Seeking harmony: CISA's proposed cyber reporting rules for critical infrastructure are an ambitious work in progress

Received (in revised form): 1st October, 2024

Joseph C. Folio III

Partner, Morrison Foerster, USA

Joseph C. Folio III is a Partner at Morrison Foerster LLP, where he focuses on cyber security issues and white-collar investigations. As Chief Counsel for the Senate Homeland Security and Governmental Affairs Committee, he advised on the development and drafting of cyber security legislation, responses to breach and ransomware incidents affecting government agencies and the private sector and conducted oversight of the Cybersecurity and Infrastructure Security Agency (CISA).

Morrison Foerster, 2100 L Street, NW, Suite 900, Washington, DC 20037, USA
E-mail: JFolio@mofo.com

Alexandra Ross

Senior Director, Data Protection, Use & Ethics Counsel, Autodesk, USA

Alexandra Ross is Senior Director, Data Protection, Use & Ethics Counsel at Autodesk, Inc., where she provides legal, strategic and governance support for Autodesk's global privacy, security and trusted artificial intelligence (AI) programmes. She is also an adviser to BreachRx, an adviser to the University of San Francisco's Strategic AI programme and a member of Women Leaders in Data & AI (WLDA). She is a certified information privacy professional (Certified Information Privacy Professionals/United States [CIPP/US], Certified Information Privacy Professionals/Europe [CIPP/E], Certificate in Performance Measurement [CIPM], Certified Information Privacy Technologist [CIPT], Fellow Information Privacy [FIP] and Privacy Law Specialist [PLS]).

Autodesk, Inc., The Landmark, One Market, Suite 500, San Francisco, CA 94105, USA
E-mail: alexandra.ross@autodesk.com

Ian Wolfe

Security Counsel, Autodesk, USA

Ian Wolfe is a Security Counsel at Autodesk, Inc., where he provides legal support to security incident response, threat detection and intelligence, third-party risk management and global cyber security compliance programmes. Prior to Autodesk, he worked in the healthcare, cyber security software and advertising technology industries. Ian holds the Certified Information Privacy Technologist (CIPT) certification.

Autodesk, Inc., The Landmark, One Market, Suite 500, San Francisco, CA 94105, USA
E-mail: ian.wolfe@autodesk.com

Nicholas A. Weigel

Associate, Morrison Foerster, USA

Nicholas A. Weigel is an associate at Morrison Foerster LLP, where he focuses on litigation and national security matters. He has worked at the Department of Justice's National Security Division and the US Attorney's Offices for the Eastern District of New York and the District of Massachusetts, where he contributed to federal cybercrime prosecutions. He has written on artificial intelligence (AI), electronic surveillance and encryption.

Morrison Foerster, 2100 L Street, NW, Suite 900, Washington, DC 20037, USA
E-mail: NWeigel@mofo.com

Abstract The federal cyber incident reporting regulations proposed by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) are ambitious and laudable but, with some modest changes, could go even farther to protect US critical infrastructure. First, to reduce the growing burden of duplicative and overlapping reporting obligations, CISA should take more concrete steps to harmonise its proposed cyber incident reporting requirements with those of other federal, state and local agencies. Secondly, CISA should provide greater clarity on the types of data that must be preserved following a reportable cyber incident and shorten the default preservation period to six months, with an option to extend it if necessary. Finally, CISA should provide additional guidance about how the reporting requirements apply to the international operations of multinational companies. By offering additional clarity and reducing the burden on private sector entities, CISA could create a streamlined cyber incident report regime that is more closely aligned with the goal of providing timely, essential and actionable information that will better protect the US critical infrastructure.

KEYWORDS: Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), Cybersecurity and Infrastructure Security Agency (CISA), critical infrastructure, data breach

DOI: 10.69554/JHEV8231

INTRODUCTION

The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), which became law in March 2022, charged the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) with establishing a federal cyber incident reporting regime to help safeguard US critical infrastructure.[1] In its view, this new law has made CISA the 'central repository for federal cyber incident reporting'.[2] In April 2024, pursuant to this authority, CISA issued a notice of proposed rulemaking (Proposed Rule) that affirms its broad reach: its cyber incident reporting requirements will apply to an estimated 316,244 'covered entities' across 16 critical infrastructure sectors.[3] The rule is expected to be finalised in late 2025 (see Figure 1).

CISA's vision for cyber incident reporting is laudable, namely, to provide it with 'visibility into significant cyber incidents being conducted across U.S. critical infrastructure sectors and enabl[e] coordinated, informed Federal government action against perpetrators of cyberattack'.[4] If thoughtfully implemented, CIRCIA can and will strengthen the country's cyber

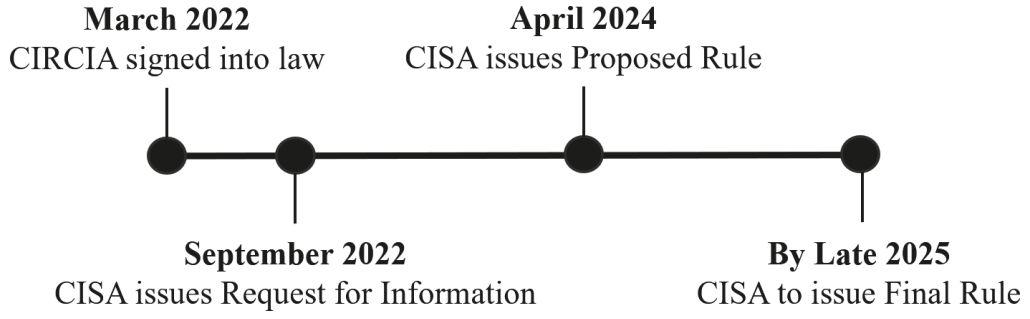

Figure 1: Timeline of CISA's cyber incident reporting rule

readiness, improve companies' cyber response capabilities and protect critical infrastructure. CISA's 133-page Proposed Rule outlines how the agency plans to achieve these goals. Yet despite its length, the Proposed Rule leaves many questions unanswered. In this paper, we focus on three ways in which the Proposed Rule could be improved.

First, the Proposed Rule could take more concrete steps to harmonise CISA's cyber incident reporting requirements with the reporting obligations of other federal, state and local agencies. In practice, a company that experiences a reportable cyber incident will have to juggle reporting obligations to a growing list of authorities with different deadlines and varied levels of required detail about the incident. These overlapping requirements place an added burden on companies experiencing cyber incidents, both in terms of compliance costs and the increased risk of enforcement for any shortfalls.

Secondly, the Proposed Rule's preservation obligations are likely to be burdensome and costly for covered entities. The Proposed Rule, which requires companies to preserve all data 'relevant' to a reportable incident for at least two years, could better specify the types of data that must be preserved. In addition, given the likelihood that initial reports will be supplemented over time, the preservation obligations are likely to extend well beyond two years, yet it is not clear that collecting two-plus years of data for every reported cyber incident will serve the aims of the Proposed Rule. Instead, the voluminous data collected for each incident — when combined with CISA's estimated 25,000 incidents to be reported annually — may make it *more* difficult for CISA to fulfil CIRCIA's purpose of analysing incidents, identifying trends, and broadly sharing relevant information.

Finally, the Proposed Rule should address and provide additional guidance about how multinational companies should assess the reporting obligations of their international operations. The Proposed Rule's focus on 'entities' risks being both over- and under-inclusive insofar as legally distinct international operations can be excluded from CIRCIA's reporting obligations. In certain instances, however, there may be international cyber incidents that nonetheless threaten domestic critical infrastructure entities.

For each of these issues, CISA should provide additional guidance to help ensure it fulfils the purposes of CIRCIA while separating the wheat from the chaff, specifying which relevant information must be reported, and minimising the burden on private sector critical infrastructure entities as they navigate responding to cyber incidents.

FURTHER HARMONISATION WITH OTHER FEDERAL REPORTING REQUIREMENTS IS NEEDED, AND CIRCIA AGREEMENTS ARE NOT (CURRENTLY) THE ANSWER

Once the regulations are finalised, companies will need to add CIRCIA to the growing list of potentially applicable global cyber reporting laws they consider if and when a cyber incident occurs. Through CIRCIA, CISA has the potential to harmonise US federal reporting requirements. This would improve federal agencies' ability to respond to cyber incidents, strengthen the nation's cyber response capabilities and allow companies to focus on other aspects of incident response, such as containment.

As it stands, however, the Proposed Rule would instead merely add another reporting requirement. For example, a public medical device company already may need to report an incident involving protected health information and health records to at least: 1) the Securities and Exchange Commission (SEC) within four days of determining the incident was material; 2) the Department of Health and Human Services (HHS) and Federal Trade Commission (FTC)

within 60 days; and 3) the Food and Drug Administration (FDA) within 30 days. Under the Proposed Rule, this company would also be required to report the incident to CISA within 72 hours.[5] Companies — even those with significant cyber security resources and well-defined incident response procedures — will need to devote additional time and resources to meeting CIRCIA's reporting requirements.

In the Proposed Rule, CISA recognised that 'the number of existing cyber incident reporting requirements at the Federal and [State, Local, Tribal or Territorial] levels' means CIRCIA could create 'potentially duplicative requirements to report cyber incidents'.[6] The Proposed Rule also cites the Department of Homeland Security's 'Harmonization of Cyber Incident Reporting to the Federal Government' report (the CIRC Report), which identified 52 federal cyber incident reporting requirements. While acknowledging the issue, however, the Proposed Rule offered only one concrete solution — 'CIRCIA Agreements' — for resolving it. A CIRCIA Agreement would exempt a company from filing a notice with CISA if it is required by 'law, regulation or contract' to report cyber incidents to another federal agency.[7] Notably, however, the exemption applies only if the other reporting regime requires the sharing of 'substantially similar' information 'in a substantially similar timeframe'.[8]

In the Proposed Rule, CISA stated, 'to the extent practicable … [it is] committed to working in good faith' to finalise CIRCIA Agreements with federal agencies.[9] Entering into these agreements may be difficult, however, given the differences in cyber incident reporting requirements. There are currently few, if any, other cyber incident reporting regimes that require 'substantially similar' information to be reported 'in a substantially similar timeframe'. For example, in contrast with the Proposed Rule's requirement that a covered entity report a covered cyber incident within 72 hours,[10] the SEC's cyber incident reporting rule requires a covered entity to publicly disclose certain cyber incidents within four business days of determining that an incident is material.[11] But the SEC rule does not require the disclosure of the types of information required by the Proposed Rule and, in practice, a materiality determination may take much longer than 72 hours.[12]

The reporting requirements of other federal agencies similarly fall short of meeting the criteria for a CIRCIA Agreement. Department of Energy (DOE) regulations require electric utilities and certain other entities to report certain cyber incidents as soon as one hour after they are discovered.[13] Although this timing would satisfy the Proposed Rule's 72-hour reporting requirement, the information that needs to be reported to DOE is much less detailed than what is required by the Proposed Rule.[14] Similarly, Department of Defense (DoD) regulations require defence contractors to report cyber incidents using an Incident Collection Form, which does not match the reporting requirements in the Proposed Rule.[15] Likewise, regulations promulgated pursuant to the Gramm–Leach–Bliley Act (GLBA) require financial institutions to report certain breaches of customer information to the FTC via an electronic form with fields far less detailed than the information that must be reported under the Proposed Rule.[16]

Even if another federal agency had reporting obligations that would satisfy the timing and substance of CISA's reporting requirements, the Proposed Rule also requires that CISA has an established agreement with the other federal agency — a CIRCIA Agreement — before it will excuse a company from having to submit a report. At time of writing of this paper, no such agreements between agencies exist, and it seems unlikely that any such agreement will be reached in the near future. As a result, companies that are deemed to fall under CIRCIA obligations likely will have

competing reporting requirements and will have to provide multiple notifications within a short time period. This presents several challenges.

First, affected companies will have to revamp compliance programmes to account for these different reporting requirements and ensure that there is a mechanism for deciding whether, when, how and to whom a cyber incident must be reported. And, because the Proposed Rule's definition of a reportable cyber incident is much broader than the definition used by other federal agencies, a company's reporting obligations are likely to be triggered at different points in time across a security incident, thereby further complicating compliance efforts. Companies will need to devote resources to modifying incident response plans, reconfiguring compliance programmes, and training staff.

Secondly, preparing and filing multiple reports and supplemental reports with varying requirements risks confusion and unintentional mistakes, especially in the fast-moving environment of a cyber security incident. For example, a financial institution that experiences an incident will need to separately determine whether the incident was 'substantial' under CIRCIA, whether it was 'material' under the SEC rule, and whether it resulted in the disclosure of more than 500 customers' financial information under GLBA. The company may need to 'start the clock' for CIRCIA on Monday, GLBA on Tuesday, and the SEC rule on Wednesday. In the fast-moving environment of incident response, these compliance requirements could distract from actually containing the incident.

The Proposed Rule offers few concrete solutions to the harmonisation issue beyond CIRCIA Agreements. After highlighting its participation in an intergovernmental council to address the issue of overlapping reporting requirements, CISA said it is 'committed to exploring ways to harmonize [the Proposed Rule] with other existing Federal reporting requirements, where practicable'.[17] Although these coordination efforts are welcome, CISA did not expressly state where harmonisation efforts would be impracticable, and the general tenor of the Proposed Rule — such as CISA referring to itself as 'the newly minted central repository for cyber incident reporting'[18] — suggests that CISA views its reporting requirements as a floor rather than a ceiling to be negotiated with other agencies.

It would be a significant improvement if CISA became the 'central repository' for cyber incident reporting and designated itself as the single point of contact for critical infrastructure entities. Instead of providing a mechanism to excuse a covered entity from having to report a cyber incident under CIRCIA, CISA should strive to position itself as the central node for all cyber incident reports from critical infrastructure entities and then be responsible for sharing that information with any relevant federal regulatory or oversight entity. Once an incident report is filed, CISA could ensure that the report is distributed to other interested federal agencies. CISA is well positioned to be such a central repository because, unlike most other federal agencies, its cyber incident reporting regime is explicitly grounded in a federal statute. If CISA were the central repository, it could facilitate coordination across the federal government and ensure that all relevant agencies, including law enforcement, would have the information they need.

Alternatively, CISA could determine that each of the 52 cyber incident reporting requirements identified in the CIRC Report satisfy CIRCIA's initial reporting requirements and not require CIRCIA Agreements with the relevant agencies. If CISA believes a specific reporting requirement does not accomplish CIRCIA's goals for a particular incident, it can require the reporting entity to provide additional information. At that time, CISA can tailor its request for additional information, thereby reducing the overall reporting

burden. If incident reporting pursuant to the standards established by another agency regularly falls short of satisfying CISA, the regulated entities, and possibly the agency itself, are likely to amend reporting requirements to more closely align with CISA's. Harmonising by default at the outset would simplify incident reporting, benefitting affected companies, CISA, and the agencies managing the other 52 reporting requirements.

THE PROPOSED PRESERVATION REQUIREMENTS ARE VAGUE AND, AS A RESULT, MORE BURDENSOME THAN NECESSARY

The Proposed Rule's preservation requirements, on which CISA received 'very few'[19] comments when it first raised the issue in 2022,[20] are likely to impose a significant cost on companies that may not become clear until a reportable incident occurs.

Although CIRCIA required CISA to provide a 'clear description of the types of data required to be preserved',[21] the Proposed Rule includes only broad descriptions of the data that must be preserved, such as 'relevant log entries, memory captures and forensic images' and 'network information or traffic related to the cyber incident'.[22] For log entries, memory captures and forensic images, CISA added that preservation is required only when 'the covered entity believes in good faith [they] are relevant to the incident'.[23] The Proposed Rule, however, does not define what it means to be 'relevant' or 'related' to an incident, and therefore the risk of over- or under-preservation is real.

Additionally, although the Proposed Rule imposes a two-year data retention period, a little-noticed part states that, '[i]f, however, a covered entity submits one or more Supplemental Reports on a single covered cyber incident or ransom payment, the two-year retention period restarts at the time of submission of each Supplemental Report'.[24] In light of the Proposed Rule's 72-hour reporting requirement, which means that companies likely will report incidents before all the facts are known, the submission of a supplemental report — and, thus, the extension of the preservation clock — is nearly inevitable.[25] In fact, in the Proposed Rule, CISA states that it 'recognizes that the data retention period may be longer than two years, particularly for the estimated 50% of covered entities that submit one or more Supplemental Reports for a covered cyber incident'.[26]

The ambiguity about what information must be preserved and the indeterminate length of time it must be preserved imposes operational burdens and expenses on companies seeking to comply with the Proposed Rule's requirements. Once a reportable incident occurs, a company must have a system in place to identify the data that is 'relevant' or 'related' to the incident, which may not be clear at the outset. This problem can be compounded if a company uses third-party service providers, including incident response vendors, that need to be read-into and part of any preservation efforts. Additionally, the period immediately after an incident is detected can be chaotic, and incident responders often work with incomplete information. Within the first 72 hours, incident responders are likely to be overly inclusive and identify data that *may* be related to the incident, but that, after further analysis, is determined to be unrelated. Typically, once a company determines data is not related to an incident, the data would not be 'tagged' for further retention, but would instead be subject to the company's standard data retention policies. To comply with the Proposed Rule, however, companies may be required to retain irrelevant data merely because the data was thought to be relevant during the first hours following an incident. This makes data retention operations more difficult for companies and will likely result in the retention — and possible submission to CISA — of irrelevant data.

The preservation of a substantial amount of data over multiple years also can be very costly. Some of the data types identified in the Proposed Rule, such as memory captures and forensic images, can be voluminous and therefore extremely costly to preserve, especially if the data needs to be replicated or transferred from a cloud provider. For example, cloud storage and data transfer costs for a cyber security incident that required imaging 100TB of data may reach tens of thousands of dollars.

CISA should consider three changes to the Proposed Rule's preservation requirements to address these issues. First, CISA should consider shortening the default preservation time requirement to 180 days unless it makes a determination that the incident merits preservation for a longer period of time. Although CISA's explanation for a longer preservation period was to 'support the ability of analysts and investigators to understand how a cyber incident was perpetrated and by whom as well as enable data and trend analysis and the investigation of incidents',[27] that reasoning fails to acknowledge that not every reportable cyber incident is likely to merit a fully fledged investigation, even if such an in-depth inquiry was feasible given staffing and time constraints. A shorter default preservation time period also will allow CISA to identify and focus on the cyber incidents that are truly concerning while minimising the burden on affected companies.

Additionally, if CISA seeks to extend a company's preservation obligations beyond the default time period of 180 days, it should be required to make a written factual determination of the basis for its request and the types of data and information it wants the company to preserve. The factual determination would be no different from a request for information provided for under the Proposed Rule.[28] Under that provision, the Director of CISA would make a request for the preservation of certain data and information, and the affected company would have an opportunity to respond and possibly negotiate the scope or duration of the preservation request. This would provide an opportunity for CISA and the company to focus on the data that matters and minimise the burden on an affected company. To the extent a company refuses to comply with a preservation request, CISA has the authority to punish non-compliance if the information sought is truly relevant to the cyber incident. Under the Proposed Rule, CISA has the authority to issue a subpoena to compel the production of information and, if necessary, enforce the subpoena by filing a civil action in federal court. A company's failure to preserve relevant materials identified by CISA could result not only in an adverse decision by the court but also potentially expose a company to spoliation sanctions if it failed to preserve relevant information. The risk of enforcement will help to ensure that companies adhere to their preservation obligations.

Finally, CISA should allow companies to submit Supplemental Reports that identify data they initially believed to be related to an incident but which, after further analysis, they determined was in fact unrelated. The Proposed Rule's preservation requirements should then not apply to this 'false positive' data. This would benefit both CISA and companies affected by an incident. CISA would receive less irrelevant data, and companies would not be required to devote resources toward the unnecessary preservation of data unrelated to cyber security incidents.

THE DEFINITION OF A 'COVERED ENTITY' DOES NOT FIT NEATLY FOR MULTINATIONAL COMPANIES

The Proposed Rule does not address whether and how the reporting obligations apply to a 'covered entity' that has international operations. Unlike the presidential directives that defined a US critical infrastructure 'operator' in terms

of systems,[29] the Proposed Rule defines 'entity' to mean 'any person, partnership, business, association, corporation, or other organization (whether for-profit, not-for profit, nonprofit, or government) regardless of governance model that has legal standing and is uniquely identifiable from other entities'.[30] It adds that '[t]he organizational structure or nomenclature chosen by the entity does not matter as long as it is a structure that imports legal presence or standing in the United States'.[31] Although the Proposed Rule specifically contemplates a parent corporation 'reporting on behalf of affected subsidiaries', it does not specify whether such subsidiaries must be based in the US.[32] For example, if a subsidiary of a company has operations in Brazil and that subsidiary experiences a cyber security incident, does that need to be reported to CISA under CIRCIA?

The Proposed Rule's focus on whether an entity 'is uniquely identifiable from other entities'[33] and the entity's 'legal presence or standing in the United States'[34] suggests that basic legal principles from other contexts — such as civil discovery and corporate veil piercing — apply to the Proposed Rule and are a basis to determine whether an entity, including a subsidiary, is covered by the reporting requirements.

This lack of certainty, however, puts multinational entities in a difficult position for several reasons. First, more than 100 jurisdictions already have breach notification obligations. Many of them require notice on a specific form in a specific language within 72 hours of determining that a breach of personal information has occurred. Other jurisdictions, such as India, have obligations to provide notice of a cyber security incident within 6 hours.[35] Secondly, security teams at multinational entities should not be expected to be familiar with the entity structure of their employer, especially because subsidiaries are routinely added or removed for business reasons unrelated to a security team's function. Moreover, in the first 72 hours of an incident, security teams' priorities should be to investigate and contain the incident, not attempt to tie the incident back to a specific corporate entity.

To address this uncertainty, CISA should provide additional guidance about how the Proposed Rule applies to multinational companies. In particular, CISA should address whether its 'entity'-based approach means that a company's international operations that do not have legal presence or standing in the US are, in fact, not subject to the Proposed Rule. Alternatively, if CISA is concerned about a cyber incident at a company's legally distinct international operations, then it should provide additional guidance about how and why the Proposed Rule and its reporting requirements apply.

CONCLUSION

When it passed CIRCIA, Congress set an ambitious goal for CISA to become the central repository for the reporting of cyber incidents related to US critical infrastructure. Although CISA's Proposed Rule shows that it is on the right track, as currently drafted, it would impose significant burdens on hundreds of thousands of companies that may not ultimately provide CISA and other federal agencies with the information they need to safeguard US critical infrastructure. By addressing certain core issues, however — namely, improving harmonisation among federal agencies, reducing preservation obligations and adding clarity about how the rules apply to multinational companies — CISA can provide much-needed certainty to companies as it works hand-in-hand with the private sector on an immensely important task: the continued protection of the US critical infrastructure.

References

1. Pub. L. No. 117-103 (2022), codified at 6 U.S.C. § 681 *et seq*.
2. Cyber Incident Reporting for Critical Infrastructure

Act (CIRCIA) Reporting Requirements, 89 Fed. Reg. 23,644, 23,704 (Apr. 4, 2024) (to be codified at 6 C.F.R. Pt. 226) (hereinafter 'Proposed Rule').
3. *Ibid*., at 23,742.
4. *Ibid*., at 23,704.
5. *Ibid*., at 23,770.
6. *Ibid*., at 23,653.
7. *Ibid*., at 23,654.
8. *Ibid*.
9. *Ibid*., at 23,654.
10. *Ibid*., at 23,770.
11. See Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 88 Fed. Reg. 51,896 (4th August, 2023).
12. *Ibid*.
13. See U.S. Department of Energy (DOE), 'Form DOE-417, Electric Emergency Incident and Disturbance Report', available at https://doe417.pnnl.gov/files/DOE-417_Form.pdf (accessed 1st October, 2024).
14. *Ibid*.
15. See U.S. Department of Defense, 'Safeguarding Covered Defense Information – The Basics', available at https://business.defense.gov/Portals/57/Safeguarding%20Covered%20Defense%20Information%20-%20The%20Basics.pdf (accessed 1st October, 2024).
16. See 16 C.F.R. § 314.1(j).
17. Proposed Rule at 23,653.
18. *Ibid*., at 23,704.
19. *Ibid*., at 23,658.
20. Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022, 87 Fed. Reg. 55,833 (12th September, 2022).
21. 6 U.S.C. § 681b(c)(6); Proposed Rule at 23,730.
22. Proposed Rule at 23,731.
23. *Ibid*.
24. *Ibid*., at 23,731–32.
25. The Proposed Rule requires the submission of a Supplemental Report whenever '(a) substantial new or different information becomes available; or (b) the covered entity makes a ransom payment after submitting a covered cyber incident report'. Proposed Rule at 23,742. 'Substantial new or different information' is defined as information that is '(1) is responsive to a required data field in a Covered Cyber Incident Report that the covered entity was unable to substantively answer at the time of submission of that report or any Supplemental Report related to that incident, or (2) shows that a previously submitted Covered Cyber Incident Report or Supplemental Report is materially incorrect or incomplete in some manner'. *Ibid*. at 23,726–27.
26. *Ibid*., at 23,746, n. 417.
27. *Ibid*., at 23,758.
28. *Ibid*., at 23,774 (§ 226.14).
29. In February 2013, President Obama issued Presidential Policy Directive 21 (PPD-21), which provided a definition of what constituted 'critical infrastructure' for the US. On 30th April, 2024, President Biden issued National Security Memorandum 22 (NSM-22), which rescinded and replaced PPD-21 even though the broad contours are similar.
30. *Ibid*., at 23,676.
31. *Ibid*.
32. *Ibid*., at 23,719.
33. *Ibid*., at 23,676.
34. *Ibid*., at 23,677.
35. Indian Computer Emergency Response Team (CERT-In) (April 2022), 'Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet', available at: https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf (accessed 1st October, 2024).