

Government Reporting

ICS4ICS Procedure Template

|  |
| --- |
| InstructionsThe following are suggestions about how you can update this template to create a procedure for your company:* Identify the roles required on the Decision Team that will manage Government Reporting decisions
* Review and update the Decision Considerations based on your company requirements
* Update the section of this procedure describing how to perform Government Reporting
* Review each law or regulation that impacts your country and industry to understand the actual trigger for when reporting is required
* Test this Procedure annually at minimum and update the procedures as needed
 |
| DisclaimerThe template was developed by ICS4ICS volunteers. The ICS4ICS Program provides this template to help asset owners create procedures to perform ICS4ICS and/or Cyber Incident Response and/or other related tasks. Each Asset Owners must update this template based on the needs of their company and ensure the procedure is review and approved by the appropriate parties (e.g., legal, senior management, corporate governance, government relations, etc.) from within their company. ISA, ISAGACA, and ICS4ICS cannot attest to the accuracy of this document.  |

# Purpose

This document is intended to provide information to describe Government Reporting requirements that can be used by the ICS4ICS Team to prepare for government reporting during an incident.

# Situation Trigger

Most laws and regulations that require Government Reporting typically begin the clock for when reporting must occur based on when the Incident Commander declares an incident. Depending on each law or regulation the timing that triggers reporting may start earlier.

# Decision Team

The following parties will be engaged to assess the situation, make decisions, and determine next steps:

* Corporate Government Relations (ICS4ICS Government Liaison Officer) - Leader
* Incident Commander
* Operations Section Chief
* Intelligence Officer (in Operations Section)
* Corporate Legal and outside council
* Privacy expert if there is any potential impact on the release or compromise of personal data

# Decision Process

The Decision Team will consider the following factors to make decisions about government reporting:

* Understand Government Reporting Requirement (e.g., an assessment must be completed prior to an incident, and a table created describing government reporting requirements that impact your operations based on countries and industries); understand the legal reporting timing based on laws and regulations
* Review Corporate Policies (e.g., an assessment must be completed prior to an incident, and a table created summarizing any Corporate Policies that may impact how the company will voluntarily report incidents to the government when not legally required)
* Ensure that all government reporting efforts are performed collectively even if there are different agencies that must receiving reporting AND that the reporting messages are consistent
* Identify reporting approval processes (e.g., identify who must approve government reports and ensure they have sufficient Delegation of Authority)

# Decision Factors (Table)

The Decision Team will consider the following factors to make decisions about the ransomware:

|  |  |  |  |
| --- | --- | --- | --- |
| Type | Enforcement | Timing | Description |
| Law and Regulations | Required | <when> | See the table below**NOTE: Ensure local laws, regulations, and reporting expectations are included** |
| Law and Regulations | Recommended |  | See the table below |
| Corp Policy | Required or recommended |  | <describe each Corp Policy requirement that impacts reporting decisions> |
| Decision Approval | Required |  | <describe company decision processes required to finalize decisions> |

# Reporting Requirements and Recommendations

## Cybersecurity Laws and Regulations

Instructions: Review this table to identify laws and regulations that are applicable to the countries and industries for your company. Include those that apply in the “Decision Factors (Table)”

| Country | Type | Enforcement | Description |
| --- | --- | --- | --- |
| Australia | Law | Required | All critical assets within a critical infrastructure sector[CISC Factsheet - Cyber Security Incident Reporting](https://www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/cyber-security-incident-reporting.pdf)[Regulatory obligations (cisc.gov.au)](https://www.cisc.gov.au/legislative-information-and-reforms/critical-infrastructure/regulatory-obligations)<https://www.pwc.com.au/cyber-security-digital-trust/critical-infrastructure/learnings-from-applying-the-soci-regime.html>`<https://www.rapid7.com/globalassets/_pdfs/Rapid7-Incident-Reporting-Regulation-Summary-Chart-080822.pdf> |
| Brazil | President Directive | Information | Critical InfrastructureNATIONAL SECURITY STRATEGY FOR CRITICAL INFRASTRUCTURES[D10566 (planalto.gov.br)](https://www.planalto.gov.br/cCivil_03/_Ato2019-2022/2020/Decreto/D10569.htm) |
| China | Regulation | Required | “Network security incidents” that are notifiable are defined by reference to seven categories of different incident types.[Breach Notification in China - DLA Piper Global Data Protection Laws of the World (dlapiperdataprotection.com)](https://www.dlapiperdataprotection.com/index.html?t=breach-notification&c=CN) |
| EU | Law | Required | European regulation relating to cyber security incident reporting in the industrial area is the NIS2 Directive. It applies to entities recognized as "Essential Services Operators" - generally all energy, water and wastewater, heat, transportation. The requirement is found in Article 23. In addition, we must remember that the Directive is a provision that must be implemented into the law of each EU member state. And each of these countries sets more specific rules for reporting incidents.Link to NIS2 Directive: [Publications Office (europa.eu)](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&from=EN). |
| India | Law | Required | India's computer and emergency response team, CERT-In, published new guidelines that require service providers, intermediaries, data centers, and government entities to compulsorily report cybersecurity incidents, including data breaches, within six hours.[Indian Govt Orders Organizations to Report Security Breaches Within 6 Hours to CERT-In (thehackernews.com)](https://thehackernews.com/2022/04/indian-govt-orders-organisations-to.html) |
| North America | Regulation | Required | Electrical: bulk electric system (BES) from NERC <https://www.rapid7.com/globalassets/_pdfs/Rapid7-Incident-Reporting-Regulation-Summary-Chart-080822.pdf>  |
| NZ | Information | Voluntary | Cyber SecurityReport an incident and if needed request help[Report an incident and request support | National Cyber Security Centre (ncsc.govt.nz)](https://www.ncsc.govt.nz/incidents/report-an-incident-and-request-support/)Phone (04) 498 7654 for immediate support, or if the incident occurs outside business hours.Email incidents@ncsc.govt.nz for non-urgent incidents |
| Singapore | Law | Required | Singapore Cybersecurity Bill 2018 (<https://sso.agc.gov.sg/Acts-Supp/9-2018/>)Cybersecurity Code of Practice (<https://www.csa.gov.sg/legislation/Codes-of-Practice>) |
| USA | Rule | Required | New rule requires publicly traded companies to publicize details of a cyber attack within four days of identifying that it has a "material" impact on their finances, marking a major shift in how computer breaches are disclosed. This mandates that companies reveal the incident's nature, scope, and timing, as well as its impact.[New SEC Rules Require U.S. Companies to Reveal Cyber Attacks Within 4 Days (thehackernews.com)](https://thehackernews.com/2023/07/new-sec-rules-require-us-companies-to.html) |
| USA | Regulation | To-be-determined | Covered entities” is still being defined by CISA.  Generally, this includes those within a critical infrastructure sector, as defined in Presidential Policy Directive 21 (“PPD-21”).[Congress Imposes New 72-Hour Reporting Requirement for Cyber Security Incidents – Freeman Mathis & Gary (fmglaw.com)](https://www.fmglaw.com/cyber-privacy-security/congress-imposes-new-72-hour-reporting-requirement-for-cyber-security-incidents/#:~:text=First%2C%20a%20covered%20entity%20experiencing%20a%20covered%20cyber,report%20the%20payment%20to%20CISA%20within%2024%20hours.)[Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) | CISA](https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia)(items 1) [Cyber Incident Reporting Requirements & Notification Timelines for Financial Institutions - Bank Policy Institute (bpi.com)](https://bpi.com/cyber-incident-reporting-requirements-notification-timelines-for-financial-institutions/#:~:text=Gramm%2DLeach%2DBliley%20Act%20(,misuse%20of%20the%20customer's%20information.) |
| USA | Guidance | Information | Cyber Security[US-CERT Federal Incident Notification Guidelines (cisa.gov)](https://www.cisa.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines.pdf)[Report to CISA | CISA](https://www.cisa.gov/report) |
| USA | Executive Order | Information | Cyber Security[Executive Order on Improving the Nation's Cybersecurity | The White House](https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/) |
| USA | Law | Definitions | Cyber SecurityHOMELAND SECURITY ACT OF 2002 with amendment in 2022[COMPS-1143.pdf (govinfo.gov)](https://www.govinfo.gov/content/pkg/COMPS-1143/pdf/COMPS-1143.pdf) |
| USA | Guidance | Information | Cyber SecurityIncident reporting and obtaining assistance from the USA government[Cyber Incident Reporting United Message.pdf (dhs.gov)](https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf) |
| USA | Advocacy | Information | Cyber Security[ITI Issues First-of-their-Kind Principles for Cyber Incident Reporting - Information Technology Industry Council (itic.org)](https://itic.org/news-events/news-releases/iti-issues-first-of-their-kind-principles-for-cyber-incident-reporting#:~:text=Among%20its%20recommendations%2C%20ITI%20suggests%20policymakers%3A%20Develop%20and,responsibility%20for%20reporting%20only%20to%20the%20compromised%20entity%3B) |
| USA | Executive Directive | Information | Cyber Security[Presidential Policy Directive -- United States Cyber Incident Coordination | whitehouse.gov (archives.gov)](https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident) |
| USA | Reporting | Required | Electric utilities that operate as Control Area Operators and/or Reliability Authorities as well as other electric utilities, as appropriate, are required to file the form[ISER - Electric Disturbance Events (DOE-417)](https://www.oe.netl.doe.gov/oe417.aspx) |
| USA | Regulation | Required | Pipeline<https://www.rapid7.com/globalassets/_pdfs/Rapid7-Incident-Reporting-Regulation-Summary-Chart-080822.pdf>  |
| USA | Regulation | Proposed | Pipeline[sd\_pipeline-2021-01b\_05-29-2022.pdf (tsa.gov)](https://www.tsa.gov/sites/default/files/sd_pipeline-2021-01b_05-29-2022.pdf) |
| USA | Law | Recommended | Ransomware reporting including observed activities:[Getting Ahead of the Ransomware Epidemic: CISA’s Pre-Ransomware Notifications Help Organizations Stop Attacks Before Damage Occurs | CISA](https://www.cisa.gov/news-events/news/getting-ahead-ransomware-epidemic-cisas-pre-ransomware-notifications-help-organizations-stop-attacks) |
| USA | Search Tool | Information | Various regulationsSearch for proposed and new regulations:[Regulations.gov](https://www.regulations.gov/) |
| USA/Canada | Regulations | Required | NERC requirements for reporting to E-ISAC |

## Privacy

Instructions: Review this table to identify privacy laws and regulations that are applicable to the countries and industries for your company. Include those that apply in the “Decision Factors (Table)”

NOTE: Typically, privacy reporting requirements are not applicable to ICS/OT.

| Country | Type | Enforcement | Description |
| --- | --- | --- | --- |
| Brazil | Law | Required | PrivacyData Breach Reporting Requirements explained [2022] | LGPD (Lei Geral de Proteção dos Dados) Security incident reporting — National Data Protection Authority (www.gov.br) |
| Canada | Law | Required | Privacy[British Columbia's privacy management, breach reporting requirements take effect (iapp.org)](https://iapp.org/news/a/british-columbias-privacy-management-breach-reporting-requirements-take-effect/) |
| EU | Law | Required | PrivacyEuropean Union General Data Protection Regulation (GDPR) (items 7)[Art. 33 GDPR – Notification of a personal data breach to the supervisory authority - General Data Protection Regulation (GDPR) (gdpr-info.eu)](https://gdpr-info.eu/art-33-gdpr/)[Cyber Incident Reporting Requirements & Notification Timelines for Financial Institutions - Bank Policy Institute (bpi.com)](https://bpi.com/cyber-incident-reporting-requirements-notification-timelines-for-financial-institutions/#:~:text=Gramm%2DLeach%2DBliley%20Act%20(,misuse%20of%20the%20customer's%20information.)[Data Breach Reporting Requirements explained [2022] | GDPR Register](https://www.gdprregister.eu/gdpr/data-breach-notification-requirements/#:~:text=When%20reporting%20a%20personal%20data%20breach%2C%20you%20will,likely%20consequences%20of%20the%20incident%3B%20and%20More%20items) |
| Global | Info | Info | PrivacyVarious Data Privacy / Health laws around the world require reporting.  Generally, this will not impact ICS/OT cybersecurity incidents.  These requirements have encouraged companies to establish “incident declaration” procedures and authorities to prevent incidents from being declared prematurely.  A company commits significant resources and possibly large funds once an incident is declared. |
| USA | Regulation | Required | Privacy (health)U.S. Department of Health and Human Services Office for Civil RightsBreach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information[Breaches Affecting 500 or More Individuals](https://ocrportal.hhs.gov/ocr/breach/breach_form.jsf)[Breaches Affecting Fewer than 500 Individuals](https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true) |
| USA | Law | Required | Privacy (health)[Reporting HIPAA Breaches: Deadline March 1, 2021 (totalhipaa.com)](https://www.totalhipaa.com/deadline-reporting-hipaa-breaches/) |
| USA | Regulation | Various | Privacy (state)[State Data Breach Notification Chart (iapp.org)](https://iapp.org/resources/article/state-data-breach-notification-chart/) |

## Finance

Instructions: Review this table to identify finance laws and regulations that are applicable to the countries and industries for your company. Include those that apply in the “Decision Factors (Table)”

NOTE: Typically, finance reporting requirements are not applicable to ICS/OT.

| Country | Type | Enforcement | Description |
| --- | --- | --- | --- |
| USA | Law | Required | Finance (banking)Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers (2022) (items 2)[Cyber Incident Reporting Requirements & Notification Timelines for Financial Institutions - Bank Policy Institute (bpi.com)](https://bpi.com/cyber-incident-reporting-requirements-notification-timelines-for-financial-institutions/#:~:text=Gramm%2DLeach%2DBliley%20Act%20(,misuse%20of%20the%20customer's%20information.) |
| USA | Law | Required | Finance (banking)Gramm-Leach-Bliley Act (1999) (items 6)[Cyber Incident Reporting Requirements & Notification Timelines for Financial Institutions - Bank Policy Institute (bpi.com)](https://bpi.com/cyber-incident-reporting-requirements-notification-timelines-for-financial-institutions/#:~:text=Gramm%2DLeach%2DBliley%20Act%20(,misuse%20of%20the%20customer's%20information.) |
| USA | Law | Required | Finance (insurance)National Association of Insurance Commissioners (NAIC) Model Law (items 9)[Cyber Incident Reporting Requirements & Notification Timelines for Financial Institutions - Bank Policy Institute (bpi.com)](https://bpi.com/cyber-incident-reporting-requirements-notification-timelines-for-financial-institutions/#:~:text=Gramm%2DLeach%2DBliley%20Act%20(,misuse%20of%20the%20customer's%20information.) |
| USA | Law | Required | Finance (New York)New York Department of Financial Services (NYDFS) Cybersecurity Regulation (items 10)[Cyber Incident Reporting Requirements & Notification Timelines for Financial Institutions - Bank Policy Institute (bpi.com)](https://bpi.com/cyber-incident-reporting-requirements-notification-timelines-for-financial-institutions/#:~:text=Gramm%2DLeach%2DBliley%20Act%20(,misuse%20of%20the%20customer's%20information.) |
| USA | Regulation | Required | Finance (SEC)[SEC.gov | SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies](https://www.sec.gov/news/press-release/2023-139) |
| USA | Law | Required | Finance (State)State Data Breach Notification Requirements (items 11)[Cyber Incident Reporting Requirements & Notification Timelines for Financial Institutions - Bank Policy Institute (bpi.com)](https://bpi.com/cyber-incident-reporting-requirements-notification-timelines-for-financial-institutions/#:~:text=Gramm%2DLeach%2DBliley%20Act%20(,misuse%20of%20the%20customer's%20information.) |