CLIENT WORKSHEET · CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT

Are you a covered entity under CIRCIA?

Fifteen minutes of checkboxes to find out. CIRCIA will require covered entities to report significant cyber incidents to CISA within **72 hours**, and ransom payments within **24 hours**. Most organizations assume they are too small to be in scope. Many are wrong.

HOW TO USE THIS

Work through Steps 1–3 in order, then read the verdict on the last page. Answer for the legal entity that owns the systems — run a separate copy for each subsidiary or affiliate that operates independently.

WHERE THE RULE STANDS

CIRCIA became law in March 2022. CISA's proposed rule (89 FR 23644, April 4, 2024) defines who is covered; the final rule is still pending as of September 2026. The criteria below follow the proposal, so treat your result as a planning position, not a legal conclusion.

0 Your organization

LEGAL ENTITY NAME

COMPLETED BY / TITLE

EMAIL

DATE

INDUSTRY (NAICS) CODE — LEAVE BLANK IF UNKNOWN

STATES / COUNTRIES YOU OPERATE IN

EMPLOYEES (INCL. AFFILIATES, 24-MO. AVG.)

ANNUAL RECEIPTS (5-YR AVG.)

1 Do you operate in a critical infrastructure sector?

Check every sector your organization operates in, or supplies directly. Sector membership is broad — it follows the sixteen sectors named in PPD-21 / NSM-22, not a list of named companies. If you are unsure, check it and note the doubt.

- ☐ **Chemical** — manufacture, store, or distribute chemicals
- ☐ **Communications** — wireline, wireless, broadcast, satellite, cable
- ☐ **Dams** — dams, levees, navigation locks, mine tailings
- ☐ **Commercial facilities** — retail, lodging, venues, real estate
- ☐ **Critical manufacturing** — metals, machinery, electrical equipment, transport equipment
- ☐ **Defense industrial base** — DoD contracts or subcontracts, R&D, sustainment

- [ ] **Emergency services** — law enforcement, fire, EMS, 911 / dispatch
- [ ] **Financial services** — banks, credit unions, insurers, advisers, payments
- [ ] **Government facilities** — incl. schools, universities, and election infrastructure
- [ ] **Information technology** — software, hardware, cloud, MSP / MSSP, data centers
- [ ] **Transportation systems** — aviation, rail, transit, maritime, trucking, pipelines
- [ ] **Energy** — electricity, oil, natural gas, pipelines
- [ ] **Food and agriculture** — farms, processing, distribution, restaurants, grocery
- [ ] **Healthcare and public health** — providers, plans, labs, pharma, devices
- [ ] **Nuclear** — reactors, materials, and waste
- [ ] **Water and wastewater** — drinking water systems, treatment works
- [ ] **None of the above** — we do not operate in, or directly supply, any of these sectors

> **Checked nothing but "None of the above"?** You are likely outside CIRCIA. Skip to Step 3 anyway — several criteria there apply regardless of sector self-identification, and one "yes" overrides this step.

2 The size test

Under the proposed rule, an organization in a critical infrastructure sector is covered if it **exceeds the SBA small business size standard** for its primary industry — a ceiling on either headcount or annual revenue that differs by industry. Every industry has its own number; parent companies and affiliates count toward yours. If you do not know your ceiling, check "unsure" and we will look it up with you.

- [ ] We **exceed** the SBA size standard for our primary NAICS code.
- [ ] We are **at or below** it — we qualify as a small business.
- [ ] Unsure — we have not run the calculation, or affiliation is unclear.

APPLICABLE STANDARD (E.G. 1,500 EMPLOYEES OR $47M RECEIPTS) AND WHERE YOU FOUND IT

3 Sector-based criteria — size does not matter here

A single "yes" below makes you a covered entity under the proposal **no matter how small you are**. This is where most organizations are surprised. Check every statement that is true of your organization.

- [ ] COMMS · IT We provide wire or radio communications service, internet access, hosting, cloud, managed IT / security services, data-center capacity, or domain-name operations to third parties.
- [ ] IT · FEDERAL We develop, manufacture, license, or support software or hardware, or provide IT services, *to the federal government* — including as a subcontractor.

- [ ] DEFENSE We hold a contract or subcontract requiring us to store, process, or transmit **controlled unclassified information**, or we provide operationally critical support to DoD.
- [ ] HEALTH We are a hospital with **100 or more licensed beds**, a critical access hospital, or we manufacture drugs / Class II or III devices listed as essential medicines or in shortage.
- [ ] GOVERNMENT We are a state, local, tribal, or territorial government entity serving a jurisdiction of **50,000 or more** people — or any SLTT entity that operates election infrastructure.
- [ ] EDUCATION We are a local educational agency, educational service agency, or state educational agency with **1,000 or more** students, or an institution of higher education receiving federal funds.
- [ ] WATER We operate a community water system or publicly owned treatment works serving more than **3,300** people.
- [ ] ENERGY We own or operate assets subject to NERC CIP reliability standards, or are otherwise required to report cyber incidents to DOE, FERC, or NERC.
- [ ] TRANSPORT We are regulated by TSA or the Coast Guard — pipeline, freight or passenger rail, over-the-road bus, aviation operator or airport, or a vessel / facility with a security plan.
- [ ] FINANCE We are a financial institution subject to federal banking, securities, or insurance cyber-incident notification rules (e.g. FDIC / OCC / Fed 36-hour notice, SEC Reg S-P or Reg SCI).
- [ ] CHEMICAL · NUCLEAR We hold an NRC license, or own or operate a facility with a chemical-security or high-risk chemical designation.
- [ ] MANUFACTURING We manufacture primary metals, machinery, electrical equipment, or transportation equipment in the critical manufacturing sector.
- [ ] EMERGENCY We provide 911, emergency dispatch, or public-safety communications for a jurisdiction of any size.
- [ ] NONE **None of these describes us.**

4 Your result

A

Covered — plan on it

You checked at least one box in Step 3, *or* a sector in Step 1 *and* "we exceed the SBA size standard" in Step 2. Assume 72-hour incident and 24-hour ransom-payment reporting obligations once the final rule takes effect.

B

Probably covered — needs a real determination

You checked a sector in Step 1 but answered "unsure" in Step 2, or your Step 3 answers were ambiguous. Resolve the size calculation and affiliation question before you decide anything else — that single number is usually what settles it.

C

Likely not covered — revisit annually

No sector, no size trigger, no sector-based criterion. Coverage can change with a new contract, a growth year, or a final rule that widens scope. Re-run this worksheet at renewal, and whenever you win federal or healthcare work.

Our working determination, based on the answers above: ☐ A ☐ B ☐ C

5 If A or B: can you actually report in 72 hours?

The clock starts when you *reasonably believe* an incident occurred — not when you finish investigating. Answer honestly; a "no" here is a scoping input, not a failing grade.

READINESS QUESTION	YES	NO	UNSURE
A written incident response plan exists and names who declares an incident.	☐	☐	☐
Someone monitors security alerts outside business hours, every day.	☐	☐	☐
Logs from endpoints, identity, and network are retained and searchable.	☐	☐	☐
One named person can authorize or refuse a ransom payment on a weekend.	☐	☐	☐
We already report cyber incidents to another federal regulator.	☐	☐	☐
We preserve forensic data for at least two years after an incident.	☐	☐	☐

A "yes" on the fifth row may qualify you for CIRCIA's substantially-similar-reporting exception — tell us which agency and we will check whether an information-sharing agreement covers it.

ANYTHING YOU WANT US TO KNOW — OPEN QUESTIONS, UPCOMING CONTRACTS, SYSTEMS YOU ARE UNSURE ABOUT

Send it back and we will confirm it

Email the completed worksheet to **compliance@kairosit.com**. You do not need to have every answer right — the "unsure" boxes are the useful ones. Here is what happens after we get it:

STEP 1 · THIS WEEK

We check your math

A 30-minute call to settle the size question and any box you marked unsure. No charge.

STEP 2 · WITHIN 10 DAYS

You get it in writing

A one-page determination you can hand to your board, your insurer, or your auditor.

STEP 3 · IF YOU ARE COVERED

We build the 72-hour plan

Who calls whom, what gets filed, and the monitoring that makes the deadline achievable.

SIGNATURE

PRINTED NAME AND TITLE

DATE

Prepared by KairosIT as a client screening aid. The criteria summarized here paraphrase CISA's CIRCIA notice of proposed rulemaking (89 FR 23644) in plain language and are abridged; the final rule may change thresholds, sectors, and exceptions. This worksheet is not legal advice and does not create an attorney–client or reporting relationship. Confirm your obligations with counsel and with the rule text at cisa.gov/circia.