This chart endeavors to track all existing and proposed cyber incident and data breach reporting requirements issued by the U.S. federal government. It was last updated as of July 26, 2022.

Please note: this chart is for research purposes only and should not be interpreted as legal advice.

For questions, please contact Ayan Islam (aislam@rstreet.org).

Name of Regulation or Other Implementing Framework	Sector	Lead Implementing Entity	Key Authorizing Mechanism or Authority; Supplementary Authorities as Applicable	Authority Type	Year Regulation Issued or Effective; Others as Applicable	Scope or Intent of Rule	Cyber Incidents: Disclosure Deadlines to External Entities	Data Breaches: Disclosure Deadlines to External Entities	Cyber Incidents: Public or Private Disclosure?	Data Breaches: Public or Private Disclosure?
Title Pending—Rulemaking pursuant to the **Cyber Incident Reporting for Critical Infrastructure Act of 2022**	**Multisectoral**	Cybersecurity and Infrastructure Security Agency **(CISA)**	**Cyber Incident Reporting for Critical Infrastructure Act of 2022** (Public Law No: 117-103 (Division Y))	Hybrid	Proposed rulemaking required: **2024**	**Cyber incident reporting**	72 hours		To government	
CISA Federal Incident Notification Requirements (US-CERT Federal Incident Notification Guidelines)	**Intra-governmental Agencies**	Cybersecurity and Infrastructure Security Agency **(CISA)**	**Federal Information Security Modernization Act of 2014** (44 U.S.C. 3553-54) Also routinely updated by White House memoranda, the most recent of which is available here.	Law	Law passed: **2014** Effective: **2017**	**Cyber incident reporting**	Varies by severity		To government; to Congress depending on severity	
Risk-Based Performance Standards (RBPS) 15—Reporting of Significant Security Incidents	**Chemical Sector**	Cybersecurity and Infrastructure Security Agency **(CISA)**	**Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014** (6 U.S.C. § 621, et seq.)	Hybrid	Updated: **2009** (Cyber incident reporting guidance under CFATS RBPS 8)	**Cyber incident reporting**	Unclear from text		To government	
CG-5P Policy Letter 08-16, Reporting Suspicious Activity and Breaches of Security	**Defense Sector**	**Coast Guard**	Issued within agency rulemaking authority under the **Maritime Transportation Security Act** (46 U.S.C. 701)	Hybrid	Issued: **2016** Additional Guidance: **2020** (NVIC 01-20)	**Cyber incident reporting**	"Without delay"		To government	

Name of Regulation or Other Implementing Framework	Sector	Lead Implementing Entity	Key Authorizing Mechanism or Authority; Supplementary Authorities as Applicable	Authority Type	Year Regulation Issued or Effective; Others as Applicable	Scope or Intent of Rule	Cyber Incidents: Disclosure Deadlines to External Entities	Data Breaches: Disclosure Deadlines to External Entities	Cyber Incidents: Public or Private Disclosure?	Data Breaches: Public or Private Disclosure?
Defense Federal Acquisition Regulation Supplement **(DFARS) Clause 252.204-7012:** Safeguarding Covered Defense Information and Cyber Incident Reporting	**Defense Sector**	Department of Defense **(DoD)**	In part, 10 U.S.C. 2545 and 50 U.S.C. 3043 and in accordance with 41 U.S.C. 1304 *Note, DFARS is a mix of law, DoD policies, delegations of FAR authorities and more. For more, see link.	Hybrid	Effective: **2017** CMMC Proposed: **2020** CMMC 2.0 Proposed: **2021**	**Cyber incident reporting**	72 hours		To government	
Defense Federal Acquisition Regulation Supplement **(DFARS) Clause 252.239-7010:** Cloud Computing Services	**Defense Sector**	Department of Defense **(DoD)**	In part, 10 U.S.C 2545 and 50 U.S.C. 3043, and in accordance with 41 U.S.C. 1304. *Note, DFARS is a mix of law, DoD policies, delegations of FAR authorities and more. For more, see link.	Hybrid	Issued: **2016**	**Cyber incident reporting**	Unclear from text		To government	
Cyber Incident Handling Program (DoD 8530.01)	**Defense Sector**	Department of Defense **(DoD)**	**DoD Directive 5144.02** (in turn, issued under the authority given to the Secretary of Defense under 10 U.S.C. 113)	Hybrid	Original: **2012** Update: **2017**	**Cyber incident reporting**	Varies by severity		To government	
Form OE-417: Department of Energy Electric Emergency Incident and Disturbance Report	**Energy Sector**	Department of Energy **(DoE)**	**Federal Energy Administration - Administrator's Information - Gathering Power** (15 U.S.C. 772(b)) *Note that entities reporting to NERC can substitute Form OE-417 for CIP-008-6.	Law	Cyber-specific reporting as of: **2012** Update: **2018** Revisions proposed: **2020**	**Cyber incident reporting**	Varies by severity		To government	

Name of Regulation or Other Implementing Framework	Sector	Lead Implementing Entity	Key Authorizing Mechanism or Authority; Supplementary Authorities as Applicable	Authority Type	Year Regulation Issued or Effective; Others as Applicable	Scope or Intent of Rule	Cyber Incidents: Disclosure Deadlines to External Entities	Data Breaches: Disclosure Deadlines to External Entities	Cyber Incidents: Public or Private Disclosure?	Data Breaches: Public or Private Disclosure?
Title Pending—Currently listed as **FAR 2021-017 - Cyber Threat and Incident Reporting and Information Sharing** (text not yet public; see reference here)	**Intra-governmental Agencies**	Federal Acquisition Regulation **(FAR) Council**	FAR was established in part by a 1979 statute. For more, see here. More recently, the Biden-era **Executive Order on Improving the Nation's Cybersecurity (EO 14028)** ordered the FAR council to update its cybersecurity incident reporting rules.	Hybrid	Update expected: **2022**	**Cyber incident reporting**	3 days (presumed)		To government	
Notification of customer proprietary network information security breaches	**Communications Sector**	Federal Communications Commission **(FCC)**	**The Communications Act of 1934** (47 U.S.C. 154, 254(k), 403(b)(2)(B), (c))	Law	Original: **2013** Proposed update: **2022**	**Data breach reporting**		7 days		To government; later to affected individuals
Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice	**Financial Services Sector**	Office of the Comptroller of the Currency **(OCC), Federal Reserve Board,** the Federal Deposit Insurance Corporation **(FDIC)**, and the Office of Thrift Supervision **(OTS)**	**Gramm-Leach-Bliley Act** (15 U.S.C. 6801) and the **Standards for Safeguarding Customer Information** (15 U.S.C. 6801(b), 6805(b)(2))	Law	Effective: **2005**	**Data breach reporting**		After internal investigation		To affected individuals
Health Breach Notification Rule	**Healthcare and Public Health Sector**	Federal Trade Commission **(FTC)**	**American Recovery and Reinvestment Act of 2009** (U.S.C. 26 Code note 1) Clarified by: **Statement of the Commission On Breaches by Health Apps and Other Connected Devices**	Law	Effective: **2009** Enforced: **2010**	**Data breach reporting**		Varies by severity		To government and affected individuals; depending on severity, to media

Name of Regulation or Other Implementing Framework	Sector	Lead Implementing Entity	Key Authorizing Mechanism or Authority; Supplementary Authorities as Applicable	Authority Type	Year Regulation Issued or Effective; Others as Applicable	Scope or Intent of Rule	Cyber Incidents: Disclosure Deadlines to External Entities	Data Breaches: Disclosure Deadlines to External Entities	Cyber Incidents: Public or Private Disclosure?	Data Breaches: Public or Private Disclosure?
Security Beyond Prevention: The Importance of Effective Breach Disclosures * and Data Breach Response: A Guide for Business (guidance)	**Multisectoral**	Federal Trade Commission **(FTC)**	**Federal Trade Commission Act** (15 U.S.C. 45) *Note: Guidance based off the rulings of two FTC actions against CafePress and Uber among others, concluding that their failure to notify customers of breach violated Sec. 5 of the FTC Act.	Hybrid	Published: **2022**	**Data breach reporting**		Unclear from text		Varies
Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime	**Financial Services Sector**	Financial Crimes Enforcement Network **(FinCEN)**	**Bank Secrecy Act** (12 U.S.C. 1813 and 1818; 31 U.S.C. 5318 and 5318)	Law	Published: **2016**	**Cyber incident reporting**	60 calendar days		To government	
Breach Notification Rule, Health Insurance Portability and Accountability Act (HIPAA)	**Healthcare and Public Health Sector**	Department of Health and Human Services **(HHS)**	**HIPAA** as updated by the **Health Information Technology for Economic and Clinical Health Act** (42 U.S.C. 17931-34)	Regulation	Original: **2009** Updated: **2013**	**Data breach reporting**		60 calendar days		To government and affected individuals; depending on severity, to media
CIP-008-6 - Cyber Security Incident Reporting and Response Planning	**Energy Sector**	North American Electric Reliability Corporation **(NERC)**	Ordered updated by FERC via **Order No. 848** (under its authority pursuant to 16 U.S.C. 824o)	Hybrid	Updated: **2019**	**Cyber incident reporting**	Varies by severity		To government	

Name of Regulation or Other Implementing Framework	Sector	Lead Implementing Entity	Key Authorizing Mechanism or Authority; Supplementary Authorities as Applicable	Authority Type	Year Regulation Issued or Effective; Others as Applicable	Scope or Intent of Rule	Cyber Incidents: Disclosure Deadlines to External Entities	Data Breaches: Disclosure Deadlines to External Entities	Cyber Incidents: Public or Private Disclosure?	Data Breaches: Public or Private Disclosure?
Cyber Security Event Notifications	**Energy Sector**	Nuclear Regulatory Commission **(NRC)**	**Atomic Energy Act of 1954** (42 U.S.C. 2073, 2167, 2169, 2201, 2210d, 2210e, 2210h, 2210i, 2273, 2278a, 2282, 2297f); **Energy Reorganization Act of 1974** (42 U.S.C. 5841, 5842); **Nuclear Waste Policy Act of 1982** (42 U.S.C. 10155, 10161; 44 U.S.C. 3504 note)	Regulation	Effective: **2015** Enforced: **2016**	**Cyber incident reporting**	Varies by severity		To government	
Title Not Public—"Procedures for reporting known or suspected compromises of [National Security Systems] NSS or otherwise unauthorized access of NSS" (National Security Memorandum 8)	**Defense Sector**	National Security Agency **(NSA)**, with the Office of the Director of National Intelligence **(ODNI)** and Central Intelligence Agency **(CIA)**	**Memorandum on improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems** (NSM 8)	Regulation	Presumed issued: **2022** *Text not public	Cyber incident reporting	Upon detection or notification (from contractors)		To government	
Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers	**Financial Services Sector**	Office of the Comptroller of the Currency **(OCC)**, **Federal Reserve Board**, and the Federal Deposit Insurance Corporation **(FDIC)**	Issued within rulemaking authorities under 12 U.S.C. 1, 93a, 161, 481, 1463, 1464, 1861-1867 and 3102 (OCC); 12 U.S.C. 321-338a, 1467a(g), 1818(b), 1844(b), 1861-1867 and 3101 et seq. (Board); 12 U.S.C. 1463, 1811, 1813, 1817, 1819 and 1861-1867 (FDIC)	Regulation	Issued: **2021** Effective: **2022**	Cyber incident reporting	36 hours		To government; to affected customers depending on severity	

Name of Regulation or Other Implementing Framework	Sector	Lead Implementing Entity	Key Authorizing Mechanism or Authority; Supplementary Authorities as Applicable	Authority Type	Year Regulation Issued or Effective; Others as Applicable	Scope or Intent of Rule	Cyber Incidents: Disclosure Deadlines to External Entities	Data Breaches: Disclosure Deadlines to External Entities	Cyber Incidents: Public or Private Disclosure?	Data Breaches: Public or Private Disclosure?
Division of Corporation Finance's Disclosure Guidance: Topic No. 2 -- Cybersecurity ("**2011 Guidance**") expanded by the Commission Statement and Guidance on Public Company Cybersecurity Disclosures ("**2018 Guidance**")	**Financial Services Sector**	Securities and Exchange Commission **(SEC)**	Issued within agency rulemaking authority under 15 U.S.C. 77-78	Regulation	Original: **2011** Update: **2018**	Cyber incident reporting	Unclear from text		Public disclosure	
Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure	**Financial Services Sector**	Securities and Exchange Commission **(SEC)**	Issued within agency rulemaking authority under 15 U.S.C. 77-78	Regulation/ Rule-Making	Draft: **2022**	Cyber incident reporting	4 business days		Public disclosure	
Security Directive 1580-21-01 (Rail)	**Transportation Systems Sector**	Transportation Security Administration **(TSA)**	Issued within agency rulemaking authority under 49 U.S.C. I 14(I)(2) (A)	Regulation	Issued: **2021** Expires: Dec. 31, **2022**	Cyber incident reporting	24 hours		To government	
Title Not Public—Issued under the **TSA's Aviation Program** (text not public; see reference here)	**Transportation Systems Sector**	Transportation Security Administration **(TSA)**	Issued within agency rulemaking authority over the aviation sector, under 49 U.S.C. I 14(I)(2) (A)	Hybrid	Presumed issued: **2021**	Cyber incident reporting	24 hours		To government	
Security Directive Pipeline-2021-01	**Transportation Systems Sector**	Transportation Security Administration **(TSA)**	Issued within agency rulemaking authority under 49 U.S.C. I 14(I)(2) (A)	Regulation	Issued: **2021** Extended as of: May **2022**	Cyber incident reporting	24 hours		To government	