EDUCAUSE

July 1, 2024

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

RE: Comments concerning Docket Number CISA-2022-0010, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements," submitted electronically at https://www.regulations.gov/commenton/CISA-2022-0010-0163

Dear Director Easterly,

On behalf of EDUCAUSE (educause.edu), the association for information technology (IT) in higher education, and the undersigned associations representing a broad cross-section of higher education leaders and professionals, I thank you and your colleagues for the opportunity to comment on the draft regulations proposed by the Cybersecurity and Infrastructure Security Agency (CISA) to implement the reporting requirements of the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) (Federal eRulemaking Portal (Regulations.gov) Docket Number CISA-2022-0010).

The response that follows addresses:

- The proposed application of the draft regulations to the higher education community writ large.
    - CISA proposes to designate all colleges and universities that participate in Federal Student Aid programs as covered entities based on the purported scope of the Education Facilities Subsector (EFS) of the Government Facilities Sector (GFS).
    - However, the basis for this decision is only tenuously supported by the documented history of the critical infrastructure sectors in general and the EFS/GFS specifically.
    - Moreover, neither CISA nor the relevant sector risk management agency (SRMA), the Department of Education (ED), have engaged the higher education institutional community regarding its proposed new designation as a critical infrastructure sector and the subsequent unanticipated application of CIRCIA covered entity status to it.

  - CISA should reconsider this dramatic expansion of regulatory scope, which it proposes to undertake without any relevant engagement with the higher education institutional community or weight given to the size, mission, and resource capacity of the wide variety of colleges and universities that its regulations may now impact.
  - At a minimum, both CISA and ED should initiate substantive outreach to the higher education institutional community about where and how the proposed regulations, including the designation of covered entities under the EFS/GFS, should be adjusted to reflect institutional realities and thereby best serve the goals of CIRCIA.

- The need to effectively address the problem of redundant reporting across federal agencies.
  - Covered entities should not have to compensate for the potential inability of the federal government to resolve redundant reporting across its agencies by bearing the ever-increasing weight of such reporting themselves.
  - If CISA is unable to secure a CIRCIA Agreement with another federal agency prior to the effective date of the regulations when such an agreement should be reasonably possible, then CISA should delay the compliance deadline for covered entities in the relevant sectors or subsectors for at least two years while it continues to pursue a CIRCIA Agreement with its fellow agency or agencies.
  - CISA should seek to leverage the web form and technical infrastructure that it develops for CIRCIA reporting to also facilitate reporting to agencies with requirements that don't lend themselves to a CIRCIA Agreement; by collaborating with federal agencies whose reporting requirements do not overlap with CIRCIA, CISA could create a one-stop site for federal incident reporting in general, and thus greatly simplify reporting by non-federal entities as a whole.
- The basis on which covered cyber incidents would have to be reported.
  - The space for covered entity discretion and judgment in the determination of what constitutes a "substantial cyber incident" is noted and appreciated.
  - However, the NPRM does not include guiding principles and/or an organizing framework that would help establish a shared understanding between CISA and covered entities regarding what constitutes "substantial," "serious," or disruptive incidents; this leaves too much room for compliance misunderstandings and missteps to emerge.
  - CISA should work with the stakeholder community for the proposed regulations to develop a shared set of guiding principles and a more informative organizing framework that both the agency and covered entities can use to ensure compliance alignment to the extent possible.

- The information a covered entity would be required to report and the associated data and records preservation requirements.
    - CISA should provide a more detailed explanation of how the CIRCIA web form and reporting process will prevent malicious actors from submitting false reports as if they originated from covered entities; this information should appear in both the analysis of the final rule as well as in the text of the rule itself.
    - The agency should work with the stakeholder community to develop an appropriate scope for the information entities would be required to report under 226.8(a)(1)(i) and (d). The requirements as currently described would likely lead to over-reporting/over-collection of highly sensitive information, thus creating concerns about the security of reported information—information that CISA may not need in many cases.
    - Concerning "Required Information for Covered Cyber Incident Reports" (226.8) in general, we note that sophisticated response capabilities may be necessary to fulfill the required reporting in many, if not most, instances.
        - In the draft regulations, CISA has not accounted for the lack of such capabilities across the broad range of colleges and universities it has unexpectedly proposed to designate as critical infrastructure/covered entities.
        - As a result, CISA must take care to consistently stress in the final rule and any subsequent guidance that it will accept good-faith efforts at fulfilling the requirements as sufficient for meeting an entity's compliance burden.
    - The proposed records preservation requirement (226.13) assumes that a two-year preservation timeframe represents a best practice for both industry and government. In making this assumption, CISA has not accounted for the diverse array of organizations that its very broad "covered entity" designations now encompass.
        - Depending on the federal agency with which an institution works, or whether it is engaged with a federal agency other than ED at all, the required preservation period for records pertaining to a reported cyber incident may be much less.
        - Combined with the volume of information that must be preserved and the requirement that information be maintained in its original format, the two-year preservation period could place significant, unnecessary cost and workload burdens on colleges and universities.
        - CISA should consider a range of more manageable options, including:
            - Limiting the types of records that must be maintained in their original formats to those where the format truly matters to forensic analysis.

    - Establishing a step-down process under which records must be preserved in their original format for ninety days, after which they could be stored in any readily accessible format unless CISA gives notice that the "original format" period should be further extended.

    - Allowing sectors and subsectors to implement preservation periods and standards appropriate to the data and records prevalent in their covered industries, given the highly diverse data and systems contexts involved.

  - CISA should clarify 226.13(e)(3) by making clear that covered entities have the discretion to determine what constitutes the "reasonable safeguards" that they must deploy to protect preserved incident data and records based on the best practices prevalent in their field or industry.

- The regulations' proposed enforcement measures, including the exemption of State, Local, Tribal, and Territorial (SLTT) Government Entities from them.

  - In the final rule, CISA should clearly identify public higher education institutions as SLTT Government Entities that are exempt from the regulations' enforcement provisions.

  - The regulations concerning the issuance of a request for information (RFI) (226.14(c)) should include an appeals process regarding the time, format, type, and volume of information requested given that the issuance of an RFI would not be subject to appeal.

  - The proposed 226.18 should provide a detailed review of how covered entities will be held harmless for the unauthorized access and disclosure of reported information once it has been submitted to CISA.

  - Given the importance of the privacy and civil liberties guidance that CISA proposes to follow under the regulations, CISA should open a separate public comment process for that guidance to allow for a full range of stakeholder input.

Applicability

The notice of proposed rulemaking (NPRM) to implement CIRCIA[1] indicates that CISA intends to pull all colleges and universities that participate in Federal Student Aid (FSA) programs established under Title IV of the Higher Education Act (HEA) into the scope of the CIRCIA regulations. Prior to the release of the CIRCIA NPRM, CISA had not given any indication that it considered higher education in general to be part of a critical infrastructure sector, nor has CISA to this point engaged with our community, and particularly our cybersecurity community, as

[1] Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements," proposed rule, *Federal Register* 89, no. 66 (April 4, 2024): 23644-23776.

such. Different critical infrastructure sectors as defined by Presidential Policy Directive 21 (PPD-21)[2] have applied to discrete functions of various institutions as the NPRM notes,[3] but the designation of the overall HEA Title IV institutional community as a critical infrastructure sector has not previously been raised.

CISA rests its extension of the scope of CIRCIA regulations to colleges and universities on references to higher education as part of the Education Facilities Subsector (EFS)[4] of the Government Facilities Sector (GFS), which is one of the sixteen critical infrastructure sectors designated under PPD-21. The higher education community finds this confusing, however, given the available critical infrastructure documentation from which the references in question derive. At present, the only EFS critical infrastructure plan dates from 2010; while it includes numerous generic references to higher education in addition to elementary and secondary education, the plan largely focuses on emergency management issues in relation to elementary and secondary educational facilities, with few and mostly noncommittal references to cybersecurity.[5] A subsequent 2015 GFS sector-specific plan[6] contains only two generic references to higher education. The primary one of those, on which the second is based, appears to be inaccurate—it states that "PPD-21 designated that… the Education Facilities Subsector, which covers schools, institutions of higher education, and trade schools, with the Department of Education as the Sector-Specific Agency, …, be included as part of the Government Facilities Sector";[7] however, PPD-21 does not refer to educational facilities or the Department of Education, much less to higher education institutions. (In contrast, where the 2015 GFS plan notes in the same section that PPD-21 identifies the national monuments sector overseen by the Department of the Interior as part of the GFS, one finds that reference in PPD-21.)[8] *We would also note that the recently released National Security Memorandum 22 (NSM-22) does not contain references to education past including the Secretary of Education among the list of NSM-22 recipients.*[9]

CISA leveraging a tenuous relationship between the EFS or GFS and higher education to designate virtually all colleges and universities as critical infrastructure, separate and apart from any of the distinct functions of some institutions that may relate to a given critical infrastructure sector (e.g., healthcare, defense), strikes the higher education community as particularly problematic. As CISA notes in the NPRM, CIRCIA requires CISA to engage in

---

[2] Executive Office of the President, United States, *Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience*, February 12, 2013.
[3] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23691 (April 4, 2024).
[4] Ibid.
[5] Departments of Homeland Security and Education, *Education Facilities Sector-Specific Plan: An Annex to the Government Facilities Sector-Specific Plan*, 2010.
[6] Department of Homeland Security and General Services Administration, *Government Facilities Sector-Specific Plan: An Annex to the NIPP 2013*, 2015.
[7] Ibid, p. ii.
[8] See *PPD-21* (2013), "Additional Federal Responsibilities" under "Roles and Responsibilities."
[9] Executive Office of the President, United States, *National Security Memorandum 22 (NSM-22): Critical Infrastructure Security and Resilience*, April 30, 2024.

substantive outreach to federal and non-federal stakeholders in developing its proposed and final regulations.[10] CISA points to its request for information (RFI) and sector listening sessions related to the rulemaking process, as well as its discussions with SRMAs, as the primary vehicles for meeting its outreach burden under CIRCIA.[11] However, the higher education community writ large has not been involved in the EFS or GFS and therefore had no practical basis for considering the RFI or listening session processes as relevant. Likewise, CISA conducted no outreach of which we are aware to any higher education leadership or professional organization that would have indicated that it might consider its CIRCIA rulemaking as applying to the higher education community. And since the higher education community has not been engaged in the EFS to any relevant degree, again as far as the information currently available indicates, it is unsurprising that points of concern to the higher education community did not arise in any discussions that CISA may have had with ED as the EFS SRMA.

For example, while CISA has proposed a size threshold for elementary and secondary education entities to be considered covered entities under the regulations,[12] no such consideration was given to colleges and universities. However, institutional size, type, and resources all may play an important role in assessing whether the proposed reporting presents an undue burden and determining whether the requirements in question can be effectively met. Likewise, CISA appears to minimize the reporting burden that higher education institutions bear by referring to what it considers to be limited incident reporting to ED under the Federal Trade Commission (FTC) Safeguards Rule, established in relation to the Gramm-Leach-Bliley Act.[13] However, higher education institutions are also now subject to incident reporting under the Safeguards Rule to the FTC itself.[14] Moreover, colleges and universities face an array of additional incident reporting requirements that span most states as well as numerous other federal agencies, all of which should have been considered in determining if, when, and how the proposed CIRCIA regulations might extend to the higher education community in general despite its historical exclusion from the critical infrastructure context.

CISA makes clear in the NPRM that its designation of the "entities in a critical infrastructure sector" that it considers "covered entities" under the proposed regulations is discretionary.[15] It notes that it must exercise such discretion given the broad way in which the critical infrastructure sectors define themselves:

---

[10] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23654 (April 4, 2024).
[11] Ibid.
[12] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23691 (April 4, 2024).
[13] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23693 (April 4, 2024).
[14] Katie Branson, "FTC Publishes Final Breach Reporting Requirements Under the Safeguards Rule," *EDUCAUSE Review*, December 13, 2023.
[15] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23704 (April 4, 2024).

> As discussed earlier, while the term "critical infrastructure sector" is not defined in PPD-21, public and private sector partners for each of the critical infrastructure sectors identified in PPD-21 jointly developed SSPs for their respective sectors that set out goals and priorities for the sector to address its current risk environment. Each of those SSPs includes a description of the entities that compose the sector in Sector Profiles. As the examples provided earlier demonstrate, most of these sectors are quite expansive, and entities "in a critical infrastructure sector" are not limited to—and are often broader than—entities that own or operate systems or assets that meet the statutory definition of "critical infrastructure." See Section IV.B.ii in this document. Based on a consolidated reading of these sector-developed descriptions in the various SSP Sector Profiles, CISA believes that the overwhelming majority of entities in the United States—though not all—fit within one or more of the critical infrastructure sectors and thus would meet the definition of "an entity in a critical infrastructure sector."[16]

However, the reference to "public and private partners for each of the critical infrastructure sectors identified in PPD-21 jointly [developing] SSPs for their respective sectors" and the implication that those "public and private partners" had a hand in defining "the entities that compose [their] sector" are simply inaccurate in relation to the higher education community. Through its interactions with ED as the SRMA for the EFS, CISA has had sufficient opportunity to determine that higher education in general and its cybersecurity community specifically were not part of, much less partners in, the EFS or GFS, and thus that meeting its burden for stakeholder outreach under CIRCIA required CISA to engage directly and substantively with the higher education community. This is especially the case given the implication in the NPRM that cyber incident reporting for a covered entity would not be restricted to an entity's functions that relate to a given critical infrastructure sector, but rather that any touchpoint between an entity and a sector would require the entity to report any incidents deemed "covered," whether they derive from a critical infrastructure function or not.

From the perspective of the higher education community, CISA has proposed a dramatic realignment of the critical infrastructure framework to encompass almost all colleges and universities without prior notice or consultation. The primary rationale for this historic action as stated in the NPRM is "…, CISA believes it is important to require reporting from IHE more broadly,"[17] so it can "ensure reporting from a sufficient cross-sector of entities to understand and be able to share information on threats to our nation's education facilities."[18] However, as we have demonstrated, the factual basis on which higher education institutions are assumed to be part of the Education Facilities Subsector remains a mystery. Similarly, our member institutions are confused by CISA and ED's lack of engagement with the higher education community regarding what might constitute an appropriate cross-section for reporting purposes, short of the entire sector, and how our substantive, pre-existing reporting

[16] Ibid.
[17] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23693 (April 4, 2024).
[18] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23691 (April 4, 2024).

requirements across a broad range of jurisdictions might be accounted for. For these reasons, we urge CISA to reconsider its unilateral reclassification of U.S. colleges and universities in general as "critical infrastructure" in relation to these proposed regulations. Should CISA continue with this action, however, then we would request substantive, sustained outreach by CISA and ED to our community in the hope that our needs and concerns might genuinely be addressed in the final rule. In addition, CISA might consider other steps, such as exploring broad-based participation by higher education institutions in the Joint Cyber Defense Collaborative (JCDC) and similar efforts at coordinating cyber response activities across sectors and agencies.

Substantially Similar Reporting Exception

CISA discusses in the NPRM the range of comments it received during its initial outreach efforts regarding the need to harmonize potential CIRCIA reporting with other processes to limit the burden of redundant reporting on covered entities.[19] As CISA states, "Many commenters, noting the language in CIRCIA to this effect, encouraged CISA to implement the reporting exemption for covered entities that submit cyber incident reports with substantially similar information to other Federal departments and agencies, within a substantially similar timeframe."[20] CISA further highlights examples of potentially similar federal reporting requirements, including a few of direct interest to colleges and universities: the Defense Federal Acquisition Regulation Supplement (DFARS) 7012 incident reporting requirement, the Health Insurance Portability and Accountability Act (HIPAA) breach notification rule, and the Health Information Technology for Economic and Clinical Health (HITECH) Act breach notification rule.[21]

CISA highlights that CIRCIA requires the agency to establish formal agreements with other federal agencies in order to implement the "substantially similar reporting exception" that the law provides, and CISA states its intention to work with its fellow agencies to achieve such agreements to the extent possible:

> Finally, CISA intends to work with other Federal departments and agencies to explore opportunities to reduce duplicative reporting of covered cyber incidents through a proposed substantially similar reporting exception to CIRCIA. Under this exception, which is authorized under 6 U.S.C. 681b(a)(5)(B), a covered entity that is required by law, regulation, or contract to report information to another Federal entity that is substantially similar to the information that must be reported under CIRCIA and is required to submit the report in a substantially similar timeframe to CIRCIA's reporting deadlines, may be excepted from reporting it again under CIRCIA. Per the statute, for covered entities to be able to leverage this specific exception, CISA and the respective Federal entity must enter into an interagency agreement, referred to as a

[19] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23658 (April 4, 2024).
[20] Ibid.
[21] Ibid.

> CIRCIA Agreement, and establish an information sharing mechanism to share reports. To the extent practicable, CISA is committed to working in good faith with its Federal partners to have CIRCIA Agreements finalized before the effective date of the final rule. Additional details on the substantially similar reporting exception to CIRCIA are discussed in Section IV.D.i in this document.[22]

CISA acknowledges, however, that the overall scope and applicability of the exception cannot be determined for some time: "…CIRCIA Agreements cannot be fully developed, and this exception cannot be fully implemented, until the final rule stage or after implementation of the regulatory program,…"[23] Thus, potentially covered entities such as colleges and universities with a variety of different functions that may connect with a variety of federal agencies will likely face a range of redundant reporting requirements for some time even after CISA releases the final rule. For example, a university with Department of Defense (DOD) research contracts and a university hospital could conceivably find itself caught between CISA, the DOD, and the Department of Health and Human Services (HHS) in terms of reporting obligations depending on the nature of the incident involved. There is no guarantee that CISA's good-faith efforts will achieve the desired outcome of sparing the university from an undue duplicative reporting burden at any point during the final rule's development or after its release.

Non-federal organizations should not have to bear the responsibility for unresolved redundancies in federal cyber incident reporting on top of what CISA acknowledges in the NPRM is a diverse set of state reporting and notification laws as well. Given the scope of compliance and reporting that many entities, including colleges and universities, must already manage—the overwhelming majority of which do not come with funding to support the reporting and related activities required—the federal government, with CISA as the lead agency in this case, should ensure that it has finally harmonized its incident reporting requirements as much as possible to ensure that CIRCIA does not become the straw that breaks the camel's back. Therefore, the higher education community urges CISA to take the following steps:

- Within six months of the end of the NPRM comment period as extended, CISA should make available for public review and comment a comprehensive list of federal cyber incident reporting requirements; the list should be organized by critical infrastructure sector and subsector as well as by whether CISA deems a federal reporting requirement to be potentially eligible for a CIRCIA Agreement or not.
- CISA should allow ninety days for the submission of proposed edits to its list, including recommendations for moving federal reporting requirements from the "non-CIRCIA Agreement eligible" category to the "CIRCIA Agreement-eligible" category.
- Within sixty days of the submission period, CISA should make publicly available its final list of federal incident reporting requirements, organized by sector and subsector as well as CIRCIA Agreement eligibility.

---

[22] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23654 (April 4, 2024).
[23] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23748-49 (April 4, 2024).

- CISA should specify in the final rule that it will delay the effective date of CIRCIA reporting in relation to CIRCIA Agreement-eligible reporting requirements for two years from the date of the publication of the final rule or until a CIRCIA Agreement has been reached with the relevant federal partner, whichever comes first.
- CISA acknowledges in the NPRM that it "may enter into other information sharing agreements with Federal agencies that do not meet the substantially similar reporting exception criteria," although such agreements would not mitigate covered entities' separate responsibilities to CISA or the other federal agencies involved.[24]
    - With that in mind, we urge CISA to work with non-CIRCIA Agreement agencies to mitigate the burden of redundant reporting on covered entities, even where that redundancy does not rise to the level of a CIRCIA Agreement.
    - We believe that CISA can accomplish this by augmenting the reporting infrastructure it plans to implement for CIRCIA to facilitate ease of reporting for non-CIRCIA federal requirements.
    - Given the reciprocal information sharing that CIRCIA mandates as well as the potential for some degree of overlap in information even with non-CIRCIA Agreement reporting processes, CISA's reporting infrastructure for CIRCIA will likely include significant elements of what would be necessary for CIRCIA reporting to mitigate covered entities' reporting burden to other federal actors.
    - Thus, even if CISA's implementation of the substantially similar reporting exception does not enable entities' reports to other agencies to mitigate their CIRCIA reporting burden, CISA and its fellow federal agencies should strive to enable CIRCIA reporting to lessen entities' overall reporting burden to the federal government.

The final rule should also make clear that a failure by a federal agency to forward an entity's report covered by a CIRCIA Agreement to CISA within the required timeframe does not constitute a compliance failure on the part of the reporting entity. Once the substantially similar reporting exception has been implemented in a given context via a CIRCIA Agreement, covered entities should be able to rest assured that they have met their burden when they submitted the necessary report to the relevant agency within the specified timeframe, regardless of the subsequent actions or lack thereof by the given agency.

Reporting Basis

We appreciate the analysis CISA provides of the definition of "cyber incident" under CIRCIA, which highlights the focus of the definition on events that actually jeopardize the confidentiality, integrity, or availability of data or systems, as compared to those that might

[24] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23708 (April 4, 2024).

"imminently" do so.[25] We also value the discussion of a "covered cyber incident" as "a substantial cyber incident experienced by a covered entity"[26] and the thoughtful review of the factors that make an incident a "substantial cyber incident," which would trigger an incident reporting obligation for a covered entity:

> While CIRCIA does not define the term substantial cyber incident, it provides minimum requirements for the types of substantial cyber incidents that qualify as covered cyber incidents. See 6 U.S.C. 681b(c)(2)(A). Consistent with these minimum requirements, CISA proposes the term substantial cyber incident to mean a cyber incident that leads to any of the following: (a) a substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network; (b) a serious impact on the safety and resiliency of a covered entity's operational systems and processes; (c) a disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services; or (d) unauthorized access to a covered entity's information system or network, or any nonpublic information contained therein, that is facilitated through or caused by either a compromise of a cloud service provider, managed service provider, other third-party data hosting provider, or a supply chain compromise.[27]

The nature and scope of the definition of "substantial cyber incident" raises a number of concerns, however, especially due to the importance of the definition to CISA's proposed reporting requirements: "Given CISA's proposal to define a covered cyber incident as a substantial cyber incident experienced by a covered entity, the term substantial cyber incident is essential to the CIRCIA regulation as it identifies the types of incidents that, when experienced by a covered entity, must be reported to CISA."[28]

First, we note that CISA rightly indicates that determining whether an incident is sufficiently "substantial," "serious," or disruptive will depend on "a variety of factors":

- "Whether a loss of CIA [confidentiality, integrity, or availability] constitutes a 'substantial' loss will likely depend on a variety of factors, such as the type, volume, impact, and duration of the loss."[29]
- "Similar to the interpretation of the word 'substantial' in the first impact type, whether an impact on the safety and resiliency of an operational system or process is 'serious' will likely depend on a variety of factors, such as the safety or security hazards associated with the system or process, and the scale and duration of the impact."[30]

---

[25] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23660 (April 4, 2024).
[26] Ibid.
[27] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23661 (April 4, 2024).
[28] Ibid.
[29] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23662 (April 4, 2024).
[30] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23662-63 (April 4, 2024).

- "…, whether a disruption rises to the level of reportability may depend on a variety of factors and circumstances, such as the scope of the disruption and what was disrupted... Generally speaking, incidents that result in minimal or insignificant disruptions are unlikely to rise to the level of a substantial cyber incident…; however, the specific circumstances of the disruption should be taken into consideration."[31]

In each case, CISA relies on a few examples to provide a general indication of what may or may not be relevant, rather than providing relevant metrics to guide a covered entity's analysis of whether it has a "reasonable belief" that an incident may be a "substantial cyber incident." We believe that CISA chose this approach to reinforce its "when in doubt, report" emphasis:

> Finally, CISA expects a covered entity to exercise reasonable judgment in determining whether it has experienced a cyber incident that meets one of the substantiality thresholds. If a covered entity is unsure as to whether a cyber incident meets a particular threshold, CISA encourages the entity to either proactively report the incident or reach out to CISA to discuss whether the incident needs to be reported.[32]

While the higher education community appreciates that the defining factors of a "substantial cyber incident" provide for the exercise of discretion and judgment on the part of a covered entity, we contend that CISA has left the key modifiers of those defining factors—"substantial," "serious," and disruptive—too vague from the perspective of potential covered entities. For example, many organizations likely have mitigations in place to minimize potential disruptions to their operations and/or ability to deliver goods and services. At least in some cases, those mitigations may limit the impact of an otherwise reportable incident such that a covered entity might validly reach a different conclusion about whether or not to report than CISA would. In the meantime, CISA may not receive relevant information in a timely fashion and the entity may face a compliance issue that it has good reason to think should not exist. Without more specific indicators, CISA leaves covered entities without an effective way to navigate the rather large compliance space between "report virtually everything" and "report only the indisputably significant."

CISA's review of these factors in the NPRM signals that it has general ranges in mind for the modifiers in question. We believe that further engagement with stakeholders on what the outlines of "serious," "substantial," and disruptive are, as well as the degree to which the criticality of the functions or services affected should impact the application of those terms, would allow for collaborative development of a more constructive compliance framework. The higher education community urges CISA to conduct such a process prior to finalizing its proposed regulations to provide both CISA and covered entities with a more effective path to compliance.

---

[31] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23663 (April 4, 2024).
[32] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23665 (April 4, 2024).

In terms of the fourth factor that would make an incident a reportable event—whether it has experienced unauthorized access of data or systems resulting from a supply chain compromise or the compromise of a cloud services provider, managed services provider, or data-hosting provider—we understand CISA's perspective that unauthorized access via a provider channel or supply chain issue may be relatively minor for a given entity but reflect a more significant overall development across a range of organizations and sectors. We also appreciate the analysis of congressional intent, indicating that significant, rolling incidents stemming from large-scale third-party providers were a key driver in the development and passage of CIRCIA.[33] However, we would again recommend that CISA re-engage with the stakeholder community as it works toward the final rule to identify some reasonable range of parameters to mitigate the burden of overreporting on both CISA and covered entities.

The proposed regulations should put the responsibility for reporting provider incidents on services and software providers, who could supply CISA with information about the scope of the affected client communities for further outreach if necessary. Unless the incident, as experienced by the client organization, rises to the "substantial cyber incident" level based on the other defining criteria, a client organization should not have to bear the weight of reporting on a provider-based incident since there would be little of significance to report on the client side and the client would likely have little, if any, information about the provider incident. While the definition of covered entities in the Information Technology (IT) Sector probably encompasses the overwhelming majority of the providers with which CISA would be concerned, the agency could also look at modifying the definition to ensure that software and services providers with client rosters above a certain threshold have the necessary reporting obligations.

However, if CISA persists in imposing a reporting obligation for provider-driven incidents on client organizations, regardless of the reporting burden they experience for non-substantive events and the overreporting that will clearly result from some number of organizations reporting what is essentially the same event, then it should, at a minimum, introduce a brief, low-overhead notification process that doesn't require completion of a full covered incident report by every organization minimally affected by the incident. For example, perhaps CISA might consider instituting a preliminary type of report for provider-based issues that only requires a minimal level of information from a covered entity when the incident it experiences is not substantial, serious, and/or disruptive. If CISA receives a volume of such submissions, it could issue a request to initial submitters for completion of an overall covered cyber incident report as well as a general alert to relevant sectors. Such a report format should be fairly straightforward to implement in the context of the overall web form for reporting that CISA proposes, given that it would be based on a subset of covered incident report fields.

The higher education community understands the importance of timeliness in identifying and responding to the types of compromises that the fourth "substantial cyber incident" factor envisions. We believe, though, that CIRCIA allows for striking a more effective balance between

[33] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23663-64 (April 4, 2024).

speed and reporting burden. This is especially the case given that the initial identification of a multi-stakeholder development could be slowed by entities trying to submit full covered cyber incident reports when quick, brief notices of third-party compromises would facilitate a more rapid response.

Returning briefly to the second factor that defines a "substantial cyber incident," we are concerned that the lack of a definition of "operational systems and processes" has the potential to create undue confusion from a compliance standpoint. We appreciate the clarification that the term is not limited to incidents involving operational technology (OT), as that removes OT from the range of criteria that would restrict the second factor's scope.[34] However, colleges and universities have multiple functions supported by diverse process and systems environments, where what is or isn't considered "operational" may vary between institutions as well as between CISA and the higher education community.

As with the prior discussion of the adjectives intended to give scope to the factors that determine what constitutes a "substantial cyber incident," the higher education community recognizes the value of the room for judgment and discretion that CISA provides by not seeking to impose overly restrictive guidance in this area of the proposed rule. However, as with those terms, the lack of more substantive content for the concept of "operational systems and processes" in the absence of a clear statement that covered entities have the discretion to determine what process and systems of theirs are "operational" makes "operational systems and processes" excessively vague. And again, while this may serve the "when in doubt, report" philosophy CISA appears to have adopted, it does not well serve the practical identification and analysis of legitimate "substantial cyber incidents." If CISA will accept and incorporate into the final rule that covered entities determine what their "operational systems and processes" are on a good-faith basis, that would be a reasonable and effective solution. If, however, CISA is not willing to take such a step, then it should work with the stakeholder community to provide sufficient scope for the term so that CISA and entities in the various sectors and subsectors have a reasonably shared context for compliance.

Report Information and Records Preservation

Starting with a point for clarification, the analysis of the deadline for submitting a supplemental report states, "CIRCIA requires Supplemental Reports be submitted 'promptly,' which CISA interprets as within 24 hours of the triggering event."[35] However, that comment does not align with the text of the proposed regulations at 226.5(d), which draws a distinction between supplemental reports in general and those related to a ransom payment:

> A covered entity must promptly submit supplemental reports to CISA. If a covered entity submits a supplemental report on a ransom payment made

[34] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23662-63 (April 4, 2024).
[35] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23709-10 (April 4, 2024).

> after the covered entity submitted a Covered Cyber Incident Report, as required by § 226.3(d)(1)(ii), the covered entity must submit the Supplemental Report to CISA no later than 24 hours after the ransom payment has been disbursed.[36]

It also does not align with the review of the meaning of "promptly" that CISA provides, where CISA "interprets 'promptly' to generally mean what it means colloquially, *i.e.,* without delay or as soon as possible," except when a ransom payment constitutes the supplemental reporting event.[37] We therefore request that CISA ensure that any analysis or narrative in the final rule regarding the deadline for supplemental reporting is fully consistent with its complete interpretation of "promptly."

Regarding the submission of CIRCIA Reports, the higher education community would ask that CISA provide more information in its analysis and potentially in the regulations themselves regarding how CISA will ensure that malicious actors are not able to submit false reports. We note that the discussion of email as one possible vehicle for submitting CIRCIA reports highlights 6 USC 681e, where subsection (a)(4) explains the requirements that CISA must follow regarding the receipt of cyber incident reports:

> (4) Digital security: The Agency shall ensure that reports submitted to the Agency pursuant to section 681b of this title, and any information contained in those reports, are collected, stored, and protected at a minimum in accordance with the requirements for moderate impact Federal information systems, as described in Federal Information Processing Standards Publication 199, or any successor document.[38]

Likewise, the discussion of 6 USC 681e(a)(4) in Section IV.H.iii of the NPRM reinforces the obligation that CISA has to "ensure that CIRCIA Reports, responses to RFIs, and any information contained therein are collected, stored, and protected in accordance with the requirements for moderate impact Federal information systems, as described in Federal Information Processing Standards Publication 199,..."[39] However, given that CISA will rely on a public web form for the submission of all CIRCIA Reports, we find that the guidance and possibly the final rule itself would benefit from a more detailed explanation of the steps CISA will incorporate into the reporting process to prevent to the extent possible the submission of CIRCIA Reports falsely identified as provided by a covered entity. In addition, since covered entity reports will generally contain information that would fall under the "Information Systems Vulnerability Information" CUI Category[40] and thus present the risk of substantial harm to the entity if

---

[36] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23770 (April 4, 2024).
[37] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23726 (April 4, 2024).
[38] 6 USC 681e; see (a)(4), "Digital security."
[39] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23741 (April 4, 2024).
[40] National Archives and Records Administration, Controlled Unclassified Information (CUI) Registry: "CUI Category: Information Systems Vulnerability Information" (as of June 12, 2024).

exposed, CISA should consider whether the "ISVI" CUI marking should automatically be applied to reports during the submission process.

Please see our prior discussion of the problems with the scope and applicability of the proposed regulations in relation to higher education in considering 226.7(b)(10), which asks organizations submitting CIRCIA Reports to identify the critical infrastructure sector or sectors of which the organization considers itself to be a part.[41] We note again that, except for discrete functions that a given institution may or may not have, colleges and universities have not historically been engaged by CISA (in general) or ED (in relation to the EFS) in critical infrastructure sectors or processes. Thus, higher education institutions in general would not consider themselves part of the EFS and would be unlikely to identify themselves as such absent a significant, substantive change in outreach and engagement by CISA and/or ED. Likewise, they may be surprised to find that the possible overlap between a discrete institutional function and a given critical infrastructure sector or subsector may now open them to cyber incident reporting across all aspects of the institution, not simply in relation to the function that the particular sector or subsector covers, based on the regulations that CISA proposes.

Concerning the proposed 226.8(a)(1)(i), the higher education community finds the requirement as written to be overly broad: "Technical details and physical locations of such networks, devices, and/or information systems;…"[42] The open-ended terms in the provision leave it with an expansive scope that would likely drive overreporting and the release of information that many institutions would view as highly sensitive from a cybersecurity standpoint; in addition, the data in question may in some instances fall under even more rigorous and restrictive federal agency reporting requirements (e.g., Defense Threat Reduction Agency mandates concerning DoD contract details and locations). Again, the incorporation of 6 USC 681e(a)(4) into the proposed rule clarifies that CISA will apply the Federal Information Processing Standards Publication 199 security requirements at the "moderate" level to CIRCIA Reports, but CISA should work with the stakeholder community to give 226.8(a)(1)(i) a reasonable scope that would mitigate the *over-collection* of sensitive information. To the extent that CISA might view additional data in relation to this requirement as relevant in any given case, it could conduct straightforward outreach to the entity in question or issue a request-for-information pursuant to CIRCIA if it determined a more formal step was necessary. Please see the proposed 226.8(d)[43] as well, for which we have the same concerns and recommendations. Also, please consider our previous comment about the applicability of the "Information Systems Vulnerability Information" CUI Category and markings in relation to this context.

[41] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23770 (April 4, 2024).
[42] Ibid.
[43] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23771 (April 4, 2024).

CISA should consider revising the proposed 226.8(a)(4), which requires the submission of information about an incident's impact on the covered entity's operations.[44] Organizations may approach a determination of an incident's "direct economic impacts to operations" in a wide variety of ways given their type and field. Preserving an entity's discretion to estimate the economic effects it experiences from an incident in ways that fit its context is important. However, both CISA and covered entities would benefit from a common, high-level frame of reference regarding the most useful factors in making such determinations—it would likely simplify the analysis an entity must conduct while providing for greater consistency and comparability of the data that CISA receives.

Regarding the proposed 226.8, "Required information for Covered Cyber Incident Reports," in general, the higher education community notes that relatively sophisticated incident response capabilities may be necessary to address most of the required reporting elements in many cases. In the higher education context, one cannot assume that the large majority of small, rural, and/or resource-challenged institutions have or have access to such capabilities. Hopefully, as discussed previously, CISA and ED will engage the higher education community in a constructive dialogue about the scope and applicability of the regulations prior to their issuance in final form, such that at least the appropriateness of pulling all HEA Title IV institutions under the proposed regulations regardless of size, mission, and institutional capacity could be revisited. However, absent that, CISA is asking the text of the introduction to 226.8 that we have italicized below to carry more weight in the minds of covered entities than they may readily recognize: "A covered entity must provide all the information identified in § 226.7 and the following information in a Covered Cyber Incident Report, *to the extent such information is available and applicable to the covered cyber incident*:…"[45] This is particularly concerning given the more expansive statement CISA makes in its analysis of this section of the proposed regulations, *"CISA is proposing that a covered entity ultimately must provide all applicable required content in either the initial Covered Cyber Incident Report or a Supplemental Report to be considered fully compliant with its reporting obligations under CIRCIA."*[46] [Emphasis added.]

Given the limited capabilities that many covered entities have with which to meet the expansive reporting requirements presented in the proposed regulations, we argue that CISA must take care in the final rule as well as in the analysis that will inevitably accompany it to stress at every turn the acceptance by CISA of good-faith efforts at fulfilling the reporting requirements as sufficient for meeting an entity's compliance burden. CISA does mention at times in the NPRM how some form of "unknown at this time" would be an acceptable response to various required reporting elements, but mostly as a way to emphasize the necessity of an entity submitting a Supplemental Report—promptly—once the entity has identified relevant information. If CISA and ED persist in extending the scope of the proposed regulations to

[44] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23770 (April 4, 2024).
[45] Ibid.
[46] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23720 (April 4, 2024).

institutions that by any objective measure do not constitute "critical infrastructure" and have not been involved in any substantive way in a critical infrastructure sector prior to these regulations, then CISA has a specific obligation to ensure that the final rule is unequivocal about expectations for compliance not exceeding a covered entity's good-faith ability to comply.

Our discussion of the proposed regulation's data and records preservation requirements (226.13) begins with referring to our prior comments about the need for more scoping guidance in relation to the definition of "substantial cyber incident." Providing a more informative basis from which to determine what is sufficiently "serious," "substantial," or disruptive to trigger a reporting obligation would help covered entities across the various affected industries to estimate the volume of likely reporting and therefore the associated burden of the proposed information preservation mandates. However, unless and until CISA engages the broad range of stakeholders in addressing that issue, the following paragraph highlights where the agency may have based the proposed requirements on some problematic assumptions:

> Based on the above, CISA believes that a data preservation requirement typically lasting anywhere between two and three years would be consistent with existing best practices across industry and the Federal government, would be implementable by the regulated community, and would achieve the purposes for which data preservation is intended under CIRCIA. Recognizing that the costs for preserving data increase the longer the data must be retained, and wanting to limit costs of compliance with CIRCIA where possible without sacrificing the ability to achieve the purposes of the regulation, CISA thus is proposing that covered entities must preserve the required data and records for the lower end of the spectrum of best practice for data preservation, *i.e.,* a period of two years, unless substantial new or different information is discovered or additional actions occur that require the submission of a Supplemental Report and a commensurate extension of the data preservation timeframe.[47]

The section of CISA's analysis from which this text is drawn discusses a few examples of industries with comparable requirements. CISA does not acknowledge, however, that its expansive determinations of which "entities in a critical infrastructure sector" constitute "covered entities" reach across a much more variable environment where a two-year preservation period may far exceed what would be "consistent with existing best practices." For example, the DFARS 7012 preservation requirement extends for only ninety days.[48] Given the volume of information that CISA expects covered entities to maintain for two years[49] and the mandate that the information be maintained in its original format,[50] this difference in

[47] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23732 (April 4, 2024).
[48] DFARS 252.204-7012; see (e), "Media preservation and protection."
[49] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23772 (April 4, 2024).
[50] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23773 (April 4, 2024).

timeframes very much matters to colleges and universities that conduct research on behalf of the DOD. The original format requirement may pose significant, increased burdens for institutions as well given that many network data systems purge older logs on a rolling basis unless express actions are taken to archive the past logs for an additional period. In some cases, those actions may require manual transfer of the log data to another system and format, given the limitations of the originating system's storage capabilities. Maintaining the logs would therefore require recurring, active management for an extended period of time regardless of whether CISA provides any indication that it might want them at some point. As another example, a reportable incident could arise in the context of a college or university's enterprise resource planning (ERP) system, where preserving a copy of all potentially relevant system software and information for two years would be cost prohibitive for even a large, well-resourced institution, much less a small, resource-challenged one. These possibilities do not seem consistent with CISA's stated desire "to limit costs of compliance with CIRCIA where possible without sacrificing the ability to achieve the purposes of the regulation." CISA should consider a range of more reasonable and manageable options, including:

- Limiting the types of data and records that must be maintained in their original format to those for which the format of the information is most relevant to forensic analysis.
- Establishing a step-down process under which data and records must be preserved in their original format for ninety days, for example, after which an entity could store them in any readily accessible format that preserves their essential meaning for the remaining preservation timeframe unless CISA gives notice that a further extension of the original format period is required.
- Allowing sectors (and subsectors) to implement preservation periods and standards appropriate to the data and records prevalent in their covered industries, given the highly diverse data and systems environments (as well as pre-existing regulatory requirements) that exist within and between sectors and subsectors.

The higher education community feels acutely the need for more reasonable and manageable preservation options under the proposed regulations. Any college or university would find the preservation volume, restrictions, and timeframe burdensome. For large, well-resourced institutions, the scope and scale of the differing compliance regimes they face and the diverse array of systems and networks they manage would make the proposed requirements challenging and hard to justify in the absence of some reasonable indication that the information involved might be used. Small, rural, and/or resource-challenged institutions, on the other hand, may lack the resources and expertise to essentially preserve data and records as forensic evidence with all of the appropriate measures that must be taken to ensure that level of integrity.

The proposed preservation requirements seem to assume that all of the entities that CISA now seeks to cover share the baseline characteristics and capabilities of the organizations and industries traditionally understood to fall within the "critical infrastructure" context. In making those assumptions, CISA has not adequately accounted for the much wider range of entity types and capacities that would have to comply with the proposed requirements. With this in

mind, we again urge CISA to reconsider trying to leverage the tenuous relationship between the Education Facilities Subsector (EFS) of the Government Facilities Sector (GFS) and the higher education community to extend the scope of the proposed regulations to virtually all colleges and universities regardless of size, mission, capacity, and other potentially relevant considerations. At a minimum, CISA should engage the higher education community in discussing the possible parameters of a covered entity threshold, which it is already prepared to accept in the elementary and secondary education context. It should also revise its approach to records preservation based on the suggestions we mention above and/or similar ideas that it or other respondents might identify.

Finally, in relation to 226.13(e)(3), we appreciate that the proposed regulations appear to provide covered entities with the discretion to determine what constitutes the "reasonable safeguards" they must deploy to protect preserved incident data and records. We also appreciate the reference to NIST SP 1800-25, "Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events,"[51] as a source of potential guidance in this regard. However, given the broad array of industries and entities that CISA intends to encompass with this rule and the widely varying levels of knowledge that they are likely to have about CISA's thinking behind its proposed provisions, we recommend that CISA make clear in the regulation that entities have the discretion to deploy reasonable safeguards based on the standards, effective practices, and related requirements prevalent within their field or industry.

Enforcement

The higher education community notes that the exclusion from the enforcement provisions of CIRCIA for state, local, tribal, or territorial government entities provided at 6 USC 681d(f)[52] is reflected in the proposed regulations at 226.14(a).[53] This regulatory provision highlights that the exclusion applies to covered entities that are "State, Local, Tribal, or Territorial (SLTT) Government entities" as defined under the proposed 226.1:

> *State, Local, Tribal, or Territorial Government entity or SLTT Government entity* means an organized domestic entity which, in addition to having governmental character, has sufficient discretion in the management of its own affairs to distinguish it as separate from the administrative structure of any other governmental unit, and which is one of the following or a subdivision thereof: …[54]

Public higher education entities, whether state colleges and universities, community colleges, systems or districts of the same, and so forth, are considered by themselves as well as their

[51] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23733 (April 4, 2024).
[52] 6 USC 681d; see (f), "Exclusions."
[53] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23773 (April 4, 2024).
[54] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23767 (April 4, 2024).

respective state, local, tribal, or territorial governments as "subdivisions" of such governments. Thus, the higher education community would understand those entities to fall under the exclusion from enforcement established in 6 USC 681d(f) and incorporated into the proposed rule at 226.14(a). Further discussion of this point as CISA deems necessary would be another item for outreach to the higher education community in relation to the proposed regulations.

Regarding the provisions concerning the issuance of a request for information (RFI) as detailed at the proposed 226.14(c), we are concerned that the issuance of an RFI could be based on virtually any reason CISA chooses per 226.14(c)(1),[55] cover any scope of information that CISA deems relevant per (c)(2),[56] impose any response deadline that CISA deems appropriate per (c)(3),[57] and seemingly be subject to no appeal per (c)(5).[58] While we have every reason to think that CISA will exercise its authority under CIRCIA and these implementing regulations in good faith, the potential for mistakes to occur and unmanageable requirements to be imposed under this structure clearly exists and must be mitigated.

Thus, it may be the case that the issuance of an RFI would not be subject to appeal, but the regulations should include a formal process of appeal in relation to the time, format, and type/volume of information requested. Covered entities should have a formal basis *in the regulations* for assurance that good-faith compliance efforts will be acknowledged and respected as such. This is especially the case given the latitude that CISA gives itself under the regulations to subject an entity to potentially unreasonable requests on whatever basis it finds appropriate and the ability of CISA to issue a subpoena only 72 hours after the date on which an RFI has been served on an entity,[59] with all of the loss of protection from further legal or regulatory action that receipt of a subpoena entails under the proposed rule.[60] With this in mind, the process for appealing the elements of an RFI, if not its issuance, should include a "stop the clock" provision on the 72-hour period during which CISA cannot issue a subpoena; this will ensure that covered entities receive a fair hearing regarding their concerns about the key elements of an RFI.

The proposed 226.18 highlights a number of protections for information submitted via CIRCIA Reports,[61] such as a shield for such information from Freedom of Information Act (FOIA) requirements and similar laws and provisions at other levels of government.[62] While the section provides significant assurance that covered entities will not face other legal and regulatory actions as a result of complying with CIRCIA and these implementing regulations, it would

---

[55] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23773 (April 4, 2024).
[56] Ibid.
[57] Ibid.
[58] Ibid.
[59] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23774 (April 4, 2024).
[60] Ibid.
[61] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," proposed rule, 89 *Federal Register* 23775 (April 4, 2024).
[62] Ibid.

benefit from a detailed discussion of how CISA will hold covered entities harmless for the unauthorized access and disclosure of reported information once it has been submitted to CISA, separate and apart from the relevant protections for personal information detailed in the privacy and civil liberties guidance for cyber incident reporting under CIRCIA.[63] History shows that no agency or organization is immune to substantial cyber incidents, including CISA itself, and thus covered entities have reasonable concerns about the potential unauthorized exposure of information incorporated in a CIRCIA Report and any liability that may attach to such exposure. CISA should ensure that its obligations in relation to such problems are clearly delineated within the regulations themselves to avoid the potential for confusion and misinformation if and when a possible breach of CIRCIA Report data occurs.

Finally, given the overall importance of the privacy and civil liberties guidance that CISA proposes to apply to its CIRCIA activities as well as the depth and breadth of the main NPRM itself, the higher education community encourages CISA to consider addressing the privacy and civil liberties guidance via a separate comment process. Even with the extension of the comment period for the NPRM, which we greatly appreciate, the privacy and civil liberties guidance may require a separate comment period to receive the level of review and comment it warrants.

Conclusion

The higher education community finds itself greatly surprised by the proposed application of critical infrastructure cyber incident reporting to colleges and universities in general. Neither CISA nor the SRMA for the subsector that CISA is leveraging to extend the scope of CIRCIA to higher education institutions writ large have a substantive history of engaging our community in critical infrastructure processes. Thus, the basis on which CISA seeks to encompass virtually all U.S. colleges and universities with its proposed regulations seems tenuous. While we urge CISA to revisit this decision in general, at a minimum, we believe that neither CISA nor the relevant SRMA have fulfilled their responsibility for outreach and engagement with the higher education community that CISA's scoping determination entails and CIRCIA itself reflects. We request that CISA and the Department of Education, as the SRMA for the relevant subsector, resolve this problem via good-faith collaboration with our community prior to the release of the final rule.

Similarly, we have significant concerns about the extent to which the burden of redundant reporting requirements across federal agencies will be exacerbated rather than relieved as a result of the proposed regulations. It is not clear that CISA and its fellow agencies can and will harmonize their respective reporting requirements via CIRCIA Agreements under CISA's formulation of the "substantially similar reporting exception." Given the reporting burdens and resource constraints that higher education institutions must already manage, the federal government, led in this case by CISA, should make every effort to minimize redundant reporting

[63] Cybersecurity and Infrastructure Security Agency, *Proposed Privacy and Civil Liberties Guidance: Cyber Incident Reporting for Critical Infrastructure Act (Draft)* (March 2024).

by covered entities to the maximum extent possible. With this in mind, we reiterate our call for the effective date of CIRCIA reporting requirements to be delayed for any given sector or subsector where a CIRCIA Agreement might reasonably apply should such an agreement not be in place at the time of the final rule's publication. We propose a delay of at least two years in such cases, in recognition of the difficulties and capacity problems that CISA and its fellow agencies face themselves. On the other hand, where federal reporting requirements exist that cannot be reasonably covered by a CIRCIA Agreement, we urge CISA to work with the respective agencies on possibly leveraging CISA's reporting infrastructure for CIRCIA to facilitate covered entity reporting in those areas, too. This would provide another way in which CISA and its fellow agencies could mitigate reporting burden on affected organizations if they cannot eliminate it.

We appreciate that CISA recognizes the need for covered entities to exercise discretion and judgment in evaluating the factors that would make a cyber incident a "substantial cyber incident" subject to reporting under the proposed regulations. However, we do not think the brief set of examples provided in relation to each of the identified factors adequately addresses the cost and compliance concerns that a covered entity might have in a given context. The higher education community urges CISA to work with covered entities to develop a clearer set of guiding principles for assessing whether an event is sufficiently "serious," "substantial," or disruptive to rise to the covered incident level. Likewise, we believe that the proposed requirement for reporting any compromise resulting from a service provider or supply chain issue, regardless of whether it is serious, substantial, or disruptive for the entity involved, to be potentially counterproductive to the goals that CIRCIA and CISA have outlined. With that in mind, we suggest that CISA consider engaging the stakeholder community for these regulations further to help it identify parameters and/or reporting options that might better serve CISA's objectives while minimizing the reporting burden placed on covered entities.

While our comments highlight a number of points for consideration (or reconsideration) in relation to reporting requirements, we note that the proposed regulations appear to call for the over-collection of sensitive technical and cybersecurity information that may both unnecessarily slow reporting and leave CISA with significant data management and security difficulties. Given the potential for these problems to frustrate the goals and objectives that CISA seeks to achieve through the proposed regulations, we encourage the agency to revisit with the overall stakeholder community the depth and breadth of information it truly needs upfront in a given instance of covered incident reporting and how it might use additional process steps to gather additional information when and where actually needed. We also find that the proposed regulations should be augmented with more information regarding elements such as estimating financial impacts of a covered incident and the degree to which covered entities maintain compliance by reporting what they reasonably can at a given time. In addition, we urge CISA to consider whether it has effectively accounted for the diversity of capabilities and available resources across the array of organizations and industries it proposes to pull into scope in designing its records preservation requirements; the higher education community does not think it has, at least in relation to small, rural, and/or resource-challenged colleges and universities, and thus we suggest some options for rebalancing as a result.

Finally, in relation to the enforcement provisions of the proposed regulations, we reiterate our assessment that public higher education institutions, as subdivisions of state, local, tribal, or territorial governments, qualify for the exclusion from enforcement provided by law and regulation, and we invite dialogue with CISA on the matter should that be needed. Furthermore, we strongly urge CISA to add an appeals process regarding the form, content, and deadlines for an RFI, if not for the issuance of an RFI itself, given the expansive discretion that CISA has under the regulations to issue an RFI, set the terms of response, and rapidly move to issuing a subpoena instead. We ask as well that CISA provide a more detailed discussion in the regulations regarding its responsibility for the legal and regulatory impacts of the unauthorized access and disclosure of the sensitive technical and security information that entities report, if and when that occurs.

The higher education community appreciates this opportunity to inform the rule-making process for CIRCIA, and we look forward to the subsequent outreach and engagement about our concerns that we hope to see in the near future.

Sincerely,

John O'Brien
President and CEO
EDUCAUSE

On behalf of:

American Association of Collegiate Registrars and Admissions Officers
Association of American Universities
Association of Governing Boards of Universities and Colleges
Association of Public and Land-grant Universities
National Association of Independent Colleges and Universities