SPECIAL REPORT

PREPARING FOR CIRCIA'S REPORTING REQUIREMENTS AND AVOIDING ITS HARSH PENALTIES

Sagar K. Ravi, Stephen E. Reynolds, Katelyn R. Ringrose

McDermott Will & Emery

McDermott Will & Emery

SPECIAL REPORT

TABLE OF CONTENTS

LEARN MORE

For more information, please contact your regular McDermott lawyer, or:

SAGAR K. RAVI
PARTNER

sravi@mwe.com
Tel +1 202 756 8043

STEPHEN E. REYNOLDS
PARTNER

sreynolds@mwe.com
Tel +1 312 984 3398

KATELYN N. RINGROSE
ASSOCIATE

kringrose@mwe.com
Tel +1 202 756 8176

For more information about McDermott Will & Emery visit mwe.com

INTRODUCTION

The US Cybersecurity and Infrastructure Security Agency (CISA) recently published a Notice for Proposed Rulemaking intended to supplement the Cybersecurity Incident Reporting for Critical Infrastructure Act (CIRCIA). The notice offers additional information on how CISA intends to implement CIRCIA, outlining how covered entities must report, and retain information on, substantial cyber incidents and ransom payments once CIRCIA's reporting and retention requirements take effect in 2026. While CIRCIA is subject to further rulemaking before a final rule is published, the reporting and retention requirements outlined within the notice are the most sweeping to date, posing harsh penalties for noncompliance.

The notice makes clear that the federal government intends to impose criminal and civil liability on individuals, including corporate employees reporting on behalf of a covered entity, who interfere with CISA's ability to obtain accurate information. The information CISA asks of those entities is wide-ranging and includes a description of security defenses the entity had in place at the time of the incident. Penalties for providing false statements or representations include fines, imprisonment of up to five years, or – if the offense involves international or domestic terrorism – imprisonment of up to eight years. Further, in cases of noncompliance with a request for information (RFI) or a subpoena, CISA reserves the right to refer cases to the attorney general for civil actions or to pursue other punitive measures against the individuals involved, such as contempt of court, penalties, suspension, or disbarment.

If CISA needs to resort to issuing a subpoena against a covered entity, CISA reserves the right to reveal the information obtained pursuant to that legal process to the attorney general or the head of a regulatory agency, who may use that information to pursue additional criminal penalties as well as regulatory enforcement actions against not only the cyber threat actors involved, but against the covered entity and its employees. CIRCIA explicitly notes that while none of those parties will receive complete immunity by cooperating, in determining whether to refer cases for enforcement, CISA's director will consider the covered entity's engagement and cooperation with CISA.

While the consequences of not complying can be very harsh, the threat of fines, incarceration, or sanctions can be mitigated through a careful approach to CIRCIA compliance. Entities and individuals responsible for cyber-incident reporting should proactively prepare for compliance soon, before reporting requirements take effect. At large companies, a proactive approach will require careful coordination among multiple teams, from cybersecurity and privacy to securities and regulatory, and may require additional help from outside counsel. Ultimately, covered entities should take proactive measures now to better understand their obligations, implement necessary reporting processes, and avoid the severe consequences associated with failing to properly comply with the requirements laid out in the notice.

IN DEPTH

CIRCIA AT A GLANCE

Under CIRCIA, covered entities must report "substantial cyber incidents" to CISA within 72 hours of a reasonable belief that such an incident has occurred, while covered entities that make a ransom payment must report that payment to CISA within 24 hours. In a bid to make interactions with CISA more collaborative, CIRCIA also allows covered entities to voluntarily exchange information with CISA and other relevant government agencies who in turn may make such information available to certain other federal agencies.

To improve intergovernmental information exchanges, CIRCIA also establishes a Joint Ransomware Task Force and a Cyber Incident Reporting Council to coordinate, deconflict, and harmonize reporting requirements. CIRCIA also leaves room for CISA to promulgate additional regulations to implement CIRCIA's requirements and to provide sector-specific guidance. The recently passed notice is CISA's first expansive attempt at offering guidance prior to the publication of a final rule in September 2025, which is expected to take effect in 2026.

REPORTING AND RETENTION REQUIREMENTS

Who Should Report?

The notice, which was proposed by the US Department of Homeland Security on April 4, 2024, helps clarify the scope of CIRCIA by providing insight into which entities are covered by the act. Covered entities include entities larger than a small business, which is generally defined as having fewer than 500 employees or having annual receipts less than $7.5 million, as well as any business (large or small) that offers services in 16 specific sectors, which were chosen for the impact those entities would have, if attacked, on the United States and trade. Those sectors, established by Presidential Policy Directive 21 (PPD-21) and reiterated in National Security Memorandum (NSM-22), are wide-ranging and include, for example, healthcare, information technology, communications, energy, financial services, and transportation.

Entities ranging from hospitals to energy providers that have not traditionally considered themselves as critical infrastructure should consider whether their sector has been named by CISA as critical by looking through the Sector-Specific Plans (SSP) as outlined by PPD-21.

What Triggers a Reporting Obligation?

After CIRCIA's requirements become effective, covered entities will be required to report substantial cyber incidents within 72 hours of a reasonable belief that such an incident has occurred. A "substantial cyber incident" is defined as causing any of the following:

- Substantial loss of confidentiality, integrity, or availability
- Serious impact on safety and resiliency of operational systems and processes
- Disruption of ability to engage in business or industrial operations or deliver goods or services
- Unauthorized access facilitated through or caused by a compromise of a provider or third party or a supply chain compromise.

In addition, a covered entity is required to report a ransom payment in response to a ransomware attack within 24 hours. The notice reaffirms the existing CIRCIA requirement that if a third party makes a

ransomware payment on behalf of a covered entity, that third party must advise the covered entity of their obligation to report.

There are three exceptions to the reporting requirements:

- The covered entity has already reported to another federal agency, when that information can be shared between that entity and CISA
- The critical infrastructure impacted concerns the domain name service (DNS), which is already governed by policies administered by the Internet Corporation for Assigned Names and Numbers (ICANN)
- The incident occurred at a federal agency that already reports incidents through the Federal Information Security Modernization Act (FISMA).

What Should Be Reported?

The report must include specific pieces of information, including:

- Contact information
- A description of the incident
- Technical details of the incident
- Whether the affected systems house information supporting the federal government's national security missions
- A timeline of the incident
- Which (if known) vulnerabilities were exploited
- A description of security defenses the entity had in place at the time of the incident
- A description of the techniques, tactics, and procedures (TTPs) used to carry out the attack
- Any known indicators of compromise (*e.g.*, known or suspected malicious internet protocol addresses, emails, or files)
- A description and samples of malware used in the attacks
- Any information the entity can provide that may lead to attribution of the adversary (*e.g.*, contact information for a ransomware gang)
- A description of how the entity responded to the attack
- Which (if any) law enforcement agencies the entity has engaged
- Which (if any) other entities (*e.g.*, a cybersecurity firm) the entity has engaged.

If a covered entity makes a ransomware payment, or has another entity make such a payment on their behalf in response to a ransomware attack, they must report all the above information, with the addition of:

- The date and amount of a ransom payment
- Any ransom payment instructions (*e.g.*, destination address and wallet, copies of instructions, and preferred cryptocurrency)
- Whether the payment ended the attack.

When Should Supplemental Reports Be Submitted?

Until a substantial cyber incident or the payment of a ransom has concluded and has been fully mitigated and resolved, a covered entity must "promptly" submit a supplemental report when new or different information comes to light than was contained in an initial or prior report. CISA interprets "promptly" to mean without

delay or as soon as possible, but at least within 24 hours of when such information comes to light, including information that:

- Is responsive to a required data field 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
- Shows that a previously submitted covered cyber incident report or supplemental report is materially incorrect or incomplete.

Finally, after reporting a substantial cyber incident or a ransom payment, covered entities must preserve records and data for at least two years after a report was, or should have been, submitted. It is important to note that this two-year requirement starts when a report should have been submitted, even if that is earlier than the actual submission date.

How Is Information Submitted to CISA Protected?

Information submitted by covered entities as part of the normal course of reporting, including through a CIRCIA report or an RFI, are covered by a number of protections. For example, covered entities can choose to designate certain information as commercial, financial, or proprietary, and such information will be treated accordingly. Further, such information will be exempt from Freedom of Information Act (FOIA) disclosures. Most importantly, covered entities do not waive any privileges or protections under the law, as the information they submitted, or the fact that a submission was made at all, cannot be used to bring a cause of action against the entity. These significant protections against liability lapse, however, if a covered entity fails to comply with relevant requirements.

PENALTIES FOR NONCOMPLIANCE

What if a Covered Entity Fails to Report?

CIRCIA grants CISA the right issue an RFI to any entity CISA considers a covered entity if CISA has reason to believe that that the entity experienced a substantial cyber incident or made a ransom payment but failed to report the incident or payment. Such a belief by CISA could be based on public reporting or any information in the possession of the federal government, which includes CISA's own analysis. As for response times, the RFI will include a date by which the covered entity must respond as well as the manner and format in which the covered entity must provide information.

If the covered entity fails to respond to CISA, CISA may issue a subpoena to compel disclosure. Such a subpoena can be issued, at the earliest, within 72 hours after the RFI was delivered. The notice makes it clear that CISA intends to impose liability on individuals, including security and privacy officers, who interfere with CISA's ability to obtain accurate information.

If CISA must resort to issuing a subpoena to retrieve information from a covered entity, CISA has made it abundantly clear that all information obtained in response to a subpoena may be referred to the attorney general or the head of a relevant regulatory agency. When determining whether to make such a referral, CISA will consider the covered entity's engagement and cooperation with CISA. It is worth noting, too, that all information revealed during CISA's engagement with a subpoenaed entity related to the cyber incident or ransom payment is considered subpoenaed information for the purpose of a referral.

Any person who knowingly and willfully makes a false or fraudulent statement or representation with, or

within, a CIRCIA report, an RFI, or in response to an administrative subpoena is subject to penalties under 18 U.S.C. § 1001. Penalties under Section 1001 include fines, imprisonment of up to five years, or – if the offense involves international or domestic terrorism – up to eight years.

What Are the Responsibilities of Third Parties?

Third parties seeking to report on behalf of a covered entity must obtain permission to do so through an attestation expressly authorized by the covered entity. This attestation should bar third parties from liability regarding knowingly providing false information if that information was provided by the covered entity.

That said, covered entities that use third parties to submit reports cannot shift their responsibilities or liability onto that third party. CISA has made it clear that covered entities are responsible for the accuracy and timeliness of all reporting, including reports offered by third parties. The notice states that "the requirement to submit a timely and accurate report under CIRCIA remains in all cases with the covered entity itself," and that an "enforcement action for noncompliance is to be brought against the covered entity, not a third party that submitted (or failed to submit) a report on the covered entity's behalf."

What Protections Does CIRCIA Offer Regarding Honest Mistakes?

While CIRCIA offers harsh penalties for noncompliance or for providing false or misleading information, it is apparent that CISA also hopes to avoid having a chilling effect on individuals' reporting of cyber incidents and ransomware payments out of a fear of being prosecuted for the contents of those reports. To achieve this balance, CIRCIA protects individuals who submit information to CISA quickly and fulsomely, either as part of a compliant CIRCIA report or in response to a request for information, and who seek to correct mistakes through supplemental reporting. Under this framework, individuals and covered entities are encouraged to submit as much information as possible as quickly as possible, in their initial CIRCIA report and beyond. Such individuals and covered entities are also encouraged to issue corrections whenever new information comes to light.

Through the notice, CISA has provided guidance that it does not consider levying penalties in instances where a covered entity reports information that it reasonably believes to be true at the time of submission, but later learns, through investigation, was inaccurate, so long as the covered entity submits a supplemental report reflecting this new information.

PRACTICAL CONSIDERATIONS FOR COVERED ENTITIES

The notice highlights CISA's continued investment in monitoring cyber threats across a broad landscape. To contribute to that investment and avoid potentially harsh penalties, entities should consider taking the following actions:

1. **Determine whether the sector in which the business operates or the size of the business qualifies it as a covered entity.**

CISA estimates that more than 300,000 entities will be covered by CIRCIA, and it is likely that many of those entities, including companies in the agriculture, healthcare, and energy sectors, do not consider themselves to fall within critical infrastructure or to be covered by the proposed rules. Entities will want to determine whether they are covered, now, at risk of being caught off guard by an investigation or sanction

at a later date, should CISA determine that they are a covered entity. Companies also should ensure that they understand their obligations under CIRCIA to avoid being unprepared and being required to comply with CISA's highly specific requirements amid a substantial cyber incident.

2. **Acknowledge that covered entities and individual employees face significant risks for noncompliance.**

The penalties associated with noncompliance do not just pertain to individuals acting as bad actors, hoping to intentionally circumvent CISA's authority. In the emergent situation posed by a substantial cyber incident, an employee could make a mistake that can be seen as a materially false or fraudulent statement or representation. Cybercrimes are dynamic and require incredibly fast response times. This, coupled with the small reporting windows at issue here (typically, 72 or 24 hours), may mean that entities that have never interacted with government officials will need to ensure that they follow a process to provide timely and accurate information. Covered entities should therefore acknowledge the risks they and their employees face in order to garner adequate resources to comply with CIRCIA's requirements.

3. **Create specific and actionable plans to ensure compliance with reporting requirements.**

The information CISA requires within the period following a substantial cybersecurity incident or the payment of ransom is incredibly granular. Companies should create a plan or even template language for compliance that can be included in a cyber incident response plan, which will save covered entities time and effort while they are navigating the high-stress situation of a cyber incident. Such a plan can ensure that companies know which questions to ask, and what information is required, in order to comply with CIRCIA's requirements.

4. **Coordinate plans to comply with reporting requirements and align information reported, pursuant to CIRCIA, with information reported elsewhere.**

CIRCIA's reporting and retention requirements exist within a broader framework, from state laws to US Securities and Exchange Commission (SEC) compliance. Covered entities should determine, before CIRCIA's reporting requirements come into effect, how those requirements align with the statements and information they make available to customers, vendors, shareholders, the public, etc. Notably, the information that CISA requires from covered entities is wide-ranging and includes a description of security defenses the entity had in place at the time of the incident. To avoid potential civil liability as well as regulatory scrutiny, covered entities, particularly public companies, should seek to align such security disclosures to CISA with public representations of their security defenses as well as internal board and senior officer reporting. Otherwise, statements made in the midst of a substantial cyber incident could have considerable consequences down the road.

5. **Outline which data and records should be retained and engage in data mapping now to ensure retention.**

Ensuring that certain data is retained in the hours following an incident or the payment of a ransom is, of course, critical to forensic analysis and legal compliance after the cyber incident is mitigated. However, retention can sometimes be the last thing on the minds of teams navigating the loss of corporate data, user data, or systems. Determining the means of retention, including data types and the technical means

of retention, will save time and energy during a cyber crisis.

6. **Collaborate with third parties to determine whether they will have the authority to submit reports on the entity's behalf.**

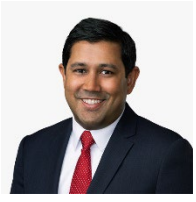
The notice lays out a framework whereby covered entities can give third parties permission to report substantial cybersecurity incidents or the payment of ransoms on their behalf. That permission can be granted by a simple click-through form. However, prior to such an incident occurring, covered entities may consider including in, for example, their data-processing agreements or vendor-risk assessments, a question as to whether third parties are willing to handle reporting on their behalf. This is critical information to know because information submitted by those third parties is the responsibility of covered entities, which will be held directly responsible for the statements made or omitted by such third parties.

WHAT'S NEXT?

Now that the comment period for the notice has closed, CISA plans to publish the final rule governing reporting requirements in September 2025, with the rule taking effect in 2026. In the meantime, entities can prepare by identifying whether they are a covered entity under the new framework, familiarizing themselves with the reporting and retention requirements, and preparing to engage in transparency with CISA – at risk of civil and criminal liability, should they fail to do so.

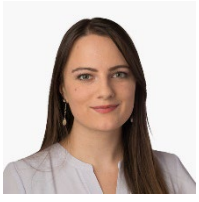
Covered entities should prepare to act quickly and exercise honesty with CISA, at risk of losing those significant protections against liability that are extended to information submitted as part of a CIRCIA report or in response to a request for information. Failing to comply and respond to CISA, or engaging in deception, can lead to individuals and entities losing CISA's goodwill and increase the risk of significant penalties.

CONTRIBUTORS



SAGAR K. RAVI
PARTNER
sravi@mwe.com
Tel +1 202 756 8043

STEPHEN E. REYNOLDS
PARTNER
sreynolds@mwe.com
Tel +1 312 984 3398



KATELYN R. RINGROSE
ASSOCIATE
kringrose@mwe.com
Tel +1 202 756 8176

McDermott
Will & Emery

mwe.com |