Ransomware, Incident Reporting, and the Critical Infrastructure Designation for Cable Networks

A technical paper prepared for presentation at SCTE TechExpo24

Brian A. Scriber
Distinguished Technologist and VP of Security Technologies
CableLabs
b.scriber@cablelabs.com

Table of Contents

List of Figures

List of Tables

Title **Page Number**

1. Abstract

New policies in the US, UK, and EU address expectations on network operators including incident reporting, patching, updates, software bill of materials (SBOM), cybersecurity bill of materials (CBOM), and zero trust architectures (ZTA). This research explores the assumptions, resourcing, and realities of having the designation of "Critical Infrastructure" and the changes in government relationships network operators can expect over the next few years. While this research focuses on the United States, much of this is relevant to other regions, particularly those within the EU or the UK. To address the operational and reporting requirements related to technical and supply-chain threats, network operators must automate several activities including threat identification, protection, detection, incident response and recovery. With ransomware and penetration threats increasing, the regulatory environment is shifting. This work focuses on how to best prioritize efforts.

2. Categories and Subject Descriptors

K.4.1 [COMPUTERS AND SOCIETY]: Public Policy Issues

K.4.3 [COMPUTERS AND SOCIETY]: Organizational Impacts

K.5.2 [LEGAL ASPECTS OF COMPUTING]: Government Issues

K.6.5 [MANAGEMENT OF COMPUTING AND INFORMATION SYSTEM]: Security and Protection

3. General Terms

Security, Economics, Operations

4. Keywords

Security, Policy, Ransomware, Critical Infrastructure, Identification, Protection, Detection, Incident Response, Recovery

5. Disclaimer

The information provided in this paper does not, and is not intended to, constitute legal advice; instead, all information, content, and materials available or referenced from this paper are for informational purposes only.

The views expressed at, or through, this paper are those of Brian Scriber writing in his individual capacity only – not those of his respective employer, CableLabs, or CableLabs membership as a whole. All liability with respect to actions taken or not taken based on the contents of this paper are hereby expressly disclaimed.

This document is furnished on an "AS IS" basis and neither CableLabs nor its members provide any representation or warranty, express or implied, regarding the accuracy, completeness, noninfringement, or fitness for a particular purpose of this document, or any document referenced herein. Any use or reliance on the information or opinion in this document is at the risk of the user, and CableLabs shall not be liable for any damage or injury incurred by any person arising out of the completeness, accuracy, infringement, or utility of any information or opinion contained in the document.

CableLabs reserves the right to revise this document for any reason including, but not limited to, changes in laws, regulations, or standards promulgated by various entities, technology advances, or changes in equipment design, manufacturing techniques, or operating procedures described, or referred to, herein.

This document is not to be construed to suggest that any company modify or change any of its products or procedures, nor does this document represent a commitment by CableLabs or any of its members to purchase any product whether or not it meets the characteristics described in the document. Unless granted in a separate written agreement from CableLabs, nothing contained herein shall be construed to confer any license or right to any intellectual property. This document is not to be construed as an endorsement of any product or company or as the adoption or promulgation of any guidelines, standards, or recommendations.

6. Introduction

This is a paper for the technical practitioner. It isn't a review of all laws or regulations. It isn't a manual explicitly for legal, policy, privacy, or product, but rather a guide to those in the security field who now have had some new obligations placed upon their operations; practitioners who are looking for resources to help them understand where incident reporting has solidified and where there are still some questions to be answered and some expectations that need to play out across the regulatory landscape.

7. Recent Criminal Activity

One must recognize that cyber incidents are not natural disasters; they do not just happen unexpectedly. Cybersecurity events are the symptom of actions taken by criminals, and those upon whom these crimes are perpetrated are victims. The global nature of the internet, the problematic aspect of crime prevention across borders, the complexities of extradition and treaty negotiation, and inconsistent definitions of criminal behavior stymie efforts to address root causes[i]. To defend networks, data, equipment, businesses, and governments, cybersecurity preparedness and incident response have taken hold. When incidents occur, it is not directly because of actions taken or not taken by the victim who is charged with juggling priorities and defensive strategies against different threat actors and budget limitations. Because cyber incident reporting efforts in legislatures have cited failures related to large ransomware activities, this paper will start with those concerns. It will address the economics of the situation and the security response related to these criminal activities. This sets the stage for a later dive into the incident reporting being requested and some of the complexities therein.

7.1. Ransomware

The Colonial Pipeline ransomware event was perpetrated by a Russian criminal group "DarkSide"[ii] on May 7, 2021, and operations were brought to a halt. The reaction from this attack included disrupted service, lines for gasoline, and five days of insecurity and concern among government officials from defense to commerce. The strategic impact of how one company in one sector could upend a massive geographical region of the US for a week led to immense scrutiny of other potential vulnerabilities and a wider recognition that forces at play in these attacks were not the Hollywood kid-in-the-basement from popular hacker movies.

7.2. Economics

Ransomware victims are faced with several impossible decisions[iii]: making the attack known, engaging cybersecurity insurance, involving law enforcement, how to negotiate, how to advise victims, and, importantly, the decision around paying the ransom[iv]. The options of paying ransoms, avoiding ransom payments, and the reality of being able to rely upon cybersecurity insurance as a backstop for continued

operations are all important factors that play into the decision-making process around critical infrastructure reporting and government engagement.

In the Colonial Pipeline attack, the attackers were ultimately paid the cryptocurrency equivalent of $US4.4M, and the pipeline operations were provided the decryption key in this case, however, that task of bringing the pipeline back online took several days[v] to completely restore operations. While some of this was returned through law enforcement engagement ($US2.3M)[vi], there are clear cases we see where criminals are able to extort significant capital from their victims, which only encourages them to engage further.

In 2017, the NotPetya attack: $US10B in damages and disabled infrastructure in several ways[vii] for extended periods of time. During hospital attacks, Boards of Directors like those during the Prospect Medical Holdings (2023) or Common Spirit Health (2022) attacks are being asked to make decisions about paying ransoms or having life-preserving services unavailable[viii]. There are some cases where rapid resolution and anti-crime principles can be in conflict. This does not stop some calls to make payment of ransoms illegal, but in late June 2024, Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly stated at the Oxford Cyber Forum that she did not see a path forward in banning ransomware payments[ix]: "I think within our system in the U.S. — just from a practical perspective — I don't see [banning ransom payments] happening."

The "NotPetya" attack victim, Mondelez International (multi-national company based out of Chicago, IL USA), filed for damages and were denied because the insurer (Zurich) didn't cover "hostile or warlike action in time of peace or war, including action in hindering, combating or defending against an actual, impending or expected attack by any … government or sovereign power" as this seemed related or targeting Ukraine by presumably Russian actors. While new "cyber terrorism" covers are available through several insurers, this limitation on how victims can rely upon cybersecurity insurers continues to have impact in the market. The Terrorism Risk Insurance Act (TRIA) of 2002[x] addresses some of these concerns, but it remains unclear on how victims can pursue aid. The fact that cybersecurity insurance can be expensive, can require operational and procedural changes, and can include audit costs – all while still not guaranteeing to pay ransoms or to be a full instrument of restoration of operations – has raised questions about the ability to rely upon such tools. Ransom payments, while distasteful, may be a faster path to restoration and resumption of operations than other recovery options drawn from backups or alternate paths where not paying ransoms, or not paying full ransoms, are the case.

7.3. Security Response

Critical infrastructure was the primary focus for the regulatory response to ransomware or destructive events such as the Colonial Pipeline and the SolarWinds[xi] attacks[xii], respectively. Within days of the former attack, the US White House issued Executive Order 14028. EO14028 established the groundwork for further response, budget, and lawmaking, while it ordered a reduction in information-sharing, created a Cyber Safety Review Board, and set expectations for preparing for and responding to a cybersecurity incident. Colonial Pipeline created what some have referred to as the Cybersecurity Pearl Harbor Moment[xiii] where the true vulnerabilities were highlighted clearly for policymakers.

8. Incident Reporting and the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)

8.1. Timeline

This is a brief timeline of relevant activities during an unusually active policymaking period over the last few years focusing on pre-CIRCIA incident reporting regulations:

2013, Feb 12	US Presidential Policy Directive 21xiv (Critical Infrastructure reporting requirements)
2022, March 15	CIRCIA passed
2024, April 3	CISA Notice of Proposed Rulemaking (NPRM) on CIRCIA released
2024, April 30	National Security Memorandum (NSM) 22 Memo: Federal Communications Commission (FCC) to coordinate with CISA when not prohibited by law
2024, July 3	NPRM comments were due

8.2. Focusing on CIRCIA Implementation

On April 3, 2024, CISA released the unusually lengthy (447 page) NPRM on CIRCIA[xv]. This author's analysis covered nine areas where there were concerns related to the implementation of the CIRCIA legislation in practice: clarity of definition of Covered Entities, clarity of definition of Covered Cyber Incident, exemptions, technology supporting Covered Cyber Incident reporting, timeline expectations, scalability and costs, CISA's power to compel disclosure, record retention, and harmonization.

8.2.1. Clarity of Definition of Covered Entities

The definition of Covered Entity is excessively broad, so much so that the definition lists those entities that are not covered instead of listing all of those which are included in the Critical Infrastructure categories defined in 2015[xvi] at https://www.cisa.gov/2015-sector-specific-plans:

> *"The overwhelming majority of entities, though not all, are considered part of one or more critical infrastructure sectors. Illustrative examples of entities that generally are not considered part of one or more critical infrastructure sector include advertising firms, law firms, political parties, graphic design firms, think tanks, and public interest groups."*
> *-- 89 FR 23678*

This categorization will require almost every organization above the sizing thresholds to establish a costly cyber incident reporting capability; it will decrease the signal to noise ratio so critical in pattern identification and threat awareness; it raises the specter of even more costs from this sector with regulatory enforcement. It is recommended to either include every organization and explicitly exempt from that list, or else to significantly refine the entities that should be subject to initial coverage and extend that definition after an initial roll-out period is completed.

8.2.2. Clarity of Definition of Covered Cyber Incident

As with the definition of Covered Entity, the scope of reportable Covered Cyber Incident is excessively wide and confusing. This should be a bright line definition that can be easily measured by even those not entirely versed in cybersecurity practice, however the terms used are vague, subjective, and lack the clarity required.

> *Cyber incidents that result in minor disruptions, such as short-term unavailability of a business system or a temporary need to reroute network traffic."*
>
> *--89 FR 23668*

Use of terms like "brief period of unavailability", "short-term unavailability" and "minor disruptions" which call upon subjective judgement should not part of a rule. Rules should also clearly define terms like

"sensitive data" which could have several different interpretations that leave covered entities at risk for misinterpretation or regulatory enforcement.

The recommendation is to define key terms, avoid terms without objective criteria, specify exact date ranges and be clear on expectations for incident impact timeframes.

8.2.3. Exemptions

There are a few exceptions listed in the NPRM that could and should be expanded. Currently, organizations like the Internet Corporation for Assigned Names and Numbers (ICANN), American Registry for Internet Numbers (ARIN) and others that engage in the Domain Name System (DNS) are called out because of their inclusion in critical infrastructure and their engagement in executing policies concerning DNS.

> *To qualify for the reporting exception provided in 6 U.S.C. 681b(a)(5)(C), a covered entity must have been determined by the Director to meet two criteria. First, the Director must have determined that the covered entity constitutes critical infrastructure. Second, the Director must have determined that the covered entity, or a specific function of that entity, is owned, operated, or governed by a multi-stakeholder organization that develops, implements, and enforces policies concerning the DNS."*
> *--89 FR 23710*

DNS is part of traffic routing, but so is Border Gateway Protocol (BGP), and perhaps at a more important level. While attacks against DNS are common, so are those against BGP, and particularly for those entities in the Communications Sector of Critical Infrastructure, reporting on all the potentially nefarious activity in these technologies is an extremely excessive burden. It is recommended that, rather than naming specific organizations, refine the definitions of Covered Entities and Covered Cyber Incident as appropriate: the Covered Entity definition should exclude organizations primarily concerned with routing internet traffic; the Covered Cyber Incident should exclude those common and noisy targeted protocols such as DNS and BGP, as well as exclude DDoS activity using ports 80 and 443 (Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS)).

8.2.4. Technology Supporting Covered Cyber Incident Reporting

While the law requires a "concise, user-friendly web-based form" as one manner of submission, this should not be the primary mechanism for receipt of Cyber Incident Reports.

> *"On balance, CISA believes that the web-based form is the most useful and cost-effective manner for the submission and receipt of CIRCIA Reports and is proposing that as the sole explicitly identified option for submission of CIRCIA Reports."*
>
> *--89 FR 23714*

Such web-based form solutions are vulnerable to attacks on the underlying protocols and potentially prone to DDoS attacks and service/software compromise; the telephonic backup proposed by CISA ("CISA also intends to maintain a capability to support reporting via telephone as a back-up option") is unrealistic and unscalable.

Ideally, there should be a Representational State Transfer (RESTful) interface allowing for the POST (this is an HTTP method not an acronym) of a new Cyber Incident Report or appending information to an already existing report per Request For Comment 9110 (RFC9110)[xvii]. This should be provided within an

authenticated enclave that acts as a primary barrier and authorization-revocation tool in the event of an attack on the infrastructure.

The exact fields required in the Covered Cyber Incident Report should be clearly identified, versioned (so that updates and changes can be tracked and submissions can show that they satisfied all requirements that were necessary at the time of submission, even if those requirements may have changed since that point), and the total of these required fields should be severely limited due to the potential for CISA's reliance upon a telephone submission method or a web-based form for which submitters may be using smart phone browsers to submit their Cyber Incident Report (they may be forced to use that method because the cyber incident they are reporting upon may have taken out other operational systems which would have otherwise enabled the required reporting).

Reporting ransom payments could become discoverable and lead to a list of targets willing to pay ransoms. Protection from unintended disclosure and breach is recommended in the highest possible terms. CISA should clarify the expectations of the compelled disclosure of ransom payments.

The recommendation is to provide an authenticated enclave for submissions and to enable an interface allowing for POST methods to submit a well-defined Cyber Incident Report with verification of receipt of the submission. It is also recommended that ransom payment history and reports be highly protected.

8.2.5. Timeframe Expectations

With cyber incidents, the entity being subjected to the attack may not even know they have been compromised until well into the actual attack; even if there were some indicators that triggered an investigation, the verification can take days or weeks in some cases, and even longer to determine the full scope of the impacted systems. The 72-hour window is untenably tight for full reporting:

> *"CIRCIA requires covered entities to report to CISA covered cyber incidents within 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred and ransom payments made in response to a ransomware attack within 24 hours after the ransom payment has been made."*
> *--89 FR 23648*

Reporting on the incident does take time away from protections and investigations, and the early hours are the most critical. Recommendation is to allow reporting in stages for those critical incidents; provide the ability to advise CISA of a suspected incident with minimal overhead, and then to complete the investigation adding updated details along the way with an outer bound of having a full report filed within 10 days.

8.2.6. Scalability and Costs

Smaller entities may be currently exempted, but smaller to mid-size operations also face similar struggles to keep pace with rapidly evolving cybersecurity threats and increasing regulatory requirements.

The recommendation is to increase the employee size minimums, increase the revenue minimums, and roll this out in phases to different sectors to stagger the impacts and necessary changes to the program.

8.2.7. Impact of Disclosure

CISA asked for subpoena power over ISPs[xviii] and this was granted in the 2022 CIRCIA legislation, which authorizes CISA with limited subpoena authority over Covered Entities:

> *"CIRCIA also authorizes CISA to request information and engage in administrative enforcement actions to compel a covered entity to disclose information if it has failed to comply with its reporting obligations."*
> *--89 FR 23648*

Cybersecurity relies upon informational asymmetries as one of the only advantages to the defender in a hostile operating environment. While it is recognized that the interests of the US Government may be served in the short-term through compelling disclosure of cyber-attack details, defender posture, countermeasures in place, exact versions of software deployed, practices used to limit scope of an attack, and mechanisms or technologies helpful in identification and isolation of those attacks, it is also clear that the information compelled through such authority cannot itself be adequately protected. Through disclosure to the government, covered entities may be providing a roadmap to attackers on how to subvert and undermine the defenses these entities have constructed to protect themselves and their subscribers from threat actors.

The software bill of materials (SBOM) is a listing of each software package and version, included directly or as a component, in each part of the critical infrastructure. A Common Vulnerability and Exposure (CVE) database such as the near quarter million records currently downloadable from cve.org shows vulnerabilities in specific software packages and versions. Tools such as metasploit, nmap, and open-sourced attack frameworks have automated the attack infrastructure so that merely knowing the software and version can yield an effective attack; the advent of some newer generative AI tools have further advantaged the attackers and made these threats increasingly economically viable. The combination of the hyper-detailed SBOM, the database of CVEs, and automated attack frameworks provide the attacker with a detailed roadmap of what to attack, how to attack it, and a toolkit enabling automation of those attacks.

Therefore, it is essential that there are adequate mechanisms in place to protect against the disclosure of such information through data breaches or other encroachment by adversarial entities.

It is recommended that the scope of required disclosure be curtailed, and incredible care be taken to protect any defensive data compelled by CISA.

8.2.8. Record Retention

Retention requirements for the Covered Entities required to submit Cyber Incident Reports face two significant challenges; the first includes the costs associated with correctly archiving records and tagging the necessary elements, and the second is understanding when those records can be safely dropped. The advice on these fronts appears to overlook the impact to private industry.

> *"Covered entities that submit CIRCIA Reports must begin preserving the required data at the earlier of either (a) the date upon which the entity establishes a reasonable belief that a covered cyber incident has occurred, or (b) the date upon which a ransom payment was disbursed, and must preserve the data for a period of no less than two years from the submission of the latest required CIRCIA Report submitted pursuant to § 226.3, to include any Supplemental Reports."*
> *--89 FR 23731*

Most cyber incidents do not result in criminal prosecution[xix], therefor the costly retention of evidence for volumes of incidents is not needed for litigation. In the communications sector, incidents such as DoS and DDoS can be frequent and clarity of definition of materiality bears on companies wishing to err on the side of caution will drive costs and task limited security resourcing toward administrative actions with little additional value. Since the reporting to CISA should already cover the necessary data, it is

recommended that CISA store the reports for the appropriate period and release the Covered Entity for responsibility of hosting duplicative information.

8.2.9. Harmonization

Differing state requirements for reporting, diverse economic sector reporting requirements, and multiple federal agencies that require incident reporting. Examples of these agencies include the Securities and Exchange Commission (SEC), Federal Communications Commission (FCC), Federal Trade Commission (FTC), Department of Defense (DOD), Department of Justice (DOJ), Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST), state governments, Department of Homeland Security (DHS), and the Cybersecurity Infrastructure Security Agency (CISA). Some of the regulations related to reporting include Federal Acquisition Regulation (FAR Council) and Federal Information Systems Management Act (FISMA). It would be ideal for those responsible for reporting incidents if all of these were to align behind a single reporting infrastructure and harmonize their statutory requirements. Confusing the industry is neither good for governmental oversight nor the regulated industries. CISA should take the lead in coordinating this across the ecosystems, finding the correct definitions, timelines, and tooling to support appropriate reporting. Additionally, CISA should lead in the defense of that data, the careful sharing of appropriate insights to only authenticated and authorized agencies, and they should provide the insight required to help legislators make informed decisions about how to best harmonize legislation going forward.

9. Impact to Cable as Critical Infrastructure

The cable industry and other ISPs, presuming the CIRCIA issues identified above, remain unresolved in the final rulemaking, will have new incident reporting waters to navigate, and new best common practices may need to be identified to help provide clarity in the implementation of the regulation. The designation of Critical Infrastructure does carry responsibilities that will require close collaboration in terms of activities and reporting expectations.

9.1. Critical Infrastructure History

The first time the term “Critical Infrastructure” (CI) was used in the US was in Executive Order 13010, which created a national commission on critical infrastructure in 1996[xx]. This order also created the initial eight sectors for which this commission was to assess and create a strategy for protecting from threats. The 1998 Presidential Decision Directive 63 (PDD-63) explicitly added “cyber” to the CI definition. The concept was expanded by the Patriot Act of 2001, the Homeland Security Act of 2002, Homeland Security Presidential Directive 7 (HSPD-7)[xxi] of 2003, and Presidential Policy Directive 21 (PPD-21), which supersedes HSPD-7.

The current sixteen Critical Infrastructure Sectors include Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Services and Facilities, Healthcare and Public Health, Information Technology, Nuclear, Transportation Systems, and Water/Wastewater. The majority of Critical Infrastructure is privately owned[xxii], and this is true for the Communications sector, which the cable industry operates within and which the Communication Sector-Specific Plan (CSSP) of 2015 references[xxiii].

The Communication Sector has several objectives (see Figure 1), and the sector has been referenced in subsequent executive orders (Executive Order (EO) 13618, Assignment of National Security and Emergency Preparedness Communications Functions and EO 13636, Improving Critical Infrastructure Cybersecurity) expanding expectations and recognizing threats.

Sector Goals	Joint Sector Priorities
1 Protect and enhance the overall physical and logical health of communications.	**Cyber and Physical Security**: Coordinate with public and private sector partners regarding cyber and physical security information and trends, strategies, initiatives, programs, and best practices. **Future State**: Enhanced cyber and physical risk identification and management capabilities through the use of existing programs.
2 Rapidly reconstitute critical communications services in the event of disruption and mitigate cascading effects.	**Resilience**: Promote and coordinate efforts to improve communications resilience by public and private sector partners before, during, and after incidents affecting communications. **Future State**: Enhanced sector programs and initiatives that increase sector-wide incident response and recovery capabilities.
3 Improve the sector's national security and emergency preparedness (NS/EP) posture with Federal, State, local, tribal, international, and private sector entities to reduce risk.	**Dependencies and Interdependencies**: Coordinate identification of sector dependencies and interdependencies with public and private sector partners and implement appropriate mitigation actions to make critical infrastructure more resilient and less vulnerable to manmade or natural threats. **Future State**: Improved ability to identify cross-sector dependencies and interdependencies and develop sector-wide risk mitigations strategies to address them.
	Partnership and Engagement: Coordinate with public and private sector partners regarding critical infrastructure security and resilience information, trends, strategies, initiatives, programs, and best practices. **Future State**: Advanced outreach and awareness programs that communicate sector-developed risk management and mitigation practices and strategies with sector stakeholders.

Figure 1 - Communications Sector Goals and Priorities (From CSSP 2015)

The Communications Sector is broken down into five sector components: Broadcast, Cable, Satellite, Wireless, and Wireline; The cable industry has companies that participate in all five of these components, but we are referenced collectively as cable. The four main risks identified for communications include Natural Disasters and Extreme Weather, Supply Chain Vulnerabilities, Global Political and Social Implications, and Cyber Vulnerabilities. CISA and DHS also identify emerging sector risks including risks to the Global Positioning System (GPS) and risks associated with vulnerable and pervasive Internet of Things (IoT) devices.

9.2. Responsibilities of the Designate

In the event of "a substantial cyber incident experienced by a covered entity", one of four mandatory reports must be filed: Covered Cyber Incident Report, Ransomware Payment Report, Joint Covered Cyber Incident Report or Ransom Payment, or a Supplemental Report. Based on the NPRM for CIRCIA, the initial reporting must occur within 72 hours.

The implication is that "Covered Entities" will need to track cyber incidents, make determinations as to whether the incidents meet the "substantial cyber incident" bar, have staff to complete and submit these reports, as well as to answer questions that may arise from the filing or modification/updates made to the reports.

CIRCIA designates the following:

Table 1 - CIRCIA Responsibilities

Report on	To Whom	Timeframe	Qualification
Incidents	CISA	Within 72 hours after the affected entity reasonably believes that the covered cyber incident has occurred.	"cyber incidents that 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 people of the United States"
Payments	CISA	Within 24 hours of payment	Ransom payment, whether or not the cyber incident is a covered incident defined above[xxiv].
Additional Information	CISA	As new information is available	Substantial new or different information after submitting a covered cyber incident report should be reported until the cyber incident at issue has concluded and has been fully mitigated and resolved.

9.3. Who Qualifies and Who Does Not

The Defense Industrial Base and defense contractors have had cyber incident reporting obligations pursuant to DFARS clause 252.204-7012[xxv] since 2017, the financial sector have had cyber incident reporting requirements since 2000 with adoption of the SEC Regulation S-P, which was amended in May of 2024. The FTC also has reporting requirements for financial institutions, some that require non-banking institutions to report on certain incidents. While these primarily notify customers, law enforcement, federal and state regulators, and Suspicious Activity Reports (SAR) are all potentially involved.

The CIRCIA statute defines "Covered Entity," and it also dictates that CISA further refine this definition. The basis for the CISA clarification will need to be consistent with statute which looks for the entity to affirmatively answer any of the 16 sector-based criteria from the proposed 6 CFR § 226.2[xxvi]:

- ☐ Owns or operates a CFATS covered chemical facility (§ 226.2(b)(1))
- ☐ Provides wire or radio communications services (§ 226.2(b)(2))
- ☐ Owns or has business operations engaging in critical manufacturing (§ 226.2(b)(3))
- ☐ Is required to report cyber incidents under Defense Federal Acquisition Regulation Supplement 252.204-7012 (§ 226.2(b)(4))
- ☐ Provides an emergency service or function to a population of 50,000 or more (§ 226.2(b)(5))
- ☐ Is a bulk electric or distribution system entity required to report cybersecurity incidents to NERC or DOE (§ 226.2(b)(6))
- ☐ Owns or operates a qualifying financial services sector entity (§ 226.2(b)(7))
- ☐ Is a State, local, Tribal, or territorial entity for a jurisdiction with a population of 50,000 or more (§ 226.2(b)(8))
- ☐ Is an education agency under 20 U.S.C. 7801 serving 1,000 or more students, or an Institute of Higher Education receiving Title IV funding (§ 226.2(b)(9))
- ☐ Manufactures, sells, or provides managed services for information and communications technology to support elections processes or report and display results (§ 226.2(b)(10))
- ☐ Owns or operates a large or critical access hospital; or manufactures certain essential drugs or Class II or III medical devices (§ 226.2(b)(11))
- ☐ Provides IT hardware, software, systems, or services to the Federal government; develops, sells, licenses, or maintains software with specific attributes; sells, manufactures, or integrates operational technology; or performs functions related to domain name operations (§ 226.2(b)(12))
- ☐ Owns or operates a commercial nuclear power reactor or fuel cycle facility (§ 226.2(b)(13))
- ☐ Is a transportation system entity required to report cyber incidents to TSA (§ 226.2(b)(14))
- ☐ Owns or operates a vessel or facility subject to MTSA (§ 226.2(b)(15))
- ☐ Owns or operates a community water system or treatment works serving more than 3,300 people (§ 226.2(b)(16))

Figure 2 - 6 CFR § 226.2 Criteria

The two criteria that almost all cable network providers satisfy are "Provides wire or radio communications services (§ 226.2(b)(2))" and "Provides an emergency service or function to a population of 50,000 or more (§ 226.2(b)(5))." Either one would satisfy the definition of "Covered Entity." Presuming an exemption from either of those criteria, the determination of whether the entity were one of the 16 Critical Infrastructure Sectors (see section 9.1) would classify network operators as part of the Communications Sector, and unless a wired (517111) or wireless (517112) telecommunications carrier has fewer than 1500 employees, they do not qualify for the final exemption option of being a small business[xxvii].

9.4. Cable Operator Activites to Undertake

One of the four most critical aspects to undertake immediately is to make sure the cyber incident response team is engaged and equipped appropriately to address the increased reporting requirements.

Second, it is important that threat management tools are in place and orchestrated. This includes ensuring that logging systems have adequate storage, Intrusion Detection and Prevention Systems (IDS/IPS) are properly configured, that archival procedures are in place and tested, and that recovery and classification systems are in place and being used. Tools used to mitigate threats, to divert malicious traffic, to watch for scanning or other Indicators of Compromise (IOC) are able to inform the reporting requirements should the event be classified as "significant." Some tools autonomously manage malicious traffic, and can also clean up after themselves (e.g., Distributed Denial of Service mitigation tools). These need to be modified to conform to new reporting requirements.

The third step Cable Operators should engage in is making sure to have Cybersecurity experience in operations and on their Board of Directors. Table-top exercises should be regular activities that explore impact from different types of events (e.g., supply chain compromise, digital certificate expiration, ransomware, physical communications severance, et alia). The FTC[xxviii] has been advocating for boards to 1) make data security a priority, 2) understand cybersecurity risks and challenges, 3) do not confuse legal compliance with security, 4) move beyond prevention in cybersecurity planning, and 5) learn from mistakes and breaches. Outside the USA, the World Economic Forum[xxix] has pushed to incorporate cybersecurity expertise into board governance with cybersecurity relationships, education of other board members, engaging third-party advisors and assessors in combination with audits and reviews of cyber policy and efficacy, and regular updates to the boards on cyber incidents, trends, vulnerabilities, predictions and applicability of cyber landscape to corporate stratagems.

The fourth step for operators is preparing for reporting and incident response with legal advice on the level of event that qualifies as "substantial." It will be important to quantify these criteria prior to being victimized by such an event. This will allow the teams to know clearly which events must be reported and which can be black-holed or mitigated without the reporting overhead and record-keeping.

9.5. Incidents and Definitions

The term Cybersecurity Incident and Cybersecurity Event have definitions that lead to questions where parsing of language and intent are used to decide upon a course of action. NIST has defined a Cybersecurity Event as "A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).[xxx]". In their Cybersecurity Framework (1.1) NIST defines a "Cybersecurity Incident" as "A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery[xxxi]" but NIST defines it differently in their Computer Security Incident Handling Guide (SP 800-61R2)[xxxii], which is referenced by CISA, where NIST defines an incident as "a violation or imminent threat of violation1 of computer security policies, acceptable use policies, or standard security practices." To further complicate matters, the Office of Management and Budget (OMB) defines an incident as "An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an

information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.[xxxiii]"

Parsing the definition has had bearing upon CISA's NPRM, and they have helped to break down which incidents qualify for cyber incident reporting.

9.5.1. What Incidents Qualify

Cyber Incident is a term that gets interpreted in multiple ways. The CIRCIA defers the definition of a "Covered Cyber Incident" to the CISA rulemaking which in turn proposes an occurrence that jeopardizes or compromises the integrity, confidentiality, or availability of an information system; it mentions both brief periods and extended periods of attack. These elements are open to some level of discretion. What exactly is a "brief period" or an "extended period?" Some initial guidelines have come from CISA's "Sharing Cyber Event Information With CISA: Observe, Act, Report (v4.0)" Fact Sheets after CIRCIA was published. Until the final rulemaking is complete, this is what operators should be looking at with respect to the activities that might qualify for sharing:

9.5.1.1. Unauthorized access to your system.

This will likely need some additional guidance. Which system was accessed? How was it accessed? For how long was there access and to whom? What if the system was not part of operations?

9.5.1.2. Denial of Service (DOS) attacks that last more than 12 hours.

DOS and DDoS attacks are not always obvious. What can look like an attack can actually be normal traffic or a software misconfiguration. Most parties will only see a DOS or DDoS attack if they are the victim. How does this play out for the communications sector of Critical Infrastructure where we may see some of the attack traffic directed at a customer rather than our own infrastructure? Scrubbing and monitoring all traffic is not scalable. Some of these may not reach levels that qualify (either through sporadic attack cycles where the traffic is not consistent for the 12 hours, or traffic levels so low as to not trigger awareness until later).

9.5.1.3. Malicious code on your systems, including variants if known

Presumptions around systems being part of the Critical Infrastructure need validation. Often there is an enterprise network and a carrier network within network operator environments. If a sales laptop has adware installed from a malicious website, is that a reportable offense?

9.5.1.4. Targeted and repeated scans against services on your systems

Considering that directed scans commonly occur against network operators, and recognizing that threat actors often spoof addresses or use proxies or intermediaries such as overlay networks utilizing home Virtual Private Network (VPN) services, it is difficult to confirm that a given scan is originating from the same point or not. Reporting of these incidents may need to move to aggregate statistics over a given period.

9.5.1.5. Repeated attempts to gain unauthorized access to your system

This area is another that will likely need additional guidance. How many attempts qualifies as "repeated?" What if the attempts were to gain authorized access but credential validation has been failing? Attempts to access which systems? Presumably only those directly supporting Critical

Infrastructure should be in scope, but if other systems had credentialing attempts made, is there a set of differentiation criteria?

9.5.1.6. Email or mobile messages associated with phishing attempts or successes

This topic could overload any business, and the raw amount of phishing attempts alone could burden the reporting infrastructure. Phishing against whom? "Attempts" is called out, but what if the attempt was successfully mitigated by a third-party Email Service Provider (ESP), and the network operator never saw the attempt or if it were shunted to a spam/junk mail folder? Again, could this be aggregated and reported en masse to CISA with some periodicity?

9.5.1.7. Ransomware against Critical Infrastructure, include variant and ransom details if known

This category of reporting obligation harkens back to the very root issues that have created this reporting need. Threat actors that have been able to infiltrate and disable components of networks designated as Critical Infrastructure need to be identified and observed before law enforcement or other government tools can be engaged to remove or defend against those threats. Identifying information that can help in this process is a benefit to the ecosystem. If additional information like variant details or payment wallets are available, it can support those governmental efforts.

It is important to note differences between a completed attack and one that is incomplete "in some manner". An incomplete attack triggers a supplemental reporting obligation, but the timeframes (72 hours) for reporting may force this for even trivial attacks, which adds steps to industry compliance.

As discussed in section 8.2.9, harmonization is necessary on incidents and definitions as well, this needs to take place between the SEC, FCC, FTC, DOJ, Far Council, FISMA, state governments, and DHS/CISA. It is possible that we see alignment as CISA moving to the role of single point of reporting and then they advise or share with other agencies as needed, but this has not yet materialized.

9.6. What's in an Incident Report

CISA has designated ten "Key Elements" of a Cybersecurity Incident Report[xxxiv], with nine designated as a priority. Only the last is left as non-priority:

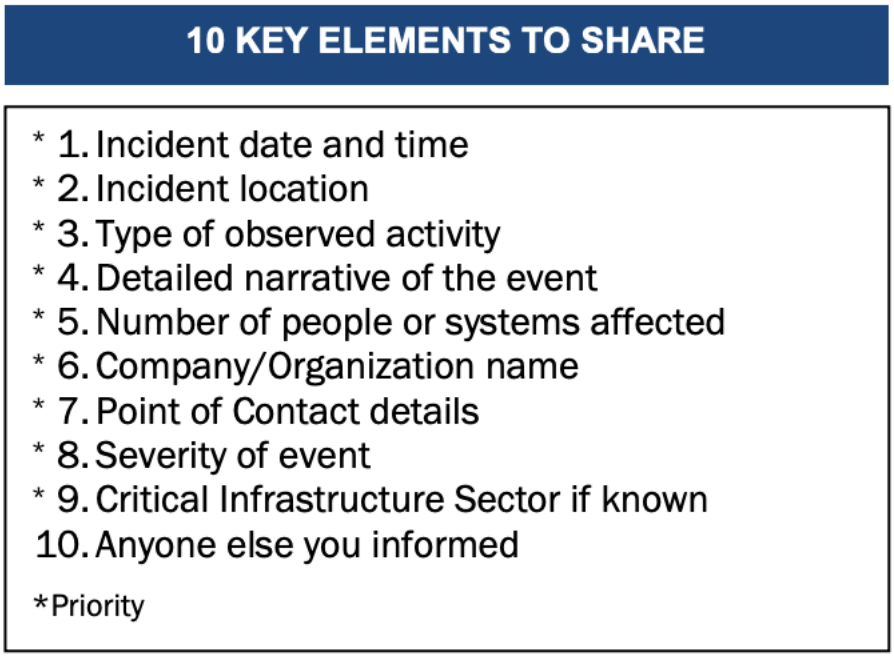

Figure 3 - CISA Sharing Cyber Event Information: 10 Key Elements to Share

The four sections identified by the current CISA reporting web tool are the Contact Information, Organization Details, Incident Description, and Impact Details. The details and method for submission could change going forward, and this is a point-in-time view of the tool; it is intended to help with process, procedures, and tooling to ensure a complete capture of relevant data for an incident report.

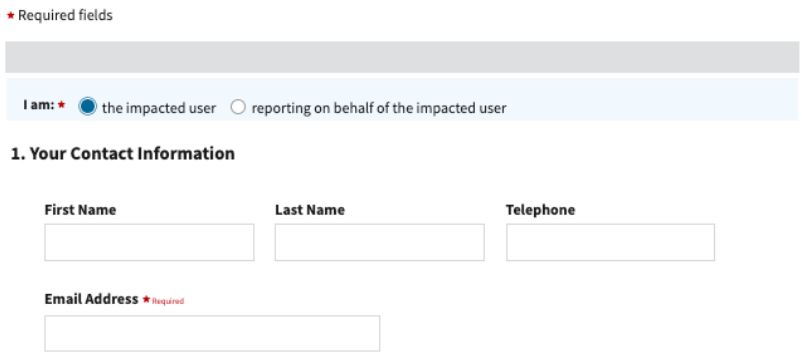

Figure 4 - Incident Reporting: Contact Information

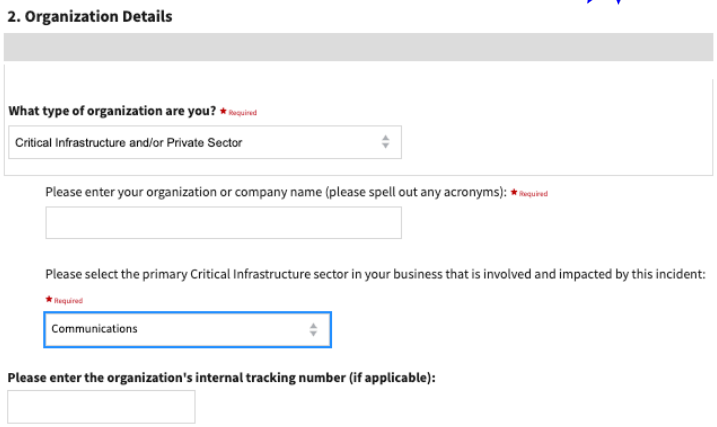

Figure 5 - Incident Reporting: Organization Details

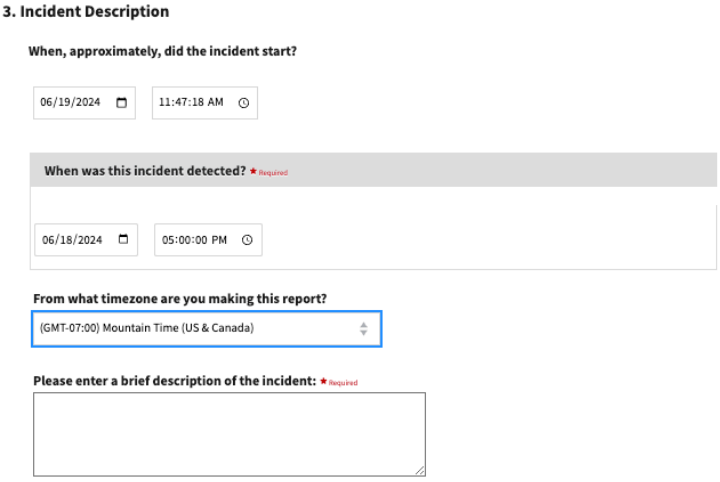

Figure 6 - Incident Reporting: Incident Description

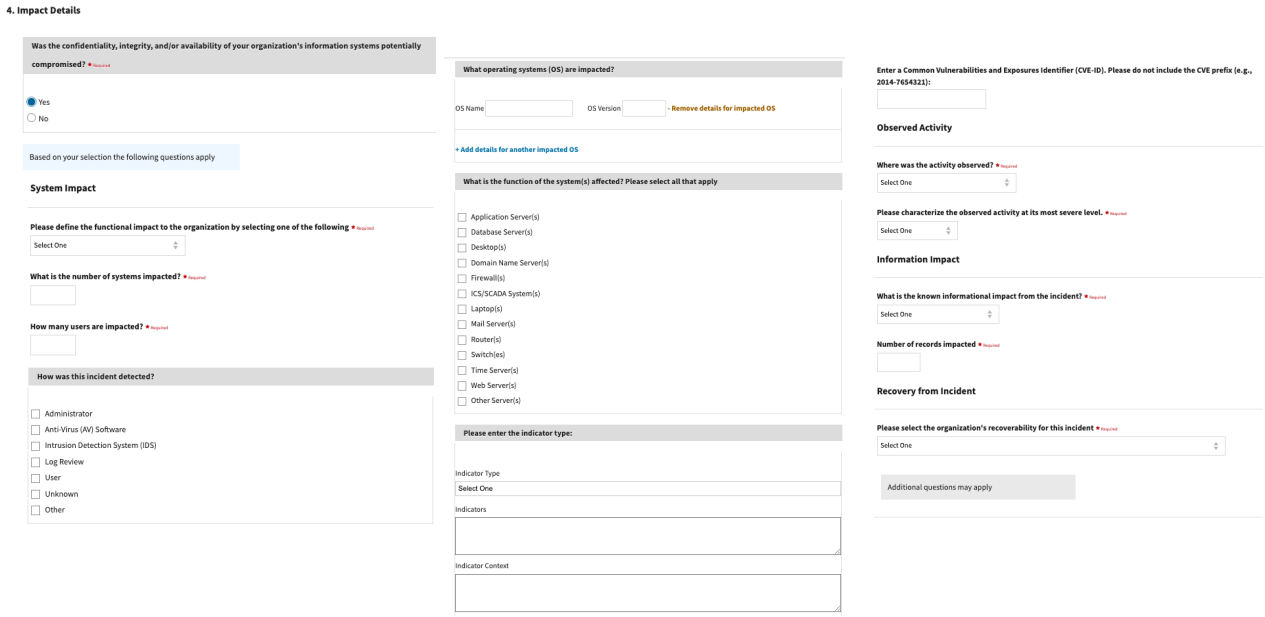

Figure 7 - Incident Reporting: Impact Details

The dropdown options for the CISA incident reporting document follow herein:

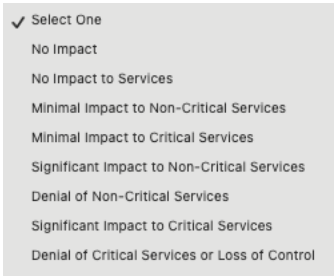

Figure 8 - Incident Reporting: Impact Details [Impact to the Organization]

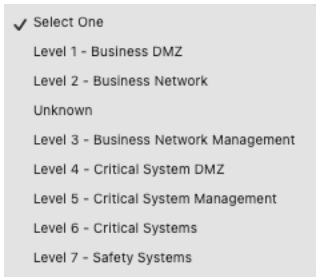

Figure 9 - Incident Reporting: Impact Details [Where was the activity observed]

Figure 10 - Incident Reporting: Impact Details [Indicator Type]

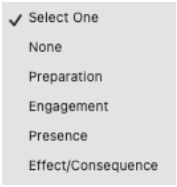

Figure 11 - Incident Reporting: Impact Details [Severity]

Figure 12 - Incident Reporting: Impact Details [Informational Impact]

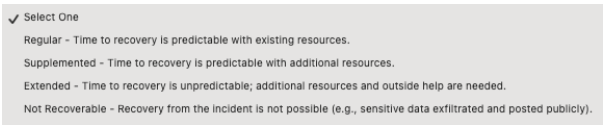

Figure 13 - Incident Reporting: Impact Details [Recoverability]

The details in these dropdown options are presented here so that mappings to internal impact, location, indicators, severity/criticality, scope, and recoverability can be considered. It is unlikely that this matches everyone's classification process, but if an organization is building out a new process, or revamping existing tools or procedures, this structure should be considered.

10. Outlook

The final rulemaking from CISA has yet to be published, the harmonization has yet to occur, and the roll-out of the reporting tools remains to have some important questions answered. There is an increasingly clear path forward in expectations for reporting on cyber incidents and ransom payments. We have increased clarity on who needs to report, we have a better idea on what needs to be reported upon, and we are beginning to see the details of what needs to go into those reports. We know we have preparations and changes in our organizations from operations, incident response, through management, compliance, legal, and ending at changes with the very structure of our boards of directors. We have tools to prepare, vendors to work with on integrations and automation, and we have new procedures and policies around retention and log management to support the reporting requirements. We know the landscape will change going forward, we know that this is a current view of that changing terrain, and it is recognized that by the time this map is published, it is likely that the terrain has changed. This harkens back to an old theme echoed by Gordon Livingston and Alfred Korzybski: "when the map and the terrain differ, believe the terrain."

Abbreviations

ARIN	American Registry for Internet Names and Numbers
BGP	Border Gateway Protocol
CI	Critical Infrastructure
CISA	Cybersecurity and Infrastructure Security Agency (part of Department of Homeland Security)
CSSP	Communications Sector-Specific Plan 2015 (Annex to NIPP 2013)
CVSS	NIST Common Vulnerability Scoring System
DHS	Department of Homeland Security
DOD	Department of Defense
DOJ	Department of Justice
EO	Executive Order
ESP	Email Service Provider
FAR	Federal Acquisition Regulatory (Council)
FCC	Federal Communications Commission
FISMA	Federal Information Security Management Act of 2002
FTC	Federal Trade Commission
GPS	Global Positioning System
HSPD-7	Homeland Security Presidential Directive 7
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICANN	Internet Corporation for Assigned Names and Numbers
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force – publishes Requests for Comment (RFC)
IOC	Indicators of Compromise
IPS	Intrusion Prevention System
IoT	Internet of Things
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PDD-63	Presidential Decision Directive 63
PPD-21	Presidential Policy Directive 21
REST/RESTful	Representational State Transfer
RFC	Request For Comment (see IETF)
SBOM	Software Bill of Materials
SEC	Securities and Exchange Commission
VPN	Virtual Private Network

Bibliography & References

[i] P. Kastner and F. Mégret, *Chapter 12 International legal dimensions of cybercrime*, Law 2021 pp 253-270, 14 Dec 2021, https://doi.org/10.4337/9781789904253.00022

[ii] https://www.wsj.com/articles/fbi-suspects-criminal-group-with-ties-to-eastern-europe-in-pipeline-hack-11620664720

[iii] https://www.m3aawg.org/sites/default/files/ransomware_bcp_2023.pdf

[iv] https://www.m3aawg.org/sites/default/files/ransomware_bcp_2023.pdf

[v] https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html

[vi] Joe R. Reeder & Tommy Hall, *Cybersecurity's Pearl Harbor Moment*, 6 The Cyber Defense Review, 15, 15 (2021).

[vii] https://www.brookings.edu/articles/how-the-notpetya-attack-is-reshaping-cyber-insurance/

[viii] https://www.nytimes.com/2023/08/05/us/cyberattack-hospitals-california.html

[ix] https://therecord.media/cisa-easterly-dismisses-ban-on-ransomware-payments

[x] https://www.congress.gov/bill/107th-congress/house-bill/3210

[xi] David Sanger & Julian Barnes, *Biden Signs Executive Order to Bolster Federal Government's Cybersecurity*, N.Y. Times (May 12, 2021 https://www.nytimes.com/2021/05/12/us/politics/biden-cybersecurity-executive-order.html; *Executive Order on Improving the Nation's Cybersecurity*, CISA (Oct. 31, 2022), https://www.cisa.gov/executive-order-improving-nations-cybersecurity

[xii] https://www.law.georgetown.edu/environmental-law-review/blog/cybersecurity-policy-responses-to-the-colonial-pipeline-ransomware-attack/

[xiii] Joe R. Reeder & Tommy Hall, *Cybersecurity's Pearl Harbor Moment*, 6 The Cyber Defense Review, 15, 15 (2021)

[xiv] https://www.energy.gov/ceser/presidential-policy-directive-21

[xv] https://federalregister.gov/d/2024-06526

[xvi] https://www.cisa.gov/2015-sector-specific-plans

[xvii] https://www.rfc-editor.org/rfc/rfc9110#section-9.3.3

[xviii] https://www.lawfaremedia.org/article/cisas-request-subpoena-power

[xix] Coveware, 21 October 2021 Quarterly Report: https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts

[xx] https://www.eac.gov/blogs/ci-scoop-history-critical-infrastructure-designation

[xxi] https://www.cisa.gov/news-events/directives/homeland-security-presidential-directive-7

[xxii] RAND Corporation, Feb 12, 2024, "Threats to America's Critical Infrastructure Are Now a Terrifying Reality", https://www.rand.org/pubs/commentary/2024/02/threats-to-americas-critical-infrastructure-are-now-a-terrifying-reality.html

[xxiii] https://www.cisa.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf

[xxiv] https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/cyber-breach-reporting-legislation.html

[xxv] https://www.summit7.us/dfars-7012

[xxvi] https://www.cisa.gov/sites/default/files/2024-05/24-0630-Covered-Entity-Infographic-04242024-508c.pdf

[xxvii] https://www.sba.gov/sites/default/files/2023-06/Table%20of%20Size%20Standards_Effective%20March%2017%2C%202023%20%282%29.pdf

[xxviii] https://www.ftc.gov/business-guidance/blog/2021/04/corporate-boards-dont-underestimate-your-role-data-security-oversight

[xxix] https://www.aicd.com.au/risk-management/framework/cyber-security/six-principles-for-boards-on-cyber-risk-governance.html

[xxx] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[xxxi] Ibid.

[xxxii] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[xxxiii] https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12.pdf

[xxxiv] https://www.cisa.gov/sites/default/files/publications/Sharing_Cyber_Event_Information_Fact_Sheet_FINAL_v4_0.pdf

