Charles Crain

Vice President,
Domestic Policy

July 2, 2024

Jennie M. Easterly
Director, Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
CISA - NGL Stop 0630
1110 N. Glebe Road
Arlington, VA 20598-0630

Re: Docket No. CISA–2022–0010, Cyber Incident Reporting for Critical Infrastructure Act Reporting Requirements

Dear Director Easterly,

The National Association of Manufacturers ("NAM") appreciates the opportunity to provide comments to the Cybersecurity and Infrastructure Security Agency ("CISA") of the Department of Homeland Security ("DHS" or "the Department") in response to its proposed rule to implement the requirements of the Cybersecurity Incident Reporting for Critical Infrastructure Act ("CIRCIA") requirements.[1]

The NAM is the largest manufacturing association in the United States, representing 14,000 manufacturers of all sizes, in every industrial sector and in all 50 states. Manufacturing employs nearly 13 million people across the country, contributing $2.89 trillion annually to the U.S. economy.[2] The NAM is the voice of the manufacturing community and the leading advocate for a policy agenda that helps manufacturers compete in the global economy and create jobs across the United States.

Manufacturers of all sizes and in all sectors understand that protecting their enterprises from cybersecurity risk is critical to their success in today's economy. Through comprehensive and connected relationships with customers, vendors, suppliers and governments, manufacturers are entrusted with vast amounts of highly sensitive data and intellectual property. The industry takes seriously its responsibility to secure information, networks, facilities and critical infrastructure against attacks by nation-state, criminal and other malicious actors. Manufacturers also know that cybersecurity is a shared responsibility, and the industry appreciates efforts by CISA and the Department of Homeland Security to build a collaborative and productive partnership with the private sector.

As CISA works to implement the reporting requirements created by CIRCIA, the NAM respectfully encourages the agency to drastically reduce the number of entities required to report, and the number of incidents they have to report. Doing so will ensure that CISA receives

[1] Federal Register Vol. 89, No. 66, Thursday, April 4, 2024, available at https://www.govinfo.gov/content/pkg/FR-2024-04-04/pdf/2024-06526.pdf
[2] National Association of Manufacturers, Facts About Manufacturing, available at https://nam.org/manufacturing-in-the-united-states/facts-about-manufacturing-expanded/

useful information about cybersecurity incidents—without overburdening manufacturers with overbroad and unworkable disclosure requirements.

CISA should limit the volume of reported cyber incident information

The stated purpose of requiring Covered Cyber Incident Reports from Covered Entities is to "assess the effectiveness of security controls, identify tactics, techniques, and procedures adversaries use to overcome those controls and other cybersecurity purposes, including to assess potential impact of cyber incidents on public health and safety and to enhance situational awareness of cyber threats across critical infrastructure sectors."[3]

Achieving such a purpose will depend on CISA's ability to process and act upon Covered Cyber Incident Reports. It is thus worth noting that, according to CISA's own estimates, in the 2026-2033 period CISA expects to receive between 83,760 and 463,850 CIRCIA reports—i.e., an average of about 10,000 to more than 57,000 reports per year.[4] Although automated technical systems, including those powered by artificial intelligence, can provide valuable assistance in the analysis and exploitation of incident reports, they cannot fully replace the work of humans. As the proposed rule says, "additional staffing would be necessary to conduct *a myriad of mission-critical activities*, such as analyzing the CIRCIA Reports to conduct trend and threat analysis, vulnerability and mitigation assessment, the provision of early warnings, incident response and mitigation, supporting Federal efforts to disrupt threat actors, and advancing cyber resiliency."[5] This is an acknowledgement by CISA that it will not be able to automate itself out of the challenge of sifting through and extracting actionable intelligence from large numbers of reports, and then disseminating that intelligence to its public and private sector partners. In other words, CISA acknowledges that this challenge will need to be met with a commensurate number of human cyber experts.

By some estimates, by 2030 the global shortage of cybersecurity talent could reach 85 million workers.[6] Even if one were to assume that Congress will appropriate to CISA the full funding necessary to recruit very large numbers of cyber experts, one knows that such a shortage means CISA will not be able to hire nearly as many experts as it will need.

This is why manufacturers harbor significant concerns about the extent to which CIRCIA reports, as envisaged by the proposed rule, will be underused—or potentially remain unused altogether—by CISA.

This prospect must be weighed against the clear downsides a covered entity will experience from having to report cyber incidents under CIRCIA. Just as CISA is extremely unlikely to find, let alone hire, cyber experts in sufficient numbers to process and leverage CIRCIA reports, industry faces the same challenge to manage and secure its own systems and networks. Any diversion of information technology ("IT") and incident response personnel towards reporting while in the midst of stopping, mitigating and recovering from a cyber incident lessens the likelihood that cyber incident response will be as rapid and effective as possible. This diversion can only be justified by the extent to which each CIRCIA report effectively contributes to CISA's cybersecurity mission. Conversely, any CIRCIA report that CISA is unable to fully leverage is a

[3] 6 U.S.C. 681a.
[4] Proposed rule, p. 23744.
[5] Proposed rule, p. 23749 (emphasis added).
[6] The $8.5 Trillion Talent Shortage, Korn Ferry, available at https://www.kornferry.com/insights/this-week-in-leadership/talent-crunch-future-of-work

clear loss for cybersecurity—that of the nation, and that of the covered entity that made that report.

The NAM therefore respectfully urges CISA to adjust the quantity of information it will receive to its ability to process and act upon that information. Simply put, if it will not be processed and acted upon, it should not be required to be reported.

1. Narrow the scope of "covered entities"

CISA estimates that 316,244 entities would be in the scope of the proposed rule. That extremely high number is a major contributor to the excessive number of incident reports, discussed above, that CISA expects to receive. Manufacturers respectfully urge CISA to consider, as a matter of priority, narrowing the scope of "covered entities." In this spirit, the NAM respectfully recommends using two criteria to define covered entities: 1.) they should own or operate particularly sensitive critical infrastructure systems and assets, and 2.) they should exceed a small business size standard.

1.1. Focus on owners or operators of critical infrastructure systems and assets

The NAM opposes the inclusion, in section 226.2(a) of the proposed rule, of any entity that is "in a critical infrastructure sector."

Manufacturers disagree with CISA's explicit rejection in section 226(a) of the "systems and assets approach" taken by Presidential Policy Directive 21, i.e., an approach focused on entities that own or operate critical infrastructure. First, this is at odds with a plain reading of the text of the CIRCIA statute itself, which defines a covered entity as "an entity in a critical infrastructure sector, *as defined in Presidential Policy Directive 21*."[7]

Second, it is also at odds with the intent of the statute, which was confirmed recently by its original sponsor, Rep. Yvette Clarke (D-NY). Rep. Clarke stated that the "consensus" among CIRCIA's congressional champions was that the implementation of CIRCIA would "benefit from a well-scoped incident reporting framework," and that Congress "[did] not expect all critical infrastructure owners and operators to be subject to [CIRCIA's] reporting requirement."[8] Congressional intent to exclude from CIRCIA's scope certain owners or operators of critical infrastructure can only mean that, by extension, entities that neither own nor operate critical infrastructure and are merely "in" a critical infrastructure sector should clearly find themselves outside that scope.

Third, the inclusion of entities that do not own or operate critical infrastructure would be at odds with the critical infrastructure mission of CISA and of the Department, which is framed by National Security Memorandum 22 of April 30, 2024 (which rescinded and replaced PPD-21): protecting "the physical and virtual assets and systems so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security, national economic security, or national public health or safety."[9]

---

[7] See 6 U.S.C. 681(4) (emphasis added).

[8] Remarks by Rep. Yvette Clark, hearing on "Surveying CIRCIA: Sector Perspectives on the Notice of Proposed Rulemaking," Subcommittee on Cybersecurity and Infrastructure Protection, Committee on Homeland Security, U.S. House of Representatives, May 1, 2024, available at https://homeland.house.gov/hearing/surveying-circia-sector-perspectives-on-the-notice-of-proposed-rulemaking/

[9] National Security Memorandum 22, available at https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/

Fourth, imposing a regulatory requirement on entities solely because they are in a critical infrastructure sector even though they do not own or operate critical infrastructure would create a disincentive for such entities to participate in sector risk management partnership activities. This public-private partnership has always been voluntary, capitalizing on the willingness of private sector companies and experts to support sector-wide information sharing, risk assessment and the development of risk mitigation practices. By stating that "some entities that do not own or operate systems or assets that meet the definition of critical infrastructure in PPD-21 but are active participants in critical infrastructure sectors and communities, are considered 'in a critical infrastructure sector,'"[10] CISA appears to make that active participation in a voluntary and collaborative endeavor an indicator that entities can and should be regulated under CIRCIA. This would subvert these vital public-private partnerships and thus harm industry participants' work to protect homeland security.

That is why the NAM respectfully opposes defining any entity "in" a critical infrastructure sector as a "covered entity," and recommends that the final rule only include, though with some adaptations, the sector-based criteria of section 226.2(b).[11]

1.2. Clarify the criterion of the critical manufacturing sector

The proposed rule designates as covered entities those that meet one or more of the 16 sector-based criteria. The NAM broadly supports such a targeted approach because it is appropriately focused on owners and operators of particularly sensitive critical infrastructure. We note, however, that this approach accounts for almost 90% of the 316,244 entities estimated to be in the scope of the proposed rule.[12] As we have said in the introduction and first section of this submission, this represents excessively broad coverage, which the NAM believes can and should be drastically narrowed in a manner that nevertheless enables CISA to fulfill its CIRCIA mandate.

One way to do that is to clarify and narrow the criterion for the critical manufacturing sector. The proposed rule defines the criterion by reference to four North American Industry Classification System codes:

- NAICS Subsector 331 for Primary Metal Manufacturing;
- NAICS Subsector 333 for Machinery Manufacturing;
- NAICS Subsector 335 for Electrical Equipment, Appliance, and Component Manufacturing; and
- NAICS Subsector 336 for Transportation Equipment Manufacturing.

This approach has the unnecessary effect of including all companies engaged in the manufacturing of every single type of product within these broad NAICS subsectors, even if any disruption or interruption in their production would not have a "debilitating impact on national security, national economic security, or national public health or safety," to quote again from NSM-22. For example, Machinery Manufacturing comprises specific product categories that

[10] Proposed rule, p. 23676.
[11] Note that, as explained below in section 2.1 of this submission, manufacturers recommend that the scope of reportable cyber incidents be narrowed to focus on incidents that affect the operation of critical infrastructure systems or assets—in other words, the critical infrastructure part of a critical infrastructure entity. The fact that an entity is "covered" by virtue of its ownership or operation of critical infrastructure systems or assets does not mean that everything that company does, owns or operates is critical infrastructure.
[12] See table 1 on p. 23742 of the proposed rule.

serve a valuable economic function but upon whose uninterrupted production the security of our homeland is not dependent, such as Lawn and Garden Tractor and Home Lawn and Garden Equipment Manufacturing (NAICS code 333112). Another example can be found in the Primary Metal Manufacturing subsector, which includes Metal Kitchen Cookware, Utensil, Cutlery, and Flatware (except Precious) Manufacturing (NAICS code 332215), which itself covers the manufacturing of barbers' scissors. At a minimum, we recommend that CISA drill down much more granularly—below 6-digit NAICS codes—to only cover the manufacturing of specific product categories that are genuinely critical to our national security, national economic security, or national public health or safety.

1.3. Apply and clarify the small business size thresholds

Another effective and necessary way to reduce the number of entities that meet a sector-based criterion would be to exclude small businesses. We understand that CISA did not propose using small business size thresholds for entities that meet a sector-based criterion (sec. 226.2(b)), but for entities in a critical infrastructure sector (sec. 226.2(a)). However, excluding small businesses that otherwise meet a sector-based criterion from the requirement to report cyber incidents to CISA is appropriate because, by virtue of their small size, any disruption of their activity would be of limited if not negligible effect on national security, national economic security or national public health or safety. Additionally, imposing complex reporting requirements on small businesses would be costly and burdensome for them.

Finally, we recommend the following clarification in the application of the small business size standard specified by the applicable NAICS code in the U.S. Small Business Administration's Small Business Size Regulations.[13] Each code sets a size threshold for each company engaged in the corresponding business activity (e.g. Farm Machinery and Equipment Manufacturing, NAICS code 333111, size threshold 1,250 employees; Construction Machinery Manufacturing, NAICS code 333120, size threshold 1,250 employees). However, many companies will find themselves engaged in more than one single line of business, and their overall size may put them above the size threshold for any one of their lines of business even though the number of employees supporting each line of business does not exceed the size threshold for the corresponding line of business. For example, a company could have 700 employees (i.e., below the 1,250 threshold) in its Farm Machinery and Equipment Manufacturing business unit, and 800 employees in another non-critical line of business, thus totaling 1,500 employees, which would put the company above the 1,250-employee threshold. To avoid this unnecessary inclusion in the scope of covered entities, the final rule should specify that size should be calculated separately for each line of business that is deemed critical for CIRCIA purposes.

2. Narrow the scope of reportable cyber incidents

The NAM respectfully submits for CISA's consideration two suggestions to further reduce the volume of reportable cyber incident information, which as explained above would lessen the diversion of critical infrastructure owners' and operators' resources away from incident response. The first is to narrow the definition of "substantial cyber incidents" that the proposed rule requires to be reported to CISA, while still comporting with the letter and the spirit of the statute; and the second is to more vigorously pursue harmonization of cyber incident reporting requirements across federal agencies.

[13] As set forth in 13 CFR part 121.

2.1. Narrow the definition of substantial cyber incidents

The NAM respectfully recommends amending the definition of substantial cyber incident in sec. 226.1 of the proposed rule as follows:

> *Substantial cyber incident means a cyber incident that leads to any of the following, whether or not 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:*
>
> *(1) A critical [substantial] loss of confidentiality, integrity or availability of a covered entity's information system or network, or of nonpublic information contained therein, upon which the operation of the covered entity's critical infrastructure systems or assets depends;*
> *(2) A critical [serious] impact on the safety and resiliency of a covered entity's operational systems and processes upon which the operation of the covered entity's critical infrastructure systems or assets depends;*
> *(3) A critical disruption of the operation of a covered entity's critical infrastructure systems or assets. [ability to engage in business or industrial operations, or deliver goods or services;*
> *(4) Unauthorized access to a covered entity's information system or network, or any nonpublic information contained therein, that is facilitated through or caused by a:*
> *(i) Compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or*
> *(ii) Supply chain compromise].*
> *(5) A "substantial cyber incident" resulting in the impacts listed in paragraphs (1) through (3) in this definition includes any cyber incident regardless of cause, including, but not limited to, any of the above incidents caused by a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; a supply chain compromise; a denial-of-service attack; a ransomware attack; or exploitation of a zero-day vulnerability.*

These proposed edits of the definition of substantial cyber incident would yield the following benefits:

- Raising the threshold from "substantial" and "serious" (prongs (1) and (2)) to "critical," while adding the same requirement of criticality of the disruption to prong (3), would curb the overreporting discussed above while still achieving CIRCIA's objective of ensuring that CISA is informed of consequential cyber incidents.
- Tying each of these three prongs to the operation of critical infrastructure systems or assets, in keeping with the letter and spirit of the CIRCIA statute and with CISA's mission,[14] would ensure that CISA receives reports focused on threats to critical infrastructure, rather than on threats to non-critical parts of a covered entity, and thus curb the overreporting discussed above.
- Subsuming the fourth prong into the definition's introduction serves two purposes. First, more and more companies rely on cloud services, managed services or other third-party data hosting services in lieu of owning and operating the totality of their information systems and networks. Therefore, applying a different impact threshold to instances of

[14] See part 1.1. of this submission.

unauthorized access through one of these service providers would lead to inconsistent reporting. Second, the absence of an impact threshold for the fourth prong would vastly and unnecessarily increase the number of incident reports. We note that this would also render the fifth prong, whose purpose and effect are unclear, unnecessary.

Manufacturers believe that these proposed edits would make the definition of "substantial cyber incident" clear and thus easy to apply for both CISA and covered entities. Further, whatever the final wording of the definition of reportable incidents, the NAM recommends that the outreach and education campaign that CIRCIA requires CISA to conduct feature practical explanations and examples of the types of incidents that present the features and reach the levels of severity that will fit the final definition.

2.2. Harmonize federal cyber incident reporting requirements

As explained above, manufacturers have two essential and related objectives: minimize the diversion of IT and incident response personnel away from these duties and towards regulatory reporting, and ensure that CISA can manage the volume of reported cyber incident information. This requires a drastic reduction of this volume. Vigorously pursuing harmonization of cyber incident reporting requirements across federal agencies would make a significant contribution towards reaching that goal. The NAM is concerned that the proposed rule does not sufficiently prioritize such harmonization.

In its Sept. 19, 2023, report to Congress mandated by sec. 107(d)(1) of CIRCIA, DHS identified no fewer than "52 in-effect or proposed federal cyber incident reporting requirements," and commented that this "highlights potentially duplicative Federal reporting."[15] This situation is simply untenable for private sector entities—even more so considering, as we explain above, that incident reporting inevitably draws resources from the essential and time-sensitive mission of stopping, mitigating and recovering from the cyber incident.

The proposed rule exempts covered entities from their obligation to report cyber incidents to CISA under CIRCIA if they must report these incidents to another federal agency. Unfortunately, this exemption suffers from two major flaws. First, it only applies to reporting requirements of "substantially similar information within a substantially similar timeframe." Second, it only applies if that federal agency has an information sharing agreement in place with CISA. Considering that CISA inventoried no fewer than 52 federal cyber incident reporting requirements, it is doubtful that it will be able to conclude a meaningful number of such agreements within a reasonable time after it has finalized its own CIRCIA reporting requirements. The NAM respectfully recommends that CISA develop a roadmap to negotiate and conclude such agreements on an expedited basis, with priority given to those that would exempt from CIRCIA reporting the greatest number of covered entities. We also recommend that CISA exempt, on a provisional basis, covered entities that are already required to report to other federal agencies with which CISA is likeliest to reach an agreement in a reasonable timeframe, to avoid imposing on such covered entities a compliance burden that is likely to be rendered unnecessary soon thereafter.

[15] Harmonization of Cyber Incident Reporting to the Federal Government, available at https://www.dhs.gov/publication/harmonization-cyber-incident-reporting-federal-government

3. Lighten and protect the contents of cyber incident reports

3.1. Lighter cyber incident reporting requirements

In addition to sec. 226.7's requirement to provide CISA with information identifying the covered entity and how to contact it, sec. 226.8, 226.9 and 226.11 detail the cyber incident information, ransom payment information, and supplemental report information, respectively, that should be reported to CISA. Given how detailed, lengthy and granular these lists are, manufacturers are concerned that this heavy and intrusive burden will force covered entities to dedicate an excessive amount of time and effort of their IT and incident response personnel to CIRCIA reporting, to the detriment of actually stopping, mitigating and recovering from the cyber incidents they experience.

The NAM therefore recommends that CISA significantly trim down the requirements of sec. 226.8 and 226.9, more closely following the cyber event reporting form it developed in April 2022 in the wake of CIRCIA's enactment, which provides a much more manageable list of "10 key elements to share."[16] The final rule should also modify sec. 226.11 to provide that it will then be in the course of CISA's provision of incident response assistance to the covered entity—if CISA offers such assistance and the covered entity is able to accept that offer—that CISA itself will be able to collect some of the more detailed incident information listed in sec. 226.8 and 226.9.

3.2. Stronger protections for the contents of cyber incident reports

Manufacturers are concerned about the protections their CIRCIA reports will be afforded once they are in CISA's custody. First, the quantity and extreme sensitivity of the incident information and ransom payment information required by sec. 226.8 and 226.9 constitute a roadmap for any malicious cyber actor who may be able to compromise the security of CISA's incident information repository. It is thus of paramount importance that CISA develop, resource and implement the most robust security posture to protect that information, heeding the cybersecurity adage "if you can't protect it, don't collect it."

Second, incident or ransom payment reports made pursuant to the proposed rule should be afforded the full legal protections stipulated by the statute itself, including exemption from the Freedom of Information Act, confidentiality safeguards, and prohibitions against legal disclosure and against use in regulatory and enforcement proceedings.[17] The NAM is concerned that the proposed rule arguably departs from the statute in a subtle but important manner. CIRCIA provides that "a Federal, State, local, or Tribal government shall not use information about a covered cyber incident or ransom payment obtained solely through reporting directly to [CISA] in accordance with this subtitle to regulate,"[18] and that "the liability protections provided in this subsection shall only apply to or affect litigation that is solely based on the submission of a covered cyber incident report or ransom payment report to the Agency." By contrast, the proposed rule explains that "a forensic incident report that was developed for the purpose of investigating the underlying incident, which happened to have been used in populating a CIRCIA Report or response to an RFI, would not be ''created for the sole purpose of preparing,

[16] Sharing Cyber Event Information: Observe, Act, Report, available at https://www.cisa.gov/sites/default/files/2023-01/Sharing_Cyber_Event_Information_Fact_Sheet_FINAL_v4.pdf
[17] 6 U.S.C. 681e.
[18] See (a)(5) PROHIBITION ON USE OF INFORMATION IN REGULATORY ACTIONS, and (c)(2) SCOPE [OF LIABILITY PROTECTION], in 6 U.S.C. 681e.

drafting, or submitting'' a CIRCIA Report or response to an RFI. Therefore, CISA's view is that this bar would not create a defense to discovery for a record."[19]

While information and documents that pre-existed the cyber incident could understandably not benefit from the liability and regulatory protections of CIRCIA, the NAM respectfully disagrees with CISA's analysis that a forensic incident report, and other similar items generated by the efforts of the covered entity (and of its service providers) to understand, stop, mitigate and recover from an incident should not be afforded such protections. No meaningful distinction can be drawn between various incident response efforts. If, for example, an incident analysis can be used both to inform the company's leaders as well as to populate a report to CISA, it should be. If it cannot, then covered entities might not use the information and insights contained in such documents to inform CISA, leading to less informative—or uninformative—CIRCIA reports; alternatively, they might opt not to write up any analysis without ensuring it is either addressed to or authored by legal counsel, and thus privileged. The NAM recommends that the final rule clarify that all information and documents pertaining to incident analysis and response be afforded the legal protections of CIRCIA.

Third, the NAM recommends, contrary to what is stated in the proposed rule,[20] that the final rule clarify that where an employee of an organization that is experiencing a cyber incident (or of a service provider to such an organization) elects to report an incident despite not having authority from the entity to report on its behalf, the information contained in such a report should be imputed to the entity experiencing the incident and thus be considered a report submitted for the purposes of CIRCIA compliance that benefits from the legal protections discussed above. To do otherwise would create unwarranted legal liability for bona fide reporting, filed in the midst of the confusion that can surround a cyber incident, by individuals who may not have known that they were not properly and fully authorized to report on behalf of their employer (or customer of their employer).

* * * *

Manufacturers thank CISA for this opportunity to support the development of a rule implementing CIRCIA that contributes to improved public-private, sectoral and cross-sectoral information sharing and supports rather than impedes the incident response efforts of critical infrastructure owners and operators that are targeted by malicious cyber actors. The NAM looks forward to continuing to work with CISA in pursuit of this goal throughout the rulemaking process.

Sincerely,

Charles Crain
Vice President, Domestic Policy

[19] Proposed rule, p. 23739.
[20] Footnote 368 of the proposed rule, p. 23728.