CYBER INCIDENT REPORTING REQUIREMENTS SUMMARY

Last updated Aug. 8, 2022 - *This summary is for educational purposes only. Nothing in this summary constitutes legal advice.*

Regulation	In force?	Applicable organizations	Covered incidents	Reporting Requirements	Reporting deadline	Required Format	Publicly disclosed?	Penalty for noncompliance	Additional Notes	Official Text
Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)	Signed into law in March 2022. Not in force until CISA issues final rules, which must occur within 42 months of bill signing (up to October 2025). *6 USC 681b(b).*	Entities in a critical infastructure sector, as defined by PPD-21 and forthcoming CISA rulemaking. *6 USC 681(5).*	A "covered cyber incident" is an occurrence that substantially jeopardizes integrity, confidentiality, or availability of information or systems without lawful authority. *6 USC 681(4).* This includes incidents that lead to a serious impact on safety and resiliency of operational systems. A forthcoming CISA rule will provide additional details on what qualifies as a "covered cyber incident." *6 USC 681b(c)(2).* Any payment delivered as ransom in connection with a ransomware attack must also be reported. *6 USC 681(13).*	Report must include (1) identification of the covered entity, (2) description of affected systems; (3) description of the incident, including estimated date range and impact; (4) exploited vulnerabilities, security defenses in place, and tactics used in the attack; (5) information that may identify the attacker; (6) categories of compromised information; and (7) if applicable, full details of ransom payment. *6 USC 681b(c)(4)-(5).* A forthcoming CISA rule will provide comprehensive reporting requirements prior to law entering into force. *6 USC 681b(c)(4).*	Incident must be reported within 72 hours of determination of reportable event. *6 USC 681b(a)(1)(A)-(B).* Ransomware payments must be reported within 24 hours after payment. *6 USC 681b(a)(2)(A).*	Format requirements are not specified in the law and will be announced by CISA during their subsequent rulemaking process. *6 USC 681b(a)(6).* The procedure shall include a web-based form. *6 USC 681b(c)(8)(A).*	No, reports will remain confidential and is exempt from the Freedom of Information Act (FOIA). *6 USC 681e(b).*	CISA may issue a subpoena to compel information, and refer to Department of Justice (DOJ) to enforce subpoena. Court may enforce subsequent failure to comply with a subpoena as contempt of court. *6 USC 681d (c).*	Covered entities must preserve information related to their incident reports. *6 USC 681b(a)(4).* Reports cannot be used in regulatory action and are not admissible as evidence in a court of law. *6 USC 681e(c).*	https://rules.house.gov/sites/democrats.rules.house.gov/files/BILLS-117HR2471SA-RCP-117-35.pdf#page=2524
Proposed SEC Rule for public companies on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure	Not currently in force. Final rule expected Apr. 2023.	All companies that have stock traded on public US exchanges (i.e. any company that files a 10-K). *87 Fed. Reg. 16595.*	"Material cybersecurity incidents," i.e., any incident that a reasonable shareholder would consider important in making an investment decision. This includes accidents and deliberate attacks, such as but not limited to incidents that: (1) compromise data or networks; (2) degrade, interrupt, damage, or impact operations; (3) involve unauthorized access, alteration, or theft of sensitive information; or (4) extortion demands such as ransomware. *87 Fed. Reg. 16596.*	Report must include: (1) timing of incident discovery; (2) whether the incident is ongoing; (3) a description of the incident; (4) whether any data was stolen, altered, accessed, or used for an unauthorized purpose; (5) impact on company's operations; and (6) status of remediation efforts. *87 Fed. Reg. 16595.*	Initial report on Form 8-K must be filed with SEC within 4 days of determination of material event. *87 Fed. Reg. 16595.* Status updates are required in subsequent 10-Q and 10-K filings. *87 Fed. Reg. 16596.*	Disclosure will be via SEC Form 8-K for disclosure of material nonpublic events. Format: Inline eXtensible Business Reporting Language (Inline XBRL). *87 Fed. Reg. 16603.*	Yes, reports are made available to the public. Form 8-K is a publicly disclosed SEC filing. https://media2.mofo.com/documents/faq-form-8-k.pdf	The proposed Amendment does not detail specific penalties, but SEC Regulation S-K violations most often result in a modest fine for first offense. Multiple violations may be referred to the Department of Justice (DoJ) for criminal prosecution. https://www.sec.gov/about/offices/oia/oia_enforce/overviewenfor.pdf	Amends Form 10-K disclosure requirements to require reporting when a series of previously undisclosed individually immaterial cybersecurity incidents has become material in the aggregate. *87 Fed. Reg. 16595.* For Foreign Issuers: amends Form 6-K to include "cybersecurity incident" as optional disclosure, and amends Form 20-F to require annual cyber incident disclosures. *87 Fed. Reg. 16597, 16602.*	https://www.federalregister.gov/documents/2022/03/23/2022-05480/cybersecurity-risk-management-strategy-governance-and-incident-disclosure See also https://www.sec.gov/rules/proposed/2022/33-11038.pdf
Proposed Amendment to FTC's GLBA rule: Standards for Safeguarding Customer Information	Not currently in force. Effective date will be 6 months after final rule is released. As of July 2022, no final rule has been released. *86 Fed. Reg. 70067.*	Non-banking financial instutions under FTC jurisdiction. *16 CFR 314.2 (h).*	An incident where the "misuse of customer information has occurred or is reasonably likely, and where at least 1,000 consumers have been affected or reasonably may be affected." *86 Fed. Reg. 70067.*	Report must include: (1) Name and contact info of the reporting financial institution; (2) description of the types of information involved; (3) the date or date range of the security incident; and (4) a general description of the security event. *86 Fed. Reg. 70067.*	As soon as possible, no later than 30 days after discovery of the event. *86 Fed. Reg. 70067.*	Reporting will be via a standard form available on the FTC website. *86 Fed. Reg. 70067.*	Yes, reports are made available to the public. *86 Fed. Reg. 70064.*	Depending on the conduct, penalties can include cease and desist orders, injunctions and equitable relief, consent decrees, audits, civil penalties for violating orders, and criminal referral to the US Justice Dept. 15 USC 6805. https://www.ftc.gov/about-ftc/mission/enforcement-authority	This proposed rule is distinct from the 86 Fed. Reg. 70272 amendment to 16 CFR Part 314 (released concurrently), which provides security governance guidance but does not address incident reporting. 86 FR 70272 came into effect in January 2022. *16 CFR. 314.*	https://www.federalregister.gov/documents/2021/12/09/2021-25064/standards-for-safeguarding-customer-information
FDIC, Federal Reserve, and OCC - Computer Security Incident Notification Requirements	Rule effective date: Apr. 1 2022. Compliance date: May 1, 2022. *86 Fed. Reg. 66424.*	US "banking organizations," including national banks, federal savings associations, US branches of foreign banks, Savings and loan holding companies, state member banks, Edge and agreement corporations, FDIC-insured state nonmember banks, and FDIC-insured state savings associations. Note, Financial Market Utilities (FMUs) are excluded. *86 Fed. Reg. 66427.*	Any "notifcation incident," defined as an occurrence that causes actual compromise to information or systems and is reasonably likely to materially disrupt: (1) Banking operations or product/service delivery; (2) any business line that, upon failure, it would result in a material loss in profit or revenue; or (3) operations for which failure would pose a threat to the financial stability of the United States. *86 Fed. Reg. 66439.*	No specific information is required in the notification other than that a "notification incident" has occurred. This rule is designed to be an early alert system where banking organizations will general information known at the time of the incident. *86 Fed. Reg. 66433.*	Reporting required "as soon as possible" and no later than 36 hours after determination that a "notification incident" has occurred. *86 Fed. Reg. 66424.*	The rule does not prescribe any form or template. Applicable organizations are required to report only to their primary regulator, not all three. Notification may be provided to a designated point of contact via email, phone, or similar method that the agency may prescribe. *86 Fed. Reg. 66433.* FDIC: Contact case manager or email incident@fdic.gov Federal Reserve: Email incident@frb.gov or call (866) 364-0096 OCC: Call supervisory office, notify via BankNet, or call (800) 641-5925	No, reports are subject to agency confidentiality rules. However, agencies must respond to FOIA requests on a case-by-case basis. *86 Fed. Reg. 66437.*	Civil monetary penalties (CMPs) ranging from $5,000 per day to $1M per day, depending on severity of violation. CMPs are usually only applied after multiple violations that demonstrate "a pattern of misconduct." https://www.fdic.gov/regulations/safety/manual/section14-1.pdf https://www.federalreserve.gov/aboutthefed/section29.htm https://www.occ.treas.gov/news-issuances/federal-register/2022/87fr1657.pdf	Bank service providers subject to the Bank Service Company Act must also notify banking organizations when a computer security incident is reasonably likely to materially disrupt services to the banking organization for four or more hours. The banking organization is responsible for notifying its regulator if a notification incident has occurred. *86 Fed. Reg. 66439.*	https://www.federalregister.gov/documents/2021/11/23/2021-25510/computer-security-incident-notification-requirements-for-banking-organizations-and-their-bank See also https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20211118a1.pdf
Proposed NCUA rule for Cyber Incident Notification Requirements for Federally Insured Credit Unions	Not currently in force. The rule was proposed July, 27, 2022.	Federally insured credit unions (FICUs), federally chartered corporate credit unions and federally insured, state chartered corporate credit unions. *87 Fed. Reg. 45029.*	A "reportable cyber incident" is a substantial occurrence that actually or imminently jeopardizes the integrity, confidentiality, or availability of member information or systems, and that leads to any of the following: (1) A substantial compromise of a member system that results from unauthorized access to or exposure of sensitive data, disrupts vital member services, or has a serious impact on safety and resiliency of operational systems and processes; (2) a disruption of business operations, vital member services or systems resulting from a cyberattack; and/or (3) a disruption of business operations or unauthorized access to sensitive data caused by a compromise of a third party service provider or other supply chain source. *87 Fed. Reg. 45030.*	A basic description of the reportable incident, including what functions were affected; the estimated date range of the incident; a description of exploited vulnerabilities or techniques used to perpetrate the incident; any identifying information of the responsible actors; the impact to operations. Follow-up comunications will occur through supervisory processes. *87 Fed. Reg. 45032.*	Reporting required within 72 hours after forming a reasonable belief that a reportable cyber incident occurred. *87 Fed. Reg. 45032.*	The proposed rule does not include any prescribed reporting forms or templates. Notice may be provided to a designated point of contact at the agency via email, telephone, or similar method the agency may prescribe through guidance. *87 Fed. Reg. 45032.*	Reports are subject to NCUA's confidentiality rules. *87 Fed. Reg. 45032.* Depending on the information, not all records would be exempt from FOIA. *12 CFR 792.*	NCUA penalties may include consent orders, Administrative orders, and civil monetary penalties ranging from $320 to $2.2M, depending on the severity and conduct of the organization. *12 CFR 747.1001.* https://www.ncua.gov/regulation-supervision/enforcement-actions	As part of existing regulations requiring an incident response plan, FICUs must notify NCUA Regional Directors when they become aware of unauthorized access or use of sensitive member information. FICUs are also required to notify NCUA within five bsuiness days or any catastrophic act that occurs in their offices. *12 CFR. 748.*	https://www.federalregister.gov/documents/2022/07/27/2022-16013/cyber-incident-notification-requirements-for-federally-insured-credit-unions See also https://www.ncua.gov/files/agenda-items/cyber-incident-proposed-rule-20220721.pdf

RAPID7

CYBER INCIDENT REPORTING REQUIREMENTS SUMMARY

Last updated Aug. 8, 2022 - *This summary is for educational purposes only. Nothing in this summary constitutes legal advice.*

Regulation	In force?	Applicable organizations	Covered incidents	Reporting Requirements	Reporting deadline	Required Format	Publicly disclosed?	Penalty for noncompliance	Additional Notes	Official Text
New York Department of Financial Services, 23 NYCRR 500.17	Effective as of March 1, 2017. *23 NYCRR 500.21.*	Organizations regulated, chartered, or licensed by NYDFS. This includes financial institutions doing business in New York such as state-chartered banks, trust companies, private bankers, mortgage companies, insurance companies, licensed lenders, and non-US banks. *23 NYCRR 500.1(c).*	An incident must be reported if: (1) notice is required to be provided to any government body under existing law. For example, a cybersecurity incident involving PII must be reported to customers under existing state privacy law; or (2) the event is reasonably likely to materially harm operations. This includes third party incidents that impact first party operations. *23 NYCRR 500.17.* Note, attempted (i.e. thwarted) cyber intrusions may be reportable if, in the covered entity's reasoned judgement, the event is sufficiently serious to raise concern. https://www.dfs.ny.gov/industry_guidance/cybersecurity	The rule does not specifiy what information is required in the report beyond notification of an incident.	Reporting is required "as promptly as possible" but no later than 72 hours after determination that a reportable event occurred. *23 NYCRR 500.17(a).*	The rule does not specify formatting requirements. Reports should be submitted via New York State Department of Financial Services website. https://myportal.dfs.ny.gov/web/cybersecurity/	No, information is not publicly disclosed and will remain confidential. *23 NYCRR 500.18.*	The Cybersecurity Regulation does not specify a penalty, but may be enforced under NYDFS authorities. Depending on the conduct and institution, NYDFS may levy civil penalties ranging from $2,500 per day to $75,000 per day, consent orders, or revocation of licensure. https://www.rapid7.com/globalassets/_pdfs/whitepaperguide/whitepaper-simplifying-the-complex-120821.pdf	Annual follow up reports are required every year by April 15th. *23 NYCRR 500.17.(b).* Records retention is required for five years after the incident. Retained records must be able to demonstrate that the organization is in compliance with the cybersecurity event notice rule. *23 NYCRR 500.17.(b).*	https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=I5be30d2007f811e79d43a037eefd0011&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default)
NERC Critical Infrastructure Standard: CIP-008-6: - Cyber Security - Incident Reporting and Response Planning	Effective as of January 1, 2021. https://www.provencompliance.com/news/cip-008-6/#:~:text=NERC'S%20RESPONSE&text=Those%20efforts%20resulted%20in%20FERC's,date%20of%20January%201%2C%202021.	"Responsible entities" that operate bulk electric system (BES) systems of high or medium impact, as defined by CIP-002. This includes but is not limited to: Distribution providers, generator owners/operators, reliability coordinators, and transmission owners/operators. *CIP-008-6. R4.1-4.2.* https://www.nerc.com/pa/Stand/Project%202021081%20Phase%201%20of%20Glossary%20Updates%20Statut/2012-08.1_Implementation_Plan_Redline.pdf	A "reportable incident" includes malicious or suspicious events that disrupt, or attempts to disrupt, the operations of a high or medium impact BES Cyber System performing reliability tasks. A reportable incident also includes compromise, or attempts to compromise the electronic or physical security perimeter, access control, or monitoring system of a high or medium impact BES Cyber System. Incidents that are failed "attempts" to compromise a system must also be reported. *CIP-008-6 R4.*	Report must include, at minimum, (1) the functional impact; (2) the attack vector used; (3) and the level of intrustion that was achieved or attempted. *CIP-008-6 R4.1.*	A breach must be reported within one hour after determining that it is reportable. *CIP-008-6 R4.2.* An "attempted" breach must be reported within one day of determination. *CIP-008-6 R4.2.* Required report information must be provided in full within seven days of initial report. *CIP-008-6 R4. 3.*	Responsible entities may submit notification using any method or format that is supported by E-ISAC and NCCIC. https://www.nerc.com/pa/Stand/Project%20201802%20Modifications%20to%20CIP008%20Cyber%20Secur/CIP_Technical_Rationale_for_CIP-008_Final%20Ballot_Clean_01152019.pdf	No, reports will remain confidential. However, the rule does not contain an explicit FOIA exemption. https://www.nerc.com/pa/Stand/Project%20201802%20Modifications%20to%20CIP008%20Cyber%20Secur/CIP-008-6_Consideration_of_Comments_Draft_11152018.pdf	Failure to comply with CIP Standards can include orders to mitigate violations and track improvements, as well as civil fines ranging to more than a million dollars per violation, per day. Fines will escalate after multiple violations. https://www.nerc.com/AboutNERC/RulesOfProcedure/Appendix_4B_effective%2020210119.pdf	Evidence retention is required for three calendar years after incident report. *CIP-008-6.C.1.2.* CIP-008-6 also includes requirements for incident response and remediation planning, testing, and governance. *CIP-008-6 R1-4.*	https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-6.pdf
TSA Security Directive Pipeline - 2021-01B	Effective as of May 29, 2021. *SD-2021-01B.*	Owners and operators of a hazardous liquid and natural gas pipeline or a liquefied natural gas facility identified by TSA as critical. *SD-2021-01B Definitions F.*	Reporting is required for (1) Unauthorized access to, or discovery of malicious software on, information or operations systems; (2) Service interruption of information or operations systems; (3) Physical attack against network infrastructure; and (4) Any cybersecurity incident that results in, or may cause, operational disruptions that adversely effects safe and timely transfer of liquids and gases. *SD-2021-01B Actions B.1-5, Definitions A.*	Report must include: (1) Contact info of the reporter; (2) The affected pipelines or facilities; (3) Incident description, including mitigiation steps taken and relevant information regarding type of attack or the threat actor; (4) An assessment of the incident's impact on systems and operations; (5) description of all responses that are planned or under consideration; (6) any additional relevant information. *SD-2021-01B Actions D.1-6.*	Reporting is required no later than 24 hours after incident is identified as reportable. If the required information is not available within 24 hours, Owner/Operators must still submit an initial report and then supplement as additional information becomes available. *SD-2021-01B Actions C.*	Reports must be submitted via CISA's Reporting System form at https://us-cert.cisa.gov/forms/report or by calling (888) 282-0870. *SD-2021-01B Actions C.*	Reported information is sensitive security information, not publicly disclosed, and exempt from FOIA. Information will be shared internally within the Department of Homeland Security. *SD-2021-01B Purpose and General Information. 49 CFR 1520.*	The Directive does not detail penalties specific to this regulation. Violations of non-aviation TSA regulations incur civil monetary penalties of up to a maximum of $13,900 per violation. Penalties increase in severity with multiple violations. https://www.tsa.gov/sites/default/files/enforcement_sanction_guidance_policy.pdf	Rule expires May 29, 2023. The previous version of this rule expired, then was subsequently updated and renewed. *SD-2021-01B Expiration Date.*	https://www.tsa.gov/sites/default/files/sd_pipeline_2021-01b_05-29-2022.pdf
Proposed EU NIS-2 Directive - Document 52020PC0823	Not currently in force. European Parliament expected to vote on final Directive in plenary in mid to late 2022. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333	The Directive applies to "essential and important entities." EU Member States are required to compile a list of such entities. *Art. 2.1-2.* Annex I of the Directive defines "essential" sectors to include healthcare, financial services, transport, public utilities, and digital infrastructure. Annex II defines "important" sectors to include manufacturing, food production, waste management, and postal services. *Annex I-II.*	Any "significant" cyber incident, which is defined as an event that either: (1) has caused or has the potential to cause substantial operational disruption or financial losses for the entity; and/or (2) has affected or has the potential to affect other natural or legal persons by causing considerable material or non-material losses. *Art. 20.3.*	Initial report (24 hours) need only include notification that an incident occurred and whether it was likely caused by an unlawful actor. Regulatory authorities may request intermediate status reports. The comprehensive follow-up report (1 month) must include: (1) A detailed description of the incident and its impact; (2) the type of threat or cause of the incident; and (3) applied and ongoing mitigation measures. *Art. 20.4.*	Initial notification must be filed within 24 hours of organization "becoming aware" of the incident. *Art. 20.(4).(a).* A final report that meets all requirements is required within one month of initial report. *Art. 20.(4).(c).*	No specific format requirements are included, but the proposed Directive would empower the European Union Agency for Cybersecurity (ENISA), after final passage of the directive, to develop a common reporting template in order to streamline the process. *Recital 56.*	No, information is kept confidential by default. But reports may be released if doing so is deemed to be in the public interest. *Art. 20.6-7.*	The Directive requires EU Members States to impose administrative fines to entities for noncompliance. The size of the fine is not specified and is at the discretion of the member state. *Art. 31.1-5.*	In addition to regulatory notification, organizations must notify customers if the incident is likely to adversely affect the service. *Art. 20.1.*	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0823
CERT-IN's Direction - No. 20(3)/2022	Effective as of June 28th, 2022. https://www.natlawreview.com/article/cyber-security-india-revamps-rules-mandatory-incident-reporting-and-allied#:~:text=The%20CERT%2DIn%20Rules%20do,maximum%20penalty%20of%20INR%2025%2C000.	All organizations that come under the purview of the Information Technology Act, 2000. Including, but not limited to, all service providers, intermediaries, data center, body corporate and government organizations, VPS providers, cloud service providers, and VPN providers. *No. 20(3) Whereas, pg. 2 (ii).*	The law provides an extensive list of covered incidents, including any event that involves: (1) Targeted scanning or probing of a critical network, (2) unauthorized access to a system, network, or information, (3) disruption of systems, operations, or customer service, (4) attacks on critical infrastructure, and (5) data leaks or breaches. The list also calls out risks to IoT, AI/ML, SCADA, digital assets, and manufacturing. *No. 20(3) Annexure I.*	The reporting form includes the following (1) Contact info of the reporter; (2) identification of the affected entity; (3) the type of cyber incident; (4) whether the affected system is critical to operations; (5) information on the affected system, such as Domain/URL, IP address, affected application, physical location, etc.; (6) A written description of the incident'; (7) any other relevant info. https://www.cert-in.org.in/PDF/certinirform.pdf	Reporting is required six hours after noticing the incident. *No. 20 (3) Whereas, pg. 2 (ii).* Additional information may be reported later within a "reasonable time" to CERT-In. https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf#page=15	Incidents can be reported to CERT-IN via email (incident@cert-in.org.in), Phone (1800-11-4949) and Fax (1800-11-6969). *No. 20(3) Whereas, pg. 2 (ii).* See aso the reporting template. http://cert-in.org.in/PDF/certinirform.pdf The point of contact information must be formatted as follows: (1) name, (2) designation, (3) organization name, (4) office address, (5) email ID, (6) mobile number, (7) office phone, (8) office fax. *No. 20(3) Annexure II.*	Not specified in the rule.	Non-compliance with the CERT-In Rules may be penalized under subsection 70B(7) of the IT Act, 2000 which provides for penalties that include up to a year of imprisonment and/or one lakh rupees. https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf#page=28	Logs of information technology and computer (ITC) systems must be maintained securely for 180 days. CERT-IN may order reporting of the logs. *No. 20(3) Whereas, pg. 3 (iv).*	https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf See also https://www.cert-in.org.in/Directions70B.jsp
Australia Security of Critical Infrastructure Act of 2018 - Amended in April 2022	Effective as of July 8, 2022. https://www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/cyber-security-incident-reporting.pdf	All critical assets within a critical infrastructure sector, including (a) communications; (b) data storage or processing; (c) financial services and markets; (d) water and sewerage; (e) energy; (f) healthcare and medicine; (g) higher education and research; (h) food and grocery; (i) transport; (j) space technology; and (k) defence industry. *Part 1 Division 2.8D-8E.*	The law defines a cybersecurity incident as unauthorized access to, modification, or impairment of a computer, data, or program. Both critical and non-critical cybersecurity incidents require reporting, but with different deadlines. An incident is critical if it has significantly impacted the availabilty of a critical infrastructure asset. An incident is non-critical if it is likely to have a relevant impact on the asset. *Part 1 Division 2.12M; Part 2B.30BC-30BD*	The report must include (1) Point of contact info; (2) organization ID number; (3) critical infrastructure sector; (4) date of incident discovery; (5) whether the incident is ongoing; (6) whether the incident is having a significant impact on the asset; (7) how the incident was discovered; (8) the type of attack; (9), what systems or data have been impacted; (10) whether the incident has been reported elsewhere; and (11) other relevant info.	If an incident is critical, reporting is required within 12 hours of the entity becoming aware of the incident. (If the report is given orally, a written report is due 84 hours later.) If non-critical, the initial report is required within 72 hours after the entity becomes aware. (If the report is given orally, a written report is due 48 hours later.) *Part 2B.30BC-30BD.*	Reports may be submitted over the phone or in writing. If reported over the phone, a subsequent written report is required. Forms may be submitted online via a tailored webform on the ACSC website. *Part 2B.30BC-30BD.*	The report will not be released publicly but will be shared with the Department of Home Affairs, with the reporting organization's consent.	Civil penalties pursuant to Part 4 of the Regulatory Powers Act. *Part 5 Division 2.49*	Critical infrastructure operators are required to register with ACSC. *Part 2.*	https://www.legislation.gov.au/Details/C2022C00160 See aso https://www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/cyber-security-incident-reporting.pdf