Comments of the National Chicken Council
in connection with the Cybersecurity and Infrastructure Security Agency's
Notice of Proposed Rulemaking regarding the
Cyber Incident Reporting for Critical Infrastructure Act of 2022

The National Chicken Council and its member organizations appreciate the opportunity to comment on the Cybersecurity and Infrastructure Security Agency's ("CISA" or the "Agency") proposed rule (the "Proposed Rule" or "Proposal") to implement the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"). The NCC shares CISA's commitment to protecting the nation's critical infrastructure against cyber threats, and we recognize that sharing information regarding cyber incidents is an integral part of protecting the U.S. national security, economy, and public health and safety. Accordingly, we commend CISA's efforts to develop a robust reporting framework that will help to achieve these goals, and we respectfully offer the following comments on certain key areas where we think there are opportunities for improvement. We hope that this feedback will help CISA to develop a workable reporting framework that will ensure that the Agency receives the threat intelligence it needs to effectively manage and mitigate the nation's cyber risk, while also minimizing the compliance burden on many critical infrastructure entities, including small businesses.

Discussion

We respectfully request that CISA consider revising the Proposed Rule to address the issues discussed below:

1. **The expansive definition of "covered entity" and, relatedly, the potential burden on many small businesses.**

The size-based criteria for qualification as "covered entity" should be revised to help ensure that the Proposed Rule does not overly burden small businesses that may be unable to comply with the Proposed Rule's requirements and that are unlikely to present significant risk to the U.S. national security, economy, or public health and safety if impacted by a cyber incident.

For the chicken industry, and the Food and Agriculture sector more broadly, the Proposed Rule would apply to all entities in the sector *other than* those that constitute a "small business" based on the applicable size threshold prescribed by the Small Business Administration ("SBA"). CISA has explained that the reason for taking this approach for the Food and Agriculture sector is that "CISA believes that given the scale of this sector and the general substitutability of the products that entities within the sector produce, the Food and Agriculture Sector entities with the greatest potential to experience a cyber incident resulting in significant consequences are the largest entities in this sector."[1] For this reason, CISA believes that the Proposed Rule's size-based applicability criterion will capture the most critical Food and Agriculture Sector entities within the description of "covered entity."

[1] Proposed Rule, 89 Fed. Reg. 23,644, 23,702.

However, utilizing the SBA's small business size standards for the Food & Agriculture sector (and for the chicken industry in particular) will lead to far more than only the largest and most critical entities constituting "covered entities" under the Proposed Rule. Some of the SBA's size standards relevant to the chicken industry are relatively low and easy to exceed. For example, the applicable threshold for "Poultry and Poultry Product Merchant Wholesalers" is 150 employees.[2] Further, the SBA's regulations make clear that employees of both domestic and foreign affiliates are counted for purposes of determining whether an entity exceeds the applicable size threshold.[3] As a result, affiliated poultry wholesalers—each of which may have only a small number of employees, and each below the 150 threshold—may be rendered "covered entities" by virtue of their affiliation with other small poultry wholesalers, or ownership by a larger enterprise.

These small poultry merchants, like many other small companies that may be swept in by the expansive definition of "covered entity," may have less sophisticated cybersecurity and regulatory compliance programs, and thus may need to incur substantial costs in order to comply with the Proposed Rule—for example, by hiring external legal counsel or cybersecurity firms. As another example, many small companies are unlikely to have implemented sufficient logging, monitoring, and forensic capabilities to provide the information required by Covered Cyber Incident Reports or Ransom Payment Reports, such as information regarding the specific vulnerability exploited, threat actor attribution, indicators of compromise, and threat actor tactics, techniques, and procedures.

Moreover, many of these small companies are not likely the kind of entities that would pose a risk to the U.S. national security, economy, or public health and safety if impacted by a cybersecurity incident. Thus, requiring them to report cybersecurity incidents to CISA will lead to the Agency receiving large volumes of reports regarding insignificant incidents that pose minimal, if any, risk to the U.S.

For these reasons, we recommend that CISA revise the size-based criteria for qualification as a "covered entity" to include higher employee and/or revenue thresholds, in order to avoid subjecting many small companies in the Food & Agriculture sector to the Proposed Rule.

2. The expansive definition of "substantial cyber incident" and the overreporting of incidents to CISA.

The definition of "substantial cyber incident" should be revised to (i) require that there be some impact to a critical portion of a covered entity's systems or operations, and (ii) with respect to prong (4) of the definition, require that incidents triggering only on impact to data involve data of a certain sensitivity level or that relates to a certain number of individuals.

The text of CIRCIA suggests that Congress was primarily concerned with identifying and preventing "demonstrable harm to the national security interest, foreign relations, or economy of the United States..."[4] or "consequences … to … public health and safety."[5] But because the definition of "substantial

[2] *See* 13 C.F.R. § 121.201 (Subsector 424).
[3] *See* 13 C.F.R. § 121.106(b)(1).
[4] *See* 6 U.S.C. § 681(9).
[5] *See* 6 U.S.C. § 681b(c)(1)(A).

cyber incident" does not require that such incidents involve impact to a critical systems or operations of a covered entity, the definition would not limit the scope of reportable incidents to those that would actually have the consequences with which Congress was primarily concerned. For example, a cyber incident that impacted only a covered entity's marketing/advertising operations or systems could be a reportable incident, even if the incident presented no risk of harm or disruption to the critical services that the covered entity provides, and therefore presented no risk to the U.S. national security, economy, or public health and safety. This would not only be inconsistent with the fundamental purpose of CIRCIA, but would also result in CISA receiving large volumes of reports regarding insignificant incidents.

For these reasons, we recommend that CISA revise the definition of "substantial cyber incident" to require that reportable incidents involve impact to a critical portion of a covered entity's systems/operations, which may actually have the potential to pose risk to the U.S. national security, economy, or public health/safety if disrupted. For example, CISA may consider revising the definition of "substantial cyber incident" as follows:[6]

> *Substantial cyber incident* means a cyber incident that leads to any of the following:
>
> (1) A substantial loss of confidentiality, integrity or availability of a critical portion of a covered entity's information system or network;
>
> (2) A serious impact on the safety and resiliency of a critical portion of a covered entity's operational systems and processes;
>
> (3) A disruption of a covered entity's ability to engage in critical business or industrial operations, or deliver critical goods or services;
>
> (4) Unauthorized access to a critical portion of 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.

In addition to generally requiring that there be some impact to critical portions of a covered entity's systems or operations, CISA may also consider revising prong (4) of the definition of "substantial cyber incident" to require that, for incidents triggering based merely on impact to data, that data be of a certain sensitivity level or relate to a certain number of individuals. As currently drafted, an incident would be reportable under prong (4) if it involves unauthorized access to nonpublic information contained on a covered entity's systems or network, even if that information is of a non-sensitive nature,[7] and regardless of how many individuals are affected. Thus, entities may be required to report incidents involving inconsequential data impact, which will further exacerbate the issue of overreporting of minor incidents to CISA.

We also note that revising prong (4) in this way would render it more consistent with the text of CIRCIA. The text of CIRCIA provides that unauthorized access is a *minimum* requirement for an incident to

[6] Proposed Rule § 226.1.

[7] While we recognize that the information must be "nonpublic," that term is not defined in the Proposal and, as commonly understood, could include a broad range of information that is non-sensitive.

constitute a "substantial cyber incident"—not that unauthorized access, in and of itself, is sufficient to constitute a "substantial cyber incident." Rather, CIRCIA makes clear that CISA's definition of "substantial cyber incident" must consider "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" and "the number of individuals directly or indirectly affected or potentially affected by such a cyber incident."[8]

For these reasons, we recommend that CISA consider revising prong (4) of the "substantial cyber incident" definition to require that data be of a certain sensitivity level or relate to a certain number of individuals.

3. The short timeline for reporting covered cyber incidents.

The Proposed Rule should be revised to require that covered entities report covered cyber incidents within 72 hours of a *determination* that a substantial cybersecurity incident occurred—not within 72 hours of a *reasonable belief* that such an incident occurred.

Requiring covered entities to report covered cyber incidents within 72 hours after the entity "reasonably believes" that it has experienced such an incident will likely lead many entities to report incidents that, upon further investigation, ultimately do not result in any of the four impact triggers set out in the definition of "substantial cyber incident." This over-reporting of incidents will further contribute to CISA receiving vast amounts of reports and information that ultimately are not useful to CISA in its goal of protecting the nation's critical infrastructure, but instead serve only to drown out signal with noise.

Additionally, because the Proposed Rule's size-based criteria will likely render many smaller, unsophisticated companies in the chicken industry and Food and Agriculture sector "covered entities" (as discussed above), many of those entities will lack the resources needed to simultaneously conduct incident response and recovery efforts while also addressing regulatory reporting obligations on such a short timeline. Faced with this dilemma, these entities may be forced to shift resources away from important investigation and recovery efforts toward regulatory compliance—especially in light of the large volume of information required to be included in Covered Cyber Incident Reports. Such resource shifting may ultimately have the effect of making the entity more vulnerable in the event of a real cyber incident. And in the case of suspected, but not actual, incidents, smaller companies will have expended their limited resources to report incidents that the entity "reasonably believed" may have occurred, but ultimately did not.

To help avoid these issues, we recommend that that the Proposed Rule be revised to require that covered entities report covered cyber incidents within 72 hours of a covered entity's "determination" that it has experienced such an incident.

[8] *See* 6 U.S.C. 681b(c)(2)(B)(i)-(ii).

4. The need for greater flexibility when responding to requests for information.

The Proposed Rule should be revised to provide covered entities with greater flexibility when responding to a request for information ("RFI") issued by CISA.

Under the Proposed Rule, the Director of CISA may issue an RFI to a covered entity "if there is reason to believe that the entity experienced a covered cyber incident or made a ransom payment but failed to report the incident or payment in accordance with § 226.3,"[9] and a covered entity must by the deadline specified by the Director.[10] As currently drafted, the Proposed Rule appears to allow CISA's Director to specify a response deadline as short as 72 hours,[11] and RFIs cannot be appealed.[12] Responding to an RFI in such little time will likely be virtually impossible in many cases, for a number of reasons. For one, because of the complex nature of many cyber incidents, providing CISA with the requested information may involve analysis of large amounts of data, logs, and other documentation relevant to the incident, which may take significant time to thoroughly review. Moreover, a covered entity itself might not have all of the requested information and may need to seek relevant information from a third party, who may be uncooperative or slow to respond. And regardless of whether the requested information is held by the covered entity itself or a third party, procuring and validating the information may be difficult if a significant amount of time has passed since the cyber incident occurred.

The Proposed Rule further provides that the Director may issue subpoenas to compel disclosures of information from a covered entity if the entity fails to reply to an RFI by the specified deadline (or if the Director deems the provided response inadequate).[13] Thus, covered entities—including smaller companies with limited resources—may be in position where, despite their good-faith efforts to timely provide CISA with requested information, may be subject to subpoenas for their inability to provide a complete response in an unrealistic timeframe.

For these reasons, we recommend that the Proposed Rule be revised to either (a) require that RFI deadlines not be less than a reasonable minimum amount of time (such as 14 calendar days), or (b) at the very least, expressly provide covered entities with the right to receive an extension of an RFI deadline where the covered entity can explain why meeting the deadline set by the Director would be impractical.

Conclusion

We sincerely appreciate the Agency's consideration of our comments, and we look forward to continued engagement with the Agency and other stakeholders in our shared pursuit of protecting the nation's

[9] Proposed Rule § 226.14(c)(1).
[10] Proposed Rule § 226.14(c)(3).
[11] This is implied by the combination of Proposed Rule § 226.14(d)(1) (providing that the Director "may issue a subpoena to compel disclosure of information from a covered entity if the entity fails to reply by the date specified … or provides an inadequate response") and § 226.14(d)(2) (providing that a "subpoena to compel disclosure of information from a covered entity may be issued no earlier than 72 hours after the date of service of the request for information").
[12] Proposed Rule § 226.14(c)(5).
[13] Proposed Rule § 226.14(d)(2).

critical infrastructure. If you have any questions or would like to discuss these comments further, please do not hesitate to contact us.