Baker McKenzie.

Cybersecurity
FACT SHEET

Critical Infrastructure Risk Management Cybersecurity Improvement Act (CIRCIA)

Who?

- The **Critical Infrastructure Risk Management Cybersecurity Improvement Act (CIRCIA)** applies to "covered entities" that operate in a "critical infrastructure sector."
- "**Covered entity**" is not yet defined and will be determined by the Cybersecurity and Infrastructure Security Agency (CISA) pursuant to a rulemaking process.
- "**Critical infrastructure sectors**" include (1) Chemical; (2) Commercial Facilities; (3) Communications; (4) Critical Manufacturing; (5) Dams; (6) Defense Industrial Bases; (7) Emergency Services; (8) Energy; (9) Financial Services; (10) Food & Agriculture; (11) Government Facilities; (12) Healthcare & Public Health; (13) Information Technology; (14) Nuclear; (15) Transportation; and (16) Water & Wastewater Systems.

What?

- CIRCIA is a Presidential Policy Directive 21 (PPD-21).
- CIRCIA will require covered entities that operate in critical infrastructure sectors to report "covered cyber incidents" and ransom payments to CISA.
- "Covered cyber incident" is defined as a "substantial cyber incident."
- "Cyber incident" is defined as "an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system."

Where?

- CIRCIA applies to covered entities within the United States. CIRCIA does not expressly state any geographic restrictions if the cyber incident occurs outside the United States. Accordingly, businesses that operate critical infrastructure within the United States may be required to report even if the cyber incident did not occur within the United States.
- CISA may provide additional detail on the geographical application of CIRCIA when defining "covered entities" subject to rulemaking.

Why?

- Approximately 85% of the United States critical infrastructure is owned by the private sector.
- The purpose of CIRCIA is to improve the cybersecurity of critical infrastructure by requiring covered entities to report cybersecurity incidents and ransom payments to CISA. Such information will provide CISA with information to identify cyber threats and vulnerabilities, respond to cyber incidents, and prevent threats of harm.
- Failure to adhere to CIRCIA reporting obligations could result in court proceedings.

When?

- CIRCIA requires covered entities that operate in critical infrastructure sectors to report covered cyber incidents within **72 hours** of the companies' reasonable belief that a cyber incident has occurred and to report ransom payments within **24 hours** after a payment is made.
- Mandatory reporting is not required until the effective date of the final rule, which is likely in September 2025. CISA encourages voluntary reporting until then.
- CIRCIA requires CISA to publish a Notice of Proposed Rulemaking (NPRM) by March 2024.

How Baker McKenzie Can Help

- **Consult with outside counsel to issue a legal opinion as to whether you are a covered entity**
- **Refresh playbooks and develop frameworks for determining whether a cyber incident is reportable and/ or "substantial cyber incident"**
- **Train and exercise your IR team to understand the new reporting obligations**
- **Stay updated on new developments and regulations by subscribing to Connect on Tech, our blog and podcast series**

PROUD SPONSOR OF
INFRAGARD NATIONAL MEMBERS ALLIANCE
2023

bakermckenzie.com

Baker McKenzie.

Cybersecurity
FACT SHEET

Network and Information Security Directive 2 (NIS2)

Who?

- The **Network and Information Security Directive 2 (NIS2)** applies to entities deemed '**essential**' and '**important**' and depends on a number of factors including the size of the company and whether the organization is a "**critical sector**" or "**very critical sector.**" Both important and essential entities must comply with the same legal requirements, but the penalties for noncompliance may vary.
- "**Critical sectors**" include: digital providers; postal and courier services; waste management; manufacturing, production, and distribution of chemicals; production, processing, and distribution of food; research; and manufacturing.
- "**Very critical sectors**" include: energy; transport; banking; financial markets infrastructure; health care; drinking water; digital infrastructure; ICT services management (business-to-business); waste water; public administration; and space activities.

What?

- Both essential and important entities must (1) adopt technical and organizational security measures; (2) ensure their "management bodies" have appropriate oversight and accountability for and training on cybersecurity functions that they manage; and (3) notify relevant EU state authorities upon learning of a cybersecurity incident as follows:
- Within **24 hours** of becoming aware of the incident – an "early warning report" indicating whether the significant incident is suspected of being caused by unlawful or malicious acts
- Within **72 hours** of becoming aware of the incident – an "incident notification", updating the early warning report as necessary, and indicating including its severity and impact, as well as indicators of compromise
- When requested by national authorities – an "intermediate report" with status updates
- Within **one month** of the submission of the "incident notification" – a "final report" including a detailed description of the incident, its root cause, mitigation measures taken, and potential crossborder impacts of the incident

Where?

- NIS2 applies to public and private entities "which provide their services or carry out their activities within the [European] Union." Accordingly, organizations that are active within the EU will be required to adhere to NIS2 requirements regardless of where the organization is formally registered or headquartered.

Why?

- In 2016 the European Parliament adopted the Network and Information Security Directive (NISD), the first EU-wide legislation on cybersecurity. NIS2 is the successor legislation to NISD. The new directive seeks to address perceived flaws in the previous version, protect essential and important organisations and infrastructure from cyber threats and attacks, and achieve a high level of common security across the EU. The NIS2 Directive affects many more sectors than the original NIS Directive.
- Member states may impose robust penalties for noncompliance with NIS2 including:
- Essential entities: fines of at least up to €10 million or 2% of the worldwide annual turnover.
- Important entities: fines of at least up to €7 million or 1.4% of the worldwide annual turnover.

When?

- NIS2 came into force on January 16, 2023 but is not effective immediately.
- NIS2 requires EU member states to publish necessary compliance requirements in their local laws by October 17, 2024.

How Baker McKenzie Can Help

- **Consult with outside counsel to issue a legal opinion as to whether you are a covered entity**
- **Refresh playbooks and develop frameworks for determining whether a cyber incident is reportable and/or "substantial cyber incident"**
- **Train and exercise your IR team to understand the new reporting obligations**
- **Stay updated on new developments and regulations by subscribing to Connect on Tech, our blog and podcast series**

PROUD SPONSOR OF
INFRAGARD NATIONAL MEMBERS ALLIANCE
2023

bakermckenzie.com

Baker McKenzie.

Cybersecurity
FACT SHEET

SEC's Rules On Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure (the SEC Rules)

Who?

- The SEC's rules on cybersecurity risk management, strategy, governance and incident disclosure (the **SEC Rules**) apply to all public companies that are required to register and file reports with the SEC under the Securities Exchange Act of 1934 or the Investment Company Act of 1940. This includes domestic and foreign issuers.

What?

- The SEC Rules impose new reporting obligations.
- In their annual reports (Form 10-K or Form 20-F for foreign issuers) public companies must now report on their process for:
  - » assessing, identifying, and managing risk rom cyber threats and
  - » board and management oversight of cyber risks
- In a Form 8-K, public companies must report material cybersecurity incidents and include the material aspects of the incident's nature, scope, and timing, its impact or reasonably likely impact. Companies must make an initial determination as to whether the cybersecurity incident is material "without unreasonable delay." "Material incidents" must be reported using Form 8-K, **within four (4) days** of the materiality determination.

Where?

- The SEC Rules apply both to domestic US issuers (those incorporated in a US state) as well as to foreign private issuers subject to registration with the SEC.

Why?

- While the SEC Rules are silent on specific penalties, the SEC treats a company's failure to report material events very seriously and such failure may result in fines, sanctions, investigations and referral to the Justice Department for potential criminal prosecution.

When?

- Adopted September 5, 2023.
- Form 10-K or 20-F must comply with SEC Rules for fiscal years ending on or after December 15, 2023.
- Registrants must comply with the incident reporting requirements (i.e., Form 8-K) starting December 18, 2023. Smaller reporting entities will have until June 15, 2024.

How Baker McKenzie Can Help

- **Refresh playbooks and develop frameworks for determining whether a cyber incident is "material"**
- **Design programs, including tabletop exercises, to build board and leadership expertise**
- **Implement processes to manage and respond to cybersecurity risks, including training and exercising your IR team to understand the new reporting obligations**
- **Review and update contractual obligations for reporting cybersecurity obligations**
- **Develop proactive and reactive cyber language that will be used in SEC filings**

bakermckenzie.com

Baker McKenzie.

Cybersecurity
FACT SHEET

NY-DFS Cybersecurity Regulation (23 NYCRR 500)

Who?

- The **NYDFS Cybersecurity Regulation (23 NYCRR 500)** requires New York insurance companies, banks, and other regulated financial services institutions—entities operating under license, registration, charter, certificate, permit, or accreditation under New York banking, insurance or financial services law—to maintain a cybersecurity program.
- Under proposed amendments to NYCRR 500, enhanced requirements would apply to Class A companies.
- Class A companies are those covered entities with at least $20 million in gross annual revenue in each of the last two fiscal years from the business operations of the entity (including affiliates) within New York State and that have either: (1) more than 2,000 employees as averaged over the past two fiscal years (including affiliates), or (2) over $1 billion in gross annual revenue in each of the last two fiscal years from all business operations (including affiliates).

What?

- Under NYCRR 500 covered entities must:
  - maintain a cybersecurity program designed to identify and assess cyber risks
  - take defensive measures to protect their systems
  - detect and respond to cybersecurity events
  - appoint a CISO
  - conduct regular penetration testing and vulnerability assessments
  - engage cybersecurity personnel
  - maintain a third party provider security policy, and
  - implement technical and organizational security measures like encryption, multifactor authentication and limited access privileges.
- NYCRR 500 also expands existing **72 hour** notice obligations if a cybersecurity incident occurs requirements, to include **24 hour** notice if ransom is paid.

Where?

- NYCRR 500 applies to entities operating under license, registration, charter, certificate, permit, or accreditation under New York banking, insurance or financial services law including branches of foreign banks and financial institutions regulated by NY DFS.

Why?

- Entities found to violate their obligations under NYCRR 500 may be subject to financial penalties. NY DFS has been very active in enforcing NYCRR 500, with announcement settlements with alleged infringers regularly running to the millions of dollars.

When?

- NYCRR 500 has been effective since 2017.
- In June 2023, NY DFS proposed amendments to NYCRR 500 that would expand the scope of NYCRR 500's requirements. These amendments are not yet finalized.

How Baker McKenzie Can Help

- **Determine the applicability of NYDFS to your organization**
- **Work with your stakeholders to customize and operationalize a cybersecurity program in compliance with NYCRR 500**
- **Conduct customized training of personnel. Baker McKenzie is certified by the New York State CLE Board as an accredited provider of CLE in Cybersecurity, Privacy and Data Protection – Ethics and Cybersecurity, Privacy and Data Protection – General**
- **Create a defensible and reasonable vendor management program**
- **Train and exercise your IR team to understand these new reporting obligations**
- **Stay updated on new developments and regulations by subscribing to Connect on Tech, our blog and podcast series**

PROUD SPONSOR OF
INFRAGARD NATIONAL MEMBERS ALLIANCE
2023

bakermckenzie.com

Baker McKenzie.

Cybersecurity
FACT SHEET

Health Insurance Portability and Accountability Act (HIPAA)

Who?

- The **HIPAA Privacy, Security and Breach Notification Rules (HIPAA Rules)** apply to covered entities and their business associates.
- **Covered entities** include health plans, health care clearinghouses (outside entities that process health information), and most health care providers.
- **Business associates** are persons or entities that perform functions or activities on behalf of, or provide services to, a covered entity and use or disclose protected health information (PHI) in the course of performing such functions.

What?

- The HIPAA Privacy Rule requires appropriate safeguards to protect the privacy of PHI and sets limits and conditions on the uses and disclosures that may be made of such information without an individual's authorization
- The HIPAA Security Rule requires covered entities and business associates to protect against any reasonably anticipated threats or hazards to the security or integrity of any PHI that is maintained or transmitted in electronic form, protect against any reasonably anticipated unauthorized uses or disclosures of such information, and ensure compliance with the HIPAA Security Rule by its workforce.
- The HIPAA Breach Notification Rule requires covered entities, in the event of certain breaches of unsecured PHI, to notify the individuals whose PHI has been compromised, report the breach to HHS, and, in certain cases, also notify
- the media. Covered entities may push down some of these obligations on to their business associates.

Why?

- Violations of HIPAA can have significant consequences for companies, including financial penalties (up to approximately $2 million per year for the most serious violations), criminal prosecution, and reputational harm.

When?

- The HIPAA Rules are already fully effective.
- Under the HIPAA Breach Notification Rule, notice to individuals must be made without unreasonable delay and in no case later than **60 days** after discovery of a notifiable breach. For breaches of unsecured PHI involving 500 or more individuals, the covered entity must notify HHS contemporaneously with the notification made to the affected individual(s). Breaches of unsecured PHI involving fewer than 500 individuals must be reported annually by the covered entity.
- In the event a business associate suffers a breach of unsecured PHI that it handles on behalf of a covered entity, it must notify the covered entity without unreasonable delay and in no case later than 60 days after discovery of the breach.
- The parties' responsibilities with respect to breach notification obligations can also be addressed in Business Associate Agreements.
- Under the HIPAA Security Rule, covered entities and business associates are required to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by the organization. The HIPAA Security Rule does not specify how frequently the risk analysis must be performed, but the risk analysis process should be ongoing.

How Baker McKenzie Can Help

- **Conduct healthcare privacy impact assessments**
- **Conduct HIPAA compliance gap assessments**
- **Advise on legal requirements to comply with the HIPAA Rules**
- **Direct technical providers under privilege to conduct HIPAA security risk assessments, as well as third party tracking technology analysis**
- **Refresh incident response plan to include PHI playbook**
- **Develop template contractual terms for vendors and customers to address HIPAA Rules**

PROUD SPONSOR OF
INFRAGARD NATIONAL MEMBERS ALLIANCE
2023

bakermckenzie.com

Baker McKenzie.

Cybersecurity
FACT SHEET

NERC CIP-008-6 standard for Cyber Security — Incident Reporting and Response Planning

Who?

- The NERC CIP-008-6 standard for Cyber Security — Incident Reporting and Response Planning (the **NERC Cybersecurity Standard**) requires certain entities responsible for the provision of energy infrastructure to adhere to certain cybersecurity requirements.
- NERC Cybersecurity Standard applies to balancing authorities, distribution providers, generator operators, generator owners, reliability coordinators, transmission operators, and transmission owners.

What?

- The NERC Cybersecurity Standard requires entities to document, implement and maintain a cybersecurity response plan to identify, classify, and respond to incidents.
- NERC also requires businesses to notify NERC's Electricity Information Sharing and Analysis Center, as well as the National Cybersecurity and Communications Integration Center (NCCIC), of any reportable cybersecurity incidents.
- When an entity subject to the NERC Cybersecurity Standard discovers a reportable cybersecurity incident, it must give notice within one hour. Additional updates should be provided within seven days.
- The notification should indicate the incident's functional impact, the attack vector used, and the level of intrusion achieved or attempted.

Where?

- NERC is a non-profit organization that oversees six regional entities across North America, including the power systems of Canada, the contiguous US states, and a portion of the Mexican state of Baja California.

Why?

- Although NERC is a voluntary organization it is authorized by FERC (a US government agency) and Canadian and Mexican regulators to levy monetary penalties and nonmonetary sanctions for violations of its standards. The maximum allowable monetary penalty is $1 million per day per violations.

When?

- The NERC Standard was adopted in 2019 and is fully effective.

How Baker McKenzie Can Help

- **Keep incident response policies and plans updated and operational**
- **Train and exercise your IR team to understand new reporting obligations**
- **Stay updated on new developments and regulations by subscribing to Connect on Tech, our blog and podcast series**

bakermckenzie.com

Baker McKenzie.

Cybersecurity
FACT SHEET

FTC Safeguards Rule

What?

- The purpose of the **FTC Safeguards Rule** is to ensure that covered "financial institutions" maintain safeguards to protect the security of customer information and 2021 revisions provide more concrete guidance on data security principles that businesses must implement.
- Financial institutions subject to the Safeguards Rule must develop, implement, and maintain a written information security program with administrative, technical, and physical safeguards designed to protect customer information. The program should be appropriate to the size and complexity of the business, the nature and scope of activities, and the sensitivity of the information at issue.
- The Rule specifies nine elements of a "reasonable" information security program: (1) designating a "qualified individual" to implement and oversee the program, (2) conduct a risk assessment, (3) implement safeguards to control risks identified in the assessment, (4) monitor and test the effectiveness of safeguards, (5) staff training, (6) monitoring service providers, (7) keeping the program current, (8) creating an incident response plan, and (9) requiring the "qualified individual" to report to the Board.

Who?

- The FTC Safeguards Rule applies to financial institutions.
- "Financial institutions" are organizations engaged in activities that are "financial in nature" or "incidental to such financial activities" **and** subject to the FTC's jurisdiction.
- Financial institutions subject to the enforcement authority of another regulator under section 505 of the Gramm-Leach-Bliley Act are exempt. Certain requirements of the Safeguards Rule do not apply to financial institutions with fewer than 5000 customers.
- Examples of covered "financial institutions" include: finance companies, retail credit card issuers, auto dealerships, real estate appraisers, wire transferors, check cashing businesses, accountant or tax preparation services, and mortgage brokers and lenders.

Where?

- The Safeguards Rule applies to financial institutions doing business in the United States that are subject to the jurisdiction of the FTC.

Why?

- FTC is responsible for enforcing GLBA and FTC may seek fines up to $100,000 per violation.
- FTC revised the rule to keep pace with evolving technology.
- Individuals in charge of ensuring compliance with the Safeguards Rule may be personally liable up to $10,000 per violation and criminal sanctions are available.

When?

- The Safeguards Rule was originally mandated by the Gramm-Leach-Bliley Act of 1999. In 2021 the FTC finalized updates to the Rule, many of which went into effect in 2021. Other sections of the Rule were supposed to be effective on December 9, 2022. However, the effective date for those requirements was delayed by six months, to June 9, 2023, due to shortages of qualified security personnel.

How Baker McKenzie Can Help

- **Determine the applicability of the Safeguards Rule to your organization**
- **Work with your stakeholders to customize and operationalize a written security program that complies with Safeguards Rule requirements**
- **Conduct customized training of personnel as required by the Safeguards Rule**
- **Create a compliant incident response plan and playbooks**
- **Create a defensible and reasonable vendor management program to monitor service providers**

bakermckenzie.com