Business Roundtable

1000 Maine Avenue, SW, STE 500
Washington, DC 20024
202.872.1260
brt.org

July 3, 2024

RE: Comments on 89 Fed. Reg. 23644 (April 4, 2024); RIN 1670-AA04; Docket number CISA-2022-0010

Business Roundtable (BRT) appreciates the opportunity to comment on the Cybersecurity and Infrastructure Security Agency's (CISA) proposed regulation implementing the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) reporting requirements.[1]

BRT is an association of more than 200 chief executive officers (CEOs) of America's leading companies, representing every sector of the U.S. economy. BRT CEOs lead U.S.-based companies that support one in four American jobs and almost a quarter of U.S. GDP. BRT member companies invest heavily in cybersecurity safeguards designed to protect sensitive information and implement robust compliance programs.

Regulatory requirements should be appropriately scoped to address consumer protections and national security risks while avoiding unnecessary impacts on business operations, customer services or global competitiveness. BRT urges CISA to tailor the proposed rule to avoid unnecessary redundancy of cyber incident reporting while focusing its resources on the covered entities and incidents of greatest impact to cybersecurity. CISA should not move to finalize the proposed rule until it has addressed the various recommendations within this letter.

Below, BRT answers key questions posed by the proposed rule.

A. Potential Approaches to Harmonizing CIRCIA's Regulatory Reporting Requirements with Other Existing Federal or SLTT Laws, Regulations, Directives, or Similar Policies [Q1]

Harmonizing CIRCIA's reporting requirements with existing laws and regulatory requirements is needed to promote an effective, efficient and cohesive cybersecurity reporting ecosystem. Effective cyber incident reporting mechanisms can be useful to strengthen awareness of cyber threats and trends. However, this potential value must be balanced against avoiding redundant or conflicting compliance requirements, especially for businesses operating across multiple regulatory structures and/or jurisdictions. Congress recognized this priority in CIRCIA by creating an exemption for substantially similar reporting requirements and directing the

[1] Proposed Rule Cyber Incident Reporting for Critical Infrastructure Act Reporting Requirements, Cybersecurity and Infrastructure Security Agency, 89 Fed. Reg. 23644, Apr. 4, 2024, https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements.

Department of Homeland Security (DHS) to establish the Cyber Incident Reporting Council (CIRC).[2] The White House also recognizes that the lack of cybersecurity regulatory harmonization and reciprocity poses a challenge to cybersecurity outcomes and business competitiveness across sectors.[3]

Streamlined reporting requirements across jurisdictions and sectors will avoid the drain on resources for organizations working quickly to mitigate a serious cyber incident while complying with reporting requirements. Importantly, compliance burdens stemming from reporting requirements do not end after report submission; reporting can trigger requests for additional documentation, interviews, audits or assessment reports. As noted in the CIRC report, 52 cyber incident reporting requirements are either in effect or proposed across the federal government, including requirements across 22 agencies.[4] Due to differing reporting mechanisms, entities regulated by more than one agency are required to submit multiple reports at the same time that they are managing and responding to an incident and its immediate impact. Further, many companies in critical infrastructure sectors also face cyber incident reporting duties in other countries.

CISA should leverage its CIRCIA implementation process to establish a common reporting framework. This could include developing unified reporting standards that reflect commonalities with other existing federal and state, local, tribal and territorial (SLTT) laws to reduce confusion, address conflicting requirements and streamline compliance efforts. We urge CISA to work with agencies and other regulators to standardize definitions of key terms such as "cyber incident" and "substantial cyber incident" across all regulations. Further, as indicated in the CIRC report, the federal government should adopt a model definition of a "reportable cyber incident" wherever practical and work to adapt current and future cyber incident reporting requirements.[5] Standard definitions will increase clarity and allow companies to direct resources towards incident response and reporting by avoiding substantial unnecessary compliance costs associated with understanding the nuances of different definitions. Except where there are compelling and necessary reasons, federal and SLTT agencies should accept cyber incident reports that are consistent with the model definitions as sufficient to fulfill other cyber incident reporting requirements elsewhere in law.

To further help with streamlining reporting, CISA should also develop a secure portal that can serve as a centralized point for the private sector to submit cyber incidents. The portal submissions can be distributed to required federal and SLTT agencies. A single reporting

---

[2] 6 U.S.C. § 681f.

[3] Office of the National Cyber Director, We Need to Harmonize Cybersecurity Regulations, What We Heard From our Partners, White House, Jun. 4, 2024, https://www.whitehouse.gov/oncd/briefing-room/2024/06/04/we-need-to-harmonize-cybersecurity-regulations-what-we-heard-from-our-partners.

[4] Department of Homeland Security, Harmonization of Cyber Incident Reporting to the Federal Government, Sep. 19, 2023, pg. 9, Appendix B, https://www.dhs.gov/sites/default/files/2023-09/Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf.

[5] Ibid.

gateway with uniform submission processes would reduce the administrative burden on entities required to report similar incidents to multiple agencies. Given the sensitive nature of the information provided, it should be clear to reporting entities which agencies and who within those agencies have access to the information provided in the reports, either through a notification process or other transparency measures.

At the same time, covered entities that submit CIRCIA-compliant incident reports should be granted the option of using the CIRCIA reports for compliance with other cyber incident reporting regulations or submitting separate reports. The centralized cyber incident reporting portal and web form should enable covered entities to indicate whether they wish for their CIRCIA report to also be used for compliance with separate cyber incident reporting regulations. Covered entities should retain the option to submit separate reports if desired or appropriate.

If the proposed rule is finalized without the addition of the streamlining mechanisms enumerated above, many companies will be faced with uncertainty and unnecessary compliance burdens.

B. How to Reduce Actual, Likely, or Potential Duplication or Conflict Between Other Federal or SLTT Laws, Regulations, Directives, or Policies and CIRCIA's Reporting Requirements [Q2]

While BRT appreciates CISA's efforts to facilitate harmonization through the CIRC and other initiatives, more work is needed to reduce conflicting requirements. In particular, DHS and the Administration should coordinate with independent agency regulators such as the U.S. Securities and Exchange Commission, SLTT agencies and international partners on more consistent cyber reporting requirements and processes.

Options for harmonization could include seeking regulatory amendments to impose greater consistency for existing cyber incident reporting laws, in coordination with industry stakeholders, and establishing formal mechanisms for cross-agency collaboration where multiple regulations overlap. CISA, the White House Office of the National Cyber Director and other federal partners should work to consolidate similar reporting forms, synchronize reporting deadlines and standardize data elements towards the goal of a uniform cyber incident reporting process.

As part of implementation, CISA should also establish a regulatory feedback mechanism for businesses to provide information on the operational challenges they encounter due to redundant or conflicting reporting requirements. CISA should also use the feedback to consider the extent to which reporting is achieving its regulatory objectives, in particular the goal of information sharing expressed in this Notice of Proposed Rule Making (NPRM). Some cyber incident reporting regulatory requirements have only come into force relatively recently, and

their implementation challenges are still emerging. CISA could use the feedback it receives through this mechanism to continuously improve regulatory approaches and harmonization efforts.

C. Proposed Definitions of Cyber Incident, Covered Cyber Incident, and Substantial Cyber Incident [Q3]

CISA's broad interpretations of "covered cyber incident" and "covered entity" may lead to many more incident reports per covered entity than anticipated. While the first two types of covered incidents are caveated by the words "substantial" and "serious," the types of incident in paragraph (3) – the disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services – or in paragraph (4) – the unauthorized access to information – do not have a similar caveat. This is likely to lead to a much larger-than-expected volume of inconsequential reports and could hinder a primary purpose of CIRCIA, which is to share actionable information that can strengthen cybersecurity. In the NPRM, CISA notes "there is a great deal of uncertainty regarding the number of CIRCIA Reports that would be required to be submitted upon implementation of this proposed rule."[6] A focus on higher priority reporting would help to reduce the number of reports and maximize CISA's capacity to leverage the information received.

BRT recommends against defining "covered cyber incidents" to include all substantial cyber incidents experienced by a covered entity.[7] Within CIRCIA, Congress defined a covered cyber incident as "a substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established by the Director [of CISA] in the final rule[.]"[8] Congress also instructed CISA to consider the severity of impact in deciding what types of substantial cyber incidents constitute covered cyber incidents.[9] A more focused definition of "covered cyber incidents" would be consistent with a risk management approach and would better leverage the limited resources of CISA and incident responders for more actionable reports.

CISA should leverage the National Cyber Incident Scoring System and define "covered cyber incident" to encompass substantial cyber incidents that result in demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties or public confidence.[10] This aligns with the descriptions of "critical infrastructure" in NSM-22 and 6 U.S.C. § 101(4) as assets so vital to the United States that their disruption would have a

[6] 89 Fed. Reg. 23743.
[7] 89 Fed. Reg. 23660-23661.
[8] 6 U.S.C. § 681(3).
[9] 6 U.S.C. § 681b(c)(2)(B).
[10] CISA National Cyber Incident Scoring System, High (Orange), Sep. 30, 2020, https://www.cisa.gov/news-events/news/cisa-national-cyber-incident-scoring-system-nciss.

debilitating impact on security, national economic security, or national public health or safety.[11] The covered cyber incident should focus on the information and systems that directly relate to the covered entity's provision of a National Critical Function and the covered entity's participation in a critical infrastructure sector. Many businesses with a digital presence experience routine or negligible security events at the medium, low and baseline levels of the National Cyber Incident Scoring System, which do not indicate a "substantial" incident with a realistic risk of systemic damage. Creating a common scale for measuring the severity of cyber incidents, based on the National Cyber Incident Scoring System, would help reduce confusion, especially for entities reporting to multiple authorities.

In a few instances a cyber incident should be excluded from mandatory reporting requirements. First, CISA should clarify that non-exploited vulnerabilities are excluded from any reporting requirements. The final rule should also clarify that "substantial cyber incident" does not include an event where the cyber incident is perpetrated 1) in good faith but in error, such as an employee's technical mistake causing a brief outage; or 2) by good faith security research, including independent research performed out of scope of a vulnerability disclosure policy or bug bounty.[12] Though neither scenario may be "in response to a specific request by the owner or operator of the information system," neither scenario involves malicious intent or a "cybersecurity threat" seeking to adversely impact information or systems.[13]

CISA should provide more examples of cyber incidents that may or may not be covered to better inform businesses and reduce subjectivity in determinations of covered cyber incidents. While the examples of significant incidents and incidents unlikely to qualify are helpful, a greater scale of examples would provide clearer guidelines for covered entities.

D. Adding qualifiers to subparagraph 3 of the definition of substantial cyber incident [Q4]

CISA should add a qualifier to subparagraph 3 of the definition of "substantial cyber incident" to clarify the required level of impact on a disruption of a covered entity's ability to engage in business or operations.[14] While adding "substantial" or "significant" to the beginning of the subparagraph, as CISA proposes, would be helpful, such terms alone are insufficiently detailed or defined for conveying the seriousness of the incident. As currently drafted, a lack of definitional clarity and misaligned definitions across federal statutes will lead to inconsistent reporting across covered entities. Adding these qualifiers aligns with the recommendation above to revise the definition of "covered cyber incident" to incorporate language from high-

[11] White House, National Security Memorandum Critical Infrastructure Security and Resilience (NSM-22), Apr. 30, 2024, https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/.
[12] 89 Fed. Reg. 23661, 23667.
[13] 6 U.S.C. § 650(8)(A).
[14] 89 Fed. Reg. 23675.

level (orange) incidents in the National Cyber Incident Scoring System, which uses a repeatable and consistent mechanism for estimating the risk of an incident to critical infrastructure.[15]

In addition, CISA should consider adding a qualifier to subparagraph 4 on cloud, managed and similar service providers to add a required level of impact. In line with the recommended changes to subparagraph 3, this qualifier would provide greater clarity and increase alignment with incident categorizations in the National Cyber Incident Scoring System. In addition, CISA should further explore avenues to streamline reporting of incidents impacting multiple customers, given that one cyber incident within a service provider could induce several substantially similar reports between multiple entities.

E. Role of Tactics and Zero-Day Vulnerabilities in Defining Substantial Cyber Incidents [Q7-8]

Mandatory cyber incident reporting should not be viewed as a threat intelligence service provided by the private sector. Cyber incident reporting requirements should focus narrowly on the degree of risk to national critical functions. Overemphasis on technical details of attacker tactics can lead to overreporting that dilutes the focus on genuinely "substantial" incidents.

Novel or sophisticated tactics, techniques and procedures (TTPs) or zero-day vulnerability exploitation should be factors in whether a cyber incident report is required only to the extent that those factors elevate systemic risk.[16] The presence of a sophisticated or novel TTP or vulnerability should not in itself be determinative in classifying an incident as a substantial cyber incident but would be an appropriate part of a covered entity's analysis of the impact of the incident.

F. CISA's Interpretation of the Terms "Entity" and "In a Critical Infrastructure Sector" [Q27-31]

CISA's proposed application of "in a critical infrastructure sector" and the size-based threshold is vague, overbroad and risks weakening the effectiveness of CIRCIA to enable CISA to better protect critical infrastructure from cyber attacks that threaten national security, economic security or public welfare.[17] Rather than applying cyber incident reporting requirements to all entities that are active participants in a critical infrastructure sector, CISA should take a risk management approach.

---

[15] CISA National Cyber Incident Scoring System, Sep. 30, 2020, https://www.cisa.gov/news-events/news/cisa-national-cyber-incident-scoring-system-nciss.

[16] 89 Fed. Reg. 23675.

[17] 89 Fed. Reg. 23706.

BRT recommends that CISA clarify that business units that are not in critical sectors are not "covered entities." Many BRT member companies are large, diversified companies with business units in many different economic sectors. CISA should not consider incidents affecting business units in non-critical sectors with no overlap of affected networks a "covered cyber incident." In addition, enterprise or group-level systems that do not materially affect operations of the critical infrastructure business unit/entity should be exempted, such as talent management software. CISA should define "covered entities" as entities in critical infrastructure sectors that own or operate assets or services that directly and primarily provision a National Critical Function.[18]

BRT further urges CISA to clarify that CIRCIA applies only to U.S. entities and that CIRCIA applies to neither foreign subsidiaries of a U.S. parent company nor foreign parent companies. However, to the extent that an incident that occurs at a foreign subsidiary or foreign parent implicates a U.S. covered entity, CIRCIA would apply to that U.S. entity. We recommend CISA consider issuing guidance on CIRCIA scope and compliance for multi-business enterprises across geographic jurisdictions.

In addition, CISA's current proposed definition of "covered entity" implies that implicated entities include not only owners and operators of critical infrastructure but practically any organization that merely exists within the sector. Ancillary involvement in a critical infrastructure sector should not be sufficient to be considered "in" a sector based merely upon size of the entity, without any regard for the actual impact to critical infrastructure. CISA directs entities to reference Sector-Specific Plans to understand their involvement in a critical infrastructure sector. However, some Sector-Specific Plans were last updated many years ago and contain broad groupings, which were not created with this purpose in mind. The Chemical Sector Plan, for example, lists cosmetics along with pesticides. A more refined purpose test based on risk to strategic interests and potential harm should be developed, rather than size and inclusion within broad and poorly defined sectors. These distinctions are especially useful for service providers that operate across sectors.

Additionally, CISA should base the scope of "covered entity" on the severity of impact that disruption would cause, rather than using entities' annual revenue as a proxy metric. CISA could adopt its proposed "Alternative B," remove the size-based threshold and focus on specific sector-based criteria developed in conjunction with the Sector Risk Management Agencies (SRMAs). However, CISA should not then revise its sector-based criteria to be overly broad but continue to focus sector-based criteria on entities whose disruption would have severe consequences. This approach would remain consistent with the definition of "critical infrastructure" (as defined in NSM-22 and in 6 USC 101), while acknowledging CISA's reticence to rely solely on entities' own judgements as to whether an incident would have a "debilitating impact." These criteria should leverage the National Cyber Incident Scoring System and align

[18] CISA National Critical Functions Set, Apr. 2019, https://www.cisa.gov/national-critical-functions-set.

with other efforts by the White House, CISA and SRMAs to designate certain critical infrastructure as systemically important.[19]

CISA should clarify that the existence of a "covered entity" within the affiliated companies of a large multinational does not render the entire consolidated company's operations in scope. CISA should clarify that a cyber incident involving an affiliate to a covered entity that does not substantially affect the critical infrastructure operations of that covered entity is not a covered cyber incident simply by virtue of corporate affiliation.

Finally, it is crucial that CISA clarify that covered entities who are service providers to other covered entities are not required to submit CIRCIA reports on the impact of an incident to its customers' information or systems. Typically, the service provider would notify the customer of the incident, and the customer would determine whether a report must be filed. BRT urges CISA to clarify that individual covered entities are independently responsible for determining the impact to their information and systems and, where applicable, filing their CIRCIA report.

G. CISA's Proposed Interpretations of Substantially Similar Information and Substantially Similar Timeframe, and Application to Supplemental Reports [Q38-39]

BRT supports the establishment of a robust exception for substantially similar reporting to reduce unnecessary and redundant reporting that weakens the utility of incident reporting to critical infrastructure cybersecurity. However, exceptions for substantially similar reports should not be restricted to agencies that have established agreements with CISA.[20]

As written, CISA's broad and prescriptive approach to the scope of the proposed rule suggests that CISA is unlikely to designate existing sector-based cyber incident reporting regulations as substantially similar, posing a challenge to meaningful adoption of CIRCIA agreements by other agencies. CISA's proposed rule interprets "substantially similar" to mean "equivalent" in terms of both information and timeframe.[21] CISA should work with its federal partners, including independent regulatory agencies, to facilitate reciprocity and streamlined incident reporting without requiring CIRCIA agreements, rather than shifting additional burdens on entities that are already required to report cyber incidents.

To the extent that CISA relies heavily on CIRCIA agreements to streamline reporting efforts, CISA should prioritize establishing such agreements quickly and with as many partners as possible. Once agreements are finalized, they should be maintained in a public repository to clearly enumerate participating authorities. In this event, CISA should not finalize the CIRCIA

---

[19] White House, Letter from the President to Select Congressional Leadership on the Nation's Critical Infrastructure, Nov. 7, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/07/letter-from-the-president-to-select-congressional-leadership-on-the-nations-critical-infrastructure.

[20] 89 Fed. Reg. 23708-23709.

[21] *Id.*

reporting obligations until substantial progress has been made in the adoption of CIRCIA agreements with sector specific regulators.

CISA should accept cyber incident reports, including supplemental reports, that comply with sector-based regulations as also compliant with CIRCIA. If necessary, CISA may consider requesting additional information about the reported incident from the reporting entity. CISA should also work with federal partners to accept CIRCIA-compliant incident reports as also compliant with sector-based cyber incident reporting regulations, given the detailed reporting requirements proposed for CIRCIA. In addition, CISA should define a "substantially similar" timeframe as a period during which the facts of the cyber incident remain unchanged to an extent that requiring additional reporting would not yield substantially new information or alter the course of incident response.

H. Proposed Use of a Web-Based Form as the Primary Means of Submission of CIRCIA Reports [Q52-53]

As noted in the response to Q1, CISA should establish a common reporting framework and a centralized point for the submission of cyber incident reports. BRT supports the use of a secure web-based form as the primary means of submitting CIRCIA reports, as well as the proposed maintenance of telephonic reporting as a back-up option. BRT also supports continued exploration of the viability of a secure, automated (machine-to-machine) reporting option. CISA should host and maintain each of these options.[22] Any report submission process should include mechanisms for CISA to validate the authenticity of reports, potentially including a pre-registration process, even outside of third-party submission contexts.

I. Proposals Related to the Content of CIRCIA Reports [Q54]

BRT urges CISA to simplify the content that would be required in CIRCIA reports. Many of the report elements CISA proposes are difficult and time-consuming to ascertain, especially soon after a cyber incident. The highly detailed proposed reporting requirements will inflate the cost and time required to prepare CIRCIA reports, diverting resources from cyber incident response. This also runs counter to the goal of regulatory harmonization. The greater the complexity of the information required by CISA, the less likely it is that their reporting requirements can be harmonized with other agencies, which must have substantially similar requirements.

This burden is deeply exacerbated by CISA's proposed requirement that covered entities issue supplemental reports within 24 hours of discovery of any "new or different information."[23] Many cyber incident investigations take several days or weeks, and the value of continually updating developments relating to the complex data elements required under CISA's proposed

[22] 89 Fed. Reg. 23729-23730.
[23] 89 Red. Reg. 23726.

CIRCIA reports is unclear. Accordingly, BRT urges CISA to extend the supplemental reporting deadline to no sooner than 72 hours of discovery of a significant update.

J. Proposals Related to the Timing of Reports [Q55]

BRT agrees with CISA's position that the question of when a covered entity should have reasonably believed a covered cyber incident occurred is subjective and that a covered entity should not be expected to reach a reasonable belief that a covered cyber incident occurred immediately upon occurrence.[24] A challenging part of cyber incident response is accurately assessing the severity of an incident, especially in early stages.[25]

The appropriate point for the 72-hour incident reporting timeframe to begin is the point at which the covered entity forms a reasonable belief that a cyber incident has occurred and should be considered covered. Starting the 72-hour timeframe at the point that the cyber incident occurred would be inappropriate and burdensome given that incident responders must detect and assess the severity of the incident before determining that a report under CIRCIA is required. Additionally, some consideration should be given to the reporting timelines for different aspects of the attack and level of detail required. If an entity cannot accurately report the required information within 72 hours of the attack, there should be opportunities beyond the 72 hours to clarify or add details when needed or to correct previous submissions.

Most companies have a structure and process in place for determining whether an incident is material or substantial. Company officers and executives are often involved in this type of decision making as a part of the responsibilities included in corporate bylaws and governance models, particularly amongst publicly traded companies. Notably, the proposed rules indicate that the belief formation that matters "generally would occur at the subject matter expert level and not the executive officer level."[26] However, the opinion of executive leaders can be essential in determining the harm suffered from a covered incident and therefore the required reporting obligations. These necessary processes can affect the speed at which a determination can be definitively made.

K. Data Preservation Requirements [Q58-61]

BRT urges CISA to clarify and narrow the scope of the incident data that organizations must preserve and to reduce the retention period.[27] The broad scope of data that must be preserved under the proposed rule risks prompting organizations to retain unnecessarily large datasets for two years, creating a high compliance cost and a potential security risk while providing little

---

[24] 89 Fed. Reg. 23725.
[25] See e.g., NIST Computer Security Incident Handling Guide, NIST SP 800-61r2, Aug. 2012, pg. 26, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.
[26] 89 Fed. Reg. 23725
[27] 89 Fed. Reg. 23730-23733.

additional value in the vast majority of cases. We recommend instead that data preservation requirements should apply only to records that are directly relevant to the covered cyber incident.

L. RFI Authority and Penalties [62-66]

BRT urges CISA to clarify that only CISA employees designated by the Director of CISA have the authority to issue requests for information (RFIs).[28] BRT would not support an approach that enabled the CISA Director to designate employees or agents external to CISA with authority to issue RFIs.

BRT additionally urges CISA to modify Section 226.20 to clarify that liability for false statements or representations does not apply to information that the covered entity reasonably believed was true but later turned out to be inaccurate. This is consistent with CISA's commentary on Section 226.20, but this limitation is not present in the language of 226.20 itself.[29]

M. Confidentiality Protections for Reports Required Under CIRCIA [Q67-70]

BRT supports the protections codified in CIRCIA for required reports and responses to RFIs.[30] BRT agrees with CISA's overall approach to enable covered entities or third parties to easily avail themselves of these protections. We urge CISA to clarify that the protections apply to incident reports submitted voluntarily from entities that are not affiliated with the covered entity affected by the incident, and who are not authorized by the covered entity affected by the incident to submit a report. These confidentiality protections help provide assurance that sensitive cybersecurity information will not be widely accessible and at risk of being misused to undermine security or competition.

BRT opposes CISA's proposal that liability, privacy and civil liberties protections would be stripped from information and reports submitted in response to a subpoena from CISA. CISA's broad definition of "covered cyber incident" leaves room for reasonable but differing interpretations. Covered entities that disagree with CISA in good faith regarding whether a cyber incident is a "covered cyber incident," and are then subject to a subpoena, should not face punitive loss of protections intended to preserve individual privacy, safeguard, enterprise security, and encourage candor.[31] In fact, such a result, requiring potential public disclosure of sensitive information relating to network operations, protections and/or vulnerabilities, could provide information to potential threat actors and broadly undermine cybersecurity efforts.

---

[28] 89 Fed. Reg. 23671, 23733.
[29] 89 Fed. Reg. 23737, 23776.
[30] 89 Fed. Reg. 23737-23738.
[31] 89 Fed. Reg. 23774-23775.

CISA should clarify the data protection and confidentiality requirements that apply when it shares CIRCIA reports with government and non-government partners. While CIRCIA requires CISA to anonymize personal information prior to sharing, it is unclear whether only personal information will be removed from shared reports, or whether information identifying the submitting entity will be retained prior to sharing. BRT recommends that CISA develop guidance for federal agencies and other partners with whom CISA may share information derived from CIRCIA reports and RFI responses. This guidance should clarify the application and extension of these liability, privacy and civil liberties, and evidentiary protections for information shared to organizations other than CISA, including but not limited to the National Cybersecurity and Communications Integration Center (NCCIC).[32]

Further, CIRCIA reports and RFI responses should be designated as commercial, financial and proprietary information by default, rather than requiring covered entity or third-party submitters to select this designation.[33] BRT agrees with CISA's approach to Freedom of Information Act (FOIA) exemption, whereby CISA asserts the exemption from disclosure in the event CISA receives a FOIA request for CIRCIA reports or RFI responses.[34] BRT also agrees with CISA's interpretation of CIRCIA provisions establishing that no privileges are waived in all circumstances where state or federal privileges and protections may attach, including under common law.[35]

BRT appreciates that CISA notes the importance of appropriately protecting the information it receives. As with any database, the data gathered by CIRCIA will be a valuable trove of information and must be protected through cutting edge cyber defense techniques and other strong precautions. We encourage CISA to integrate additional data privacy safeguards to ensure that any sensitive information reported by covered entities is sufficiently protected. A list of agencies who will receive access to this information should also be shared with covered entities.

N. Restrictions on the Use of CIRCIA Reports or RFI Responses in Regulatory Actions or as Independent Causes of Liability [Q71]

CISA proposes that information in CIRCIA reports and RFI responses may be used to regulate if a federal or SLTT entity allows the covered entity to meet separate regulatory reporting requirements through the submission of a CIRCIA report to CISA.[36] While BRT supports the option of reciprocity in compliance with CIRCIA and separate cyber incident reporting regulations, it is crucial that covered entities have discretion to exercise the option of reciprocity. Agencies should not assume covered entities are seeking reciprocity in each

[32] 6 U.S.C. § 681a(a).
[33] 89 Fed. Reg. 23737.
[34] 89 Fed. Reg. 23738.
[35] *Id.*
[36] 89 Fed. Reg. 23738.

circumstance. The covered entity may have reasons to submit cyber incident reports separately, such as if there are distinctions in the reporting triggers or report contents.

Accordingly, the exception to the prohibition on regulatory use of CIRCIA reports and RFI responses should apply only when the covered entity chooses to submit a CIRCIA report or RFI response to comply with the separate cyber incident reporting regulation. If the covered entity submits a CIRCIA report for purposes of compliance with CIRCIA only, other regulators should not presume that the CIRCIA report is intended for compliance with separate cyber incident reporting regulations, unless the covered entity indicates otherwise.

Regarding the use of CIRCIA reports or RFI responses as an independent cause of liability, the prohibition on regulatory actions based on information "obtained solely through a CIRCIA report" or RFI response should apply not just to the contents of the submission but should extend to the fact that the covered entity submitted a report or response.[37] That is, regulators should not rely solely on the fact that a covered entity submitted a CIRCIA report or response as the basis to initiate an investigation into the covered entity.

O. Restrictions on the Receipt of CIRCIA Reports or RFI Responses as Evidence [Q72]

Consistent with BRT's response to Q71, the scope of liability protection from "litigation solely based on the submission of a CIRCIA report" or RFI response should extend not just to the contents of the submission but also extend to the fact that the covered entity submitted a report or response.[38] Litigants, regulatory bodies and other authorities should not rely on the fact that a covered entity submitted a CIRCIA report or response as the basis to initiate action to obtain the underlying information contained in the report or response.

P. Proposed Privacy and Civil Liberties Protections, Including the Steps Proposed by CISA to Minimize the Collection of Unnecessary Personal Information in CIRCIA Reports [Q73]

BRT strongly supports privacy and civil liberties protections for persons whose information may be swept up in a covered cyber incident.[39] CISA and NCCIC should take all feasible steps to ensure personal information is comprehensively minimized unless there is a direct relation to a cybersecurity threat and the personal information is strictly necessary for CISA to accomplish a cybersecurity purpose.

Reports and responses submitted under CIRCIA will include sensitive security, business and other confidential information. It is crucial that CISA maintain robust digital security safeguards

[37] *Id.*
[38] 89 Fed. Reg. 23739.
[39] 89 Fed. Reg. 23739-23741.

to protect this information from unauthorized access, acquisition, disclosure and use.[40] CISA should conduct regular assessments of its privacy and digital security protections and adjust protocols as needed to ensure ongoing effectiveness.

* * *

BRT members have a strong commitment to collaborative solutions balancing national security, privacy and business innovation and appreciate CISA's engagement with the private sector. If you have any questions regarding these comments, please contact Amy Shuart, Vice President, Technology & Innovation, at AShuart@brt.org.

[40] 89 Fed. Reg. 23741.