July 3, 2024

Submitted electronically via Regulations.gov

Ms. Jen Easterly
Director, Cybersecurity and Infrastructure Security Agency
CISA Mailstop – 0630
Department of Homeland Security
1100 Hampton Park Blvd.
Capitol Heights, MD 20743-0630

Dear Ms. Easterly:

Re: Docket Number CISA-2022-0010: Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements

The undersigned national real estate associations represent a broad coalition of housing providers and commercial property owners that are committed to working together with policymakers and to safeguard our nation's businesses against rising cybersecurity risks. We submit these comments in response to the Cybersecurity and Infrastructure Security Agency's ("CISA" or "the agency") Proposed Rule related to Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements.[1] We support a unified but flexible regulatory framework for data security and incident notification. We believe it is important to have a balanced approach to providing consumers with meaningful information about material cybersecurity risks and incidents, while also not imposing overly burdensome regulations on the real estate/rental housing industry or unintentionally exposing our members to substantially greater cybersecurity risks.

Perspective on the Proposal

Our members understand the critical importance of maintaining the integrity of the highly sensitive data collected, used, and maintained to support applicants, residents, and employees in the real estate and rental housing industry. In the course of doing business, property and rental

[1] Cybersecurity Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 Fed. Reg. 23644 (proposed Apr. 4, 2024).

housing owners and operators, and their third-party service providers, collect, use, and maintain a significant amount of highly sensitive personal data about applicants, residents, and employees. This information is used in a wide variety of essential business operations but also makes rental housing firms a target of malicious actors.

Given the ever-expanding cyber-threat landscape, the rental housing and real estate industry has made defense against these vulnerabilities a top priority. We have undertaken efforts within the rental housing and real estate industry to mitigate cybersecurity risks, to implement policies to prevent and mitigate such risks, and to encourage investments in bolstering cyber defenses to protect data. To those ends, we have commissioned white papers on the threat landscape and provide resources and best practices for the rental housing industry.

Our groups are broadly supportive of CISA's efforts to bolster cybersecurity and to ensure that consumers receive material information regarding companies' cyber risk management and incidents. However, our comments provided here concerns specific elements of the Proposed Rule that are overly burdensome given the complexity of cybersecurity incidents that may result in increased cyber risks and liability for public companies.

Executive Summary

The Proposed Rule imposes overly burdensome requirements and requires companies to assume unnecessary, but significant, legal and cybersecurity risks. The following details our concerns, which are addressed in more depth in the "Detailed Discussion" section below:

1. **The Proposed Rule's reporting requirements are overly burdensome and do not provide industry with the right amount of flexibility.**
2. **The cost of compliance with the Proposed Rule is disproportionate to the value of risk reduction and cyber resilience.**
3. **The Proposed Rule's reporting deadlines are unclear and increase risk of attack from additional bad actors.**
4. **The Proposed Rule adds another reporting requirement to an already cluttered landscape.**

Detailed Discussion

1. **<u>The Incident Reporting Requirements are Overly Burdensome.</u>**
   The Proposed Rule defines the term "covered cyber incident" to mean a "substantial cyber incident experienced by a covered entity."[2] CISA should revise the definition of "covered cyber incident" to establish a higher threshold for reporting and avoid over-reporting of incidents that cause minimal harm or impact. For instance, the requirement to report a "disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services" is too vague and could lead to a large number of immaterial or less significant incidents being reported. The CIRCIA statute includes additional language that should prove helpful to refining this definition. CIRCIA provides that disruptions to business or industrial operations includes "a denial-of-service attack, ransomware attack, or exploitation of a zero-

[2] Cybersecurity Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 Fed. Reg. 23644 (proposed Apr. 4, 2024) at §226.1

day vulnerability."[3] Congress clearly intended for a covered cyber incident to mean a specific operational disruption that is much narrower than the type of disruption contemplated by the proposed rule.

The disclosures under the Proposed Rule require detailed information about the cybersecurity incident that goes well beyond Congress's intent that CIRCIA promote "shared awareness of the cyber threats across the public and private sectors."[4] As drafted, the proposed rule would lead to large-scale data collection that goes beyond any existing reporting requirement. Instead, CISA should recognize CIRCIA meant to strike a balance between CISA's need for quick access to data and allowing victims to respond to the immediate concerns of the cyberattack without concern for burdensome reporting requirements. The Proposed Rule upsets this balance by requiring victims to quickly report information, even if it is unknown at the time, which will ultimately require victims to file numerous supplemental reports.

2. **The Cost of Compliance with the Proposed Rule is Disproportionate to the Value of Risk Reduction and Cyber Resilience.**

CISA estimates that the rule will apply to over 300,000 entities who will submit over 200,000 reports over an 11-year period.[5] CISA further estimates that the cost of compliance will exceed $1.4 billion during that period, with most of those costs accruing between 2026 and 2033, when the rule is in effect. Costs include the labor required to review incidents and submit a report, as well as the costs of data retention.[6] These costs are substantial. As we have indicated, our members take cybersecurity seriously and we have invested a significant amount of resources into building robust cybersecurity measures to ensure our customers' data is secure. Requiring additional investment to comply with the broad cyber incident reporting requirements outlined in the Proposed Rule will take away valuable resources that could otherwise be used to make systems more secure and could increase the cost of risk management which given the already ballooning costs of insurance coverage and their impact on property operations.

Additionally, CISA's own analysis recognizes substantial uncertainty in the agency's calculation for affected entities and their costs. Previous reporting requirements, such as the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, focused on specific sectors and allowed regulators to tailor both their analysis and the rule. In comparison, the broad applicability of CIRCIA across sectors and the varying capabilities of entities among different sectors to address cybersecurity risks makes it challenging to estimate compliance costs for all covered entities. CISA should look at the financial burdens placed on all entities for compliance with the rule when considering the potential benefits. One way to reduce compliance costs would be to reduce the data-retention threshold, which is estimated to cost more than $306 million. These funds could instead be repurposed for security mitigation measures.

3. **Reporting Deadlines are Unclear and Increase Risk of Attack from Additional Bad Actors**.

While CIRCIA mandates that covered entities file a report with CISA within 72 hours of a cyber incident, the Proposed Rule adds that a report must be submitted 24 hours after a ransom

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

[4] S. Rep. No. 117-249, at 2

[5] Cybersecurity Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 Fed. Reg. 23644 (proposed Apr. 4, 2024).

[6] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements," 89 Federal Register 23644-23776

payment is made. Strict enforcement of the 72-hour and 24-hour timeframes will result in reporting before a threat is contained or eradicated.[7] Requiring reporting within such a short time after a cyber security incident occurs pulls resources away from efforts to address the on-going incident and could lead to additional cybersecurity risks. For example, a covered entity subject to a cyber attack may be required to disclose the incident while negotiating with the cybercriminals, which could undermine the covered entity's negotiating position and enhance the cybercriminals bargaining power. With the focus on reporting, a covered entity may not be able to contain an incident in an efficient manner, leaving that entity open to further cyberattacks. As such, our groups request CISA lessen the reporting burdens and extend the 24-hour ransom payment reporting timeframe so that covered entities have appropriate time to contain and eradicate cyber incidents before reporting is required.

While CISA cannot extend the 72-hour reporting requirement, CISA can take additional measures to clarify a covered entity's reporting requirements and lessen the burden on covered entities to allow their focus to be on addressing a cyber incident. The Proposed Rule requires a covered entity file a report when it "reasonably believes" that a covered incident has occurred, leaving it to the judgment of the covered entity to determine when it is required to report a cyber incident.[8] CISA should provide flexibility in initiating the 72-hour clock as it can be challenging for covered entities to identify a "reasonable belief" that an incident has occurred. In addition, requiring a complete initial report will require covered entities expend considerable time reporting an incident that is not fully unknown, resulting in incorrect reporting, constant corrections and convoluted reports. As such, CISA should allow flexibility to report only certain critical information in an initial report, with the remainder of information submitted with supplemental reports once the covered entity has had more time to investigate the incident. Finally, requiring covered entities submit supplemental reports "promptly" provides little clarity on when supplemental reports must be filed and increases the risk covered entities inadvertently fail to comply with the supplemental reporting requirements. CISA should clarify when additional information must be submitted following an initial report filing.

4. **The Proposed Rule Adds Another Reporting Requirement to an Already Cluttered Landscape**.

The Proposed Rule adds another reporting requirement to the numerous federal and state data reporting laws already in place. This makes it increasingly challenging to address a cyber incident while simultaneously navigating the applicability of cyber reporting laws. Many of our members own or operate or provide technology solutions to properties in multiple states, and the patchwork of cybersecurity laws results in additional costs to comply with reporting requirements and increases the risk that a covered entity unintentionally fails to properly comply. As such, CISA should harmonize its reporting obligations so that it is consistent with other federal and state reporting laws.

While the Proposed Rule contains an exception for covered entities that are required to file "substantially similar" information to another federal agency that has an information-sharing agreement with CISA, is it not clear what other reporting requirements are considered "substantially similar" to CISA's requirements and places the burden on covered entities to

[7] Cybersecurity Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 Fed. Reg. 23644 (proposed Apr. 4, 2024) at §226.5, available at Federal Register :: Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements.

[8] Cybersecurity Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 Fed. Reg. 23644 (proposed Apr. 4, 2024) at §226.5, available at Federal Register :: Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements.

make this determination.[9] In addition to requiring CISA post its information-sharing agreements online, CISA should provide additional clarify on what information and reporting timeframes it considers "substantially similar" to CISA's required information and reporting timeframes.

Conclusion

We appreciate the opportunity to submit these comments on this important topic and hopes it can serve as a resource to assist CISA in the development of clear, effective and secure cyber incident reporting rules. We trust that CISA will find our comments helpful, and we stand ready to assist CISA in its work. Thank you for the opportunity to comment on this important issue.

Respectfully,

BOMA International

Council for Affordable and Rural Housing

Enterprise Community Partners

ICSC

Institute of Real Estate Management

Manufactured Housing Institute

National Affordable Housing Management Association

National Apartment Association

National Association of Home Builders

National Association of Housing Cooperatives

National Multifamily Housing Council

National Rental Housing Council

Real Estate Roundtable

[9] Cybersecurity Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 Fed. Reg. 23644 (proposed Apr. 4, 2024) at §226.4, available at Federal Register :: Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements.