooperation of other Federal agencies through the coordinating efforts of the Cyber Incident Reporting Council, we encourage you to consider how the final rule will impact the ability of CISA to harmonize CIRCIA requirements with other existing Federal agency incident reporting mandates.

One aspect of CIRCIA designed to reduce duplicative reporting requirements is the provision exempting covered entities from CIRCIA reporting requirements if they have reported substantially similar information to another agency and that agency has an information sharing agreement in place with CISA.[35] As you finalize the rule, we encourage you to ensure that the definition of substantially similar information provides enough flexibility to facilitate the use of this reporting exemption. Considering the wide variety of information required by different regulatory agencies, a too rigid approach to defining substantially similar information could risk rendering this provision ineffective.

As CISA refines requirements on the information that reporting entities must submit as part of an incident report, we encourage you to balance CISA's need for information with the risk that excessive mandates could inhibit regulatory harmonization efforts.

III. Ongoing Stakeholder Input

As you continue your evaluation of submitted comments in advance of the publication of the final rule in September 2025, we encourage you to consider more flexible opportunities for receiving feedback from relevant stakeholders. Proper implementation of CIRCIA requires a full understanding of the many technical issues involved in a rule of this significance and complexity, and consultation with impacted entities will be essential to determining how the rule will affect

[35] 6 U.S.C. 681b(b)(5)(B)

critical infrastructure. We are concerned that limiting feedback to written comments received in advance of the published deadline will be insufficient for CISA to fully engage with stakeholders.

We encourage CISA to develop a process that facilitates ongoing, transparent stakeholder engagement. We understand the complexity of CIRCIA rulemaking is burdensome on CISA's limited resources, but the significance of this rule requires fulsome stakeholder engagement. We are confident that if CISA engages in ongoing stakeholder engagement to receive necessary clarification and context on written submissions, it can develop a process in line with the Administrative Conference's recommendations that efficiently utilizes CISA's resources, ensures public transparency, and maximizes stakeholder input.

IV. Miscellaneous

Digital Security

CIRCIA reports and responses to Requests for Information will be attractive targets for our adversaries and CISA must undertake every effort to protect them. The NPRM states that CISA will protect CIRCIA reports, responses to Requests for Information, and related information "in accordance with the requirements for moderate impact Federal information systems, as described in Federal Information Processing Standards Publication (FIPS) 199."[36] In light of recent compromises[37] and the nature of the information that will be reported to CISA, we urge you to consider protecting CIRCIA information in accordance with the requirements for high impact Federal information systems, as described in FIPS 199.[38]

Building Confidence in CIRCIA through Transparency and Buy-In

No formula can ensure that CIRCIA reporting detects every malicious cyber campaign or identifies every new adversary trend or tactic, but we are confident that it will serve as a catalyst to mature existing operational collaboration efforts. We are also confident in CISA's ability to work with the stakeholder community to get the final rule right and continue to build the analytical capacity that will be necessary to process, analyze, and action CIRCIA reports.

Despite our confidence, the stakeholder community has raised concerns about the trajectory of CIRCIA implementation. In our view, more robust engagement with the private sector and increased transparency about how CISA plans to execute its CIRCIA obligations will build the stakeholder confidence necessary to generate buy-in for the program. In addition to establishing a transparent process for accepting ongoing stakeholder input as CISA develops the final rule, there are several aspects of CIRCIA implementation that CISA can engage stakeholders on now, and we encourage CISA to do so. For example, CISA suggests advances in technology will enable the technical capacity to rapidly process cyber incident reports and identify actionable security

---

[36] 89 Fed. Reg. at 23741.

[37] *See* Benedict Collins, *CISA Warns Chemical Facilities May Have Been Hacked in CSAT Breach,* TechRadar (Jun. 25, 2024), https://www.techradar.com/pro/cisa-warns-chemical-facilities-may-have-been-hacked-in-csat-breach.

[38] *See* Federal Information Processing Standards Publication: Standards for Security Categorization of Federal Information and Information Systems, Nat'l Inst. on Standards and Tech. (Feb. 2004), https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf.

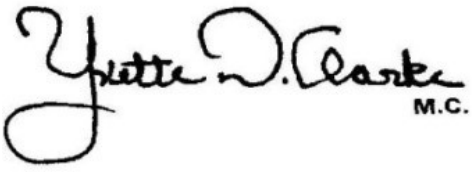
information.[39] CISA should consult with stakeholders to ensure confidence in whatever technology it chooses to use to process and analyze reports so stakeholders have confidence in the insights derived and shared more broadly. Additionally, CISA can engage stakeholders on what kind of products developed from CIRCIA data would be beneficial to critical infrastructure.

Our shared goal is CISA's successful implementation and administration of CIRCIA. That success rests on both CISA's ability to rapidly ingest incident reports, analyze data, and action insights and on the buy-in from the stakeholder community. We look forward to continuing to work with CISA on the successful implementation of CIRCIA.

Sincerely,

Bennie G. Thompson
Ranking Member
Committee on Homeland Security

Eric M. Swalwell
Ranking Member
Subcommitte on Cybersecurity and
Infrastructure Protection



Yvette D. Clarke
Member of Congress

[39] 89 Fed. Reg. at 23652.