Meat Institute
Nourishing Today
Sustaining Tomorrow

July 3, 2024

Jennie M. Easterly
Director
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
1100 Hampton Park Blvd
Capitol Heights, MD 20743 - 0630

Re: *Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements*; Docket No. CISA-2022-0010; (April 4, 2024)

Dear Ms. Easterly:

The Meat Institute submits these comments concerning the above-referenced proposal to establish cyber incident reporting requirements for critical infrastructure (proposal or proposed requirements) under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA or the Act). The Meat Institute is the nation's oldest and largest trade association representing packers and processors of the majority of U.S. beef, pork, lamb, veal, turkey, and processed meat products. The Meat Institute provides regulatory, scientific, legislative, public relations, and educational services to the meat and poultry packing and processing industry. Meat Institute member companies play a key role in the food and agriculture critical infrastructure sector to provide safe and wholesome meat and poultry products as a nutrient dense source of protein for consumers.

In 2021, the Meat Institute[1] Executive Board voted unanimously to declare cybersecurity a non-competitive issue for its members. Under direction from the Board, the Cybersecurity Committee was formed and continues to operate today. This group of cyber experts from member companies meets regularly to discuss best practices and recommend or create resources for the benefit of all member companies. The Meat Institute is a proud partner of the Food and Agriculture-Information Sharing and Analysis Center (FA-ISAC) and recently participated for the first time in Cyber Storm. Though early in its maturity on cybersecurity, the Meat Institute is committed to improving the security posture of the meat and poultry industry.

The Meat Institute appreciates the opportunity to provide comments on the requirements proposed by the Cybersecurity and Infrastructure Security Agency (CISA or the agency). The proposed regulations will increase costs for covered entities, require them to report on incidents of little meaning, and overwhelm CISA

[1] Formerly, the North American Meat Institute

with information it is unable to properly vet or analyze. The Meat Institute recommends the agency make substantive changes to the proposal to ease the burden of compliance. Given the sensitivity of the information that may be included in these reports, there are significant concerns regarding data security. Additional clarity is warranted on how information collected will be shared, secured, and properly disclosed.

Cybersecurity maturity varies greatly amongst businesses.

The definition of a "Covered Entity" for the food and agriculture sector is straight forward—all companies in the sector, other than those that meet the Small Business Administration's (SBA) definition of small business for their industry, are covered entities. Although the SBA small business criteria were not developed for this purpose, using it here at least has the benefit of being clear. However, there are many companies who exceed the SBA definitions and are still comparatively small, facing the prospect of complicated and costly compliance.

The threshold to be considered a "small business" for meat and poultry companies is 1,000 – 1,250 employees, depending on the species and type of processing.[2] Meat and poultry processing is unique to most food manufacturing. It is often referred to as "reverse manufacturing," because the carcass is disassembled into parts rather than assembled food from ingredients. Despite advancements in automation and robotics, the process of disassembling individual carcasses, which are not uniform since they were once living animals, requires substantial human labor. Robotics often cannot match the skill of experienced workers. Therefore, what may seem like a high threshold for the number of employees is fairly low given that most of those positions are manual labor. A company with 1,300 employees may run a single slaughter plant, or three small plants, and likely not have a corporate structure with dedicated cybersecurity staff. The agency should reconsider its definition of a covered entity.

Also, many companies are likely unaware of the proposal. CISA must address how it will engage companies for education and compliance assistance, as directed by Congress.

> When determining whether to exercise the authorities provided under this section, the Director shall take into consideration—
> (2) prior interaction with the Agency or awareness of the covered entity of the policies and procedures of the Agency for reporting covered cyber incidents and ransom payments. (Emphasis added.)

[2] U. S. Small Business Administration Table of Small Business Size Standards Matched to North American Industry Classification System Codes.

Victims of cyber incidents must focus on restoring systems and resuming normal operations.

The most critical aspect in the response to a cybersecurity incident in most all cases is maintaining the safety of the company's assets and stakeholders, especially its employees. The Meat Institute strongly recommends implementing a practiced response plan supported by the organization's executive management. Congress recognized this, directing CISA to "balance the need for situational awareness with the ability of the covered entity to conduct cyber incident response and investigations."[3] The onerous reporting requirements proposed risk shifting the balance by diverting limited resources from security and recovery to compliance.

The information required to report should be limited and fit for purpose. The intent of CIRCIA is clear, for CISA to assess potential impacts of cyber incidents on public health and safety and enhance situational awareness. Many of the detailed requirements in the proposal are overly burdensome and will not help the agency achieve its mission. The agency failed to support the value in the proposed requirements, especially when considering the scale and scope of the information that would be poured into the agency should the proposal become final. In general, the sheer volume of data requested via reporting should be scaled down.

Reporting entities should be only required to provide a simple notification within the initial reporting period, with additional information to follow, if available.

In many cases, little is known during the initial phase of responding to a cyber incident and critical resources must be focused on recovery. The agency should recognize this reality and mirror its reporting requirements accordingly. The Meat Institute recommends a simplified and structured framework for reporting, broken down into two main parts, though certain information is sensitive and not appropriate to share externally at any point.

Initial Report

The agency should limit the information it solicits from covered entities during the initial reporting period (72 hours for cyber incidents and 24 hours for ransom payments) so companies can focus on response. Many entities will not have detailed information within the initial reporting period anyways. The agency seemingly understands this to some degree, stating in the preamble to the proposed rule and in outreach efforts with stakeholders that the required information can be provided in subsequent reports if not available during the initial reporting period. However, the agency could make that intent much clearer by delineating the reporting requirements into separate parts, and only soliciting the most basic facts about the incident and the current impact on the company's ability to operate. In some

[3] Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)

instances, a 72-hour reporting timeline might not be possible regardless of the extent of information required in such a report. An entity might not be able to submit a report because its systems are unavailable, or it is unsafe for them to do so. CISA should recognize this reality and establish accommodations for such circumstances.

Follow-up Report(s)

The reporting framework should allow covered entities to submit a follow-up report(s) to provide additional information after the initial reporting period. This will relieve pressure from companies and ensure better data. Soliciting detailed information at the onset of a cyber incident may lead to inaccurate information being unintentionally shared, because the true nature and extent of the incident may not be known for some time as an investigation is conducted. Again, cyber maturity varies greatly between companies. Some companies may not have the expertise to ever determine certain information, or even if they have the expertise, sometimes certain information is still impossible to determine. The agency must account for the reality that many entities will not be able to provide some information and clearly communicate that entities will not be deemed noncompliant by not reporting information that is not available.

Attachment 1 categorizes some of the proposed reporting requirements according to this suggested framework. Reporting requirements for cyber incidents (Section 226.8) and ransom payments (Section 226.9) are organized side by side because many are identical or similar.

- Green: This information will likely be available and reportable within the initial reporting period. The agency should only solicit this information for the initial report. All proposed reporting requirements within Section 226.7 fall under this category and thus have been excluded from Attachment 1.
- Yellow: This information may become available as the incident is investigated but will not likely be available within the initial reporting period. The agency should only solicit this information in a follow-up report after the initial report.
- Red: This information is either 1) not appropriate to share due to the risk posed to the victim company or 2) not likely to ever be available. The agency should reconsider requiring this information at all. At a minimum, the agency should adjust the requirements to allow for generic, less sensitive information to be provided.

Specific considerations are provided on some of the proposed reporting requirements.

- 226.8 (a)(1) and 226.9 (a)(1): The Act only refers to a generic identification and description of affected networks, device, and/or systems. Even meeting the intent of the Act will prove difficult for companies, let alone the additional details proposed.

- 226.8 (a)(2) and 226.9 (a)(2): There is context from the Act missing. The Act requires "a description of the unauthorized access **with substantial loss of confidentiality, integrity, or availability** of the affected information system or network **or disruption of business or industrial operations**;" (emphasis added) ostensibly to emphasize that not all unauthorized access need be report, only that which has a substantial impact. However, the proposal simply requires "a description of **any** unauthorized access." (Emphasis added.) There is a large discrepancy between the two and the agency must default to the Act.
- 226.8 (a)(3) and 226.9 (a)(3): The Act only requires a date range to be reported. The additional details included in the proposal are overly burdensome and provide little to no value for the intended use.
- 226.8 (a)(4) and 226.9 (a)(4): Member input on these requirements were divided, with some categorizing as yellow and some red. The Act only requires a generic description of the impact. The agency should default to only requiring a generic description in a follow-up report.
- 226.8 (d) and 226.9(c): There are serious concerns with providing this information, because it could unintentionally provide a roadmap to adversaries should the reporting data become compromised. It is not material to trending incidents and should not be required.
- 226.9(i): There are serious concerns with providing the amount of ransom paid, because it could unintentionally aid adversaries in understanding what amount to set ransom requests for to best illicit payments if the reporting data is compromised. There are additional business reasons for keeping exact amounts unknown. If the agency deems it necessary to collect this information, it should allow reporting entities to select from a preset list of ranges to help keep the data less specific.
- 226.9(l): This requirement is not listed in the Act. It is overly burdensome and should be excluded. It is not material to the intent of reporting. Also, even if operations are restored by paying a ransom, it does not mean the vulnerability has been remediated. There is too much nuance and detail involved to be included in the reporting scheme.

Entities should only be required to report on cyber incidents with a significant impact.

The reporting requirements were intended to only apply to significant cyber incidents, which the Act defines as

> —a cyber incident, or a group of related cyber incidents, that the Secretary determines is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States.[4]

[4] CIRCIA

Which is further described to

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

(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,[5]

Yet the agency created its definition ignoring these clear signals from Congress to limit reportable incidents to those with severe impacts and simply reiterated the **minimum** requirements from the Act.

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 covered entity's information system or network;

(2) A serious impact on the safety and resiliency of a covered entity's operational systems and processes;

(3) A disruption of a covered entity's 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

[5] CIRCIA

> compromise; a denial-of-service attack; a ransomware attack; or exploitation of a zero-day vulnerability.[6]

To match the intent of the Act, CISA should amend its definition of a substantial cyber incident.

- The "system or network" referenced in criteria (a) should be one that is critical to a covered entity's operations.
- Criteria (b) should be limited to an entity's critical operations or system.
- Criteria (c) should be limited to severe disruptions in the covered entity's ability to engage in its critical operations.
- Reporting requirements on supply chain incidents described in (d) should be limited to incidents that otherwise meet the reporting triggers.

Significant will mean something different to companies of different sizes, maturity, etc. The agency should recognize and allow for that and let the covered entity determine whether the incident critically impacted its operations or system. A disruption in one segment of the business without a meaningful impact on the overall business itself may not have a substantial impact. A network that is down for a couple hours could impact a business's ability to process payments, without impacting its ability to deliver products and collect payment later. While the inability to accept payment is disrupting the business, it may not be a significant disruption.

The clock for the initial reporting period should start only after the entity confirms a covered incident has occurred.

The Act requires that covered entities report covered incidents "not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred" and "not later than 24 hours after the ransom payment has been made."[7] The 24-hour clock based on when the ransom payment was made is clear. The 72-hour clock for cyber incidents is somewhat ambiguous.

Given that Congress stated

> When determining whether to exercise the authorities provided under this section, the Director shall take into consideration—
> (1) the complexity in determining if a covered cyber incident has occurred;[8]

[6] 89 *Fed. Reg.* 23766 (April 4, 2024) Proposed regulation 6 CFR 226.1
[7] CIRCIA
[8] CIRCIA

it is reasonable to conclude that Congress intended for companies to have the opportunity to triage incidents to verify validity and impact. The 72-hour clock for reporting a cyber incident should begin when a covered entity definitively determines and confirms it has experienced a reportable incident, per the entity's incident response process. Entities should not be compelled to report on potential cybersecurity incidents or unconfirmed incidents, nor should they report on routine incidents affecting non-critical or ancillary systems. Many covered entities lack the resources to do incident response and investigation as well as incident reporting and compliance simultaneously. Expending resources on an incident that turned out not to be a substantial cyber incident strains limited resources and may unintentionally misinform CISA, distracting from efforts on legitimate critical incidents.

Also, and again, an entity might not be able to submit a report within the 72-hour window if its systems are unavailable or it is unsafe to do so. CISA must recognize this reality and establish accommodations for such circumstances. Good faith cooperation should not qualify as "inadequate," and be a factor in determining whether a subpoena is necessary. Additionally, the scope of information that CISA could attempt to compel through subpoena should be clearly defined in the final rule.

Information reported to the agency must be kept confidential and secure.

The individual reports would be of tremendous interest to a range of adversaries. Compiling all the data from all these reports in one place makes the system where the data is stored a highly attractive target. Unfortunately, the federal government does not have a great track record of maintaining confidentiality or security, and CISA is not immune.[9] Although the incident reports are protected from disclosure under the Freedom of Information Act (FOIA), there is a long history of government inadvertently releasing protected information via FOIA request and generally being unable to secure sensitive information. Given the sensitivity of the data that will be included in these reports, the agency simply must do better.

The proposal cites various rules and statutes about how the information is to be stored, yet the question remains, is it enough? The agency should provide additional information on controls in place, and penalties imposed on people or entities that misuse the information, improperly release it, or fail to secure it, to bolster confidence in the process. If there is unauthorized access to information submitted by a covered entity, will the impacted entity be notified? What recourse would the entity have? CISA must strongly evaluate its ability to protect the reported information and/or sincerely consider revising the solicited information to still provide value but contain less sensitive data.

[9] https://www.cnn.com/2024/03/08/politics/top-us-cybersecurity-agency-cisa-hacked/index.html

Covered entities should not be required to retain incident data.

Retaining cyber incident data is a really a bad idea that adds another level of cybersecurity risk. For example, if a vulnerability is maintained on a backup simply to retain information and it is inadvertently brought back into the operational environment. Best practice is to delete or eliminate the cyber vulnerability as best as possible and recover to a normal operation. This removes the added risk of retaining vulnerabilities somewhere in the environment. If for any reason the vulnerability leaves a hidden residual or time-based code, a resurgence of the vulnerability is possible. The agency should remove the proposed requirement for retention.

The reporting portal should be user-friendly and meet company needs.

The reporting portal should only solicit basic information for the initial report as previously discussed. Follow-up reports should amend the existing initial report so that companies can add on to the existing information and the data will be linked accordingly. It should allow a third party to submit the initial report and the company to submit the follow-up(s), if that works best for the company. Also, the portal should allow for internal legal review prior to submission to CISA. The agency should provide a test environment of the portal for covered entities to test and provide feedback to the agency to ensure usability prior to implementation.

* * * * *

The Meat Institute appreciates the opportunity to provide these comments and requests the agency amend the proposed requirements accordingly. Reporting should be refined so that CISA is provided with only the most relevant information, which will also reduce the burden of compliance on the covered entities. We look forward to engaging with CISA to advance cybersecurity. Please contact us if you have questions about these comments or anything else regarding this matter. Thank you for your consideration.

Respectfully submitted,

Casey Lynn Gallimore
Director, Regulatory Policy

Cc: Julie Anna Potts
Mark Dopp
Nathan Fretz

Attachment 1. Proposed reporting requirements by category. Green: This information will likely be available and reportable within the initial reporting period. Yellow: This information may become available as the incident is investigated but will not likely be available within the initial reporting period. Red: This information is either 1) not appropriate to share due to the risk posed to the victim company or 2) not likely to ever be available.

Cyber Incident (Section 226.8)	**Ransom Payment (Section 226.9)**
(a)A description of the covered cyber incident, including but not limited to:	(a) A description of the ransomware attack, including but not limited to:
(1)Identification and description of the function of the affected networks, devices, and/or information systems that were, or are reasonably believed to have been, affected by the covered cyber incident, including but not limited to: (i) Technical details and physical locations of such networks, devices, and/or information systems; and (ii) Whether any such information system, network, and/or device supports any elements of the intelligence community or contains information that has been determined by the United States Government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in 42 U.S.C. 2014(y);	(1)Identification and description of the function of the affected networks, devices, and/or information systems that were, or are reasonably believed to have been, affected by the covered cyber incident, including but not limited to: (i) Technical details and physical locations of such networks, devices, and/or information systems; and (ii) Whether any such information system, network, and/or device supports any elements of the intelligence community or contains information that has been determined by the United States Government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in 42 U.S.C. 2014(y);
(2) A description of any unauthorized access, regardless of whether the covered cyber incident involved an attributed or unattributed cyber intrusion, identification of any informational impacts or information compromise, and any network location where activity was observed;	(2) A description of any unauthorized access, regardless of whether the ransomware attack involved an attributed or unattributed cyber intrusion, identification of any informational impacts or information compromise, and any network location where activity was observed;
(3) Dates pertaining to the covered cyber incident, including but not limited to: (i) The date the covered cyber incident was detected; (ii) The date the covered cyber incident began; (iii) If fully mitigated and resolved at the time of reporting, the date the covered cyber incident ended; (iv) The timeline of compromised system communications with other systems; and (v) For covered cyber incidents involving unauthorized access, the suspected duration of the unauthorized access prior to detection and reporting;	(3) Dates pertaining to the ransomware attack, including but not limited to: (i) The date the ransomware attack was detected; (ii) The date the ransomware attack began; (iii) If fully mitigated and resolved at the time of reporting, the date the ransomware attack ended; (iv) The timeline of compromised system communications with other systems; and (v) For ransomware attacks involving unauthorized access, the suspected duration of the unauthorized access prior to detection and reporting;

(4) The impact of the covered cyber incident on the covered entity's operations, such as information related to the level of operational impact and direct economic impacts to operations; any specific or suspected physical or informational impacts; and information to enable CISA's assessment of any known impacts to national security or public health and safety;	(4) The impact of the ransomware attack on the covered entity's operations, such as information related to the level of operational impact and direct economic impacts to operations; any specific or suspected physical or informational impacts; and information to enable CISA's assessment of any known impacts to national security or public health and safety;
(b) The category or categories of any information that was, or is reasonably believed to have been, accessed or acquired by an unauthorized person or persons;	
(c) A description of any vulnerabilities exploited, including but not limited to the specific products or technologies and versions of the products or technologies in which the vulnerabilities were found;	(b) A description of any vulnerabilities exploited, including but not limited to the specific products or technologies and versions of the products or technologies in which the vulnerabilities were found;
(d) A description of the covered entity's security defenses in place, including but not limited to any controls or measures that resulted in the detection or mitigation of the incident	(c) A description of the covered entity's security defenses in place, including but not limited to any controls or measures that resulted in the detection or mitigation of the incident
(e) A description of the type of incident and the tactics, techniques, and procedures used to perpetrate the covered cyber incident, including but not limited to any tactics, techniques, and procedures used to gain initial access to the covered entity's information systems, escalate privileges, or move laterally, if applicable;	(d) A description of the tactics, techniques, and procedures used to perpetrate the ransomware attack, including but not limited to any tactics, techniques, and procedures used to gain initial access to the covered entity's information systems, escalate privileges, or move laterally, if applicable;
(f) Any indicators of compromise, including but not limited to those listed in § 226.13(b)(1)(ii), observed in connection with the covered cyber incident;	(e) Any indicators of compromise the covered entity believes are connected with the ransomware attack, including, but not limited to, those listed in section 226.13(b)(1)(ii), observed in connection with the ransomware attack;
(g) A description and, if possessed by the covered entity, a copy or samples of any malicious software the covered entity believes is connected with the covered cyber incident;	(f) A description and, if possessed by the covered entity, a copy or sample of any malicious software the covered entity believes is connected with the ransomware attack;
(h) Any identifying information, including but not limited to all available contact information, for each actor reasonably believed by the covered entity to be responsible for the covered cyber incident;	(g) Any identifying information, including but not limited to all available contact information, for each actor reasonably believed by the covered entity to be responsible for the ransomware attack;
(i) A description of any mitigation and response activities taken by the covered entity in response to the covered cyber incident, including but not limited to:	(m) A description of any mitigation and response activities taken by the covered entity in response to the ransomware attack, including but not limited to:
(1) Identification of the current phase of the covered entity's incident response efforts at the time of reporting;	(1) Identification of the current phase of the covered entity's incident response efforts at the time of reporting;

(2) The covered entity's assessment of the effectiveness of response efforts in mitigating and responding to the covered cyber incident;	(2) The covered entity's assessment of the effectiveness of response efforts in mitigating and responding to the covered cyber incident;
(3) Identification of any law enforcement agency that is engaged in responding to the covered cyber incident, including but not limited to information about any specific law enforcement official or point of contact, notifications received from law enforcement, and any law enforcement agency that the covered entity otherwise believes may be involved in investigating the covered cyber incident;	(3) Identification of any law enforcement agency that is engaged in responding to the covered cyber incident, including but not limited to information about any specific law enforcement official or point of contact, notifications received from law enforcement, and any law enforcement agency that the covered entity otherwise believes may be involved in investigating the covered cyber incident;
(4) Whether the covered entity requested assistance from another entity in responding to the covered cyber incident and, if so, the identity of each entity and a description of the type of assistance requested or received from each entity;	(4) Whether the covered entity requested assistance from another entity in responding to the covered cyber incident and, if so, the identity of each entity and a description of the type of assistance requested or received from each entity;
(j) Any other data or information as required by the web-based CIRCIA Incident Reporting Form or any other manner and form of reporting authorized under § 226.6.	(n) Any other data or information as required by the web-based CIRCIA Incident Reporting Form or any other manner and form of reporting authorized under § 226.6.
	(h) The date of the ransom payment;
	(i) The amount and type of assets used in the ransom payment;
	(j) The ransom payment demand, including but not limited to the type and amount of virtual currency, currency, security, commodity, or other form of payment requested;
	(k) The ransom payment instructions, including but not limited to information regarding how to transmit the ransom payment; the virtual currency or physical address where the ransom payment was requested to be sent; any identifying information about the ransom payment recipient; and information related to the completed payment, including any transaction identifier or hash;
	(l) Outcomes associated with making the ransom payment, including but not limited to whether any exfiltrated data was returned or a decryption capability was provided to the covered entity, and if so, whether the decryption capability was successfully used by the covered entity;