REN-ISAC Alert (April 12th, 2024)
Notice of Proposed Federal Rulemaking With Significant Potential Impact to Colleges and Universities
DHS CISA "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements"

REFERENCES: https://federalregister.gov/d/2024-06526 (implementing 6 U.S.C. 681 through 681e, and 6 U.S.C. 681g)

WHAT IS CIRCIA: "CIRCIA requires covered entities to report to CISA within certain prescribed timeframes any covered cyber incidents, ransom payments made in response to a ransomware attack, and any substantial new or different information discovered related to a previously submitted report." CIRCIA has a prescribed timeframe of 72 hours for cyber incidents & 24 hours for ransom payments. Records relating to the incident must be retained for two years. Penalties will be incurred for non-compliance. The public can comment on the proposed rule as described in the Federal Register filing until June 3rd, 2024. Required reporting will commence on the date to eventually be set in the Final Rule (likely 18 months from now).

WHO DOES CIRCIA AFFECT?: Many higher education institutions may qualify as "covered entities" including

> "[Any] local educational agency, educational service agency, or state educational agency, as defined under 20 U.S.C. 7801, with a student population equal to or greater than 1,000 students; or **[any] institute of higher education that receives funding under Title IV of the Higher Education Act, 20 U.S.C. 1001 et seq., as amended**;"

Some additional criteria relevant to higher education institutions include operating a hospital with 100 or more beds, performing activities related to domain name related operations, and requirements as part of Federal contracts. Review the draft rule for additional criteria and specific details.

WHAT IS A "COVERED INCIDENT": Examples of what is and is not a "covered incident" are listed in the Federal Register Filing. Here is a selection that WOULD be considered a "covered incident" under the currently proposed rules

> *(1) A distributed denial-of-service attack that renders a covered entity's service unavailable to customers for an extended period of time.*
> *(2) Any cyber incident that encrypts one of a covered entity's core business systems or information systems. [...]*
> *(6) The exploitation of a vulnerability resulting in the extended downtime of a covered entity's information system or network.*
> *(7) A ransomware attack that locks a covered entity out of its industrial control system.*
> *(8) Unauthorized access to a covered entity's business systems caused by the automated download of a tampered software update, even if no known data exfiltration has been identified.*
> *(9) Unauthorized access to a covered entity's business systems using compromised credentials from a managed service provider.*
> *(10) The intentional exfiltration of sensitive data in an unauthorized manner for an unauthorized purpose, such as through compromise of identity infrastructure or unauthorized downloading to a flash drive or online storage account.*

HOW TO MAKE A REPORT AND WHAT TO INCLUDE: The draft rule envisions use of an online web portal. An extensive list of required-to-be-reported elements can be seen in section 226.7-226.8 of the draft rule.

ACTION: CISOs should review the proposed rule with their staff and with university counsel. Review and update (or plan to update) any incident response plans to include CIRCIA reporting. Institutions may wish to share feedback on the proposed rule as described in the Federal Register filing, coordinating with institutional leadership and their federal affairs office. The REN-ISAC is available to any US higher education institution with questions or concerns. Contact us at **soc@ren-isac.net**.