Harmonization of Cyber Incident Reporting to the Federal Government

September 19, 2023

Homeland Security

Office of Strategy, Policy, and Plans

Message from the Under Secretary for Strategy, Policy, and Plans

September 19, 2023

I am pleased to present the following report, "Harmonization of Cyber Incident Reporting to the Federal Government," which has been prepared by the Department of Homeland Security's Office of Strategy, Policy and Plans on behalf of the Secretary.

This report has been prepared pursuant to a requirement in §107(d)(1) of the Cyber Incident Reporting for Critical Infrastructure Act of 2022.

Pursuant to congressional requirements, this document is being provided to the following Members of Congress:

The Honorable Mark E. Green
Chairman, House Committee on Homeland Security

The Honorable Bennie G. Thompson
Ranking Member, House Committee on Homeland Security

The Honorable Gary C. Peters
Chairman, Senate Committee on Homeland Security and Governmental Affairs

The Honorable Rand Paul
Ranking Member, Senate Committee on Homeland Security and Governmental Affairs

Inquiries relating to this report may be directed to DHS Legislative Affairs at (202) 447-5890.

Sincerely,

Robert Silvers
Under Secretary
Office of Strategy, Policy, and Plans

Executive Summary

- This report, entitled "Harmonization of Cyber Incident Reporting to the Federal Government," has been prepared by the Department of Homeland Security (DHS) through the Office of Strategy, Policy, and Plans pursuant to a requirement in §107(d)(1) of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), which requires the Secretary of Homeland Security to submit such a report.
- In CIRCIA, Congress established a Cyber Incident Reporting Council (CIRC) to coordinate, deconflict, and harmonize Federal incident reporting requirements, including those issued through regulation. Secretary of Homeland Security Alejandro N. Mayorkas delegated to Under Secretary for Strategy, Policy, and Plans Robert Silvers responsibility to chair the CIRC.
- The CIRC led an intensive process to identify the actionable recommendations to harmonize cyber incident reporting requirements reflected in this report. To support the development of these recommendations, the CIRC took inventory of existing and proposed Federal cyber incident reporting requirements and engaged with Federal agencies and outside experts from industry and other stakeholders.
- The CIRC comprehensively assessed 52 in-effect or proposed Federal cyber incident reporting requirements. That assessment, reflected in this report, highlights potentially duplicative Federal reporting and identifies challenges to harmonization of these requirements.
- Based on the work of the CIRC, this report proposes a model definition for reportable cyber incidents; model timelines and triggers for reporting; and offers recommendations for how to align content of cyber incident reports and to move toward a model reporting form or common data elements wherever practicable.
- The report also recommends that the Federal Government should assess how best to streamline the receipt and sharing of cyber incident reports and cyber incident information, including through improvements to existing reporting mechanisms or the potential creation of a single portal, and improve processes for engaging with reporting entities following the initial report of a cyber incident.
- As required by §107(d)(1) of CIRCIA, the report also summarizes actions that the Cybersecurity and Infrastructure Security Agency (CISA) will take to facilitate harmonization of cyber incident reporting as it implements CIRCIA as well as proposals that Congress may consider for legislative changes. Proposals for congressional action include removing legal barriers to harmonizing incident reporting regimes and exempting cyber incident information reported to the Federal Government from the Freedom of Information Act.
- Following release of this report, the CIRC will take steps to begin implementing the recommendations and—under the leadership of DHS—continue to serve as the Executive Branch's forum to coordinate, deconflict, and harmonize Federal cyber incident reporting requirements. On behalf of the Secretary, the DHS Office of Strategy, Policy, and Plans will coordinate closely with agencies participating in the CIRC to keep Congress apprised of developments in the whole-of-government approach to reduce complexity, diminish regulatory overlap, and eliminate unnecessary duplication with respect to cyber incident reporting.

Harmonization of Cyber Incident Reporting to the Federal Government

Table of Contents

I. Legislative Language

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 includes the following requirement within Section 107. Congressional Reporting.

> (d) REPORT ON HARMONIZATION OF REPORTING REGULATIONS.—
>
> (1) IN GENERAL.—Not later than 180 days after the date on which the Secretary of Homeland Security convenes the Cyber Incident Reporting Council described in section 2246 of the Homeland Security Act of 2002, as added by section 103 of this division, the Secretary of Homeland Security shall submit to the appropriate congressional committees a report that includes—
>
> (A) a list of duplicative Federal cyber incident reporting requirements on covered entities;
>
> (B) a description of any challenges in harmonizing the duplicative reporting requirements;
>
> (C) any actions the Director intends to take to facilitate harmonizing the duplicative reporting requirements; and
>
> (D) any proposed legislative changes necessary to address the duplicative reporting.
>
> (2) RULE OF CONSTRUCTION.—Nothing in paragraph (1) shall be construed to provide any additional regulatory authority to any Federal agency.

Homeland Security Act of 2002 § 2246, 6 U.S.C. § 681f (as added by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), Pub. L. No. 117-103, div. Y, § 103, 136 Stat. 49, 1054)

II. Introduction

In March 2022, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022, known as CIRCIA. Among other things, the landmark legislation requires the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) to develop and implement regulations that will require covered entities to report covered cyber incidents and ransomware payments to CISA.[1] Once implemented, these regulations will constitute the first Federal cybersecurity incident reporting requirements focused specifically on reporting across all critical infrastructure sectors. The incident reports required by CIRCIA will significantly improve the Federal Government's visibility into cyber threats and vulnerabilities facing our Nation. They will also allow CISA, Sector Risk Management Agencies (SRMAs), and other relevant agencies to analyze threats and vulnerabilities across sectors, quickly share relevant information with network defenders across government and the private sector, warn and protect other potential victims, assess trends, and where appropriate rapidly deploy resources and render assistance to victims experiencing cyber incidents.

While CIRCIA directs CISA to develop new cyber incident reporting requirements, it does so in the context of an existing patchwork of incident reporting requirements across the Federal Government and the larger ecosystem. Some existing requirements are focused on national security, economic security, or public safety risks associated with particular critical infrastructure sectors or sub-sectors verticals, while others focus on consumer, investor, or privacy considerations that apply horizontally across multiple sectors. Many, but not all, cyber incident reporting requirements are also part of broader, all-hazards regulatory regimes that consider multiple risks to a sector or otherwise address a class of harms that includes but is not limited to cyber risks.

To address the potential for duplication arising from current and future cyber incident reporting regimes, CIRCIA established the Cyber Incident Reporting Council (CIRC).[2] CIRCIA also requires the Secretary of Homeland Security to provide Congress with this report on "Harmonization of Cyber Incident Reporting to the Federal Government," to identify duplicative reporting requirements, challenges to harmonization, actions the CISA Director intends to take to facilitate harmonization, and any proposed legislative changes to address duplicative reporting.[3]

Secretary of Homeland Security Alejandro Mayorkas delegated responsibility for chairing the CIRC and developing this report to Under Secretary Robert Silvers and the DHS Office of Strategy, Policy, and Plans. Led by DHS, the CIRC is responsible for coordinating, deconflicting, and harmonizing Federal incident reporting requirements, including those issued through regulations.[4] The ongoing work of the CIRC will complement and inform CISA's

1. For the purposes of this report, the term "covered entity" refers to an entity that is subject to a particular regulatory requirement to report cyber incidents to one or more Federal agencies. The identity of covered entities will vary from regulatory regime to regulatory regime based on the relevant authority and as determined by the regulator.
2. Homeland Security Act of 2002 § 2246, 6 U.S.C. § 681f (as added by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), Pub. L. No. 117-103, div. Y, § 103, 136 Stat. 49, 1054).
3. CIRCIA § 107(d)(1).
4. Biden, Joseph R., National Cyber Strategy (The White House, 2023), p. 9. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

implementation efforts under CIRCIA.[5] DHS will also work with agencies participating in the CIRC to ensure that the recommendations included in this report are considered in developing new or amended incident reporting requirements given the rapidly evolving cyber environment. Future actions should also be informed by ongoing work of the CIRC and any other insights to be gleaned from ongoing regulatory efforts of CIRC members. Moving forward, DHS will also, in consultation with the CIRC, lead efforts to review on an ongoing basis existing regulatory requirements and work with Federal agencies to "avoid conflicting, duplicative, or burdensome requirements," as well as find opportunities to streamline reporting processes.[6]

Summary of CIRC Efforts

In developing this report to Congress, DHS has relied heavily on the input of the CIRC and 33 agencies who were invited to participate as members. Participants included Executive Branch departments and agencies, independent regulatory agencies, SRMAs, law enforcement agencies, the Department of Justice (DOJ), and the Office of the National Cyber Director (ONCD).[7] A full list of CIRC members is included in Appendix A. To meet its mission of coordinating, deconflicting, and harmonizing Federal cyber incident reporting requirements, the CIRC assessed current and future reporting requirements and identified opportunities and challenges related to harmonization.

Staff from CIRC member agencies collaborated throughout June and July 2022 to survey existing Federal cyber incident reporting requirements, which are described in Appendix B. Secretary Mayorkas then convened the inaugural CIRC meeting on July 22, 2022. CIRC members reviewed the results of the initial survey to assess areas of overlap. A summary of key findings with respect to duplicative cyber incident reporting requirements is discussed in section III below. CIRC members also discussed the importance of harmonizing cyber incident reporting to minimize unnecessary burden on reporting entities. Such harmonization helps to ensure that the resources of victimized entities are dedicated to mitigating the effects of cyber incidents while also ensuring that agencies are provided with sufficient information to carry out their organizational and statutory missions. Following its inaugural meeting, the CIRC established working groups to examine four specific areas:

- Definition of "Reportable Cyber Incidents;"
- Issues Related to Timelines and Triggers for Reporting;
- Contents of Incident Reports; and
- Reporting and Enforcement Mechanisms.

5. This report does not reflect any final decision regarding the content of ongoing or future DHS rules. Cyber incident reporting regulations required by CIRCIA are still under development at CISA, as are cyber-rules by other DHS Components. Development of these rules will comply with the rulemaking procedures required by the Administrative Procedure Act (APA). DHS Components will receive and consider all comments received on the proposed rules before finalizing those regulations.
6. CIRCIA § 104(b), 6 U.S.C. § 681g(b).
7. Section 2218 of the Homeland Security Act of 2002, 6 U.S.C. § 665d, outlines SRMA roles and responsibilities. Per Presidential Policy Directive (PPD)-21, *Critical Infrastructure Security and Resilience* (2013), SRMAs (previously referred to as Sector Specific Agencies (SSAs)) coordinate and collaborate with DHS and other relevant Federal departments and agencies, with critical infrastructure owners and operators, where appropriate with independent regulatory agencies, and with SLTT entities, as appropriate, to implement PPD-21; serve as a day-to-day Federal interface for the dynamic prioritization, collaboration, and coordination of sector-specific activities; carry out incident management responsibilities consistent with statutory authority and other appropriate policies, directives, or regulations; provide, support, or facilitate technical assistance and consultations for that sector to identify vulnerabilities and help mitigate incidents, as appropriate; and support the Secretary of Homeland Security's statutory reporting requirements by providing, on an annual basis, sector-specific critical infrastructure information.

As discussed in section IV, each of these focus areas highlights challenges—but also opportunities—to harmonize cyber incident reporting to the extent practicable. Other challenges to harmonization include current statutory requirements and authorities, procedural hurdles to modifying current reporting regimes, inconsistent confidentiality protections for information submitted, and internal resource limitations of agencies.

Overview of Federal Cyber Incident Reporting Requirements

The CIRC's review of current cyber incident reporting requirements yielded several key conclusions that have informed this report.

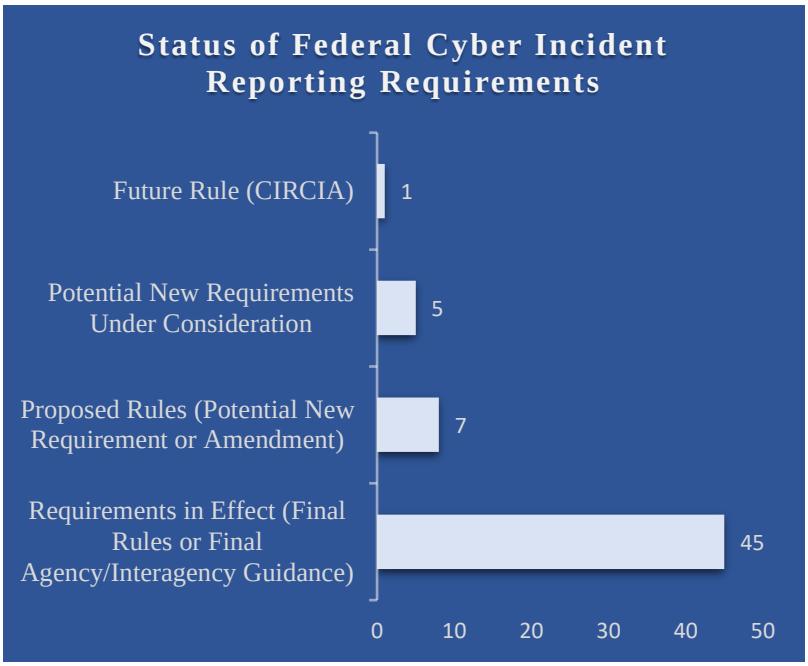
First, cyber incident reporting can serve several important governmental purposes, and disparate requirements can be driven by these differing but equally legitimate purposes. For example, many cyber incident reporting requirements are motivated by potential national security, economic security, and public safety concerns. Among these, required – and in many cases voluntary – reporting of cyber incidents is often intended to provide awareness to the Federal Government of operational threats to critical infrastructure, impacts to public health and safety, or the potential disruption of National Critical Functions (NCF) and the delivery of vital goods or services to the American people.[8] Reporting also provides CISA, and other SRMAs or Federal law enforcement agencies with the ability to provide assistance at the request of critical infrastructure operators and owners. Incident reporting is therefore essential to address a range of public safety and security concerns. Other cyber incident reporting requirements are driven by privacy, consumer protection, or investor protection considerations. Requirements to report to the Federal Government – and potentially to impacted individuals and the public – support actions that can address the loss of personally identifiable information, financial information, or other sensitive personal or commercial data. Such reporting can also inform remedies for harm to investors and consumers, such as potentially Unfair, Deceptive, or Abusive Acts or Practices.[9] Finally, reporting of cyber incidents supports law enforcement efforts to aid victims, prosecute, and otherwise disrupt those engaged in criminal activity.

Second, current requirements are derived from a patchwork of regulations and statutory authorities, many with unique and potentially overlapping information requirements, timelines, and submission methods. DHS identified 45 different Federal cyber incident reporting requirements created by statute or regulation currently in effect or final agency guidance that set an expectation for reporting to an agency.[10] In total, these 45 in-effect reporting requirements are

8. National Critical Functions (NCFs) are functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. CISA brings the private sector, government agencies, and other key stakeholders together to identify, analyze, prioritize, and manage the most significant risks – cyber, physical, supply chain and more to these important functions. *See reference in the* 2018 National Cyber Strategy of the United States. *See references in the 2018 National Cyber Strategy,* 2018 National Cyber Strategy of the United States (Trump, Donald J., National Cyber Strategy (The White House, 2018) (https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf).

9. Unfair, deceptive and abuse practices can cause significant financial injury to consumers, erode consumer confidence and undermine the financial marketplace. Unfair and deceptive acts and practices are prohibited under Section 8 of the Federal Trade Commission Act, and unfair, deceptive and abusive practices are prohibited under the Dodd-Frank Wall Street Reform and Consumer Protection Act. *Refer to* 15 USC 45 and 12 U.S.C. 5531 and 5536.

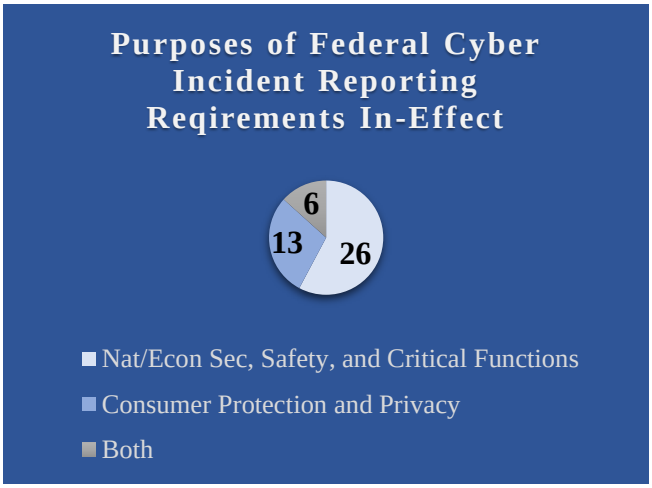
10. Through this effort, DHS worked with CIRC agencies to identify any Federal cyber incident reporting requirements, including those that are "cyber-specific," and those that are "cyber-agnostic" or "all-hazard" where reporting is required in response to covered incidents that may or may



administered by 22 Federal agencies. As of the date of drafting this report, DHS is also aware of seven proposed rules that would create a new reporting requirement or amend a current requirement, and five additional potential new requirements or amendments under consideration but not yet proposed. In addition, pursuant to CIRCIA, CISA will create a new requirement for covered entities to report covered incidents. These numbers do not include the myriad state and local requirements in place across U.S. jurisdictions or the international requirements imposed on U.S. businesses by foreign governments. This patchwork often requires entities, especially those with multiple lines of business or who operate within more than one state, local, or international jurisdiction, to report the same incident multiple times.

Of the 45 Federal requirements in effect identified by CIRC members, a majority (26) are primarily related to national security, economic security, or public safety considerations. A smaller number (13) are primarily focused on privacy or consumer or investor protection. Another six requirements appear to serve a purpose in both of those categories.

There is also significant variation in the maturity and degree of deconfliction of existing cyber incident reporting requirements within and across the 16 critical infrastructure sectors as defined by PPD-21.[11] On one end of the continuum, eight Federal agencies currently have reporting requirements applicable to the financial services sector. This sector has, however, established clear parameters and coordination mechanisms that minimize regulatory overlap and conflict among



not be cyber-related. DHS recorded in the inventory (1) any requirement created by statute or regulation and (2) any requirement created by interpretive or other final agency guidance that set or clarified an expectation for reporting based upon regulation or statute already in effect. For brevity, DHS collectively refers to both categories as "requirements" throughout this report. Also, DHS refers to both in-effect regulations and final agency guidance as "in effect." *See Appendix B: Inventory of Federal Cyber Incident Reporting Requirements*.

11. *See reference to CISA's identified critical infrastructure sectors at* https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.

the various regimes in that sector. Other sectors are only in the beginning stages of implementing cybersecurity regulations and associated cyber incident reporting requirements. The water and wastewater systems sector, for example, does not currently have any mandatory reporting requirements, as the Environmental Protection Agency (EPA) has advised DHS that it does not have statutory authority to mandate cyber incident reporting. Entities in that sector are currently only subject to applicable cross-sector privacy, consumer protection, or investor protection (if a publicly traded company) requirements.

The means of collecting incident reports are similarly varied across existing regimes. Based on discussions among CIRC members, 14 of the 22 agencies with cyber incident reporting requirements provide an online submission option (i.e., web form, web portal, secure file transmission system, or email form). Eight of those agencies afford reporting entities additional flexibility through another submission option for an initial report (e.g., telephone, other verbal communication, or unstructured email). Such flexibility can be important for reporting entities who may be operating under degraded technological capability or time pressures. The remaining eight agencies do not use a form to receive reports but instead leverage email, phone, mail, or other similar methods to receive reports. There are currently 13 separate forms and 10 websites in use by the Federal Government for incident reporting. Of the 22 Federal agencies with current cyber incident reporting requirements, only three recognize or accept another agency's form. Specifically, the Transportation Security Administration (TSA) recognizes a report to CISA; the Department of Energy (DOE) enables the submission of an incident report collected via its DOE-417 (Form OE-417) *Electric Emergency Incident and Disturbance Report* to be submitted to the Electricity Information Sharing and Analysis Center (E-ISAC), the North American Electric Reliability Corporation (NERC), and CISA (if the industry member elects to submit to other agencies to fulfill additional reporting requirements); and the Federal Communications Commission (FCC) requires customer proprietary network information (CPNI) breaches to be reported to the U.S. Secret Service and the Federal Bureau of Investigation (FBI) via the Central Reporting Facility, which is operated by the Secret Service.[12] In other cases, incidents provided to one agency are shared with other agencies. For example, incident reports to the U.S. Coast Guard's National Response Center are automatically relayed to CISA in near real-time.

Insights from Stakeholder Engagements

To inform the analysis, recommendations, and proposed legislative changes discussed in this report, DHS and some CIRC members also engaged with private sector and other non-Federal stakeholders. DHS conducted sector-specific listening sessions with representatives of the financial services, transportation, energy, communications, defense, and nuclear sectors. These sectors were prioritized for engagement based on the existence of sector-specific reporting requirements. Additional cross-sector engagements were hosted by the Chamber of Commerce, the Center for Strategic and International Studies, and the National Cyber-Forensics and Training Alliance.

12. Pursuant to applicable Federal Communications Commission regulations at 47 C.F.R. § 64.2011, a telecommunications carrier or interconnected VOIP provider that determines that a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI is required to electronically notify the United States Secret Service and the Federal Bureau of Investigation through a central reporting facility. That facility is available at https://www.cpnireporting.gov.

During these engagements, non-Federal stakeholders shared the following views:[13]

- DHS should consider not only "pure cyber" incident reporting requirements as part of any harmonization efforts, but also those all-hazards and other broader reporting requirements that may include but are not limited to incidents that are triggered by a cyber or technology root cause.
- The Federal Government should minimize the burden on the private sector to report the same or similar information through multiple channels, and the Federal Government should bear the burden to "connect the dots" and disseminate information to multiple Federal agencies with legitimate need to receive the information reported.
- A common reporting platform and intra-government information-sharing infrastructure will be increasingly necessary to alleviate the burden of duplicative reporting as the number of incident reporting regimes continues to increase.
- Cyber incident reporting channels should support essential information sharing among appropriate Federal agencies during an incident, and the Federal Government should streamline communication with victims following the initial reporting of an incident to reduce confusion and avoid disjointed and uncoordinated outreach from multiple agencies.
- Clear definitions and consistent terminology across cyber incident reporting regimes would reduce confusion and burden on reporting entities. Objective questions are likely to lead to more prompt and complete responses than subjective questions given the involvement of legal teams and outside experts in submitting required reports.
- Striking the right balance between the amount of information and level of detail of the information required and the need for timely reporting is important. Initial cyber incident reports should not be delayed to collect granular information; many data elements can be provided in supplemental reports or in some cases left to direct engagements and follow up discussions with reporting entities.
- Requiring too much granularity in initial cyber incident reporting could negatively impact the ability of the Federal Government to harmonize incident reporting requirements and the contents of reports should be utilizable across sectors.
- The Federal Government should provide useful anonymized or aggregated information derived from incident reports back to reporting entities and work more closely with Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) to collect and disseminate incident information to enable improved cybersecurity outcomes across critical infrastructure.[14]
- The Federal Government should ensure that sensitive cyber incident information reported by the private sector is protected from disclosure, including but not limited to current or new Freedom of Information Act (FOIA) protections, preservation of applicable privileges and protections provided by law, and that there are sufficient cybersecurity protections in place to secure private sector information.
- The Federal Government should ensure that entities covered by the cyber incident reporting requirements are not liable for good-faith efforts to comply with the reporting requirements

13. These non-Federal stakeholder views are not listed in any particular priority order.
14. The role of ISACs and ISAOs is to assist critical infrastructure owners and operators in protecting their facilities, personnel and customers from cyber and physical security threats and other hazards. Functionally, they collect, analyze, and disseminate actionable threat information to their members and provide tools or recommendations to mitigate risks. Most sectors maintain consistent threat sharing and relationships with their member ISACs. ISAOs serve a similar function although they are typically organized around an affinity other than sector.

and that entities are protected from liability based on the information contained in required reports.
- Federal Government efforts to harmonize incident reporting should inform and be informed by efforts to harmonize state and local government requirements as well as international requirements.

DHS also reviewed written analyses of existing cyber incident reporting requirements by the Cyber Threat Alliance, CTIA—The Wireless Association (formerly known as the Cellular Telecommunications Industry Association), the R Street Institute, and the Chamber of Commerce. DHS additionally engaged the New York Department of Financial Services (NY DFS). Input from external stakeholders and from efforts of the CIRC is reflected throughout this report and the recommendations and proposed legislative changes in sections VI and VII.

III. Duplicative Federal Cyber Incident Reporting Requirements

Existing Federal cyber incident reporting regimes contain reporting requirements that were created and designed for different purposes, are independently administered, and often lead to regulatory overlap and duplicative reporting.[15] For purposes of this report, the term "duplicative reporting" or "duplication" includes regulatory requirements for the same reporting entity to report the same incident to more than one Federal agency.[16] Duplicative reporting may occur where multiple Federal agencies have overlapping jurisdiction over the same entities, where reporting requirements have overlapping definitions of a "reportable cyber incident," and where there is lack of interagency coordination and agreement to share reports and leverage common reporting systems. Duplication can also occur with voluntary reporting regimes – that is, non-mandatory reporting that entities comply with to abide by best practices, such as reporting to law enforcement (including the FBI or the Secret Service) or to CISA or another SRMA.

Duplication in Federal Sector-Specific Regulatory Reporting Requirements

As reflected in Appendix B, there are 52 cyber incident reporting requirements either in effect or proposed across the Federal Government. Of these, DHS has identified 45 requirements are currently in effect across 22 agencies. Agencies with cyber incident reporting requirements typically have their own reporting mechanisms and methods for ingesting reports. As a result, reporting entities that are regulated by more than one agency are required to submit multiple reports while potentially managing and responding to an incident and its immediate impact. The following are examples of potentially overlapping reporting requirements that can lead to duplication for a particular sector. As discussed below, duplication for entities in these sectors is often magnified by the application of cross-sector regulatory requirements.

- In the Financial Services Sector, there are eight Federal agencies that require reporting of incidents that have or potentially have a cyber nexus.[17] The Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), and the Federal Reserve Board (FRB) require cyber incident notification under the Computer-Security Incident Notification rule. Although the OCC, FDIC, and FRB issued joint guidance to improve harmonization, financial institutions only must notify their primary regulator of significant incidents, not all three agencies. The OCC, FDIC, and FRB also have notification requirements based on the Gramm-Leach-Bliley Act (GLBA), which may, in some cases, also be covered under the Computer-Security Incident Notification rule.[18] More broadly, financial institutions that have identified certain types of suspicious activity must file Suspicious Activity Reports (SARs) under the Bank Secrecy Act to the Financial Crimes

15. Pursuant to Section 107 of CIRCIA, DHS must, among other things, submit "a list of duplicative Federal cyber incident reporting requirements on covered entities." As discussed in the text, regulatory overlap and duplicative reporting requirements may result from the varied purposes of different reporting requirements. Each of the "duplicative" requirements may serve an equally legitimate purpose and efforts to eliminating duplication must account for the separate and distinct information needs of agencies under their respective mission and authorities.
16. For the purpose of this report, a reporting entity includes any individual legal corporate organization, or broader corporate organization with subsidiaries, that reports an incident to the Federal government in fulfillment of a regulation, interpretative or other Federal guidance requirement, or voluntarily chooses to provide that information to the Federal Government.
17. *See* OCC (12 C.F.R. part 53); OCC (12 C.F.R. part 30, app. B); FDIC (12 C.F.R. part 304, subpart C); FDIC (12 C.F.R. part 364, app. B); FRB (12 C.F.R. §§ 225.300-225.303); FRB (12 C.F.R. part 208, app. D-2, 12 C.F.R part 225, app. F); FinCEN (31 C.F.R. chapter X); CFTC (17 C.F.R. part 37, subpart O); CFTC (17 C.F.R. part 38, subpart U); CFTC (17 C.F.R. part 39, subpart B); CFTC (17 C.F.R. § 49.24); FHFA (Advisory Bulletins (Abs): AB 2020-05, Enterprise Cybersecurity Incident Reporting; AB 2017-02, Information Security Risk Management; 12 C.F.R. part 1214); NCUA (12 C.F.R. part 748, apps. A, B); SEC (17 C.F.R. §§ 242.1002, 242.1003).
18. OCC (12 C.F.R. part 30, app. B, supp. A).

Enforcement Networks (FinCEN) at the Department of the Treasury. In addition, Designated Contract Markets, Swap Execution Facilities, Derivatives Clearing Organizations, and Swap Data Repositories must report cyber incidents or targeted threats to the Commodity Futures Trading Commission (CFTC) to secure derivative trading markets. Freddie Mac and Fannie Mae (Enterprises) and Federal Home Loan Banks must report cyber incidents to the Federal Housing Finance Agency (FHFA), and Credit Unions must report cyber incidents to the National Credit Union Administration (NCUA) under the GLBA obligation to safeguard member information. In addition, the Securities and Exchange Commission (SEC) has rules in effect for designated Systems, Compliance, and Integrity (SCI) entities and publicly-listed companies and is considering additional rule changes for other entity types (e.g., registered broker-dealers, investment advisers, and investment companies).

- Some entities in the communications sector could be subject to two FCC reporting requirements for the same incident when a communications outage that meets the threshold for reporting service outages also results in exposure of CPNI. Generally, the FCC requires certain communications service providers to report, within two hours of discovery, communications outages that meet certain user impact and duration thresholds to the FCC's Network Outage Reporting System (NORS). The FCC's outage reporting requirements cover all causes of outages; a cyber-related event is one of many outages that can be reported in NORS. Additionally, FCC requires Telecommunications Carriers and Interconnected VoIP Service Providers to notify law enforcement of a breach of their customers' CPNI as soon as practicable, and in no event later than seven business days after reasonable determination of the breach.[19] To ensure physical and cybersecurity of telecommunications infrastructure, FCC licensees and authorization holders covered by the CPNI rules are subject to mitigation measures imposed pursuant to Executive Order 13913 and must report to DOJ within 48 hours after an incident is known or expected if certain mitigation measures are not taken.[20]

- Within the transportation sector, multiple Federal agencies impose reporting requirements, including the United States Coast Guard (USCG), TSA, and the Department of Defense (DOD). Entities in the sector are thus potentially subject to multiple reporting requirements for the same cyber incident if the incident affects operations in multiple modes of transportation. The USCG requires reports to the National Response Center of breaches of security from owners or operators of vessels, waterfront facilities, and/or outer continental shelf facilities, that may include cyber incidents.[21] TSA has eight requirements applicable to aviation and surface transportation. The requirements cover passenger railroad carriers, rail transit systems, hazardous and natural gas pipelines or liquefied natural gas facilities, freight railroad carriers, airport operators, aircraft operators, indirect air carriers, and certified cargo screening facilities. Applicable cyber incident reports are submitted to CISA and shared with TSA. Depending on the scope of the incident and whether the reporting entity is a covered defense contractor, the entity may also have to report to DOD under applicable Defense

19. 47 C.F.R. § 64.2011. In December 2022, the FCC proposed to update its breach reporting rules, proposing to, among other things, expand the Commission's definition of "breach" to include inadvertent disclosures of customer information; require telecommunications carriers and interconnected VoIP Providers to notify the Commission, in addition to the Secret Service and FBI, as soon as practicable after discovery of a breach; and to eliminate the mandatory waiting period before notifying customers and instead require carriers to notify customers of CPNI breaches without unreasonable delay after discovery of a breach unless requested by law enforcement. *Data Breach Reporting Requirements*, WC Docket No. 22-21, Notice of Proposed Rulemaking, FCC 22-102 (2022).
20. Executive Order No. 13913, § 9(a) (2020).
21. 33 C.F.R. parts 104, 105, and 106.

Federal Acquisition Regulation Supplement (DFARS) procedures. Natural gas pipeline entities may also have to report certain cyber incidents to the DOE.

- Within the health and public health sector, authorities to regulate companies with respect to cyber incident and breach reporting are divided among the Department of Health and Human Services (HHS), the Federal Trade Commission (FTC), and the Food and Drug Administration (FDA), which is an operating division of HHS.[22] Health plans and certain health care providers covered under the Health Insurance Portability and Accountability Act (HIPAA) must report data breaches to HHS under the HIPAA Breach Notification Rule. In a scenario where there is a compromise of Personal Health Records (PHR) due to unauthorized acquisition of unsecured PHR identifiable health information, data breach notifications must be sent to the FTC, to consumers, and in some cases, to the media.[23] In some instances, an entity that is a HIPAA business associate that also supplies PHR services to the public subject to FTC jurisdiction (i.e., to the extent it is also acting as other than a HIPAA-covered entity or business associate in some other capacity) may be required to report the same incident to a HIPAA covered entity, which is required to report breaches of unsecured protected health information (PHI) to HHS, and to the FTC provided that a single cyber incident compromises both PHI and PHR identifiable health information. Although the regulators may regard this as separate breaches, since the two information types are typically stored on separate systems, the breaches may occur as the result of the same cyber incident. When medical devices are impacted in addition to compromising PHI and PHR, there are additional reporting obligations to notify manufacturers and/or the FDA.[24]

Duplication from Cross-Sector Reporting Requirements

The potential for regulatory overlap and duplicative reporting is compounded by current and future reporting requirements that apply across multiple sectors. Such requirements apply to entities who are already subject to sectoral requirements like those discussed in the prior section. Although cross-sectoral reporting requirements have developed to advance specific goals, such as such as the ability to assess potential impacts to financial markets and investors (SEC) and response to covered cybersecurity incidents (CISA), entities will be required to comply with these reporting requirements in addition to those from sector-specific agencies. Based on information from CIRC members, DHS has identified at least one such rule currently in effect, one proposed rule, one future rule, and one instance of Federal agency supplemental reporting guidance:

- **FTC Health Breach Notification Rule:** The FTC requires reporting under 16 C.F.R. part 318 from vendors of PHR, PHR related entities, and third-party service providers when there has been unauthorized acquisition of unsecured PHR. This rule covers any reporting entity servicing the public that is responsible for handling or maintaining PHR. In addition, some intentional disclosures of PHR not authorized by the individual data subject are treated as data breaches by the FTC.[25]

22. HHS (45 C.F.R. §§ 164.400 to 164.414); FTC (16 C.F.R. part 318); FDA (21 C.F.R parts 803, 806).
23. *See* 16 C.F.R. § 318.3(a), § 318.5(b).
24. *See* 21 C.F.R. § 803.10.
25. *See https://www.ftc.gov/business-guidance/resources/complying-ftcs-health-breach-notification-rule-0* ("Keep in mind, though, that a "breach" is not limited to cybersecurity intrusions or nefarious behavior by hackers or insiders. Incidents of unauthorized access, including a company's disclosure of covered information without a person's authorization, triggers notification obligations under the Rule."

- **SEC Public Company Reporting Guidance:** Before the July 2023 SEC final rule discussed below, disclosure requirements under the Securities Act of 1933 (the "Securities Act") and the Securities Exchange Act of 1934 (the "Exchange Act") did not specifically address cybersecurity. However, 2011 and 2018 interpretive guidance from the staff and the Commission, respectively, reiterated that a number of the existing statutory disclosure requirements may impose an obligation for companies to disclose cyber-related matters. The Commission's interpretive guidance suggested that, in determining their obligations to disclose cyber-related matters, companies weigh "the potential materiality of any identified risk and, in the case of incidents, the importance of any compromised information and the impact of the incident on the company's operations."

- **SEC Final Rule Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure:** In July 2023, the SEC issued final rules and amendments to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934. The final rules and amendments, in relevant part, require public companies to disclose in their Form 8-Ks material cybersecurity incidents within four days of determining the incident is material (*i.e.,* is important to an investment or voting decision). These requirements are applicable to public companies, including across critical infrastructure sectors, and are intended to better inform investors about a registrant's cybersecurity risk management, strategy, and governance and to provide timely notification to investors of material cybersecurity incidents.

  Case Study: Duplicative Reporting in the Financial Sector

  The financial sector contains entities that provide a large gamut of financial services, such as banking, broker dealing, investment advising, clearing, etc. As a result, these entities are subject to several incident reporting requirements. Each of these requirements was established for unique and legitimate government purposes. Examples of reporting requirements include the OCC's Computer-Security Incident Notification Rule, the SEC's July 2023 final rule, and the NY DFS's rule. Many of these entities are also obligated to report incidents to FinCEN within 30 days with a maximum extension of 30 additional days and could also be subject to proposed or future cross-sector requirements. Despite government efforts to minimize the burden of these multiple and complex reporting obligations, they were still highlighted as a challenge by industry in meetings with DHS.

- **CISA Future Rule:** Pursuant to CIRCIA, CISA will undergo a rulemaking to implement a 72-hour cyber incident reporting requirement and 24-hour reporting requirement for ransom payments made in connection with a ransomware attack. These requirements will be applicable to covered entities across critical infrastructure sectors. A forthcoming Notice of Proposed Rulemaking (NPRM) will propose definitions of covered entities. Although CIRCIA has the potential to create duplicative reporting with current sectoral and cross-sector requirements, Congress built in mechanisms to avoid such duplication. This includes an exemption for covered entities from the reporting requirements to CISA if the entity is

required to report substantially similar information to another federal agency within a substantially similar timeframe and CISA and the Federal agency have an agreement and information sharing mechanism in place. Section V discusses how CISA will facilitate harmonization and work with agencies with current or proposed cyber incident reporting requirements to minimize duplication where feasible.

Duplication Resulting from Voluntary Reporting to CISA, SRMAs, and Law Enforcement

In addition to mandatory requirements, entities frequently report cyber incidents on a voluntary basis to CISA, their SRMA, regulators, and/or one or more Federal law enforcement agencies. Such reporting alerts appropriate Federal officials to the incident and can facilitate forensic and incident response support or other government services to victims. Such reporting also ensures that there is a better understanding of current threats faced by critical infrastructure owners and operators, potential impacts to the delivery of critical goods or services, and trends impacting one or more sectors. In addition to CISA, SRMAs, and law enforcement, affected entities can also report incidents to relevant ISACs and ISAOs. These information sharing organizations provide actionable threat information and incident response support to critical infrastructure owners and operators after an incident occurs.

As with mandatory requirements, entities frequently provide reports to multiple agencies and/or information sharing organizations to independently alert each of the incident. Some examples of voluntary reporting relationships that were highlighted during DHS engagements include:

- CISA operates a web-based Incident Reporting System through which any entity can report a cyber incident. Voluntary cyber incident reports to CISA enhance CISA's capabilities to assess potential impact across critical infrastructure, provide forensic support to victim companies, assist law enforcement investigations, and coordinate the national response to significant cyber incidents.

- Many entities elect to voluntarily report cyber incidents to various Federal, state, or local law enforcement agencies. The Secret Service, FBI, and other Federal law enforcement have field offices throughout the United States that investigate cybercrimes and receive reports of cyber incidents through a variety of means, to include in-person and by email, phone calls, and Internet-accessible website forms. For example, the FBI operates the Internet Crime Complaint Center (IC3), to receive reports from the public on Internet crime. The FBI shares reports received with other appropriate federal partners and uses reports for investigative, bank funds recovery, and other cybercrime disruption purposes.

- The electricity subsector, including bulk electric entities who operate operational technology subject to the NERC CIP Reliability Standards, must report relevant cyber incidents to both E-ISAC and CISA.[26] However, other entities in the subsector also choose to voluntarily report cyber incidents to the E-ISAC. The E-ISAC is the primary nongovernmental partner that electricity companies leverage to prepare and respond to cyber incidents. The E-ISAC works closely with the DOE, as the SRMA for the energy sector, on reporting and incident

26. NERC and the E-ISAC accept the DOE-417 Electric Emergency Incident and Disturbance Report to fulfill reporting requirements under NERC CIP-008-6, as well as under non-cyber reporting requirements.

response. This voluntary reporting to E-ISAC remains a critical option for other entities to increase awareness and aid response efforts across the subsector.

- Reporting entities in the communications sector are encouraged to report to the National Coordinating Center for Communications (NCC), which is located within CISA and serves as the Communications Sector ISAC. The NCC shares information on vulnerabilities, threats, intrusions, and anomalies to carriers, Internet Service Providers, satellite providers, broadcasters, vendors, and other stakeholders. Federal law enforcement agencies also recommend that communications providers report incidents to them to better coordinate investigations and incident response. Depending on the scope of the cyber incident and resulting impact, the Federal Emergency Management Agency (FEMA) may also encourage reporting from the communications sector to inform and aid in disaster relief and recovery.

Duplication from State, Foreign, and Other Nonfederal Regulatory Requirements

State, local, tribal, and territorial (SLTT) governments and foreign governments also impose reporting requirements, whether mandatory or voluntary. For example, every U.S. State has passed data breach notification laws that require covered entities to notify affected customers of certain breaches of personal information.[27] Therefore, following a data breach affecting customers in multiple states, a reporting entity may be required to notify multiple state regulators or law enforcement agencies, media outlets, credit bureaus, and/or affected individuals across multiple states with disclosures that contain different information elements, as required under state laws. Other State requirements, such as the NY DFS' *Cybersecurity Requirements for Financial Services Companies*, apply for the banking, insurance, and financial services sectors. Internationally, multinational covered entities may also be subject to the European Union's General Data Protection Regulation and other privacy regulations, as well as other applicable laws from jurisdictions in which they operate. Federal, SLTT, and foreign reporting requirements can engender duplicative reporting across jurisdictions.

27. *See, e.g.*, N.Y. Gen. Bus. Law § 899-aa (McKinney 2022); Ca. Civ. Code § 1798.82 (West 2023).

IV. Challenges to Harmonization

There are many challenges to harmonizing 45 in-place Federal cyber incident reporting requirements. As discussed above and throughout this section, substantive differences among the current incident reporting requirements are often driven by diverse national and economic security considerations across critical infrastructure sectors as well as varied government interests in consumer and investor protection. Among the most significant challenges to harmonization are varying definitions, timelines and triggers for reporting, report content requirements, and reporting mechanisms. In addition, there are also procedural and resource challenges, as well as legal barriers to harmonization.

Differences in Definitions, Timelines and Triggers, Content of Reports, and Reporting Mechanisms

A significant challenge to harmonizing current and future Federal Government cyber incident reporting requirements is the substantive variation between the regimes themselves. The CIRC reviewed current and proposed cyber incident reporting regimes to identify areas of commonality and divergence. Based on that assessment and informed by discussions with relevant stakeholders, DHS identified several areas where the differences between regimes are most burdensome to entities that must report to multiple agencies. The areas deemed most problematic from a harmonization standpoint were differences in the definitions of reportable cyber incidents; the timelines and triggers for when reports must be made; the content of reports; and how the reports are submitted to relevant agencies. As noted in section II, many of these variations are a function of the different government purposes animating various cyber incident reporting regimes, which may reflect differences in operational impacts, economic impacts (such as supply chain-considerations), and privacy. The linkage between the purpose of a regime and specific requirements is perhaps clearest when it comes to reporting timelines and the content of reports. Those regimes focused on potential national security, economic security, and public safety concerns are likely to have shorter timelines for reporting than those regimes focused on privacy and consumer protection. As discussed below, the type of information about an incident—impact on services, root cause, nature of malicious activity, etc.—is also shaped by the responsibility of the requiring agency and the purpose of the reporting regime.

i. Definitions of Reportable Cyber Incidents and Thresholds for Reporting

Existing regulatory frameworks have employed different language to define reportable cyber incidents or otherwise describe the threshold of what is reportable. Existing definitions and thresholds and those proposed in forthcoming regulatory frameworks will need to be considered as part of future harmonization efforts. One key different in existing regimes is how they characterize the impact of incidents that must be reported. Cyber incident reporting regimes or their underlying statutory authorities generally use a range of terminology such as "substantial loss," "disruption," and "serious impact" to describe the thresholds for incidents that must be reported. Each of these thresholds envisions some tangible impact before reporting is required, but they all can be interpreted to define relevant impact differently. Other agencies define the mere presence, or even suspicion of presence, of malicious code or unauthorized activity as a reportable incident. Examples of various definitions and thresholds include:

> *A cyber incident that leads to **substantial loss** of confidentiality, integrity, or availability of such information system or network, **or a serious impact** of the safety and resiliency of operational systems and processes…* [*Source*: *CIRCIA, section 2242*][28]
>
> *A cybersecurity incident means an event that, without lawful authority, jeopardizes, disrupts or otherwise impacts, or is **reasonably likely to jeopardize, disrupt or otherwise impact, the integrity, confidentiality, or availability** of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident on the system.* [*Source: TSA, Security Directive 1582-21-01*]
>
> *"Cyber incident" means actions taken through the use of computer networks that result in a compromise or an actual or **potentially adverse effect** on an information system and/or the information residing therein, or affect the contractor's ability to perform the requirements of the contract that are designated as operationally critical support.* [*Source: DoD, DFARS 252.204-7012*]

There is also inconsistency across incident reporting regimes as to whether incidents that are still under internal investigation are defined as reportable cyber incidents. For example, TSA explicitly includes cyber incidents under investigation within the definition. TSA's decision to include cyber incidents under investigation was driven by the potential for cascading impacts to other critical infrastructure sectors.

> *This definition **includes an event that is under investigation** or evaluation by the owner/operator as a possible cybersecurity incident without final determination of the event's root cause or nature (such as malicious, suspicious, benign). [Source: TSA, Security Directive 1580/82-2022-01]*

Other agencies exclude from the definition of reportable incidents those would-be incidents that were effectively mitigated by defensive measures or the adoption of cybersecurity best practices and thus did not result in unauthorized compromises:

> *An impermissible use or disclosure of protected health information is presumed to be a breach **unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information** has been compromised based on a risk assessment of at least the following factors…* [*Source: HHS, HIPAA Breach Notification Rule 45 C.F.R 164.400-414*]

Another definitional issue directly linked to the purpose of a reporting regime is whether unauthorized access or disclosure of personal data constitutes a reportable incident. Such disclosures are at the heart of reporting under various HHS and FTC regimes, but not necessarily covered by regimes in other critical infrastructure sectors where the focus is on incidents that can have an operational disruption on the delivery of goods or services.[29]

ii. Timelines and Triggers for Reporting

Divergent timelines and triggers for reporting cyber incidents also present a significant challenge to harmonized reporting. Reporting timelines for national or economic security regimes range from "immediately" (FHFA and SEC in certain cases) or "promptly" (CFTC, SEC in certain cases, DOJ, and CISA's Chemical Facility Anti-Terrorism Standards program) and "one hour"

28. As previously noted, cyber incident reporting regulations required by CIRCIA are still under development. Development of these rules, including interpretation of this and other statutory requirements, will comply with the rulemaking procedures required by the Administrative Procedure Act (APA).
29. *See* 45 C.F.R. § 164.402 (defining "breach" of protected health information triggering notification requirements under HIPAA).

(DOE[30]) to 72 hours (CIRCIA and DOD) or simply "without delay" (USCG).[31] In contrast, most of the timelines for reporting privacy and consumer protection incidents range from 7 business days after reasonable determination of a breach for FCC's CPNI data breach rule and 10 days under FTC's Health Breach Notification Rule, to 60 days from discovery of the breach or the end of the calendar year for HIPAA covered entities. An outlier among privacy and consumer protection-focused requirements, the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice provides that an institution should have procedures to notify its primary federal regulator "as soon as possible."[32]

There are also "tiered" reporting timelines, where agencies have required entities to report either sooner or later based upon the severity of the impact or significance of the impacted system:

> *Depending upon the severity of impact to the digital computer and communications systems, reporting is required within 1-hr, 4-hrs, or 8-hrs[33] [Source: NRC, 10 C.F.R. 73.77]*
>
> *Reports are required to be submitted within 1-hour for Reportable Cyber Incidents or non-Reportable incidents that cause interruptions of electrical system operations; 6-hours for a cyber event that could potentially impact electric power system adequacy or reliability [Source: DOE-417 Electric Emergency Incident and Disturbance Report]*
>
> *One hour after the determination of a Reportable Cyber Security Incident. Or by the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the "Applicable Systems" column of the standard. [Source: DOE-417 Electric Emergency Incident and Disturbance Report & FERC/NERC, Critical Infrastructure Protection Reliability Standard CIP-008-6]*

Tiered reporting timelines can also be based upon the amount of data exposed in the context of privacy and consumer protection focused regimes. For example:

> *If a breach of unsecured protected health information affects 500 or more individuals…. [Source: HHS, HIPAA Breach Notification Rule, 45 C.F.R 164.400-414]*
>
> *If the breach involves the unsecured PHR identifiable health information of 500 or more individuals [Source: FTC, Health Breach Notification Rule 16 C.F.R Part 318]*

Even where timelines can be aligned, there are also different triggers for when the obligation to report inures and the "clock starts to run" on the reporting timeline. CIRCIA, for example, requires a covered entity to report a covered cyber incident "not later than 72 hours after the

30. DOE is authorized to collect the information on Form DOE-417 under the Federal Energy Administration Act of 1974 (Pub. L. No. 93-275, 15 U.S.C. §§ 761 *et seq.*) as amended, the Federal Power Act (16 U.S.C. §§ 791a *et seq.*), the DOE Organization Act (Pub. L. No. 95-91, 42 U.S.C. §§ 7101 *et seq.*) as amended, and section 209 of the Public Utility Regulatory Policies Act of 1978 (Pub. L. No. 95-317, 92 Stat. 3117, 16 U.S.C. 824a-2). The timely submission of Form DOE-417 by those required to report is mandatory under Section 13(b) of the Federal Energy Administration Act of 1974 as amended. The timely submission of Form OE-417 by those required to report is mandatory under 15 U.S.C. § 772(b), as amended.

31. *See, e.g.*, FHFA (Advisory Bulletins (Abs): AB 2020-05, Enterprise Cybersecurity Incident Reporting; AB 2017-02, Information Security Risk Management; 12 C.F.R. part 1214); OCC (12 C.F.R. part 53); CFTC (17 C.F.R. part 37, subpart O); CFTC (17 C.F.R. part 38, subpart U); CFTC (17 C.F.R. part 39, subpart B); CFTC (17 C.F.R. § 49.24); SEC (17 C.F.R. § 49.24); SEC (17 C.F.R § 242); DOJ (Exec. Order No. 13913,§ 9(a) (2020)); CISA (6 C.F.R. § 27.230(a)(15) (CFATS); 6 U.S.C. § 681b(a)(1)(A) (CIRCIA)); FERC (18 C.F.R. part 40); DOE (15 U.S.C. § 772(b)); NRC (10 C.F.R. §§ 73.54, 73.77); DOD (48 C.F.R. § 252.204-7012); USCG (33 C.F.R. § 101.305); FCC (47 C.F.R. § 64.2011); FTC (16 C.F.R. part 318); HHS (45 C.F.R. §§ 164.400 to 164.414).

32. OCC (12 C.F.R. part 30, app. B, supp. A). Although not a cyber-specific incident reporting regulation, this interpretive guidance on incident notification is based on the GLBA and serves as a reporting standard for financial institutions (companies that offer consumers financial products or services).

33. *Specific detail is available in* 10 C.F.R. § 73.77.

covered entity reasonably believes that a covered cyber incident has occurred."[34] Other triggers include:

> *The clock is triggered once the licensee **discovers** that a cyberattack has occurred.[35] [Source: NRC, 10 C.F.R. 73.77]*
>
> *The first day on which such breach is **known or reasonably should have been known** to the vendor [Source: FTC, Health Breach Notification Rule 16 C.F.R Part 318]*
>
> ***Date on which a Public Company determines** that a cybersecurity incident it has experienced is material, rather than the date of discovery [Source: SEC, final rule Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 17 C.F.R Parts 220, 306, 308, and 310]*
>
> *... the **determination of** a reportable cyber security incident [Source: FERC/NERC, Critical Infrastructure Protection Reliability Standard CIP-008-6]*
>
> *...**determin[ation] that** a notification incident has occurred [Source: OCC, 12 C.F.R. part 53/FDIC, 12 C.F.R. part 304, subpart C/FRB, 12 C.F.R. part 225, subpart N]*

Some of these provisions specify that the reporting clock starts as soon as an incident is discovered. Others apply an objective reasonableness standard such as when a breach "reasonably should have been known." Still others apply a more subjective standard such as upon "determination that" the incident was reportable. Some regimes only require reporting after the reporting entity determines that the incident is assessed to meet some secondary criteria, such as materiality, beyond the existence of the incident itself.[36] As a result of differences in these triggers, regimes with the same reporting timeline (e.g., "within 72 hours") could potentially require reports that are due hours or even days apart.

While different reporting timelines are driven by the needs of particular regulators, complying with these divergent timelines and triggers may cause unnecessary complexity and confusion for a reporting entity in some sectors during the critical hours immediately after an incident. The time and effort spent by reporting entities to assess whether an incident meets multiple and potentially inconsistent requirements may detract from the important effort to respond to the incident and mitigate its consequences.

iii. Contents of Incident Reports

Various reporting regimes also include different requirements in terms of the types of information that must be submitted as part of an incident report. Appendix C summarizes the types of information identified by the CIRC which are commonly required as part of cyber incident reports to the Federal Government. Required content generally falls into five categories:

---

34. *See* Homeland Security Act of 2002 § 2242(a)(1)(A), 6 U.S.C. § 681b(a)(1)(A) (as added by CIRCIA § 103) ("A covered entity that experiences a covered cyber incident shall report the covered cyber incident to the Agency not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred.").

35. Additional guidance on this is in Regulatory Guide 5.83, "Cybersecurity Event Notifications," and NEI 15-09, "Cybersecurity Event Notification."

36. *See* SEC final rule Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 17 C.F.R Parts 229, 232, 239, 240, and 249 (July 27, 2023). The final rule modifies previous requirements for disclosing that a cyber event occurred under general disclosure timelines and now requires such disclosure within four days upon determination of a material cybersecurity incident occurred. Cf., Reg. SCI (which requires reporting by SCI entities pursuant to 17 C.F.R. §§ 242.1002, 242.1003).

(1) content related to identifying the reporting entity; (2) content related to incident impacts; (3) content related to the threat actor; (4) information on how individuals can protect themselves; and (5) response actions taken by or on behalf of the reporting entity. As is the case with timing and triggers, the variance in the content of reports required by Federal agencies is largely driven by the underlying governmental purpose of a particular regulatory regime. Reporting requirements in the context of national security, economic security, or public safety regimes tend to focus more on technical threat information and any operational consequences of the incident. Privacy and customer protection regimes tend to focus on the nature of information accessed or stolen, the risk of harm to individuals affected, and how affected individuals can protect themselves.

The degree of technical information requested about an incident also tends to vary across regimes, with many agencies seeking only a general description of the incident and in some cases only the "fact of" an incident. Examples of the kind of information that must be reported include:

> *The functional impact; The attack vector used; and the level of intrusion that was achieved or attempted. [Source: FERC/NERC, Critical Infrastructure Protection Reliability Standard CIP-008-6]*
>
> *The initial report may include information such as: the type of incident that occurred (e.g., denial of service, unauthorized access, reconnaissance/probing); the earliest known date of activity related to the incident; the most recent date of activity related to the incident; and the date when the incident was detected. [Source: NRC, 10 C.F.R. 73.77]*
>
> *A brief description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity (or business associate, as applicable). [Source: HHS, HIPAA Breach Notification Rule, 45 C.F.R 164.400-414]*
>
> *Report significant security incidents to the Department and to local law enforcement officials [Source: CISA, Chemical Facilities Anti-Terrorism Standards 6 C.F.R Part 27]*

Requiring only a general narrative description of the incident may have the advantage of promoting faster reporting and including an open-ended "description of the incident" may invite useful details in a narrative form. The information received may, however, present data aggregation and analysis challenges as narrative fields are less useful for agencies that seek to understand the evolving cyber risk to the Nation through structured data and trend analysis. Consequently, the approach taken by some agencies may not easily work for others.

There are also mission-specific differences in the kind of information that must be reported to certain agencies. For example, DOD requires reporting Defense Industrial Base contractors to provide sufficient information about the cyber incident, including the nature of the DOD information that was potentially compromised, to support a complete damage assessment.[37] The FCC requires information about the primary and secondary causes of communications outages.[38] The SEC requires SCI entities to assess impacts to markets and market participants, while agencies focused on privacy and consumer protection, such as FTC, seek information about how

37. 48 C.F.R. § 252.204-7012.
38. *See* 47 C.F.R. part 4 ("Disruptions to Communications").

individuals can contact the reporting entity for more information about how the incident impacts them.[39] In the context of voluntary reporting, law enforcement also encourages reporting of information about cyber incidents useful to help support its investigative purposes, to include communications from the criminal or ransom demands. Efforts to harmonize cyber incident reporting will need to account for these agency-specific information needs.[40]

Finally, there are different approaches among regulatory regimes to the information elements that must be included in an entity's initial incident report and what can be provided in supplemental reports or other follow up engagements. Some agencies such as the OCC, FDIC, and FRB require a notification from their covered entities when it is determined that an incident meeting the notification threshold has occurred.[41] This notification serves as an early alert, and these agencies will typically follow up, as appropriate, for additional incident details through direct engagements based on their supervisory relationships with the reporting entities. This two-phased reporting structure can be advantageous because many reporting entities express concern over unintentionally providing incomplete or inaccurate information in early reports. Other departments, such as the DOD and HHS, require specific content be submitted through their online form without a clear requirement or express opportunity for any preliminary report.[42]

Requirements to provide supplemental reports also vary across regimes, with several agencies requiring supplemental reports until the incident is closed. For example, the SEC has structured reporting processes for designated SCI entities that includes immediate notification of certain events, periodic supplemental reports (frequency depending on investigations status), and a final written notification within five business days after the resolution of such an event.[43] Similarly structured but with different timelines, the FCC requires an initial outage report, a second report within 72 hours of an outage discovery, and a third report within 30 days. USCG and the banking regulators (i.e., OCC, FDIC and FRB) do not explicitly require updates to initial reports but will follow up with reporting entities on site or through other forms of communication as needed.

iv. Reporting Mechanisms

Across the Federal Government, there are wide disparities in terms of reporting mechanisms used by agencies. The CIRC reviewed such mechanisms, and Appendix D summarizes the reporting mechanisms and formats in use across sectors and reporting requirements. Agencies that currently use an online submission system of some kind include CISA, TSA (through CISA's online submission system), the Secret Service, FBI, Treasury, NRC, FCC, FTC, HHS, DOD, DOE, FERC, FDA, SEC, OCC, and CFTC. These online submission systems consist of web forms, web portals, secure file transmission systems, or forms submitted via email. As

39. SEC Regulation Systems Compliance and Integrity ("Reg. SCI") requires reporting pursuant to 17 C.F.R. §§ 242.1002, 242.1003*; see also* 16 C.F.R. part 318.
40. Moreover, voluntary reporting expectations articulated in industry best practice or law enforcement, CISA, or SRMA guidance may add additional, unique data elements that reporting entities are strongly encouraged to include due to the mission needs to the particular receiving entity. Such voluntary reporting expectations should also be considered in future harmonization efforts.
41. *See, generally* Computer Security Incident Notification Rule: (OCC) 12 C.F.R. part 53; (FRB) 12 C.F.R. 225 Subpart N; (FDIC) 12 C.F.R. Part 304, subpart C (Computer Security Incident Rule): No specific information is required in the notification other than that a notification incident has occurred. The notification requirement is intended to serve as an early alert to a banking organization's primary Federal regulator about a notification incident. The agencies anticipate that banking organizations will share general information about what is known at the time of the incident.
42. 48 C.F.R. § 252.204-7012; 45 C.F.R §§ 164.400 to 164.414; 21 C.F.R. part 803 (medical device reporting).
43. 17 C.F.R. §§ 242.1002, 242.1003.

discussed in the prior section, the specific information that must be reported varies across these systems. Other agencies accept email messages, mail, fax, or phone communications to receive cyber incident reports in narrative form without any required format.

The diversity in reporting mechanisms increases the challenges associated with normalizing and analyzing data that is reported and harmonizing the reporting process across the Federal Government. In engagements with DHS, industry representatives asserted that the inability to easily submit information to the Federal Government via a single channel or consistent mechanism often adds to the burden and challenges faced by reporting entities during a time of crisis. On the other hand, entities may prefer having multiple options for reporting during a crisis because their systems might be down, thus the ability to submit via traditional means of communication (i.e., phone, unstructured email messages, fax, or mail) may be necessary.

Procedural and Resource Burdens

In addition to the substantive deviations among current regulatory regimes discussed above, there are several other factors that will challenge agencies' abilities to harmonize Federal incident reporting requirements. As a general matter, for agencies to adopt new or amend existing rules, the Administrative Procedure Act typically requires that agencies issue an NPRM, receive public comment, and issue a new or revised final rule.[44] In working group discussions, multiple CIRC agencies raised concerns about the potentially significant resource commitment associated with the process of updating rules. In the communications sector, for example, changing the current network outage reporting requirements to specifically address cyber incidents would require notice-and-comment rulemaking. Similarly, the USCG incident reporting requirements are derived from non-cyber specific authorities. Any effort to harmonize reporting requirements, including the definition of reportable cyber incidents or the timeline and triggers for reporting, could require an amendment to the broader regulatory regimes of these agencies.

There would similarly be resource implications associated with efforts to harmonize, or potentially centralize, cyber incident reporting mechanisms. Many agencies have invested in their own incident reporting portal or are still leveraging email or phone systems to report incidents. Movement toward a common incident reporting mechanism or to better align the content submitted through existing processes would have resource implications. Agencies willing to modify current reporting mechanisms would also likely need to comply with the Paperwork Reduction Act (PRA), which typically requires an application process and clearance from the Office of Management and Budget (OMB) prior to collecting information from the public. Several agencies identified challenges associated with updating their cyber incident reporting requirements in the context of the PRA.

Long-term maintenance of harmonized reporting mechanisms and updated requirements over time would also requires an ongoing interagency process and close coordination. Coordination and sufficient resources are required to ensure appropriate and consistent security controls to protect the sensitive data included with incident reports, especially if such information is going

44. In limited cases, such as the TSA Administrator's authority under 49 U.S.C. 114(l) to take action for an emergency requiring immediate action, agencies may have specific authorities that allow deviation from the Administrative Procedure Act.

to be aggregated. Increasing the security of Federal Government systems continues to be a priority for Federal agencies. The Federal Information Security Modernization Act of 2014 (FISMA) emphasizes the importance of risk management across Federal agencies, contractors and other sources that use or operate a federal information system.[45] FISMA requires agencies to develop and implement a risk-based approach to manage information security risk. Additional requirements for Federal agency cybersecurity—including multi-factor authentication and encryption—were included in Executive Order 14028.[46] Any cyber incident reporting efforts, including the implementation of new reporting requirements or harmonized means of collecting, sharing, and retaining reported information, must include appropriate cybersecurity protections that address evolving risks.

Legal Barriers and Limited Agency Authorities

In addition to these procedural and resource constraints, Federal agencies may not in some cases be able to make the changes necessary to bring their requirements into harmony with other agencies due to statutory and other legal constraints. For example, several agencies impose requirements to report cyber incidents with national or economic security implications in as little as 24 hours. CIRCIA, however, creates a reporting timeline of 72 hours for covered entities to report covered cyber incidents to CISA. CIRCIA may thus present a challenge to full alignment of reporting timelines for agencies that require reporting in less than 72 hours, although this can be potentially mitigated through the interagency agreements that enable the sharing of substantially similar reports. The HIPAA Breach Notification Rule is similarly based on a statutorily-established reporting timeline, which may constrain the ability of Federal agencies to harmonize incident reporting requirements absent legislative action.

In discussions among CIRC members, certain agencies indicated that lack of authority to collect or share certain information may be another potential legal barrier to eliminating reports to multiple agencies. Use of a model reporting form with common data fields to address the information needs of all agencies with incident reporting requirements is one way to reduce the need for reporting to multiple agencies. As discussed below, such an approach ensures that reporting to one agency will address most, if not all, relevant Federal Government needs. If some agencies lack legal authority to collect all the data fields included in the model reporting form, however, then the Anti-Deficiency Act (ADA) might preclude their ability to use the model form without redactions or leverage an incident report provided to another agency. Agencies may also be subject to statutory or regulatory restrictions on the sharing or onward sharing of certain non-public information. In such cases, agencies who receive information about an incident may not be able to pass that information to another agency if that agency has a legitimate regulatory or other operational need to receive the same information. Some agencies may thus be left with no alternative than to continue to require duplicative reporting through separate mechanisms and different data elements.

Another potential legal barrier to harmonization raised in discussions among CIRC members and with external stakeholders is inconsistency in current information protection regimes. Entities

45. Federal Information Security Modernization Act of 2014 (Pub. L. No. 113-283). The original FISMA was Federal Information Security Management Act of 2002 (Pub. L. No. 107-347, tit. III), in the E-Government Act of 2002.
46. Executive Order 14028, Improving the Nation's Cybersecurity (May 12, 2021).

frequently raise concerns about how information that they report to one or more agencies following a cyber incident will be protected from disclosure or impermissible use by Federal agencies. On the other hand, agencies with regulatory responsibilities expressed concern that the Federal Government's receipt of information through channels subject to legal restrictions on further use of the information received for regulatory or enforcement purposes significantly limits their ability to take appropriate and timely action to protect public safety, national security, and other important government interests.

While CIRCIA provides certain legal protections for information submitted to CISA, there are not consistent protections from public disclosure of information about cyber incidents submitted to the Federal Government under other regimes. Nor are there universal restrictions on how agencies may use information about cyber incidents that has been reported or otherwise shared with them. Reporting entities may find that the same information is subject to different information protections or use limitations when submitted to multiple agencies and that the protections they receive may be dependent on the agency to whom they opt to submit the report.

V. CISA Efforts to Facilitate Harmonization

Consistent with the requirements in CIRCIA, CISA will continue to engage in three lines of efforts to facilitate harmonization of duplicative reporting requirements: (1) participating in the CIRC to help the Council fulfill its mission; (2) performing extensive outreach with Federal and non-Federal entities to inform the forthcoming CIRCIA NPRM; and (3) exploring opportunities with Federal entities to minimize the burden on entities who report substantially similar information as part of an existing reporting requirement, where feasible.

CISA has actively participated in the CIRC to help identify potential approaches to harmonizing Federal cyber incident reporting requirements and to support the identification of best practices that could be considered by CISA and other Federal agencies as they develop or update their respective cyber incident reporting regimes.

The CISA Director is responsible for developing and implementing regulations pursuant to CIRCIA that will require covered entities to report to CISA covered cyber incidents and ransom payments resulting from a ransomware attack. The reports submitted pursuant to the final rule, once effective, will allow CISA to strengthen national security, including through rapidly deploying resources and rendering assistance to victims experiencing a covered cyber incident, analyzing incoming reporting across sectors to spot trends, and then quickly sharing that information to warn other potential victims.

CISA is committed to giving stakeholders from across the spectrum – including Federal, SLTT, and private sector entities, as well as the public at large – the opportunity to provide inputs throughout the rulemaking process. These public engagements have the potential to significantly reduce the likelihood that CISA's rulemaking will contribute to duplicative reporting requirements. Accordingly, CISA has sought public feedback to inform its proposed regulations to implement CIRCIA. CIRCIA requires CISA to develop and publish an NPRM and open it for public comment. In advance of that effort, CISA issued a Request for Information soliciting public input on approaches to implementing the cyber incident reporting requirements on September 12, 2022. The comment period for that request closed on November 14, 2022. In addition to providing an opportunity to submit written comments at the outset of its rulemaking process, CISA also held a series of public listening sessions across the country to receive input from stakeholders. Further, as part of its development of the NPRM, CISA has engaged in a series of consultations with all Federal agencies that possess current or proposed cyber incident reporting requirements. During these engagements, CISA has sought to learn about these existing and proposed regulatory regimes and discuss areas where CISA and its regulatory counterparts might want to align their respective regulations. In the coming months, CISA will work to ensure the NPRM reflects the feedback received and outlines an approach for prospective cyber incident and ransom payment reporting requirements.

CISA also recognizes that Congress included in CIRCIA a means to reduce duplicative reporting through the statutory provisions related to the reporting of "substantially similar information" to another Federal agency. CISA is committed to exploring opportunities with its Federal counterparts to take advantage of this statutory provision to minimize burden on regulated entities, where feasible.

VI. Recommendations to Streamline and Harmonize Cyber Incident Reporting

A review of current Federal cyber incident reporting requirements and discussions among CIRC members have highlighted several opportunities for the Federal Government to harmonize cyber incident reporting requirements, streamline reporting processes, and reduce current and future regulatory burdens upon reporting entities. Harmonization could be advanced by focusing upon several key actions to provide reporting entities with increased predictability, common understanding, and simplicity in their primary interactions with the Federal Government. As discussed above, efforts of the CIRC have focused on recommendations related to defining reportable cyber incidents, clarifying the timing and "triggers" for reporting, leveraging common data elements or a model form for cyber incident reports, and developing mechanisms for reporting.

The following recommendations, if adopted by Federal agencies, could help streamline and harmonize Federal cyber incident reporting.[47] SLTT and foreign governments could also consider several of these recommendations to further harmonize reporting requirements across the larger incident reporting ecosystem.

Recommendation 1: The Federal Government should adopt a model definition of a reportable cyber incident wherever practicable.[48] Federal agencies should evaluate the feasibility of adapting current and future cyber incident reporting requirements to align to a model definition of a reportable cyber incident.

Many current and proposed cyber incident reporting regimes use different definitions of reportable cyber incidents. There are, however, commonalities across those definitions that can serve as a foundation for harmonization. The CIRC identified several recommended practices used by Federal agencies for defining a reportable cyber incident. For example:

- Definitions of reportable cyber incidents should preserve flexibility and strive for applicability across as many sectors as practicable in determining impact or potential impact.
- Definitions of a reportable cyber incident should, whenever relevant, address requirements related to national security, economic security, and public safety, as well as consumer protection, and privacy.
- Definitions of a reportable cyber incident should include language to indicate that a cyber incident that is still under investigation by a reporting entity is reportable. This language will encourage timely reporting by reducing a regulated entity's concern that it must gather all relevant information prior to submitting a report.
- Definitions of a reportable cyber incident should explicitly exclude any lawfully executed activities of the U.S. government, such as those undertaken pursuant to a warrant or other judicial process.

47. While these recommendations were closely coordinated with the CIRC, they represent the recommendations of the Secretary. Consistent with the CIRC Charter, these recommendations are not binding on CIRC members. Executive Branch and independent regulatory agencies should consider adopting these recommendations to the extent they are practicable and consistent with their statutory mandates. As noted in footnote 2, this report and the recommendations in this section do not reflect any final decision regarding the content of ongoing or future DHS rules.
48. There may be several factors impacting the practicality of federal agencies fully implementing these recommendations, including statutory or legal limitations, countervailing policy considerations, or unique considerations related to the purpose of a particular agency's reporting requirement.

- Agencies should consider excluding the required reporting of data breach incidents when potentially compromised data is adequately encrypted or disassociated so that the information cannot be used, and such encryption or data disassociation has not been compromised. If the agency chooses to exclude such required reporting, the agency should determine what encryption or other technology is considered adequate consistent with evolving security risks and cryptographic capabilities.[49]

Based on these recommended practices, CIRC members developed the following model definition that could be used for reportable cyber incidents. In adopting this model definition, Federal agencies may choose to incorporate some or all the sub-elements based on their authorities and specific mission responsibilities.

> *Model Definition of a Reportable Cyber Incident*[50]
>
> *A reportable cyber incident is a cyber incident that leads to, or, if still under the covered entity's investigation, could reasonably lead to any of the following:*
>
> > *(1) a substantial loss of confidentiality, integrity, or availability of a covered information system, network, or operational technology;*
> > *(2) a disruption or significant adverse impact on the covered entity's ability to engage in business operations or deliver goods, or services, including those that have a potential for significant impact on public health or safety or may cause serious injury or death;*
> > *(3) disclosure or unauthorized access directly or indirectly to non-public personal information of a significant number of individuals; or*
> > *(4) potential operational disruption to other critical infrastructure systems or assets.*
>
> *The term "reportable cyber incident" includes, but is not limited to, indications of compromises of information systems, networks, or operational technologies of customers or other third parties as well as a business or operational disruption caused by a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider. The term "reportable cyber incident" does not include: (i) any lawfully authorized activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States, including activities undertaken pursuant to a warrant or other judicial process; (ii) any event where the cyber incident is perpetrated in good faith by an entity in response to a specific request by the owner or operator of the information system; or (iii) the threat of disruption as extortion, as described in CIRCIA section 2240(14)(A).*

49. For example, the HIPAA Breach Notification Rule (45 C.F.R §§ 164.400-414) requires the reporting of breaches of "unsecured protected health information." "Unsecured protected health information" is described as "protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary [of the Department of Health and Human Services] in guidance." *See* https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (Accessed 30 January 2023).

50. While this report recommends a model definition for a reportable cyber incident, some Federal agencies have adopted the National Institute for Standards and Technology (NIST) definition for a "Computer-security incident" (*See reference to the* NIST Glossary *at* https://csrc.nist.gov/glossary/term/computer_security_incident or "Cybersecurity incident" (*See reference to the* NIST Glossary *at* https://csrc.nist.gov/glossary/term/cybersecurity_incident). While this recommendation does not seek to define "cyber incident" separate from a "reportable cyber incident," it seeks to harmonize the thresholds and impacts that determine which incidents are reported to the Federal Government.

Note: In adopting this model definition of a reportable cyber incident, Federal agencies may choose to incorporate or tailor some or all of sub-elements (1) through (4) above, including, to ensure consistency with their statutory mandates. Federal agencies will also need to independently determine within their rules what constitutes a "covered entity," a "covered information system," and a "significant" number of impacted individuals.

CIRC members recognized that the model definition should, to the extent practicable, be considered for adoption in current and future incident reporting regimes.

Recommendation 2: **The Federal Government should adopt model cyber incident reporting timelines and triggers wherever practicable. Federal agencies should evaluate the feasibility of adapting current and future cyber incident reporting requirements to align to model timeline and trigger provisions.**

To improve harmonization of cyber incident reporting, Federal agencies should align requirements for when entities must file cyber incident reports and identify the "triggers" that elicit such a requirement, i.e., "start the clock" on the obligation to report consistent with the agency's need for information. As previously discussed, the variance in current reporting timelines is largely driven by the different purposes behind various incident reporting requirements and differing risk profiles across the critical infrastructure sectors. Of note, CIRCIA creates a reporting timeline of 72 hours for covered entities to report covered cyber incidents to CISA. Other Federal agencies have determined that certain incidents necessitate a shorter reporting timeline. For instance, the requirement to report cyber incidents in the Nuclear Reactors, Materials, and Waste Sector depends upon the severity of impact resulting from the cyber incident and can range from one hour to eight hours based on factors set forth in regulation.[51] DOE also has a one hour timeline after the determination of a Reportable Cyber Security Incident.[52] TSA has adopted a 24-hour timeline to report cyber incidents involving unauthorized access of an information or operational technology system, the discovery of malicious software, activity resulting in a denial of service, or which results in an operational disruption or the potential to cause impact on a large number of customers/passengers, critical infrastructure, core government functions, or otherwise impacts national security, economic security, or public safety.[53] In addition to NRC and TSA, SEC requires immediate reporting for any designated SCI entity upon any responsible SCI personnel having a reasonable basis to conclude that an SCI event has occurred.[54]

In cases involving consumer protection and privacy considerations, on the other hand, longer timelines may be appropriate, especially where the number of victims is small and an entity needs time to evaluate the scope of compromised information. These reporting timelines should, however, take into consideration the potential national security, economic security, or safety concerns related to high-risk scenarios or the theft of bulk personal data, especially where consumer information of some sensitivity or health information is involved. Agencies should also consider consumers' interest in timely knowing if their information has been compromised

51. *See generally* 10 C.F.R. § 73.77(a), establishing one-, four-, and eight-hour reporting deadlines depending on the severity of the incident.
52. *See supra* note 28.
53. This requirement applies to higher-risk rail operations (freight and passenger), higher-risk rail transit systems, critical pipeline systems and facilities, and certain aviation operations. TSA has issued recommendations to other owner/operators.
54. 17 C.F.R. § 242.1002.

and the importance of affording them opportunities to protect themselves from harm that could follow the incident.

CIRC members identified the following recommended practices to improve and streamline timelines and triggers for the reporting of cyber incidents:

- Agencies with requirements related to national and economic security and safety may require reporting in less than 72 hours, especially where incidents may affect NCFs or the delivery of vital goods and/or services to customers or the public.
- Agencies with requirements related to consumer protection and privacy may adopt a more flexible timeline for reports to the Federal Government if the *only* impact of a cyber incident is the compromise of personal information, although any such prolonged timelines should account for the number of impacted individuals, the potential national or economic security concerns regarding the bulk theft of personal information, and the ability of individuals to mitigate harm from disclosure of their personal information.
- Agencies should, where practicable, use objective criteria and avoid subjective criteria to describe when a reporting obligation is triggered to avoid ambiguity concerning when an obligation to report is incurred and support more timely reporting.
- Timelines for notification to affected individuals or the media (as opposed to the Federal Government) should enable the entity to first determine the incident's full impact and identify individuals that must be notified, as well as any SLTT agencies to whom covered entities must report.

Based on these recommended practices, CIRC members developed the following model timeline and trigger provisions that could be used for reporting cyber incidents. In adopting this model timeline and trigger provision, Federal agencies may choose to incorporate some or all the models' features based on the agencies' authorities and specific mission responsibilities.

> *Model Timeline and Trigger Provisions for Reporting Reportable Cyber Incidents.*
>
> *A covered entity that experiences a reportable cyber incident shall submit an initial written report to the required agency or agencies within 72 hours of when the covered entity reasonably believes that a reportable cyber incident has occurred.*
>
> *Note: For incidents that may disrupt or degrade the delivery of national critical functions or the reporting entity's ability to deliver vital goods or services to the public, or impact public health or safety, agencies may require covered entities to submit an initial report to the required agenc[ies] within less than 72 hours.*
>
> *Note: For incidents that involve the loss of personal information without further impact on business operations, agencies may include a timeline longer than 72 hours. Such a requirement should consider the potential national or economic security implications of the loss of personal information and the ability of individuals to mitigate harm from the compromise of their information.*

CIRC members also recognized that the model timeline and trigger should, to the extent practicable, be considered for adoption in current and future incident reporting regimes.

Recommendation 3: Agencies with requirements for covered entities to provide notifications to affected individuals or the public should consider whether a delay is warranted when such notification poses a significant risk to critical infrastructure, national security, public safety, or an ongoing law enforcement investigation.[55] A decision to delay the notification to affected individuals or the public would not delay required notification to regulators.

In reviewing existing regulations and laws, the CIRC observed that most existing laws and regulations requiring public disclosure of certain types of cyber incidents allowed for a covered entity to delay disclosure at the request of an appropriate law enforcement official who determined that the disclosure could impede a criminal investigation or cause damage to public safety or national security.[56] There could be cases in which a disclosure could prematurely tip off criminals that their criminal activity has been detected or enable copy-cat malicious activity. Agencies should, where practicable, consider an option for delaying public disclosure at the request of the Attorney General, the Secretary of Homeland Security, or appropriate law enforcement official. Regulations may require a covered entity to report to appropriate U.S. regulatory agencies such a request for a delay and provide for subsequent discussion on the timing and nature of public disclosure.

Model language, based on existing regulations and laws can be adapted to fit the context of a particular cyber incident disclosure rule:

> *Model language for delayed public notification*
>
> *(a) Public disclosure required by this regulation may be delayed when the Attorney General, Secretary of Homeland Security, or an appropriate law enforcement official informs a covered entity that public disclosure required by this regulation would pose a significant risk of impeding or compromising an ongoing or potential criminal investigation or cause damage to public safety, national security, or critical infrastructure. Such risk includes the potential for an adverse result, as provided by 18 U.S.C. § 2705(a)(2), or an emergency situation, as provided by 18 U.S.C § 3125(a)(1). If a delay longer than 30 days is needed, it must be specified in a written statement provided to the covered entity.*
>
> *(b) The Attorney General, Secretary of Homeland Security, or an appropriate law enforcement official shall inform the covered entity of the duration of the delay requested under paragraph (a) and may extend the period of delay for additional periods of up to 30 days if that official determines that disclosure continues to pose a significant risk in accordance with paragraph (a). The covered entity may notify appropriate U.S. regulatory agencies of such a request for delay.*

55. In some circumstances, immediately making information or data concerning a cybersecurity incident readily accessible and available could result in increased risks to affected entities or interfere in an ongoing criminal investigation. Such non-confidential disclosures (described as "public disclosures") should be coordinated with appropriate law enforcement officials.

56. *See, e.g.*, 45 C.F.R. § 164.412; 47 C.F.R. § 64.2011(b)(3), 12 C.F.R. part 30. App. B, supp. A (OCC); 12 C.F.R. part 208 app. D-2, supp. A, 12 C.F.R. part 225, app. F, supp A (FRB); 12 C.F.R. part 364. App. B, supp. A (FDIC).

Recommendation 4: The Federal Government should adopt a model reporting form for cyber incident reports wherever practicable. Agencies should evaluate the feasibility of leveraging the model form for cyber incident reporting or incorporate the data elements identified therein into reporting forms, web portals, or other submission mechanisms.

Current incident reporting requirements are driven by the mission needs of relevant agencies and the purpose of the reporting regime. Reporting requirements targeting particular sectors or focused on national security, economic security and public safety tend to focus on impact of the incident and characteristics of the attack. Reporting requirements driven by consumer protection and privacy considerations tend to include consumer-centric elements and information about notifications and assistance to affected consumers.

CIRC member agencies recognized that a model reporting form and/or common data elements could be used to simplify existing reporting regimes by standardizing the information that entities are required to report across incident reporting regimes. Such a form or common data elements can also potentially provide reporting entities subject to multiple requirements with a unified mechanism to submit a single report containing information sufficient to satisfy multiple reporting requirements. In coordination with CIRC members, DHS developed a model reporting form and template, which is included as Appendix E for a model reporting form that can further inform harmonization efforts. This model reporting form could, to the extent practicable, serve as the basis for initial reports, supplemental updates, and final reports to the Federal Government.[57] The model reporting form and associated data elements can be implemented in a variety of ways—including a fillable form, web portal, or even a list of questions for an oral report.

Such a form could standardize much of the reporting process without supplanting initial "fact-of" notifications, detailed engagements between supervisory regulators and the regulated community, or other existing channels of communications essential to the overall regulatory relationship. Indeed, CIRC members recognized that some agencies may have unique mission-driven needs to obtain additional types of information not contained in the model reporting form or conduct follow up inquiries to assess impacts of an incident or support a supervisory regime. Some Federal agencies may opt to add additional modules to seek additional information not included in the model form if needed to meet the regulatory or oversight requirement of that agency. For example, agencies with all-hazards reporting requirements that receive both cyber and non-cyber reporting could, for example, (1) leverage the model form for cyber incidents and maintain their existing reporting mechanism for non-cyber incidents or (2) incorporate the identified cyber incident data elements into an integrated all-hazards reporting form, portal, or other web submission mechanism, potentially developing a cyber-specific "Part B" module using the data elements from the model form. Other agencies may only have authority to collect some of the data elements included in the model reporting form. Agencies that only have authority to collect a subset of data elements or choose to do so as a matter of policy could incorporate those elements into a customized submission mechanism. The model form can be adapted to meet specific agency needs and use of a model form could also help to address concerns about multiple agencies needing to take separate and independent steps to update incident reporting under the PRA. In any case, harmonizing the reporting forms and data elements would help to facilitate data sharing and analysis across the Federal Government.

57. *See supra* note 2.

The model reporting form and data elements could also serve as an example for SLTT and foreign governments, which could spur additional cyber incident reporting harmonization across governments and jurisdictions.

Recommendation 5: The Federal Government should assess how best to streamline the receipt and sharing of cyber incident reports and cyber incident information, including through improvements to existing reporting mechanisms or the potential creation of a single portal.

Currently, an entity that suffers a cyber incident may submit similar reports to multiple Federal agencies via multiple mechanisms and systems. While development of a model reporting form or common data elements may help reduce duplication, depending on the source and destination of the reporting, there may be legal limitations on the ability of certain Federal agencies to fully share information from incident reports across the Federal Government.

The Federal Government should assess how reporting entities may best provide cyber incident information to the Federal Government, how relevant agencies should receive the information, and how such information can be shared across the Federal Government with those agencies that need it. Such a study could assess the feasibility of establishing a single portal or network of interconnected portals (an information technology system or multiple interconnected systems) to allow the entity to submit key information to appropriate agencies in an efficient manner. If feasible, such a mechanism could also help the Federal Government better deconflict incident information reported to multiple agencies and avoid problems associated with comparing incident data that has been provided to multiple agencies at different points in time. Better integration of incident reports could also support better automated analysis and help the Federal Government better connect the dots and more rapidly analyze trends in incidents across the ecosystem.

The assessment should consider how the various potential information sharing arrangements would be responsive to competing needs of regulators, SRMAs, law enforcement, and other agencies who receive mandatory and voluntary cyber incident reports. The assessment should also consider other advantages and disadvantages of a single portal or other means to reduce duplication and confusion, including necessary security measures to ensure the confidentiality and integrity of the reported information in the aggregate. The assessment should also consider the policy and technical feasibility of implementing controls to ensure that access to reports is limited to agencies and personnel with a legitimate need for the information and how anonymized information could potentially be shared more broadly with other agencies, ISACs, ISAOs, and others in the cybersecurity ecosystem who can use the information to increase overall cybersecurity and resilience. Finally, the assessment should consider how cyber incident reports fit into broader incident reporting schema within different sectors, including for Federal agencies who maintain all-hazards incident reporting regimes.

Recommendation 6: Federal cyber incident reporting requirements should allow for updates and supplemental reports.

The CIRC discussed how incomplete information and rapidly evolving circumstances during the early phases of detection and incident response can present challenges to timely reporting for reporting entities. A reporting entity's understanding of an incident is likely to evolve, and initial reporting can be incomplete or inaccurate due to limited information. Given this uncertainty, agencies can take steps to facilitate timely reporting by clarifying which data fields the agency considers essential for initial reports and which can be provided in an update or supplemental report.

Federal agencies should permit—and sometimes require—reporting entities to supplement or update their initial report if new, significant information about the incident is discovered. Federal agencies should also consider permitting entities to request to withdraw or archive a report if the entity and agency subsequently agree that the event did not meet the agency's definition of a reportable cyber incident. Such flexibility is important for reporting entities, who often file initial reports amidst the uncertainty of a developing situation with limited resources to respond to the cyber incident and manage its reporting obligations. Federal agencies should also underscore the value of a timely initial report based on incomplete or evolving information as compared with a delayed incident report that impedes the rapid development of situational awareness among relevant Federal agencies. Agencies also benefit from the updated situational awareness as the reporting entity increases its understanding of the incident.

Reporting entities who timely supplement their initial report to include newly discovered information should generally not be punished for incomplete or ultimately incorrect initial reports (assuming no intent to mislead, omit, neglect, or other illicit purpose).

Recommendation 7: The Federal Government should adopt common terminology regarding cyber incident reporting wherever practicable. Agencies should evaluate the feasibility of leveraging a common lexicon for initial, supplemental, updates, and final reports.

To further harmonize incident reporting efforts, there is benefit in the Federal Government adopting common terminology around the use of terms like "Initial Report" and what constitutes an update or supplemental report. There is currently some variation in how agencies refer to initial and other reports. For example, the OCC, FDIC, and FRB refer to incoming reporting by covered entities as a notification because the initial submission may be verbal, and a written report is not required. The goal of the initial notification is to provide the agencies with an early alert that there is a problem. Generally, such agencies rely on follow-up conversations to garner specific details and updates. Other agencies use "notification" in reference to notifications to the media, the public or individuals affected by some data breach or safety risk. Any harmonization effort should include the adoption of common terminology for the sake of mutual understanding and to facilitate consistent communication with the regulated entities. Appendix F provides a model for common terminology and types of reports.

Recommendation 8: The Federal Government should improve processes for engaging with reporting entities following the initial report of a cyber incident. Agencies should coordinate among themselves, whenever practicable, prior to engaging with a reporting entity to reduce the burden on the reporting entity.

Following a cyber incident, particularly one that may trigger coordination under Presidential Policy Directive 41, Federal agencies should coordinate their engagement with the reporting entity. Coordination between SRMAs, regulators, Federal law enforcement and CISA is important for effective communications with the affected entity and to avoid duplicative or uncoordinated outreach following an incident. While there are legitimate needs for multiple Federal agencies to contact reporting entities (e.g., performing independent regulatory oversight and incident response functions, requests for supplemental information about the incident, offers of assistance and other resources, or support for an ongoing investigation), uncoordinated Federal outreach from multiple agencies following an incident can introduce the potential for confusion, undue burden, or even distracting reporting entities that are in the midst of a crisis from effective risk and consequence management. During this time of increasing reporting requirements, the Federal Government must manage its own external communication with entities amid a crisis while fulfilling its governmental obligations.

VII. Proposing Legislative Changes

CIRCIA directs DHS to include in this report any proposed legislative changes necessary to address duplicative reporting to inform what additional authorities could be authorized in future congressional action. Based on deliberations of the CIRC and engagements with other stakeholders, DHS has identified the following proposals that Congress may consider to address duplicative reporting requirements and further facilitate harmonization and streamlining of Federal cyber incident reporting requirements. These proposals are aimed at a range of policy goals, including reducing the burden of reporting on the private sector, protecting information submitted to the Government, and removing legal barriers to alignment of regulatory requirements by Federal agencies.

LC 1: Congress should remove any legal or statutory barriers to harmonization identified by the CIRC, including authorizing adoption of the model definitions of a reportable cyber incident, timeline and trigger provisions, and cyber incident reporting form and/or common data elements for current and future Federal cyber incident reporting requirements.

As discussed in the recommendations above, there are potentially significant benefits from the Federal Government's adoption of a model definition, timing and trigger provisions, and incident reporting form or common data elements. Implementation of model definitions, timelines, and triggers could reduce the burden on reporting entities amid a crisis by providing consistency in their reporting obligations. And—whether implemented through a fillable form, online submission system, or other mechanism—CIRC members also agreed that a model form and/or use of common data elements may help simplify reporting, increase Federal Government visibility into incidents, and support increased analysis of incidents and trends.

Although progress toward harmonization can be made under existing regulatory authorities, there may be legal or statutory obstacles to agencies' adoption of the model provisions and forms developed by the CIRC. Although this proposal does not seek to mandate the adoption of a model definition, timing and trigger provisions, or particular incident reporting form, Congressional action may nevertheless be necessary to address current statutory limitations or otherwise remove legal barriers to agencies adopting these models consistent with mission needs and the overall goal of regulatory harmonization. Certain agencies have indicated, for example, that they may lack sufficient authority to collect all the data elements included in the model form developed by the CIRC. The statutory underpinning of certain regulatory regimes may also impose limitations on how agencies collect incident-related information, use that information for regulatory or enforcement purposes, and take appropriate and timely action to protect public safety, national security, and other important government interests. Finally, there may be budgetary or resource limitations that agencies may have to overcome to adopt a new cyber incident reporting form or mechanism. To address these barriers or other barriers that may prevent adoption by certain agencies of model provisions or forms developed by the CIRC, Congress may consider legislation, for example, that authorizes agencies to align their regulatory requirements to CIRC recommendations notwithstanding other provisions of law. Such an authorization will permit Federal agencies to assess any statutory, legal, or policy challenges to adopting the recommendations for harmonization. The CIRC will continue to assess the

significance of these potential barriers and the need for legislation as individual Federal agencies evaluate the practicality of adopting the recommendations above and incorporating input from ongoing rulemaking efforts by CISA and other agencies.

LC 2: Congress should provide authority and funding, as requested by the Administration, to Federal agencies to enable them to collect and share common cyber incident data elements that may not otherwise be authorized.

Current statutory and regulatory authorities limit the information that Federal agencies can collect from reporting entities, and agencies raised significant legal concerns with the prospect of collecting and storing information via a common form that an agency otherwise lacks authority to collect. New legislation that authorizes agencies to collect and share with each other "common data elements" will assist in harmonizing the information that Federal agencies may collect in their cyber incident reports. Any authorization to broaden Federal agency collection and sharing of cyber incident data should carefully consider any privacy, civil rights, and civil liberties implications.

LC 3: Congress should exempt from disclosure under FOIA, or other similar legal mechanisms, cyber incident information reported to the Federal Government and protect any relevant privileges.

Reporting entities frequently raise concerns about what will happen with information that they report to one or more agencies following a cyber incident. When subject to multiple reporting requirements, reporting entities may find that information submitted to one agency is subject to different information protections than for the same information submitted to another agency. Better clarity around the applicability of the FOIA and other information protections to incident-related information submitted to the Federal Government will encourage timely reporting of cyber incidents. Congress should consider an approach based on CIRCIA, which provides that reports submitted in accordance with the statute shall be exempt from disclosure under Exemption 3 of FOIA, and have protections for privileged information.[58] Congressional action could thus exempt cyber incident related information provided to any Federal Government agency under a mandatory or voluntary reporting regime from public disclosure by the Federal Government in response to FOIA or other legal mechanisms, such as compelled disclosure in litigation. These protections should not, however, impact separate regulatory requirements regarding public disclosure of cyber incidents in the ordinary course consistent with the model timelines and triggers discussed above, or impact existing disclosure practices related to incidents impacting public health or safety.

58. 6 U.S.C. § 681e.

VIII. Next Steps and Conclusion

The efforts of the CIRC are at the beginning, not the end. This report represents a key snapshot into the early efforts of the CIRC and its member agencies. The recommendations and proposed legislative changes discussed above present a roadmap to enhance alignment and harmonization of Federal cyber incident reporting requirements. But as individual agencies assess the feasibility of implementing the various recommendations, the CIRC will continue to learn from feedback from stakeholders and input into various pending or contemplated rulemaking efforts. The efforts of the CIRC and individual agencies can be informed by and evolve based on that feedback.

On behalf of the Department, the DHS Office of Strategy, Policy, and Plans will continue to leverage the CIRC to serve as the Executive Branch's forum to coordinate, deconflict, and harmonize Federal cyber incident reporting requirements and regimes. As next steps, the CIRC will support agencies' efforts to assess the feasibility of adopting the various recommendations included in this report, including the adoption of model definitions; timing and trigger provisions; and model reporting form and/or common data elements. Where possible, the CIRC will support the adoption of those models by Federal agencies, including efforts to update associated policies, guidance, or regulatory text. With respect to the model cyber incident reporting form, individual CIRC members can evaluate how they may leverage the model reporting form or incorporate the data elements within their cyber incident reporting requirements. The CIRC will also work with Federal agencies to identify specific statutory or legal limitations that will have to be overcome to achieve harmonization. The CIRC will categorize the identified policy, statutory, legal, and budgetary impediments to harmonization to inform future deliberations among CIRC members and for additional Executive Branch or congressional consideration.

Pursuant to Section 104 of CIRCIA, the CIRC will also support CISA efforts to periodically review regulatory requirements and ensure that reporting requirements and procedures avoid unnecessarily duplicative, conflicting, or burdensome requirements. The CIRC will similarly support CISA's coordination with Federal partners and regulatory authorities to streamline reporting processes and facilitate interagency agreements to permit sharing of cyber incident reports where feasible and consistent with applicable law and policy.

In addition to stewarding efforts to enhance harmonization of Federal incident reporting requirements, the CIRC will maintain and expand engagement with SLTT and foreign governments to assess how Federal harmonization efforts can support broader efforts to streamline and harmonize requirements across the global ecosystem.

Through the CIRC, DHS is prepared to lead a Federal whole-of-government approach to reduce complexity, diminish regulatory overlap, and reduce duplication. This will include continuous work to review and update the Federal cyber incident reporting requirements as the cyber threat environment evolves. DHS will coordinate closely with agencies on the efforts highlighted in this report and keep Congress apprised of their implementation and developments.

Appendix A: CIRC Member Agencies

The CIRC included membership from 33 Federal departments and agencies.

Commodity and Futures Trading Commission
Consumer Financial Protection Bureau
Cybersecurity and Infrastructure Security Agency
Department of Agriculture
Department of Commerce
Department of Defense
Department of Energy
Department of Health and Human Services
Department of Homeland Security
Department of Justice
Department of Transportation
Department of the Treasury
Environmental Protection Agency
Federal Bureau of Investigation
Federal Communications Commission
Federal Deposit Insurance Corporation
Federal Energy Regulatory Commission
Federal Housing Finance Agency
Federal Reserve Board
Federal Trade Commission
General Services Administration
National Credit Union Administration
National Security Council
Nuclear Regulatory Commission
Office of Management and Budget
Office of the Comptroller of the Currency
Office of the National Cyber Director
Securities and Exchange Commission
Small Business Administration
Transportation Security Administration
United States Coast Guard
United States Food and Drug Administration
United States Secret Service

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
General Services Administration (GSA)	National Industrial Security Program Operating Manual (In Effect) (FAR subpart 4.4 & 52.204-232, C.F.R part 117) (32 C.F.R 117.8)	Applicable Federal Contractors	Requires applicable contractors to report cyber incidents.	Not specified
GSA	Basic Safeguarding of Covered Contractor Information Systems (In Effect) (FAR subpart 4.19 & 52.204-21(b)(xii))	Applicable Federal Contractors	Requires applicable contractors to identify, report, and correct information and information system flaws.	Timely manner

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
GSA	NARA CUI Program (32 C.F.R 2002) and OMB M-17-12 (Reporting PII incidents) FAR case 2017-017 (Proposed) The status of this proposed rule is located here: https://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf	Applicable Federal Contractors	Requires applicable PII incidents to be reported and the NARA CUI program requires applicable CUI incidents to be reported.	1 hour
GSA	Cyber Threat and Incident Reporting and Information Sharing FAR case 2021-017 (Proposed) The status of this proposed rule is located here: https://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf	Applicable Federal Contractors	Sharing of information about cyber threats and incident information and reporting cyber incidents.	None specified

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
Department of Transportation (DOT)	Assigning, maintaining, and enhancing safety and security (In Effect)) (Title 49 U.S.C. § 40101(d)) Promote safe flight of civil aircraft in air commerce (In Effect) (49 U.S.C. § 44701(a)(5))	Holders of type certificates, parts manufacturer approvals, and technical standard order authorizations are required to report certain failures, malfunctions, and defects in products and articles that they have manufactured (14 C.F.R 21.3)	The FAA's regulations are generally agnostic as to the underlying cause of the failure, malfunction, or defect, which may be unknown at the time of the initial report. Part 21.3 reportable incidents are: a. Fires caused by a system or equipment failure, malfunction, or defect. b. An engine exhaust system failure, malfunction, or defect which causes damage to the engine, adjacent aircraft structure, equipment, or components. c. The accumulation or circulation of toxic or noxious gases in the crew compartment or passenger cabin. d. A malfunction, failure, or defect of a propeller control system. e. A propeller or rotorcraft hub or blade structural failure. f. Flammable fluid leakage in areas where an ignition source normally exists. g. A brake system failure caused by structural or material failure during operation. h. A significant aircraft primary structural defect or failure caused by any autogenous condition (fatigue, understrength, corrosion, etc.). i. Any abnormal vibration or buffeting caused by a structural or system malfunction, defect, or failure. j. An engine failure. k. Any structural or flight control system malfunction, defect, or failure which causes an interference with normal control of the aircraft for which derogates the flying qualities. l. A complete loss of more than one electrical power generating system or hydraulic power system during a given operation of the aircraft.	Within 24 hours after it has determined that the failure, malfunction, or defect required to be reported has occurred (14 C.F.R 21.3) If an unsafe condition exists in a product and the condition is likely to exist in other products of the same type design, including in the event the unsafe condition has a cybersecurity cause, the FAA can issue an airworthiness directive to compel action to resolve the unsafe condition." (14 C.F.R. Part 39)

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
			m. A failure or malfunction of more than one attitude, airspeed, or altitude instrument during a given operation of the aircraft.	
U.S. Coast Guard (USCG)	Suspicious Activity, Breaches of Security, or Transportation Security Incidents (In Effect) (33 C.F.R 101.305 and CG-5P Policy Letter 08-16) For more information, see https://www.dco.uscg.mil/Portals/10/Cyber/Cyber-Readiness/CG-5P%20Policy%20Letter%2008-16%20-%20Reporting%20Suspicious%20Activity%20and%20BoS.pdf?ver=2020-05-26-173911-100&timestamp=1590758815625	Owners or operators of vessels, maritime facilities, and/or outer continental shelf facilities	Breaches of security, suspicious activity, and/or activities that may result in a transportation security incident (TSI) CG-5P Policy Letter 08-16 to industry provides cyber-specific examples	Without delay Trigger: Upon occurrence of the activity and/or incident Local Captains of the Port, with support from the Coast Guard's Cyber Command, will establish contact with the reporting entity

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
USCG	Hazardous Conditions (In Effect) (33 C.F.R 160.216)	Owners, agents, masters, operators or the person in charge of a vessel	Hazardous conditions	Immediately Trigger: Upon discovery of the hazardous condition Requirement to remediate or mitigate the hazardous condition to the satisfaction of the Captain of the Port.
USCG	Evidence of Sabotage or Subversive Activity (In Effect) (33 C.F.R 6.16-1)	Principally vessel and facility owners or operators	Evidence of sabotage or subversive activity endangering any vessel, harbor, port, or waterfront facility	Immediately Trigger: Upon discovery of the evidence of sabotage or subversive activity The Captain of the Port may issue orders and require action related to the report.
Transportation Security Administration (TSA)	Enhancing Public Transportation and Passenger Railroad Cybersecurity (In Effect) (Security Directive 1582-21-01 series) For more information, see Surface Transportation Cybersecurity Toolkit	"Each owner/operator identified in 49 C.F.R 1582.101 that is a passenger railroad carrier or rail transit system."	See section "Actions Required" part B. Reporting Cybersecurity Incidents." In part the directive requires reporting of: a. Unauthorized access of an Information or Operational Technology system; b. Discovery of malicious software on an Information or Operational Technology system; c. Activity resulting in a denial of service to any Information or Operational Technology system; and/or d. Any other cybersecurity incident that results in operational disruption to the Owner/Operator's Information or Operational Technology systems or other aspects of the Owner/Operator's rail systems or facilities, or incident that has the potential to cause impact to a large number of passengers, critical infrastructure or core government functions, or impacts to national security, economic security or public health and safety.	Owner/operators must report the incidents required by this section [section B] as soon as practicable, but no later than 24 hours after a cybersecurity incident is identified

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
TSA	Enhancing Surface Transportation Security (In Effect) Surface Transportation Information Circular 2021-01 For more information, see: Surface Transportation Cybersecurity Toolkit	This information circular applies to the following owner/operators not covered under Security Directives 1580-21-01 or 1582-21-02. Specifically: "Each railroad owner/operator identified in 49 C.F.R 1580.1 (a); Each passenger railroad, public transportation agency, or rail transit system owner/operator identified in 49 C.F.R 1582.1; Each Over-the-Road-Bus owner/operator identified in 49 C.F.R 1584.1."	See section "Recommended Measures" Part B. Reporting Cybersecurity Incidents." In part this information circular recommends reporting of: a. Unauthorized access of an Information or Operational Technology system; b. Discovery of malicious software on an Information or Operational Technology system; c. Activity resulting in a denial of service to any Information or Operational Technology system; d. Any other cybersecurity incident that results in operational disruption to the Owner/Operator's Information or Operational Technology systems or other aspects of the Owner/Operator's systems or facilities or an incident that has the potential to cause impact to a large number of customers, critical infrastructure or core government functions, or impacts national security, economic security or public health and safety.	Owner/ operators should report the incidents suggested by Section B, as soon as practicable, but no later than 24 hours after a cybersecurity incident is identified.
TSA	Enhancing Pipeline Cybersecurity Security Directive (SD) Pipeline-2021-01 series	Surface Transportation: Pipeline. Specifically, "owner and operators of a hazardous and natural gas pipeline or a liquefied natural gas facility notified by TSA that their pipeline system or facility is critical."	See section "Actions Required" part B. Reporting Cybersecurity Incidents." 1. Unauthorized access of an Information or Operational Technology system; 2. Discovery of malicious software on an Information or Operational Technology system; 3. Activity resulting in a denial of service to any Information or Operational Technology system; 4. A physical attack against the Owner/Operator's network infrastructure, such as deliberate damage to communication lines; and 5. Any other cybersecurity incident that results in operational disruption to the Owner/Operator's Information or Operational Technology systems or other aspects of the Owner/Operator's pipeline systems or facilities, or otherwise has the potential to cause operational disruption that adversely affects the safe and efficient transportation of liquids and gases including, but not limited to impacts to a large number of customers, critical infrastructure or core government functions, or impacts national security, economic security or public health and safety.	Owner/Operators should report the incidents identified by this Section B as soon as practicable, but no later than 24 hours after a cybersecurity incident is identified.

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
TSA	"Enhancing Pipeline Cybersecurity" (In Effect) Information Circular Pipeline-2022-01 For more information, see: Surface Transportation Cybersecurity Toolkit	This Information Circular applies to Owner/Operators of hazardous liquid and natural gas pipelines not subject to Security Directive Pipeline-2021-01 and Pipeline-2021-02 series.	See section "Recommended Measures" Part B. Reporting Cybersecurity Incidents." In part this information circular recommends reporting of: a. Unauthorized access of an IT or OT system; b. Discovery of malicious software on an IT or OT system; c. Activity resulting in a denial of service to any IT or OT system;, and/or d. Any other cybersecurity incident that results in operational disruption to the Owner/Operator's IT or OT systems or other aspects of the Owner/Operator's systems or facilities, or an incident that has the potential to cause impact to critical infrastructure or core government functions, or impacts national security, economic security, or public health and safety.	Owner/Operators should report the incidents identified by this Section B as soon as practicable, but no later than 24 hours after a cybersecurity incident is identified.
TSA	"Enhancing Rail Cybersecurity" (In Effect) Security Directive 1580-21-01 series For more information, see: Surface Transportation Cybersecurity Toolkit	Surface Transportation: Freight Rail. Specifically: "Each freight railroad carrier identified in 49 C.F.R 1580.101 and other TSA-designated railroads"	See section "Actions Required" part B. Reporting Cybersecurity Incidents." In part the directive requires reporting of: a. Unauthorized access of an Information or Operational Technology system; b. Discovery of malicious software on an Information or Operational Technology system; c. Activity resulting in a denial of service to any Information or Operational Technology system; d. Any other cybersecurity incident that results in operational disruption to the freight railroad carrier's Information or Operational Technology systems or other aspects of the Owner/Operator's rail systems or facilities, or incident that has the potential to cause impact to a large number of customers or passengers (as applicable), critical infrastructure or core government functions, or impacts to national security, economic security or public health and safety.	Owner/Operators must report the incidents identified by this Section B as soon as practicable, but no later than 24 hours after a cybersecurity incident is identified.

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
TSA	Airport Security Program (ASP) (In Effect) For more information, see…	Airport Operators	An event that, without lawful authority, jeopardizes, disrupts or otherwise impacts, or is reasonably likely to jeopardize, disrupt or otherwise impact, the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident on the system. This definition includes an event that is under investigation or evaluation by the aircraft operator as a possible cybersecurity incident without final determination of the event's root cause or nature (such as malicious, suspicious, benign).	As soon as practicable, but no later than 24-hours after a cybersecurity incident is identified.
TSA	Aircraft Operator Standard Security Program (AOSSP) Full All Cargo Aircraft Operator Standard Security Program (FACAOSSP) Twelve Five Standard Security Program (TFSSP) Private Charter Standard Security Program (PCSSP) (In Effect)	Aircraft Operators (Passenger / Cargo)	An event that, without lawful authority, jeopardizes, disrupts or otherwise impacts, or is reasonably likely to jeopardize, disrupt or otherwise impact, the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident on the system. This definition includes an event that is under investigation or evaluation by the aircraft operator as a possible cybersecurity incident without final determination of the event's root cause or nature (such as malicious, suspicious, benign).	As soon as practicable, but no later than 24 hours after a cybersecurity incident is identified.
TSA	Indirect Air Carrier Standard Security Program (IACSSP) Certified Cargo Screening Standard Security Program (CCSSSP) (In Effect)	Indirect Air Carriers (IACs)/Certified Cargo Screening Facilities (CCSF)	An event that, without lawful authority, jeopardizes, disrupts or otherwise impacts, or is reasonably likely to jeopardize, disrupt or otherwise impact, the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident on the system. This definition includes an event that is under investigation or evaluation by the CCSF as a possible cybersecurity incident without final determination of the event's root cause or nature (such as malicious, suspicious, benign).	As soon as practicable, but no later than 24 hours after a cybersecurity incident is identified.

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
Cybersecurity and Infrastructure Security Agency (CISA)	Chemical Facility Anti-Terrorism Standards (CFATS) (In Effect) For more information, see 6 C.F.R Part 27	High-risk Chemical Facilities (as determined by possession of any Chemical of Interest at or above the screening threshold quantity and concentration listed on Appendix A to 6 C.F.R Part 27 and through a risk-based methodology to determine if a facility is "high-risk")	Significant cyber incidents must be reported, and this includes "any incident with malicious intent to adversely affect operations of critical cyber assets, including IT equipment used to provide security for the facility or to manage processes involving COI or critical assets of the facility."	Promptly after a significant cyber incident is identified
CISA	Rulemaking pursuant to the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (Under Development) 6 USC § 681 et seq. For more information, see https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia.	Covered Critical Infrastructure Entities as defined by CISA pursuant to rulemaking.	Covered cyber incidents as defined by CISA pursuant to rulemaking.	Covered Cyber Incidents: Not later than 72 hours after the covered entity reasonably believes that a covered cyber incident occurred. Ransomware payments: 24 hours after the ransom payment is made. Any requirements for Supplemental/Updates are TBD through the rulemaking process.
Department of Defense (DOD)	Safeguarding Covered Defense Information and Cyber Incident Reporting (In Effect) DFARS 252.204-7012 For more information, see https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012 Cyber incident reporting for cloud computing services (In Effect) (DFARS § 252.239-7010(d))	A contractor who owns or operates an unclassified information systems that processes, stores, or transmits controlled unclassified information or a contractor who is designated as providing operationally critical support	"Cyber incident" means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein, or affect the contractor's ability to perform the requirements of the contract that are designated as operationally critical support.	Within 72 hours of discovery of the incident

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
DOD	Reporting on cyber incidents with respect to networks and information systems of operationally critical contractors and certain other contractors (In Effect) (10 U.S.C. § 391 - U.S. Code - Unannotated Title 10. Armed Forces § 391)	Contractors designated by the Secretary of Defense as a critical source of supply for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.	"Cyber incident" means actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system or the information residing therein.	Rapidly after a cyber incident occurs
DOD	Reporting on penetrations of networks and information systems of certain contractors (In Effect) (10 U.S.C. § 393 - U.S. Code - Unannotated Title 10. Armed Forces § 393)	Any private entity granted clearance by the Department of Defense to access, receive, or store classified information for the purpose of bidding for a contract or conducting activities in support of any program of the Department of Defense.	Successful penetration of a network or information system that contains or processes information created by or for the Department of Defense with respect to which such contractor is required to apply enhanced protection.	Rapidly after network or information system is successfully penetrated
Department of the Treasury	Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime (In Effect) Bank Secrecy Act (12 U.S.C. 1813 and 1818; 31 U.S.C 5318 and 5318) For more information, see… https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a005	Financial Institutions	Suspicious transaction conducted or attempted by, at, or through the institution that involves or aggregates to $5,000 or more in funds or other assets.	No later than 30 calendar days after the activity is detected with a maximum extension of 30 additional days.

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
Nuclear Regulatory Commission	"Cyber security event notifications" (In Effect) 10 C.F.R 73.77 A copy of the rule can be found via: https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0077.html For more information, see https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html	Each NRC's nuclear power plant licensee subject to the provisions of 10 C.F.R 73.54, "Protection of digital computer and communication systems and networks."	For digital computer and communications systems and networks that are within the scope of the nuclear power plant licensee's cyber security program, the licensee must report any cyber-attack that adversely impacted or could have caused adverse impact to safety-related or important-to-safety functions, security functions, or emergency preparedness functions (including offsite communications); or that compromised or could have compromised support systems and equipment resulting in adverse impacts to safety, security, or emergency preparedness functions. The licensee must also report the discovery of a suspected or actual cyber-attack initiated by personnel with access to the digital computer and communications systems and networks within the scope of the licensee's cyber security program.	Depending upon the severity of impact to the digital computer and communications systems, reporting is required within 1-hr, 4-hrs, or 8-hrs, with specific detail available in 10 C.F.R 73.77. The clock is triggered once the licensee discovers that a cyberattack has occurred. Additional guidance on this is located in Regulatory Guide 5.83, "Cyber Security Event Notifications," and NEI 15-09, "Cyber Security Event Notification." For more information, see: https://www.nrc.gov/docs/ML1426/ML14269A388.pdf and https://www.nrc.gov/docs/ML1606/ML16063A063.pdf Initial telephonic notifications must be followed by a written security report within 60 days of the telephonic notification Licensees must update reporting if significant supplemental information becomes available. Reports may be retracted if the licensee subsequently determines the reporting threshold was not met.

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
Department of Justice	Reporting Incidents and Breaches (In Effect) For more information, see https://www.justice.gov/nsd/committee-assessment-foreign-participation-united-states-telecommunications-services-sector-0	FCC licensees subject to mitigation measures imposed pursuant to Exec. Order 13913, including a Letter of Agreement (LOA) with DOJ.	Licensees typically must report (subject to negotiation with DOJ): Any known or suspected (a) Security Incident; (b) Unauthorized Access to, or disclosure of, any information relating to services provided by [Company Name], or referring or relating in any way to [Company Name]'s customers in the United States or its territories; (c) Any unauthorized Access to, or disclosure of, [Domestic Communications] in violation of federal, state, or local law; or (d) Any material breach of the commitments made in this LOA. "Security Incident" means: (i) Any known or suspected breach of this LOA, including a violation of any approved plan, policy, or procedure under this LOA; (ii) Any unauthorized Access to, or disclosure of, U.S. Records; (iii) Any unauthorized Access to, or disclosure of, information obtained from or relating to Government entities; or (iv) Any one or more of the following which affect the company's computer network(s) or associated information systems: (A) Unauthorized disruptions to a service or denial of a service; (B) Unauthorized processing or storage of data; (C) Unauthorized modifications to system hardware, firmware, or software, including the identification of vulnerabilities introduced through a cyber supply chain compromise; (D) Unplanned incidents that cause activation of [Company Name]'s Cybersecurity Incident Response Plan; (E) Attempts from unauthorized sources to Access systems or data if these attempts to Access systems or data may materially affect the company's ability to comply with the terms of this LOA; or (F) An unauthorized occurrence that (1) actually or imminently jeopardizes the integrity, confidentiality, or availability of information or an information system;	Licensees typically are required to report promptly, but no later than 48 hours (subject to negotiations with DOJ) after the incident is known or suspected. Updates are required upon request by DOJ.

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
			or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.	
Federal Communications Commission (FCC)	Network Outage Reporting System (NORS) (In Effect) For more information, see https://www.fcc.gov/network-outage-reporting-system-nors	Cable service providers, satellite operators, satellite communications providers, SS7 providers, wireless service providers, wireline communications providers, interconnected Voice-over IP (VoIP) providers, covered 911 service providers, and submarine cable licensees.	Communications service outages including on wireline, wireless, VoIP, and submarine cable networks, which may be caused by cyber incidents. Reportable outages meet threshold requirements for duration and magnitude.	Within at least four hours of discovery by the service provider (most communications service providers are required to report faster – within two hours). A second report is generally due within 72 hours of the outage discovery (and is the time when a filer is required to specify whether the cause of the report is a cyber incident). A third report is due within 30 days of the outage discovery.
FCC	"Notification of customer proprietary network information (CPNI) security breaches" (In Effect) 47 C.F.R 64.2011 For more information, see https://www.ecfr.gov/current/title-47/chapter-I/subchapter-B/part-64/subpart-U/section-64.2011	Telecommunications Carriers and VoIP Service Providers	Breaches of customers' CPNI. A "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.	As soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach Although section 64.2011 does not include requirements to amend the initial report, carriers/VoIP's do regularly amend their initial report to incorporate any updates regarding the breach.
FCC	Proposed Rulemaking to Strengthen the Security of Nation's Alerting Systems (NPRM) (Proposed) For more information, see https://www.fcc.gov/document/fcc-proposes-strengthen-security-emergency-alert-systems	Emergency Alert System (EAS) Participants and Commercial Mobile Service providers that participate in Wireless Emergency Alerts	Reporting for EAS equipment defects, which may include defects caused by cyber incidents. Reporting for unauthorized access of EAS equipment or WEA systems or services, regardless of whether that compromise has resulted in the transmission of a false alert.	For equipment defects, the NPRM sought comment on possible timeframes (e.g. 24 hours). For unauthorized access, within 72 hours of when the EAS Participant or Participating CMS Provider knew or should have known that an incident has occurred.

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
FCC	Proposed Rulemaking to update Customer Proprietary Network Information Data Breach Notification Rules (Proposed) For more information, see https://www.fcc.gov/document/fcc-proposes-updated-data-breach-reporting-requirements	Telecommunications Carriers and VoIP Service Providers	NPRM proposes clarifying its rules to require consumer notification by carriers of inadvertent breaches	NPRM proposes to eliminate the current seven business day mandatory waiting period for notifying customers of a breach.
Federal Trade Commission	Health Breach Notification Rule (In Effect) For more information, see https://www.ftc.gov/legal-library/browse/rules/health-breach-notification-rule. and https://www.ftc.gov/business-guidance/resources/health-breach-notification-rule-basics-business	Vendors of personal health records (PHRs), PHR related entities, and third party service providers	"Breach of security" Breach of security means, with respect to unsecured PHR identifiable health information of an individual in a personal health record, acquisition of such information without the authorization of the individual. Unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless the vendor of personal health records, PHR related entity, or third party service provider that experienced the breach has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information.	For reports to individuals: without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach of security. For reports to FTC: If the breach involves the unsecured PHR identifiable health information of 500 or more individuals, then notify as soon as possible and in no case later than ten business days following the date of discovery of the breach. If the breach involves the unsecured PHR identifiable health information of fewer than 500 individuals, the vendor of personal health records or PHR related entity may maintain a log of any such breach and submit such a log annually to the FTC no later than 60 calendar days following the end of the calendar year, documenting breaches from the preceding calendar year. For reports to media: If the unsecured PHR identifiable health information of 500 or more residents of such State or jurisdiction is, or is reasonably believed to have been, acquired during such breach, then the vendor of PHRs or PHR related entity shall provide notice to prominent media outlets serving a State or jurisdiction, following the discovery of a breach of security.

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
Department of Health and Human Services	The HIPAA Breach Notification Rule (In Effect) 45 C.F.R §§ 164.400-414 For more information, see: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D and https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.	HIPAA covered entities and their business associates	1. Breaches Affecting 500 or More Individuals. 2. Breaches affecting fewer than 500 individuals. A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment.	If a breach affects 500 or more individuals, notify HHS "without unreasonable delay and in no case later than 60 calendar days" from the discovery of the breach. If a breach affects fewer than 500 individuals, notify HHS within 60 days of the end of the calendar year in which the breach was discovered. If a covered entity discovers additional information that supplements, modifies, or clarifies a previously submitted notice to HHS, it may submit an additional form by checking the appropriate box to indicate that it is an addendum to the initial report, using the transaction number provided after its submission of the initial breach report. Breach reporting portal: https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
Department of Energy	DOE-417 Electric Emergency Incident and Disturbance Report (In Effect)	Electric Utilities; Balancing Authorities; Reliability Coordinators; Generating Entities (greater than 300 MW); Local Utilities in Alaska, Hawaii, Puerto Rico, U.S. Virgin Islands, and U.S. Territories; and Computer, telecommunication, and physical security offices that support the Balancing Authority, Reliability Coordinator, and electric utility or located within the entity	The DOE-417 Electric Emergency Incident and Disturbance Report covers a range of cyber and non-cyber incidents. Reportable cyber-incident include: 1. Reportable Cyber Incident (defined by NERC CIP-008-6) 2. Cyber event that is not a Reportable Cyber Security Incident that causes interruptions of electrical system Operations 3. Cyber event that could potentially impact electric power system adequacy or reliability 4. Cyber Security Incident that was an attempt to compromise a High or Medium Impact Bulk Electric System, Cyber System or their associated Electronic Access Control or Monitoring Systems	DOE-417 Reports are required to be submitted within 1-hour; 6-hours; 24-hours; or 1-business day after determination that an incident occurred/is occurring, depending on reporting criteria. For cyber related criteria: 1-Hour: 1. Reportable Cyber Incident (defined by NERC CIP-008-6) 2. Cyber event that is not a Reportable Cyber Security Incident that causes interruptions of electrical system operations 6-Hours: Cyber event that could potentially impact electric power system adequacy or reliability 24-Hours: Cyber Security Incident that was an attempt to compromise a High or Medium Impact Bulk Electric System Cyber System or their associated Electronic Access Control or Monitoring Systems Entities may file updates as needed. Update or final report is required within 72-hours

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
Federal Energy Regulatory Commission (FERC) (designated to North American Energy Reliability Corporation (NERC) through the Electricity Information Sharing and Analysis Center (E-ISAC))	Critical Infrastructure Protection Reliability Standards CIP-003-8 (Cyber Security – Security Management Controls) and CIP-008-6 (Cyber Security – Incident Reporting and Response Planning) (In Effect) For more information, see https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-003-8.pdf and https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-6.pdf	Users, owners, and operators of the Bulk Electric System (BES) that are registered with NERC and identified in the standard as "Responsible Entities." The standards also include additional detail on which applicable systems are subject to (or excluded from) the reporting requirements.	A Reportable Cyber Security Incident is a Cyber Security Incident that compromised or disrupted a BES Cyber System that performs one or more reliability tasks of a functional entity; an Electronic Security Perimeter of a high or medium impact BES Cyber System; or an Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System. A Cyber Security Incident is a malicious act or suspicious event that compromises, or was an attempt to compromise, the Electronic Security Perimeter (ESP) or Physical Security Perimeter (PSP) or, disrupts, or was an attempt to disrupt, the operation of a BES Cyber System. low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.	For "Reportable Cyber Incident:" 1 hour for after the determination of a Reportable Cyber Security Incident. For a "Cyber Security Incident:" by the end of the next calendar day after the determination that a Cyber Security Incident was an attempt to compromise a system identified in the "Applicable Systems" Provide updates, if any, within 7 calendar days of determination of new or changed attribute information

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
Food and Drug Administration (FDA)	Medical Device Reporting (In Effect) 21 C.F.R Part 803 For more information, see https://www.fda.gov/medical-devices/medical-device-safety/medical-device-reporting-mdr-how-report-medical-device-problems	Device User Facilities, Medical Device Manufacturers, and Importers.	For User Facilities: Reports of death and/or serious injury are mandatory. For medical device manufacturers: reportable death, serious injury, or device malfunctions are mandatory. A reportable death, serious injury, or malfunction is based on information a manufacturer receives or otherwise becomes aware of, from any source, which reasonably suggests that one of its marketed devices: • May have caused or contributed to a death or serious injury; or • Malfunctioned and the malfunction of the device or a similar device marketed by the manufacturer would be likely to cause or contribute to a death or serious injury if the malfunction were to recur. For importers: reports of death and/or serious injury and malfunctions are mandatory.	For User Facilities: The user facility must submit report(s) to the manufacturer and FDA not later than 10 workdays after the day the user facility becomes aware of information, from any source, that reasonably suggests that a device has or may have caused or contributed to the death or a serious injury to a patient in the facility; or The user facility must submit report(s) to the manufacturer not later than 10 workdays after the day that the user facility becomes aware of information that reasonably suggests that a device has or may have caused or contributed to a serious injury. If the manufacturer is not known, the user facility must submit this report to FDA. (21 C.F.R §803.20(b)(2), 803.30(a)) For medical device manufacturers: The device manufacturer must submit report(s) to FDA not later than 30 calendar days after the day the manufacturer becomes aware of information that reasonably suggests that a device may have caused or contributed to a death or serious injury; or The device manufacturer must submit report(s) to FDA not later than 30 calendar days after the day the manufacturer becomes aware of information that reasonably suggests a device has malfunctioned and that this device or a similar device that the manufacturer markets would be likely to cause or contribute to a death or serious injury if the malfunction were to recur; or The device manufacturer must submit a “5-day report” (or five-day report) within five workdays after the day the manufacturer becomes aware of a reportable event: • That necessitates remedial action to prevent an unreasonable risk of substantial harm to public health; or • For which FDA has made a written request for the submission of 5-day reports (21 C.F.R 803.10(c), 803.20, 803.53).

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
				For Importers: The importer must submit report(s) to the manufacturer and to FDA no later than 30 calendar days after the day that the importer becomes aware of information that reasonably suggests that a device has or may have caused or contributed to a death or serious injury; or The importer must submit report(s) to the manufacturer no later than 30 calendar days after receiving information that a device the importer markets has malfunctioned and that this device or a similar device that the importer markets would be likely to cause or contribute to a death or serious injury if the malfunction were to recur. (21 C.F.R 803.20(b)(2)) Supplemental reports: FDA considers a supplemental report to be required when new facts prompt an alteration or supplement any information or conclusions contained in the original MDR or in any prior supplemental reports. (21 C.F.R 803.10(c)(3)). If FDA requires more information, the agency will notify the user facility, medical device manufacturer, importer, or distributor of the additional information that is required. (21 C.F.R §803.15) For manufacturers: Whenever manufacturers obtain information required under 21 C.F.R 803.50 that was not known or available to them at the time they submitted their initial 30-day or 5-day report, they must submit supplemental information to FDA within 30 calendar days of the day the manufacturer receives the information (21 C.F.R 803.56).

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
FDA	Corrections and Removals of Medical Devices (In Effect) 21 C.F.R 806, Medical Devices For more information, see https://www.fda.gov/medical-devices/postmarket-requirements-devices/recalls-corrections-and-removals-devices.	Manufacturers and importers	Each device manufacturer or importer must submit a written report to FDA of any correction or removal of a device(s) if it was initiated by such manufacturer or importer to reduce a risk to health posed by the device or to remedy a violation of the Federal Food, Drug, and Cosmetic Act caused by the device, which may present a risk to health. If this criterion is met, a report must be made even if the event was caused by user error. A report is not required if the information has already been provided to FDA under Medical Device Reporting (21 C.F.R 803) or Repurchase, Repairs or Replacement of Electronic Products (21 C.F.R 1004) or if the action was initiated by an FDA order under FDA's device recall authority (see section 518(e) of the Federal Food, Drug, and Cosmetic Act and 21 C.F.R 810).	Within 10 working days of the time the manufacturer or importer initiates the correction or removal. (21 C.F.R 806.10(b)) If, after submitting a report, a manufacturer or importer determines that the same correction or removal should be extended to additional lots or batches of the same device, the manufacturer or importer must amend the original report by submitting an amendment within 10-working days of initiating the extension of the correction or removal (21 C.F.R 806.10(d)).
Securities and Exchange Commission (SEC)	Regulation Systems Compliance and Integrity ("Reg. SCI") (In Effect) For more information, see www.ecfr.gov/current/title-17/chapter-II/part-242/subpart-ECFRe106e84e67e2bc9	Designated "SCI entities" that directly support any one of six key securities market functions: trading, clearance and settlement, order routing, market data, market regulation, and market surveillance. Note: On March 15, 2023, SEC proposed amendments to Reg. SCI that would expand the scope of SCI entities to include registered security-based swap data repositories; all clearing agencies that are exempt from registration; and certain large broker-dealers. For more information see: www.sec.gov/news/press-release/2023-53.	SCI entities are required to notify the Commission of "SCI events", defined as: • Systems disruptions – an event in an SCI entity's SCI systems that disrupts or significantly degrades, the normal operation of an SCI system; • Systems intrusions – any unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity; and • Systems compliance issues – an event at an SCI entity that has caused any SCI system to operate in a manner that does not comply with the Act and the rules and regulations thereunder or the entity's rules or governing documents Note: "SCI Systems" are defined as all computer, network, electronic, technical, automated, or similar systems of, or operated by or on behalf of, an SCI entity that, with respect to securities, directly support trading, clearance and settlement, order routing, market data, market regulation, or market surveillance. Note: On March 15, 2023, the SEC proposed amendments to Reg. SCI that would expand the definition of systems intrusion to include a broader range of cyber incidents experienced by an SCI entity, and require additional policies and procedures to help an SCI entity ensure that relevant systems are robust, resilient, and secure. For more information see: https://www.sec.gov/news/press-release/2023-53	Immediately upon any responsible SCI personnel having a reasonable basis to conclude that an SCI event has occurred. (with delayed reporting permitted for SCI events with de minimis impact). (Reference: SEC Form SCI at https://www.sec.gov/files/form-sci.pdf). Following the initial notification, SCI entities are required to file a written notification with the SEC within 24 hours. Additional updates are required until such time as the SCI event is resolved and the SCI entity's investigation of the SCI event is closed. (Frequency of ongoing updates are situation dependent as determined by a representative of the SEC.) A final written notification is required within five business days after the resolution of an SCI event and closure, including details of the investigation regarding such SCI event, submit a final written notification pertaining to such SCI event to the SEC. Other related reporting requirements include the requirement for SCI entities to file a quarterly report of systems disruptions and systems intrusions with no or a de minimis impact. (Reference: SEC Form SCI at https://www.sec.gov/files/form-sci.pdf).

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
SEC	SEC Regulation S-P: Privacy of Consumer Financial Information ("Reg. S-P") (In Effect) For more information, see www.ecfr.gov/current/title-17/chapter-II/part-248.	Broker-dealers, investment companies and investment advisers registered with the Commission.	Current Reg. S-P does not set forth any obligations to report incidents to the Commission. It does, however, set forth certain obligations regarding the provision of privacy notices to customers. Note: On March 15, 2023, the SEC proposed amendments that would broaden Reg. S-P to require broker-dealers, investment companies, registered investment advisers, and transfer agents (collectively, "covered institutions") to notify affected individuals whose sensitive customer information was or is reasonably likely to have been accessed or used without authorization. In addition, the proposed amendments would extend the application of the safeguards provisions in Regulation S-P to transfer agents.. For more information see: www.sec.gov/news/press-release/2023-51	N/A
SEC	SEC Regulation S-ID: Identity Theft Red Flags (Reg. S-ID) (In Effect) For more information, see: www.ecfr.gov/current/title-17/chapter-II/part-248#sp17.4.248.c	Broker-dealers, investment companies and investment advisers that are registered with the Commission.	Reg. S-ID does not set forth any obligations to report incidents to the Commission. It does, however, require covered financial institutions to provide notice to customers about its privacy policies and practice.	N/A
SEC	Amendments Regarding the Definition of "Exchange" and Alternative Trading Systems ("ATSs") That Trade U.S. Treasury and Agency Securities, National Market System (NMS) Stocks, and Other Securities (Proposed) For more information, see https://www.govinfo.gov/content/pkg/FR-2022-03-18/pdf/2022-01975.pdf	ATSs that meet certain volume thresholds.	Same as under Reg. SCI.	Same as under Reg. SCI.

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
SEC	Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies (Proposed) For more information, see www.sec.gov/news/press-release/2022-20.	Investment advisers registered or required to be registered with the Commission, and registered investment companies and business development companies ("funds").	Cybersecurity incident means an unauthorized occurrence on or conducted through [an adviser's or a fund's] information systems that jeopardizes the confidentiality, integrity, or availability of [an adviser's or a fund's] information systems or any [adviser or fund] information residing therein.	Promptly, but in no event more than 48 hours, after having a reasonable basis to conclude that a significant adviser cybersecurity incident or a significant fund cybersecurity incident had occurred or is occurring. Proposed rule 204-6 would also require advisers to amend any previously filed Form ADV-C promptly, but in no event more than 48 hours, after information reported on the form becomes materially inaccurate; if new material information about a previously reported incident is discovered; and after resolving a previously reported incident or closing an internal investigation pertaining to a previously disclosed incident.
SEC	Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies (In Effect on September 5, 2023) For more information, see https://www.sec.gov/news/press-release/2023-139	Public companies subject to the reporting requirements of the Securities Exchange Act of 1934	Cybersecurity incident means an unauthorized occurrence, or a series of related unauthorized occurrences, on, or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein.	Within four business days after a registered public company determines that it has experienced a material cybersecurity incident has occurred. Disclosure may be delayed if the United States Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety. For more information, see https://www.investor.gov/introduction-investing/investing-basics/glossary/form-8-k.
SEC	Cybersecurity Risk Management Rule (Proposed) For more information, see www.sec.gov/news/press-release/2023-52.	Broker-dealers, clearing agencies, major security-based swap participants, the Municipal Securities Rulemaking Board, national securities associations, national securities exchanges, security-based swap data repositories, security-based swap dealers, and transfer agents ("Market Entities")	Significant cybersecurity incidents, defined as a cybersecurity incident, or a group of related cybersecurity incidents, that: • Significantly disrupts or degrades the ability of the market entity to maintain critical operations; or Leads to the unauthorized access or use of the information or information systems of the market entity, where the unauthorized access or use of such information or information systems results in or is reasonably likely to result in: (a) substantial harm to the market entity; or (b) substantial harm to a customer, counterparty, member, registrant, or user of the market entity, or to any other person that interacts with the market entity.	All Market Entities would need to give the SEC immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident had occurred or is occurring. In addition, after providing immediate written electronic notice of a significant cybersecurity incident, Covered Entities would need to report to the SEC promptly (but no later than 48 hours) information about the significant cybersecurity incident by filing Part I of proposed Form SCIR. Thereafter, Covered Entities would need to file an updated Part I of Form SCIR when information on the previously filed report materially changes or the incident is resolved or an internal investigation of the incident is concluded.

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
Office of the Comptroller of the Currency (OCC)	Computer-Security Incident Notification Rule (In Effect) 12 C.F.R Part 53 For more information, see OCC Bulletin 2021-55, Computer-Security Incident Notification: Final Rule, Nov. 23, 2021, at https://www.occ.gov/news-issuances/bulletins/2021/bulletin-2021-55.html and OCC Bulletin 2022-8, Information Technology: OCC Points of Contact for Banks' Computer-Security Incident Notifications. Mar. 29, 2022, at https://www.occ.gov/news-issuances/bulletins/2022/bulletin-2022-8.html	National banks; Federal savings associations; and Federal branches and Federal agencies of foreign banks are required to provide notice of "notification incidents" to the OCC. "Bank service providers" are required to provide notice of certain "computer-security incidents" to their customers that are banking organizations. The rule carves out designated financial market utilities (defined per 12 USC 5462(4)). Those entities are subject to separate requirements promulgated by the Federal Reserve Board.	Computer-security incident - an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits. Notification Incident - a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's - (i) Ability to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business; (ii) Business line(s), including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value; or (iii) Operations, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States.	National banks, Federal savings associations, and Federal branches and agencies of foreign banks must notify the OCC of notification incidents as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred. Bank service providers must provide notice to each affected customer that is a banking organization as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for four or more hours.

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
OCC	Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (Final Interagency Guidance) 12 C.F.R Part 30 For more information, see OCC Bulletin 2005-13 at https://www.occ.treas.gov/news-issuances/bulletins/2005/bulletin-2005-13.html	National banks, Federal savings associations, Federal branches and Federal agencies of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers) Entities subject to direct supervision by the FDIC. Also includes "Bank service providers," which are required to provide notice of certain "computer-security incidents" to their customers that are banking organizations.	"…[A]n incident involving unauthorized access to or use of sensitive customer information ... " (12 C.F.R Part 30, App. B, Supp. A, section II.A.1.b.) and "Notifying customers when warranted" (12 C.F.R Part 30, App. B., Supp. A, section II.A.1.e.). The supplemental guidance further provides: "For purposes of this Guidance, sensitive customer information means a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name or password or password and account number." (Section III.A, Supplement A to Appendix B, 12 C.F.R Part 30.)	As soon as possible Primary Federal regulator notification: "[W]hen the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information.";". (Section II.A.1.b, Supplement A to Appendix B, 12 C.F.R Part 30.) Customer notification: "When a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible. Customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay. However, the institution should notify its customers as soon as notification will no longer interfere with the investigation." (Section III.A., Supplement A to Appendix B, 12 C.F.R Part 30)

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
Federal Deposit Insurance Corporation (FDIC)	Computer-Security Incident Notification Rule (In Effect) For more information, see FDIC Financial Institution Letter FIL-12-2022 at https://www.fdic.gov/news/financial-institution-letters/2022/fil22012.html	Entities subject to direct supervision by the FDIC. Also includes "Bank service providers," which are required to provide notice of certain "computer-security incidents" to their customers that are banking organizations.	Computer-security incident - an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits. Notification Incident - a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's - (i) Ability to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business; (ii) Business line(s), including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value; or (iii) Operations, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States.	Banking organizations subject to the rule must notify the FDIC as soon as possible, and no later than 36 hours after the banking organization determines that a notification incident has occurred. Bank service providers must provide notice to each affected customer that is a banking organization as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for four or more hours.

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
FDIC	Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (Final Interagency Guidance) 12 C.F.R pt. 364 For more information, see FDIC Financial Institution Letter FIL-27-2005 https://www.fdic.gov/news/financial-institution-letters/2005/fil2705.html	All insured state nonmember banks, insured state-licensed branches of foreign banks, and insured State savings associations, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers).	"[A]n incident involving unauthorized access to or use of sensitive customer information, as defined below." (12 C.F.R. pt. 364, app. B, supp. A, sec.II.A.1.b). "For purposes of this Guidance, sensitive customer information means a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name or password or password and account number." (12 C.F.R. pt. 364, app. B, supp. A, sec. III.A.1).	"[A]s soon as possible." (Section II.A.1.b, supp. A to app. B, 12 C.F.R. pt. 364.) Notification to primary federal regulator: "[W]hen the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information, as defined below." (Section II.A.1.b, supp. A to app. B, 12 C.F.R. pt. 364.) Customer notification: "When a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible. Customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay. However, the institution should notify its customers as soon as notification will no longer interfere with the investigation." (Section III.A., supp. A to app. B, 12 C.F.R. pt. 364).

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
Federal Reserve Board (FRB)	Computer-Security Incident Notification Rule (In Effect) For more information, see Supervision and Regulation Letter SR-22-4 at https://www.federalreserve.gov/supervisionreg/srletters/SR2204.htm	"Banking organizations" must notify the Board of "notification incidents". Banking organizations for the Board include U.S. bank holding companies; U.S. savings and loan holding companies; state member banks; the U.S. operations of foreign banking organizations; and Edge or agreement corporations; provided, however, that no designated financial market utility shall be considered a banking organization. "Bank service providers" are required to provide notice of certain "computer-security incidents" to their affected banking organization customers. The rule carves out designated financial market utilities (defined per 12 USC 5462(4)). Those entities are subject to separate requirements promulgated by the Federal Reserve Board.	"Computer-security incident" - an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits. Notification Incident - a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's - (i) Ability to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business; (ii) Business line(s), including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value; or (iii) Operations, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States.	A Board-regulated banking organization must notify the Board as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred. A bank service provider must notify each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for four or more hours. The Board must receive the notice from a banking organization as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred. A bank service provider must notify each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for four or more hours.

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
FRB	Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (Final Interagency Guidance) For more information, see Supervision and Regulation Letter SR-05-23 at https://www.federalreserve.gov/boarddocs/srletters/2005/SR0523.htm	State member banks and their nonbank subsidiaries (except for brokers, dealers, persons providing insurance, investment companies, and investment advisors); Edge and agreement corporations, and uninsured state-licensed branches or agencies of a foreign bank; and bank holding companies and their nonbank subsidiaries or affiliates (except brokers, dealers, persons providing insurance, investment companies, and investment advisors), for which the Board has supervisory authority	"…[A]n incident involving unauthorized access to or use of sensitive customer information ... " (12 C.F.R Part 208, App. D-2, Supp. A, section II.A.1.b. and 12 C.F.R Part 225, App. F, Supp. A, section II.A.1.b) and "Notifying customers when warranted" (12 C.F.R Part 208, App. D-2, Supp. A, section II.A.1.e., and 12 C.F.R Part 225, App. F, Supp. A, section II.A.1.e). The Supplemental Guidance further provides: "For purposes of this Guidance, sensitive customer information means a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name or password or password and account number." (Section III.A.1, Supplement A to Appendix D-2, 12 C.F.R Part 208, and Section III.A.1, Supplement A to Appendix F, 12 C.F.R Part 225.)	As soon as possible Primary Federal regulator notification: Under the Supplemental Guidance, "[W]hen the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information, as defined below;". Customer notification: Under the supplemental guidance, "When a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible. Customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay. However, the institution should notify its customers as soon as notification will no longer interfere with the investigation."
Commodity and Futures Trading Commission (CFTC)	System Safeguards for Swap Execution Facilities (In Effect) 17 C.F.R Part 37 For more information see https://www.cftc.gov/PressRoom/PressReleases/7442-16	Swap Exchange Facilities	Cybersecurity incidents or targeted threats that actually or potentially jeopardize automated system operation, reliability, security, or capacity, or the availability, confidentiality, or integrity of data. §37.1401 [Swap Execution Facilities] (e) A swap execution facility shall notify Commission staff promptly of all: (1) Electronic trading halts and material system malfunctions; (2) Cyber security incidents or targeted threats that actually or potentially jeopardize automated system operation, reliability, security, or capacity; and (3) Activations of the swap execution facility's business continuity-disaster recovery plan.	Promptly The expectation is to provide updates to CFTC as important information becomes available, and to provide a full report once the entity's investigation is complete. There is a credentialed portal provided to registrants.

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
CFTC	System Safeguards for Designated Contract Markets (In Effect) 17 C.F.R Part 38 For more information see https://www.cftc.gov/PressRoom/PressReleases/7442-16	Designated Contract Markets	Cybersecurity incidents or targeted threats that actually or potentially jeopardize automated system operation, reliability, security, or capacity, or the availability, confidentiality or integrity of data. §38.1051 [Designated Contract Markets] (e) A designated contract market must notify Commission staff promptly [we tell them this means in hours not days] of all: (1) Electronic trading halts and significant systems malfunctions; (2) Cyber security incidents or targeted threats that actually or potentially jeopardize automated system operation, reliability, security, or capacity; and (3) Activation of the designated contract market's business continuity-disaster recovery plan. (f) A designated contract market must give Commission staff timely advance notice of all material: (1) Planned changes to automated systems that may impact the reliability, security, or adequate scalable capacity of such systems; and (2) Planned changes to the designated contract market's program of risk analysis and oversight.	Promptly The expectation is to provide updates to CFTC as important information becomes available, and to provide a full report once the entity's investigation is complete. There is a credentialed portal provided to registrants.

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
CFTC	System Safeguards for Derivatives Clearing Organizations (In Effect) 17 C.F.R Part 39 For more information see https://www.cftc.gov/PressRoom/PressReleases/7442-16	Derivatives Clearing Organizations	Cybersecurity incidents or targeted threats that actually or potentially jeopardize automated system operation, reliability, security, or capacity, or the availability, confidentiality or integrity of data. §39.18 System Safeguards [Derivatives Clearing Organizations] (g) Notice of exceptional events. A derivatives clearing organization shall notify staff of the Division of Clearing and Risk, or any successor division, promptly of: (1) Any hardware or software malfunction, security incident, or targeted threat that materially impairs, or creates a significant likelihood of material impairment, of automated system operation, reliability, security, or capacity; or (2) Any activation of the derivatives clearing organization's business continuity and disaster recovery plan. (h) Notice of planned changes. A derivatives clearing organization shall provide staff of the Division of Clearing and Risk, or any successor division, timely advance notice of all material: (1) Planned changes to the derivatives clearing organization's automated systems that may impact the reliability, security, or capacity of such systems; and (2) Planned changes to the derivatives clearing organization's program of risk analysis and oversight.	Promptly The expectation is to provide updates to CFTC as important information becomes available, and to provide a full report once the entity's investigation is complete. There is a credentialed portal provided to registrants.

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
CFTC	System Safeguards for Swap Data Repositories (In Effect) 17 C.F.R Part 49 For more information see https://www.cftc.gov/PressRoom/PressReleases/7442-16	Swap Data Repositories	Cybersecurity incidents or targeted threats that actually or potentially jeopardize automated system operation, reliability, security, or capacity, or the availability, confidentiality or integrity of data. §49.24 System Safeguards [Swap Data Repositories] (g) A swap data repository shall notify Commission staff promptly of all: (1) Systems malfunctions; (2) Cyber security incidents or targeted threats that actually or potentially jeopardize automated system operation, reliability, security, or capacity; and (3) Any activation of the swap data repository's business continuity-disaster recovery plan. Appendix A provides guidance on the development and implementation of member information security programs including the creation of response programs that specify actions to be taken when the credit union suspects or detects that unauthorized individuals have gained access to member information systems, including appropriate reports to regulatory and law enforcement agencies.	Promptly The expectation is to provide updates to CFTC as important information becomes available, and to provide a full report once the entity's investigation is complete. There is a credentialed portal provided to registrants.

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
National Credit Union Administration	Guidelines for Safeguarding Member Information (Final Agency Guidance) 12 C.F.R 748, Appendix A Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice 12 C.F.R 748, Appendix B These Appendices interpret sections 501 and 505 of the Gramm Leach Bliley Act. For more information, see…	Federally insured credit unions.	12 C.F.R 748, Appendix A provides guidance on the development and implementation of member information security programs including the creation of response programs that specify actions to be taken when the credit union suspects or detects that unauthorized individuals have gained access to member information systems, including appropriate reports to regulatory and law enforcement agencies.	12 C.F.R 748, Appendix B advises that at minimum, a credit union's response program should contain procedures for notifying the appropriate NCUA regional director as soon as possible when the credit union becomes aware of an incident involving unauthorized access to or use of sensitive member information. Credit unions are also advised to notify appropriate law enforcement authorities in situations involving federal criminal violations requiring immediate attention. Notification to NCUA: As soon as possible. Notification to Member: If the credit union determines that misuse of its information about a member has occurred or is reasonably possible, it should notify the affected member as soon as possible. Member notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the credit union with a written request for the delay. However, the credit union should notify its members as soon as notification will no longer interfere with the investigation.

Appendix B: Federal Cyber Incident Reporting Requirements Inventory

Agency	Requirement or Expectation Name (Status), Authority/Document, and additional information website link	Entities Subject to Reporting Requirements or Expectations	Reportable Cyber Incidents / Threshold Information	Timeline and Trigger Information / Requirements or Expectations for Update/Supplemental Reports
Federal Housing Finance Agency	Enterprise Cybersecurity Incident Reporting (Final Agency Guidance) (FHFA Advisory Bulletin 2020-05) For more information, see https://www.fhfa.gov/SupervisionRegulation/AdvisoryBulletins/Pages/Enterprise-Cybersecurity-Incident-Reporting.aspx Information Security Risk Management (FHFA Advisory Bulletin 2017-02) For more information, see https://www.fhfa.gov/SupervisionRegulation/AdvisoryBulletins/Pages/Information-Security-Management.aspx Supplemental Guidance to Advisory Bulletin 2017-02 - Information Security Management (FHFA Advisory Bulletin 2023-02). For more information, see https://www.fhfa.gov/SupervisionRegulation/AdvisoryBulletins/Pages/Supplemental-Guidance-to-Advisory-Bulletin-2017-02-Information-Security-Management.aspx	No regulatory requirement. This guidance is applicable to Freddie Mac and Fannie Mae (Enterprises); Federal Home Loan Banks; Office of Finance	An occurrence that: -occurs at an Enterprise or at a third party that actually or potentially jeopardizes the confidentiality, integrity, or availability of an Enterprise system or Enterprise information the system processes, stores, or transmits; or -constitutes a violation or imminent threat of violation of the Enterprise's security policies, security procedures, or acceptable use policies.	Regulated entity plans should identify triggers and establish timing for incident notifications. For the Enterprises, FHFA expects immediate notification after incident detection for major incidents and 24-hour notification for significant incidents. Guidance directs regulated entities to maintain communication protocols; Enterprises should update reports periodically and include a description of the incident

Appendix C: Widely Used Contents of Reports Across Current Requirements

Widely Used Contents of Reports for Reporting Requirements Related to National/Economic Security, Safety, and Critical Functions			
Identifying the Covered/Subject Entity	Incident and Impacts (i.e., real or potential impacts)	Threat Actor- and Malicious activity-related content	Reporting Entity Response Actions (planned or taken)
• Reporting Entity legal/trade name and state of incorporation • Reporting individual • Contact Information such as email address or phone number	• Impacts to Operations- (e.g., impacts to business, infrastructure operations, Information Technology and Operational Technology, delivery of functions or services) • Information Systems, networks, or Functions affected • Types of information that were accessed or acquired • Whether data was stolen/altered/accessed • Secondary/Cascading impacts (e.g., # of market participants affected; impacts on market; physical hazards such as hazardous materials released)	• Date/Time discovered • Suspected time range of the incident • Description of the unauthorized access • Duration of unauthorized access • Security defenses that were in place • Threat actor identifying or contact information • Technical threat data, including TTPs, malicious IP addresses, domains, malware, vulnerabilities exploited	• Remediation and Mitigation actions taken or planned • Notifications made or planned • Time of event resolution

Widely Used Contents of Reports for Reporting and Public Notification Requirements Purposed for Consumer Protection and Privacy			
Identifying the Covered/Subject Entity and how to contact them	Incident and Impacts	What customers can do to protect themselves?	Reporting Entity Response Actions (planned or taken)
• Reporting Entity • Contact procedures for customers to ask questions or learn additional information (including phone number, email address, website, or postal address)	• Description of the incident, including date of breach and discovery • Description of types of unsecured, customer information (e.g., Personal Health Records, customer information, etc.) that were accessed or acquired in the breach* • Whether data was stolen, altered, or accessed	• Steps individuals should take to protect themselves from harm • Reminder to remain vigilant over a recommended time • Request that customers promptly report incidents	• Investigation actions • Actions mitigating harm to customers • Actions to protect against further breaches

Appendix D: Variance Across Reporting Mechanisms

Note: Appendix D summarizes the reporting mechanisms in use and the differences in reporting formats across infrastructure sectors, Federal agencies, and reporting requirements. The following reporting mechanisms are inclusive of both private industry and Federal contractors reporting to the Federal Government. The reader should refer to Appendix B for more details about the reporting requirements and expectations.

Infrastructure Sector	Agency to Whom Report Must be Submitted	Incident Reporting Requirement/ Interpretive Guidance (In-effect)	Format that Reports Can Be Submitted
All sectors	Contracting and/or Funding Agency for the Applicable Contract	National Industrial Security Program Operating Manual (FAR subpart 4.4 & 52.204-232 C.F.R part 117, 32 C.F.R 117.8) Basic Safeguarding of Covered Contractor Information Systems (FAR subpart 4.19 & 52.204-21(b)(xii))	None specified
Transportation	DOT - FAA	Assigning, maintaining, and enhancing safety and security (Title 49 U.S.C. § 40101(d)) Promote safe flight of civil aircraft in air commerce (49 U.S.C. § 44701(a)(5))	Email, Phone, Mail, or other similar method for initial notification or submitting incident reports *Note: As far as how the reports are submitted, it's in the manner the FAA has agreed to with the individual design approval holder (DAH) (type design holder, parts manufacturer approval and Technical Standard Order Approval holder).*
Transportation	USCG	Suspicious Activity, Breaches of Security, or Transportation Security Incidents (33 C.F.R. § 101.305 and CG-5P Policy Letter 08-16) Hazardous Conditions (33 C.F.R. § 160.216) Evidence of Sabotage or Subversive Activity (33 C.F.R. § 6.16-1)	Email, Phone, Mail, or other similar method for initial notification or submitting incident reports Contact USCG National Response Center (Phone: 1-800-424-8802; Email: NRC@uscg.mil)

Transportation	TSA (through CISA)	Enhancing Public Transportation and Passenger Railroad Cybersecurity (Security Directive, SD 1582-21-01 series) Enhancing Surface Transportation Security Cybersecurity, Surface Transportation Information Circular (IC) 2021-01 Enhancing Pipeline Cybersecurity Security Directive Pipeline-2021-01 series Enhancing Pipeline Cybersecurity, Information Circular (IC) Pipeline-2022-01 Enhancing Rail Cybersecurity Security Directive 1580-21-01 series Airport Security Program (ASP) National Amendment TSA-NA-21-05: "Cybersecurity Incident Reporting" (Airports) Aircraft Operator Standard Security Program (AOSSP) Full All Cargo Aircraft Operator Standard Security Program (FACAOSSP) Twelve Five Standard Security Program (TFSSP) Private Charter Standard Security Program (PCSSP) via security program changes) Indirect Air Carrier Standard Security Program (IACSSP) Certified Cargo Screening Standard Security Program	Online Submission System, Email, Phone, or other similar method for initial notification or submitting incident reports to CISA Contact CISA Central (Online: https://us-cert.cisa.gov/forms/report; Phone: 888-282-0870; Email: report@CISA.gov) (Submissions go to the CISA Incident Reporting System or by calling CISA Central, who then fills out the CISA Incident Reporting System form for the caller. Or, by email in which case the reporter is directed to fill out the Incident Reporting System form.)

		(CCSP) via security program changes	
Chemical	CISA	Chemical Facility Anti-Terrorism Standards (CFATS)[59] (See 6 C.F.R part 27)	Online Submission System, Email, Phone, or other similar method for initial notification or submitting incident reports Contact CISA Central (Online: https://us-cert.cisa.gov/forms/report; Phone: 888-282-0870; Email: report@CISA.gov) (Submissions go to the CISA Incident Reporting System or by calling CISA Central, who then fills out the CISA Incident Reporting System form for the caller. Or, by email in which case the reporter is directed to fill out the Incident Reporting System form.)
Defense Industrial Base	DoD	Safeguarding Covered Defense Information and Cyber Incident Reporting (48 C.F.R. § 252.204-7012) Cyber incident reporting for cloud computing services (DFARS § 252.239-7010(d))	Online Submission System Contact DoD (Online: https://dibnet.dod.mil)
Defense Industrial Base	DoD	Armed Forces § 391. Reporting on cyber incidents with respect to networks and information systems of operationally critical contractors and certain other contractors (10 U.S.C. § 391) Armed Forces § 393. Reporting on penetrations of networks and information systems of certain contractors (10 U.S.C. § 393)	Online Submission System Contact DoD (Online: https://dibnet.dod.mil; Phone: (877) 838-2174; Email: DC3.DCISE@us.af.mil)

59. The CFATS regulation requires any facility which possesses certain chemicals of interest to report their holdings and therefore regulates not just the Chemical Sector, but facilities within other sectors which possess dangerous chemicals such as the Food and Agriculture Sector and Oil and Natural Gas Sector, among others.

Nuclear	NRC	"Cyber security event notifications" (10 C.F.R. § 73.77)	Initial notification via dedicated Emergency Notification System telephone. In the event a reporting entity cannot make the notification via Emergency Notification System telephone, reports are accepted through other means (e.g., commercial telephone, email). Online submission system or other means for subsequent notifications (e.g., written reports). Contact NRC Headquarters Operations Center (Email/Phone/Mail: https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-appa.html; Form: https://www.nrc.gov/reading-rm/doc-collections/forms/nrc366info.html)
Communications	DOJ	Reporting Incidents and Breaches (In Effect)	Email, Phone, Mail, or other similar method for initial notification or submitting incident reports Contact DOJ: (Email: compliance.incidents2@usdoj.gov)
Communications	FCC	Network Outage Reporting System (NORS) "Notification of customer proprietary network information (CPNI) security breaches" (47 C.F.R. § 64.2011)	Online Submission System. In the event reporting entity cannot access the online system, reports are accepted through other means (e.g., email or phone) Contact Public Safety and Homeland Security Bureau, Cybersecurity and Communications Reliability Division (Online: Network Outage Reporting System (NORS) | Federal Communications Commission (fcc.gov); Email/Phone/Mail: Contact | Federal Communications Commission (fcc.gov)) Contact United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) via a link to the reporting facility maintained by the FCC (Online: http://www.fcc.gov/eb/cpni)
Health and Public Health	FTC	Health Breach Notification Rule	Online Submission System Contact FTC (Online: https://www.ftc.gov/business-guidance/resources/health-breach-notification-rule-basics-business)
Health and Public Health	HHS	The HIPAA Breach Notification Rule (In Effect) (45 C.F.R. §§ 164.400-414)	Online Submission System Contact HHS (Online: https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf)

Health and Public Health	FDA	Medical Device Reporting (21 C.F.R Part 803) Corrections and Removals (21 C.F.R Part 806)	Online and Paper Submission System Contact FDA CDRH (Online: https://www.fda.gov/media/69876/download)
Energy	DOE	DOE-417 Electric Emergency Incident and Disturbance Report	Online Submission System. Email, Phone, Mail, or other similar method for initial notification or submitting incident reports Contact DOE (Online: ISER - Electric Disturbance Events (DOE-417); Email: oe417@doe.gov)
Energy-Electricity	E-ISAC and CISA	Critical Infrastructure Protection Reliability Standards CIP-003-8 (Cyber Security – Security Management Controls) CIP-008-6 (Cyber Security – Incident Reporting and Response Planning)	Online Submission System. Email, Phone, Mail, or other similar method for initial notification Contact CISA Central (Online: https://us-cert.cisa.gov/forms/report; Phone: 888-282-0870; Email: report@CISA.gov) Contact E-ISAC (Online: Sign In (eisac.com))
Financial Services	Treasury	Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime (In Effect) Bank Secrecy Act (12 U.S.C. §§ 1813 and 1818; 31 U.S.C. § 5318)	Online Submission System Contact FinCEN (Online: BSA E-Filing (treas.gov))
Financial Services	SEC	Regulation Systems Compliance and Integrity ("Reg. SCI", 17 C.F.R § 242.1000)	Online Submission System. Phone for initial notification Contact SEC (Online: EDGAR Login (sec.gov))
	SEC	SEC Regulation S-P: Privacy of Consumer Financial Information ("Reg. S-P")	*Note: Regulation S-P does not require a report to the SEC. However, it requires the provision of privacy notices to customers.*
	SEC	SEC Regulation S-ID: Identity Theft Red Flags (Reg. S-ID)	*Note: Regulation S-ID does not require a report to the SEC. However, it requires the provision of privacy notices to customers.*
	SEC	Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure	*Note: The SEC Final Rule Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure does not require a report to the SEC. However, it requires registrants to disclose the*

			material cybersecurity incident on the company's Form 8-K.
Financial Services	OCC	Computer-Security Incident Notification Rule (12 C.F.R. part 304)	Online Submission System. Email, Phone, Mail, or other similar method Contact OCC (Online: BankNet; OCC supervisory office or designated point of contact through email, telephone, or other similar method)
		Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (Final Interagency Guidance) (12 C.F.R. part 30)	*Note: This interagency guidance does not require a report to the OCC. However, it requires the provision of privacy notices to customers. The reporting mechanism for the customer notice is not specified in the interagency guidance.*
Financial Services	FDIC	Computer-Security Incident Notification Rule (12 C.F.R. part 304)	Email, Phone, Mail, or other similar method for initial notification or submitting incident reports Contact FDIC (Supervisory Case Manager; Email: incident@FDIC.gov)
		Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (Final Interagency Guidance) (12 C.F.R. part 364)	*Note: This interagency guidance does not require a report to the FDIC. However, it requires the provision of privacy notices to customers. The reporting mechanism for the customer notice is not specified in the interagency guidance.*
Financial Services	FRB	Computer-Security Incident Notification Rule (12 C.F.R. §§ 225.300 to .303)	Email, Phone, Mail, or other similar method for initial notification or submitting incident reports Contact FRB (Email: incident@frb.gov; Phone: 866-364-0096)
	FRB	Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (Final Interagency Guidance) (12 C.F.R. part 208, app. D-2, 12 C.F.R. part 225, app. F)	*Note: This interagency guidance does not require a report to the FRB. However, it requires the provision of privacy notices to customers. The reporting mechanism for the customer notice is not specified in the interagency guidance.*

Financial Services	CFTC	System Safeguards for Swap Execution Facilities (17 C.F.R. part 37) System Safeguards for Designated Contract Markets (17 C.F.R. part 38) System Safeguards for Derivatives Clearing Organizations (17 C.F.R. part 39) System Safeguards for Swap Data Repositories (17 C.F.R. part 49)	Online Submission System Contact CFTC (Online: https://portal.cftc.gov)
Financial Services	NCUA	Guidelines for Safeguarding Member Information (Final Agency Guidance) (12 C.F.R. part 748, Appendix A) Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice (12 C.F.R. part 748, Appendix B)	Email, Phone, Mail, or other similar method for initial notification or submitting incident reports
Financial Services	FHFA	Enterprise Cybersecurity Incident Reporting (Final Agency Guidance) (FHFA Advisory Bulletin 2020-05) Information Security Risk Management (FHFA Advisory Bulletin 2017-02)	Email, Phone, Mail, or other similar method for initial notification or submitting incident reports

Appendix E: A Model Reporting Form and Reference Sheet

Model Reporting Form

FOIA Exemptions:

Information in this form (identify section) will not be disclosed to the public to the extent that a government agency in receipt of an applicable Freedom of Information Act (FOIA) request determines that it satisfies the criteria for an exemption under FOIA. If the reporting entity believes that some or all the information included in this form meets the criteria for a FOIA exemption, identify (by selecting all that apply) whether the information contains:

Choose an item

☐ Trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential

☐ Other information exempt from FOIA (include a description of the exemption below)

Please identify the section(s) below that should be exempt from FOIA:

Choose an item

Choose an item

Choose an item

Section A: Identifying the Reporting Entity/Contact Information

Choose an item

Choose an item

Choose an item

Model Reporting Form

A. Identifying the Reporting Entity/Contact Information

Name of Reporting Entity:		**Name of Sub-Entity:**	
Organization Web Site:		**Entity Type:** Choose an item	
What critical infrastructure sector(s) does your entity fall under (if applicable)? Choose an item Choose an item Choose an item			
Organization Internal Incident Tracking Number (if applicable):			
Business Identifier (if applicable): ☐ **North American Industrial Classification System (NAICS):** ☐ **General Services Administration-Issued Unique Entity Identifier (UEI):** ☐ **Other/Miscellaneous:**			
Name of Reporting Individual (First, Middle, Last, Suffix): .			
Classified Phone Number, if applicable:	**Unclassified Phone Number:**	**Classified Email, if applicable:**	**Unclassified Email:**
Physical Address (Street Address, City, State, Zip code):		**Reporting Individual Position:**	

Model Reporting Form

Name of Person Available 24/7 (First, Middle, Last, Suffix):			
Classified Phone Number, if applicable: .	**Unclassified Phone Number:**	**Classified Email, if applicable:**	**Unclassified Email:**
Report Type and Status (Select all that apply): ☐ Initial Report ☐ Update/Supplemental ☐ Final Report			
Other Comments: .			

B. Information on Assistance

Do you require outside support to diagnose, mitigate, or recover from this incident? ☐ Yes ☐ No
Are you or do you plan to retain assistance of a non-Federal entity for the reported incident? ☐ Yes ☐ No
Have you requested on-site or remote assistance from any Federal Agency? ☐ Yes ☐ No
Would you like to make a request to the Federal government for support? ☐ Yes ☐ No
Provide any additional detail regarding nature of assistance being requested:

Model Reporting Form

C. Other Notifications or Publicity

Please indicate Agencies with whom you have an existing reporting relationship and to whom this information will be provided:

Choose an item

Choose an item

Choose an item

Click or tap here to enter text.

Has your regulator been notified?

☐ Yes ☐ No

Please provide the Date & Time of notification (if applicable):

Has this incident been reported to law enforcement?

☐ Yes ☐ No

Name of law enforcement agency(ies) (if applicable):

Name of law enforcement official (First, Middle, Last, Suffix): .

Classified Phone Number:	**Unclassified Phone Number:**	**Classified Email:**	**Unclassified Email:**

Please provide additional law enforcement contacts below:

Has this been reported to the U.S. Congress?	**Is there media coverage or other widely available public coverage of the incident?**
☐ Yes ☐ No	☐ Yes ☐ No

If known, are discussions about the incident taking place in online communities? ☐ No ☐ Yes

D. Incident Impacts

Description of Incident:

Did this incident involve an attributed cyber intrusion? Please provide a source of vetting below: ☐ Yes ☐ No ☐ Under Investigation ☐ Unknown	**Is this activity associated with a previously reported incident?** ☐ Yes ☐ No ☐ Under Investigation ☐ Unknown
Did this incident involve exposure of classified information? ☐ Yes ☐ No ☐ Under Investigation ☐ Unknown	**Please characterize the observed activity at its most severe level:** Choose an item ☐ Under Investigation ☐ Unknown

Type of Incident:

Choose an item

What is the known physical impact from the incident? (Physical Impact)

☐ No Impact
☐ Damage or destruction to Non-Critical Property
☐ Damage or destruction to Critical Property
☐ Damage or destruction to Non-Critical Systems
☐ Damage or destruction to Critical Systems
☐ Under Investigation
☐ Unknown

Model Reporting Form

Identify the current level of impact on your entity's functions or services (Functional Impact):

☐ No Impact (Fully mitigated)
☐ No Impact to Delivery of Services
☐ Minimal Impact to Non-Critical Services
☐ Minimal Impact to Critical Services
☐ Significant Impacts to Non-Critical Services
☐ Significant Impact to Critical Services
☐ Denial of Non-Critical Services
☐ Denial of Critical Services/Loss of Control
☐ Under Investigation
☐ Unknown

What is the known or suspected informational impact from the incident? (Informational Impact)

☐ No Impact (Fully mitigated)
☐ Suspected, But Not Identified
☐ Loss or compromise of Personal or Customer Data
    ☐ PII
    ☐ PHI
    ☐ Other (Please specify below)
☐ Loss or compromise of Proprietary Information
☐ Loss or compromise of data about Critical Systems
☐ Core Credential Compromise
☐ Under Investigation
☐ Unknown

Types of systems and devices that were impacted (check all that apply):

☐ Operational Data (e.g., network diagrams, configuration files, traffic flows)
☐ Operational Technology/technologies
☐ Operational Functionality
☐ Operating Systems
☐ Industrial Control System(s)
☐ Server Types
☐ Network Devices
☐ Identity Providers

Model Reporting Form

☐ Users ☐ Other (Please specify below)	
Name of Impacted System or Device:	**Nature of Impact: Unauthorized-** ☐ Modification ☐ Deletion ☐ Exfiltration ☐ Access ☐ N/A ☐ Other
	System or Device Description:
	When was the activity first detected?
	Technical details of what was identified:
	Does the impacted system/device contain or process information created by or for an element of the Intelligence Community? ☐ Yes ☐ No ☐ Under Investigation ☐ Unknown
	Did the impacted system/device contain classified information? ☐ Yes ☐ No ☐ Under Investigation ☐ Unknown

Model Reporting Form

	Physical location(s) of impacted system (if applicable):
Please provide additional impacted systems or devices using the same set of questions identified above (if applicable):	
Please identify the direct number of customers affected by the incident (if applicable): Choose an item	**If you are a Managed Service Provider or other Third-Party Service Provider, please identify the number of customers affected by the incident (if applicable):** Choose an item
Identify the number of individuals whose PII is impacted (if applicable): Choose an item Enter number here	**Was any PII observed on the Internet? (if applicable)** ☐ Yes ☐ No ☐ Under Investigation ☐ Unknown
	Were impacted individuals notified? ☐ Yes ☐ No **If so, how were individuals notified?** ☐ Email ☐ Short Message Service ☐ Verbal ☐ Parcel ☐ Other (Please list method used)
	Number of Individuals notified?

Model Reporting Form

	Were services provided? ☐ Yes ☐ No
Was this incident considered a ransomware incident? ☐ Yes ☐ No ☐ Under Investigation ☐ Unknown	**If yes, please provide the following (if applicable):** **Date of payment:**
	Text of ransom requested:
	Type of ransom demand currency:
	Text of payment instructions:
	Where was payment sent (virtual wallet or physical address):
	Amount of payment:
	Other information regarding the ransomware incident:

As far as is known, which of the following best describes the incident outcome:

☐ Blocked: The incident was blocked by pre-emptive measures including rate limiting or spam filters

☐ Successful attempt: The incident has been determined to have caused at least some harm

☐ Failed attempt: The incident didn't succeed, but not due to any affirmative defense

☐ False positive: An incident was determined to have been triggered by a false alert and no actions, including automatically performed automated actions, were needed to remediate the issue.

☐ Low value: An incident that has been deemed to be sufficiently unimportant for human intervention or may otherwise be considered noise. ☐ Suspected: An incident is suspected, but not yet confirmed.
Identify any known or potential secondary or cascading impacts (if applicable): ☐ Financial Loss ☐ Reputation/Credibility ☐ Impact Across National Critical Functions and/or Critical Infrastructure ☐ Other (Please specify below)

E. Cyber Threat Activity and Discovery

Date/Time Discovered:	**Date/Time Reported:**
Describe how the incident was identified?	
Have you identified the initially affected device? ☐ Yes ☐ No **If yes, please describe the initially affected device (i.e., point of detection or access point).**	**What detection methods were used to discover this activity?** ☐ Administrator ☐ Anti-Virus Software ☐ Commercial and/or publicly available solution ☐ External source notification ☐ Human review ☐ Internally developed/proprietary solution ☐ Intrusion Detection System (IDS) ☐ Log Review ☐ User ☐ Unknown ☐ Other (Please specify detection method)

Model Reporting Form

What network location(s) was the activity observed in (if applicable)?	**What information system(s) and/ or devices was the activity initially observed in?**
	What network segments(s) and virtual Local Area Network(s) was the activity observed in?
Suspected Duration of Unauthorized Access Prior to Detection and Reporting:	
Do you have applicable logs available (e.g., network, system logs, and memory captures)? ☐ Yes ☐ No	
Technical Threat Profile (Indicators of Compromise):	
Technical Threat Profile (Techniques, Tactics, and Procedures) **Please select the attack vector(s) that led to the incident:** ☐ Drive-by Compromise ☐ Exploit Public-Facing Application ☐ Exploitation of Remote Services ☐ External Remote Services ☐ Hardware Additions ☐ Internet Accessible Device ☐ Lockscreen Bypass ☐ Phishing ☐ Remote Services ☐ Replication Through Removable ☐ Media ☐ Rogue Master ☐ Supply Chain Compromise ☐ Spearphishing Attachment ☐ Transient Cyber Asset ☐ Trusted Relationship ☐ Valid Accounts	

Model Reporting Form

☐ Wireless Compromise
☐ Other (Please specify below)

Please select the enterprise attack vectors detected during the investigation (MITRE ATT&CK matrices):	**Please select the mobile attack vectors detected during the investigation (MITRE ATT&CK matrices):**	**Please select the ICS attack vectors detected during the investigation (MITRE ATT&CK matrices):**
☐ Reconnaissance ☐ Resource Development ☐ Initial Access ☐ Execution ☐ Persistence ☐ Privilege Escalation ☐ Defense Evasion ☐ Credential Access ☐ Discovery ☐ Lateral Movement ☐ Collection ☐ Command and Control ☐ Exfiltration ☐ Impact ☐ N/A	☐ Initial Access ☐ Execution ☐ Persistence ☐ Privilege Escalation ☐ Defense Evasion ☐ Credential Access ☐ Discovery ☐ Lateral Movement ☐ Collection ☐ Command and Control ☐ Exfiltration ☐ Impact ☐ Network Effects ☐ Remote Service Effects ☐ N/A	☐ Initial Access ☐ Execution ☐ Persistence ☐ Privilege Escalation ☐ Evasion ☐ Discovery ☐ Lateral Movement ☐ Collection ☐ Command and Control ☐ Inhibit Response Function ☐ Impair Process Control ☐ Impact ☐ N/A

Assessed Advanced Persistent Threat or other Threat Actor Identification (if known):

If known and applicable, what security defenses were in place and compromised? (Optional):

Please identify the specific security controls that were compromised that led to this event: (1) If known and applicable, please identify the security controls that were implemented and could have averted this attack? (2) Have the security controls been implemented in one business system or entity-wide; and (3) any other details?

Choose an item

Choose an item

Choose an item

Choose an item

Choose an item

Please refer to NIST 800-53 or relevant security overlays (e.g., NIST 800-82, NIST 800-161, NERC CIP).

F. Consumer Data Breach, Privacy and Protections (if applicable)

Communications to Individuals:

Has your entity provided guidance or steps for how individuals impacted by loss or compromise of PII can protect themselves during the ongoing incident?

☐ Yes ☐ No ☐ N/A

Has your entity reminded individuals to remain vigilant over a recommended time period?

☐ Yes ☐ No ☐ N/A

Has your entity requested that individuals promptly report incidents involving use of compromised PII directly to law enforcement?

☐ Yes ☐ No ☐ N/A

G. Reporting Entity Response Actions (if known)

Which phase of incident response actions are you currently in?

Choose an item

What remediation and/or mitigation actions has your entity taken or have planned?

Date/time of event resolution?

Estimated recovery date and time?

Model Reporting Form Reference Sheet

Background: This Model Reporting Form (MRF) Reference Sheet can be used as supporting documentation when a reporting entity fills out the MRF or responds to the "data elements" identified therein.[60] The bolded print below directly corresponds to the sections identified in the MRF (e.g., Section B: Information on Assistance, Section C: Other Notifications or Publicity, Section D: Incident Impacts). The italicized questions under each bolded section correspond to the data elements identified under that particular section of the MRF in the order as they appear. Finally, the Roman numerals under the italicized print contain references to assist the reporting entity in completing the requested information. *Please note that this reference sheet does not incorporate references for every question on the MRF.*

FOIA Exemptions (p. 1):

- Reference: FOIA.gov - Freedom of Information Act, (https://www.foia.gov/faq.html)
- Reference: To make an initial request for information exempt from FOIA, the reporting entity should identify the type of information meeting a FOIA exemption and select the section(s) of the MRF that should be exempt from FOIA.

A. Identifying the Reporting Entity/Contact Information (pp. 2-3):

- *What critical infrastructure sector(s) does your entity fall under (if applicable)?*
  - *i.* Reference: Critical Infrastructure Sectors | CISA (https://www.cisa.gov/critical-infrastructure-sectors)
  - *ii.* Reference: The reporting entity should select "Other" if uncertain about which critical infrastructure sector it falls under and provide additional details in the text box.

- *Business Identifier (if applicable):*
  - *i.* Reference: North American Industry Classification System (NAICS), U.S. Census Bureau (https://www.census.gov/naics/)
  - *ii.* Reference: US Federal Contractor Registration (USFCR) | SAM.gov Registrations (https://usfcr.com/?utm_medium=ppc&utm_term=sam.gov&utm_campaign=SAM&utm_source=bing&hsa_tgt=kwd-73736180510968:loc-190&hsa_ad=&hsa_src=o&hsa_mt=e&hsa_ver=3&hsa_cam=122161541&hsa_acc=1449812725&hsa_kw=sam.gov&hsa_grp=1179776864573879&hsa_net=adwords&msclkid=1174023f65b61d5ca57b61ec913ad6c2)
  - *iii.* Reference: American LEI: LEI number | Official Registration Agent (https://americanlei.com/?utm_source=bing&utm_medium=cpc&utm_campaign=%28S%29%20-%20USA&utm_term=LEI%20%2B%20Legal%20Entity%20Identifier%20%28BM%29&utm_content=Legal%20Identifier&msclkid=dc63681ab2ad161d44ed0c1d3a8006b4)

60. In coordination with CIRC members, DHS developed a model reporting form and template. Additional review and refinement of the MRF may be necessary as a future project of the CIRC.

B. Information on Assistance (p. 3):

- *Provide any additional detail regarding nature of assistance being requested:*
  - *i.* Reference: DHS Role in Cyber Incident Response | CISA (https://www.cisa.gov/resources-tools/resources/dhs-role-cyber-incident-response)
  - *ii.* Reference: Information regarding the nature of assistance could include but is not limited to incident response resources, security assessments, investigative, potential attribution, and assistance with news media.

C. Other Notifications or Publicity (pp. 4-5):

- *Please indicate Agencies with whom you have an existing reporting relationship and to whom this information will be provided:*
  - *i.* Reference: This data element includes a list of Federal departments and agencies, Information Sharing and Analysis Centers, and an option to include other stakeholders that receive Federal cyber incident reporting via Federal regulations and voluntary reporting. This list allows the Federal government to coordinate on the backend with whom the reporting entity has reported or plans to provide the information.
  - *ii.* CFTC – Commodity and Futures Trading Commission
  - *iii.* CISA – Cybersecurity and Infrastructure Security agency
  - *iv.* DOD – Department of Defense
  - *v.* DOE – Department of Energy
  - *vi.* DOJ – Department of Justice
  - *vii.* DOT – Department of Transportation
  - *viii.* FAA – Federal Aviation Administration
  - *ix.* FBI – Federal Bureau of Investigation
  - *x.* FCC – Federal Communications Commission
  - *xi.* FDA – Food and Drug Administration
  - *xii.* FDIC – Federal Deposit Insurance Corporation
  - *xiii.* FEMA – Federal Emergency Management Agency
  - *xiv.* FERC – Federal Energy Regulatory Commission
  - *xv.* FHFA – Federal Housing Finance Agency
  - *xvi.* FRB – Federal Reserve Board
  - *xvii.* FTC – Federal Trade Commission
  - *xviii.* GSA – General Services Administration
  - *xix.* HHS – Department of Health and Human Services
  - *xx.* ISAC – Information Sharing and Analysis Center
  - *xxi.* NCUA - National Credit Union Administration
  - *xxii.* NRC – Nuclear Regulatory Commission
  - *xxiii.* OCC – Office of the Comptroller of the Currency
  - *xxiv.* SEC – Securities and Exchange Commission
  - *xxv.* SRMA – Sector Risk Management Agency
  - *xxvi.* Treasury – Department of the Treasury
  - *xxvii.* TSA – Transportation Security Administration
  - *xxviii.* USCG – United States Coast Guard
  - *xxix.* USSS – United States Secret Service
  - *xxx.* Other – Please specify in the narrative text box

- *Please provide the Date & Time of notification (if applicable):*
  i. Reference: National Institute of Standards and Technology | NIST (https://time.gov/)

- *Please provide additional law enforcement contacts below:*
  i. Reference: The reporting entity should use the same format for reporting additional law enforcement contacts (e.g., Name of law enforcement agency(ies) (if applicable), Name of law enforcement official (First, Middle, Last, Suffix), Classified Phone Number, Unclassified Phone Number, Classified Email, and Unclassified Email) to include State, Local, Tribal, and Territorial or international authorities. If the reporting entity reported the incident to law enforcement using a law enforcement-hosted website, please list the website (e.g., https://www.ic3.gov/).

- *Is there media coverage or other widely available public coverage of the incident?*
  i. Reference: The reporting entity should answer "Yes" if the reporting entity has made a public statement on the incident.

D. Incident Impacts (pp. 5-10):

- *Did this incident involve an attributed cyber intrusion?*
  i. Reference: For the purposes of this report, an attributed cyber intrusion refers to an intrusion that has been ascribed to a responsible party. A cyber intrusion would be unattributed if the reporting entity is not aware of a vetted (*see reference below for further information on "vetted" sources*) determination of a party responsible for the intrusion based on any identified Techniques, Tactics or Procedures, previously attributed Indicators of Compromise, or other evidence collected during the incident response process or investigation.
  "Vetted" could be provided by internal (i.e., through attacker self-identification, Cyber Security Service Provider, etc.) or external sources (i.e., Law Enforcement, Intelligence, CISA, commercial cyber security organization, etc.).
  ii. Reference: An intrusion is a security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without having authorization to do so: intrusion - Glossary | CSRC (https://csrc.nist.gov/glossary/term/intrusion)
  iii. Reference: If the reporting entity selects "No", the reporting entity will have a chance to identify whom they are attributing the cyber incident to under Section E: Cyber Threat Activity and Discovery.

- *Did this incident involve exposure of classified information?*
  i. Reference: classified information - Glossary | CSRC (https://csrc.nist.gov/glossary/term/classified_information)
  ii. Reference: According to NIST, classified information or classified national security information means information that has been determined pursuant to E.O. 12958 as amended by E.O. 13292 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

- *Is this activity associated with a previously reported incident?*
  i. Reference: If the reporting entity selects "Yes", information on the previously reported incident can be collected during follow-on engagements or during supplemental reporting.

- *Please characterize the observed activity at its most severe level:*
  i. Reference: The ODNI Cyber Threat Framework:
  ii. https://www.dni.gov/files/ODNI/documents/features/A_Common_Cyber_Threat_Framework_Overview.pdf
  iii. https://www.dni.gov/files/ODNI/documents/features/Threat_Framework_A_Foundation_for_Communication_short_version.pdf
  iv. https://www.dni.gov/files/ODNI/documents/features/Cyber_Threat_Framework_Lexicon_20180718.pdf

- *Type of Incident:*
  i. Reference: The most recent version of the STIX 2 specification, 2.1: https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html
  ii. Reference: Section 3.6 of the STIX common objects: https://github.com/oasis-open/cti-stix-common-objects/raw/main/extension-definition-specifications/incident-core/incident-core-extension.docx
  iii. Reference: "STIX" (Structured Threat Information eXpression) is a standardized XML programming language for conveying data about cybersecurity threats in a common language that can be easily understood by humans and security technologies. Designed for broad use, there are several core use cases for STIX. First, it is used by threat analysts to review cyberthreats and threat-related activity. Threat analysts also use STIX to identify patterns that could indicate cyberthreats. Any sort of decision maker or operations personnel may use STIX data to help facilitate cyberthreat response activities, including prevention, detection and response. The final core use for STIX is the sharing of cyber threat information within an organization and with outside partners or communities that benefit from the information." Definition from TechTarget: https://www.techtarget.com/searchsecurity/definition/STIX-Structured-Threat-Information-eXpression
  iv. Reference: A "significant cyber incident" is a cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. (Presidential Policy Directive -- United States Cyber Incident Coordination | whitehouse.gov (archives.gov))

- *What is the known physical impact from the incident? (Physical Impact)*
  i. Reference: Physical, Functional, Informational Impact questions are derived from the Federal Incident Notification Guidelines (FING) and will be republished in the upcoming Federal Incident Reporting Requirements (FIRR). https://www.cisa.gov/uscert/incident-notification-guidelines#impact-category-descriptions

ii. Reference: The questions are based on years of cyber incident work CISA has led as well as a synthesis of governing body of knowledge such as NIST 800-61 r2 as well as industry/educational institute leaders such as Carnegie Mellon University, Software Engineering Institute: SEI Digital Library (https://resources.sei.cmu.edu/library/), and the European Union Agency for Cybersecurity (ENISA) ENISA (https://www.enisa.europa.eu/) and by Forum of Incident Response and Security Teams, Inc., CSIRT Services Framework Version 2.1 (https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1)

- *Identify the current level of impact on your entity's functions or services (Functional Impact):*
  i. Reference: Physical, Functional, Informational Impact questions are derived from the Federal Incident Notification Guidelines (FING) and will be republished in the upcoming Federal Incident Reporting Requirements (FIRR). https://www.cisa.gov/uscert/incident-notification-guidelines#impact-category-descriptions
  ii. Reference: The questions are based on years of cyber incident work CISA has led as well as a synthesis of governing body of knowledge such as NIST 800-61 r2 as well as industry/educational institute leaders such as Carnegie Mellon University, Software Engineering Institute: SEI Digital Library (https://resources.sei.cmu.edu/library/) and the European Union Agency for Cybersecurity (ENISA) (https://www.enisa.europa.eu/) and by Forum of Incident Response and Security Teams, Inc. CSIRT Services Framework Version 2.1 (https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1)

- *What is the known or suspected informational impact from the incident? (Informational Impact)*
  i. Reference: Physical, Functional, Informational Impact questions are derived from the Federal Incident Notification Guidelines (FING) and will be republished in the upcoming Federal Incident Reporting Requirements (FIRR) (https://www.cisa.gov/uscert/incident-notification-guidelines#impact-category-descriptions).
  ii. Reference: The questions are based on years of cyber incident work CISA has led as well as a synthesis of governing body of knowledge such as NIST 800-61 r2 as well as industry/educational institute leaders such as Carnegie Mellon University, Software Engineering Institute: SEI Digital Library (https://resources.sei.cmu.edu/library/), and the European Union Agency for Cybersecurity (ENISA) ENISA (https://www.enisa.europa.eu/) and by Forum of Incident Response and Security Teams, Inc. CSIRT Services Framework Version 2.1 (https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1). Reference: Personally Identifiable Information (PII) is any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. PII - Glossary | CSRC (https://csrc.nist.gov/glossary/term/PII)
  iii. Reference: Personal Health Information (PHI) is information, including demographic data, that relates to the individual's: past, present or future physical or mental health

or condition; the provision of health care to the individual; or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. (https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html)

- *Types of systems and devices that were impacted (check all that apply):*
  i. Reference: This question is derived from the Federal Incident Notification Guidelines (FING) and will be republished in the upcoming Federal Incident Reporting Requirements (FIRR) (https://www.cisa.gov/uscert/incident-notification-guidelines#impact-category-descriptions). The question is based on years of cyber incident work CISA has led as well as NIST 800-61 r2 (Chapter 3): SP 800-61 Rev. 2, Computer Security Incident Handling Guide | CSRC (https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final)

- *Nature of Impact: Unauthorized-*
  i. Reference: OMB M-21-02: "Unauthorized modification" is the act or process of changing components of information and/or information systems without authorization or in excess of authorized access.
  ii. Reference: OMB M-21-02: "Unauthorized deletion" is the act or process of removing information from an information system without authorization or in excess of authorized access.
  iii. Reference: OMB M-21-02: "Unauthorized exfiltration" is the act or process of obtaining, without authorization or in excess of authorized access, information from an information system without modifying or deleting it.
  iv. Reference: OMB M-21-02: "Unauthorized access" is the act or process of logical or physical access without permission to a Federal agency information, information system, application, or other resource.

- *When was the activity first detected?*
  i. Reference: National Institute of Standards and Technology | NIST (https://time.gov/)

- *Does the impacted system contain or process information created by or for an element of the Intelligence Community?*
  i. Reference: The Authorities and Activities of the Intelligence Community: The National Security Act of 1947, as amended. Executive Order 12333 of December 4, 1981 as amended July 30, 2008 by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008)
  ii. Reference: Members of the IC (https://www.dni.gov/index.php/what-we-do/members-of-the-ic)

- *Identify the number of individuals whose PII is impacted (if applicable):*
  i. Reference: Personally Identifiable Information (PII) is any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. PII - Glossary | CSRC (https://csrc.nist.gov/glossary/term/PII)

- *Was any PII observed on the Internet? (if applicable)*
  i. Reference: Personally Identifiable Information (PII) is any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. PII - Glossary | CSRC (https://csrc.nist.gov/glossary/term/PII)

- *Was this incident considered a ransomware incident?*
  i. Reference: Ransomware is a type of malicious attack where attackers encrypt an organization's data and demand payment to restore access. Ransomware | NIST (https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware)

- *Amount of payment:*
  i. Reference: As appropriate, please provide the quantity of cryptocurrency or tokens demanded and its U.S. Dollar Value.

- *Other information regarding the ransomware incident:*
  i. Reference: The following are examples of information the reporting entity can provide within this data element: the ransomware variant, whether the reporting entity is still in contact with the ransomware actors, and any third parties that are involved with negotiating and paying ransom, and the availability of decryption capabilities obtained from the ransomware actors or other sources.

- *As far as is known, which of the following best describes the incident outcome:*
  i. Reference: The most recent version of the STIX 2 specification, 2.1 (https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html)
  ii. Reference: Section 4.1 of the STIX common objects (https://github.com/oasis-open/cti-stix-common-objects/raw/main/extension-definition-specifications/incident-core/incident-core-extension.docx)
  iii. Reference: "STIX" (Structured Threat Information eXpression) is a standardized XML programming language for conveying data about cybersecurity threats in a common language that can be easily understood by humans and security technologies. Designed for broad use, there are several core use cases for STIX. First, it is used by threat analysts to review cyberthreats and threat-related activity. Threat analysts also use STIX to identify patterns that could indicate cyberthreats. Any sort of decision maker or operations personnel may use STIX data to help facilitate cyberthreat response activities, including prevention, detection and response. The final core use for STIX is the sharing of cyber threat information within an organization and with outside partners or communities that benefit from the information." Definition from TechTarget (https://www.techtarget.com/searchsecurity/definition/STIX-Structured-Threat-Information-eXpression)

- *Identify any known or potential secondary or cascading impacts (if applicable):*
  i. Reference: National Critical Functions (NCFs) are functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security,

national public health or safety, or any combination thereof. CISA, through the National Risk Management Center (NRMC)(https://www.cisa.gov/nrmc), brings the private sector, government agencies, and other key stakeholders together to identify, analyze, prioritize, and manage the most significant risks, including cyber, physical, and supply chain risks, to these important functions. *See references in the 2018 National Cyber Strategy* (https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf) *and at CISA.gov,* National Critical Functions | CISA (https://www.cisa.gov/national-critical-functions).

ii. Reference: Critical Infrastructure is systems and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. "critical infrastructure" – Glossary | CSRC (https://csrc.nist.gov/glossary/term/critical_infrastructure)

E. Cyber Threat Activity and Discovery (pp. 10-13):

- *Date/Time Reported:*
  - *i.* Reference: National Institute of Standards and Technology | NIST (https://time.gov/)
  - *ii.* Reference: If the reporting entity has an online submission mechanism in place, it may capture the Date/Time reported upon submission of the cyber incident report. For those Federal agencies that do not use an online submission mechanism, but receive reports by phone or email, the agency may need to capture the Date/Time reported. Reporting entities should provide the Date/Time they are submitting the initial report, update, or supplement.

- *Technical Threat Profile (Techniques, Tactics, and Procedures) Please select the attack vector(s) that led to the incident:*
  - *i.* https://attack.mitre.org/techniques/enterprise/
  - *ii.* https://attack.mitre.org/techniques/mobile/
  - *iii.* https://attack.mitre.org/techniques/ics/

- *Please select the enterprise attack vectors detected during the investigation (MITRE ATT&CK matrices):*
  - *i.* https://attack.mitre.org/techniques/enterprise/
  - *ii.* https://attack.mitre.org/techniques/mobile/
  - *iii.* https://attack.mitre.org/techniques/ics/

- *Please select the mobile attack vectors detected during the investigation (MITRE ATT&CK matrices):*
  - *i.* https://attack.mitre.org/techniques/enterprise/
  - *ii.* https://attack.mitre.org/techniques/mobile/
  - *iii.* https://attack.mitre.org/techniques/ics/

- *Please select the ICS attack vectors detected during the investigation (MITRE ATT&CK matrices):*
  - *i.* https://attack.mitre.org/techniques/enterprise/
  - *ii.* https://attack.mitre.org/techniques/mobile/

iii. https://attack.mitre.org/techniques/ics/

- *Assessed Advanced Persistent Threat or other Threat Actor Identification (if known):*
  i. Reference: An Advanced Persistent Threat (APT) is an adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception), to generate opportunities to achieve its objectives, which are typically to establish and extend its presence within the information technology infrastructure of organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future. The advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives. "advanced persistent threat" - Glossary | CSRC (https://csrc.nist.gov/glossary/term/advanced_persistent_threat)

F. Consumer Data Breach, Privacy and Protections (if applicable, p. 13):

- Consumer Data Breach, Privacy and Protections (if applicable)
  i. Reference: See guidance in HIPAA Breach Notification Rule. Breach Notification Rule | HHS.gov (https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html)
  ii. Reference: See guidance in Health Breach Notification Rule. 16 C.F.R Part 318 -- Health Breach Notification Rule (https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-318)

G. Reporting Entity Response Actions (if known, p. 13):

- *Which phase of incident response actions are you currently in?*
  i. Reference: *NIST SP 800-61 Rev 2, Computer Security Incident Handling Guide*, p. 21, phases of incident response. SP 800-61 Rev. 2, Computer Security Incident Handling Guide | CSRC (nist.gov) (https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final)
  ii. Reference: Phases of Incident Response: 1) Detection/Identification; 2) Analysis; 3) Containment; 4) Eradication; 5) Recovery; and 6) Post-Incident Activity

Appendix F: Potential Common Terminology for Types of Cyber Incident Reports

Type of Report	Purpose/Definition	Mandatory or Optional?	Method of Transmission
Initial Incident Report	An initial incident report provides information about a reportable incident.	Mandatory if the incident meets the definition of a reportable incident.	Telephone/voice, email, Model Reporting Form, or agency online submission system adapted to the Model Reporting Form.
Supplemental Incident Report	A supplemental incident report to an initial incident report makes the report more complete.	Mandatory if the reporting entity becomes aware of significant new information.	Update the Model Reporting Form or online submission system adapted to the Model Reporting Form. If initial incident report was by telephone, then this supplemental incident report may take the form of submission of Model Reporting Form.
Incident Update	An incident update to an incident report corrects or amends the information previously provided to make the report more accurate.	Mandatory if reporting entity realizes that significant previously submitted information was erroneous.	Update the Model Reporting Form or online submission system adapted to the Model Reporting Form. If initial incident report was by telephone, then this incident update may take the form of submission of Model Reporting Form.
Final Incident Report	An optional final report is one submitted by the reporting entity to affirmatively complete the record or communicate that it considers the incident resolved.	Generally optional. Mandatory if the incident may impact delivery of NCFs, vital goods or services to the public.	Update the Model Reporting Form or online submission system adapted to the Model Reporting Form.

Appendix G: DHS Recommendations

DHS Recommendations on Harmonization of Federal Cyber Incident Reporting	
Recommendation 1:	The Federal Government should adopt a model definition of a reportable cyber incident wherever practicable. Federal agencies should evaluate the feasibility of adapting current and future cyber incident reporting requirements to align to a model definition of a reportable cyber incident.
Recommendation 2:	The Federal Government should adopt model cyber incident reporting timelines and triggers wherever practicable. Federal agencies should evaluate the feasibility of adapting current and future cyber incident reporting requirements to align to model timeline and trigger provisions.
Recommendation 3:	Agencies with requirements for covered entities to provide notifications to affected individuals or the public should consider whether a delay is warranted when such notification poses a significant risk to critical infrastructure, national security, public safety, or an ongoing law enforcement investigation.[60] A decision to delay the notification to affected individuals or the public would not delay required notification to regulators.
Recommendation 4:	The Federal Government should adopt a model reporting form for cyber incident reports wherever practicable. Agencies should evaluate the feasibility of leveraging the model form for cyber incident reporting or incorporate the data elements identified therein into reporting forms, web portals, or other submission mechanisms.
Recommendation 5:	The Federal Government should assess how best to streamline the receipt and sharing of cyber incident reports and cyber incident information, including through improvements to existing reporting mechanisms or the potential creation of a single portal.
Recommendation 6:	Federal cyber incident reporting requirements should allow for updates and supplemental reports.
Recommendation 7:	The Federal Government should adopt common terminology regarding cyber incident reporting wherever practicable. Agencies should evaluate the feasibility of leveraging a common lexicon for initial, supplemental, updates, and final reports.
Recommendation 8:	The Federal Government should improve processes for engaging with reporting entities following the initial report of a cyber incident. Agencies should coordinate among themselves, whenever practicable, prior to engaging with a reporting entity to reduce the burden on the reporting entity.

60. In some circumstances, immediately making information or data concerning a cybersecurity incident readily accessible and available could result in increased risks to affected entities or interfere in an ongoing criminal investigation. Such non-confidential disclosures (described as "public disclosures") should be coordinated with appropriate law enforcement officials.

Appendix H: Proposed Legislative Changes

DHS Proposed Legislative Changes to Address the Duplicative Reporting	
Legislative Change 1:	Congress should remove any legal or statutory barriers to harmonization identified by the CIRC, including authorizing adoption of the model definitions of a reportable cyber incident, timeline and trigger provisions, and cyber incident reporting form and/or common data elements for current and future Federal cyber incident reporting requirements.
Legislative Change 2:	Congress should provide authority and funding, as requested by the Administration, to Federal agencies to enable them to collect and share common cyber incident data elements that may not otherwise be authorized.
Legislative Change 3:	Congress should exempt from disclosure under FOIA, or other similar legal mechanisms, cyber incident information reported to the Federal Government and protect any relevant privileges.