**Cyber Incident Reporting for Critical Infrastructure – Considerations for the Space Industry**

**David Bernstein**

*On March 15, 2022, President Biden signed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) into law.[[1]](#footnote-1) Bipartisan lawmakers championed the legislation in response to the growing number of cyber intrusions against critical infrastructure.[[2]](#footnote-2) In particular, the May 2021 ransomware attack against the Colonial Pipeline was a “watershed moment” that laid bare how cyber incidents can have rippling impacts on the American economy and people’s daily lives.[[3]](#footnote-3)*

**CIRCIA mandates the Cybersecurity and Infrastructure Security Agency (CISA) develop regulations requiring entities in the sixteen critical infrastructure sectors specified in Presidential Policy Directive 21 to report cyber incidents to CISA within seventy-two hours of when they believe the incident occurred.[[4]](#footnote-4) CISA is directed to provide “a clear description” of what specific** entities will be required to report cyber incidents based on the probability and magnitude of malicious cyber disruptions.[[5]](#footnote-5)

Space is not enumerated as a critical infrastructure sector that will be covered by the proposed rules; however, some satellite operators may be required to report cyber incidents because they are integral to critical infrastructure operations, most obviously in sectors such as communications and financial services. CISA should resist the temptation to require that all satellite operators report cyber incidents because not all space assets support critical infrastructure. By properly scoping these reporting requirements, CISA can encourage industry compliance with reporting requirements and focus its efforts on responding to high severity cyber incidents.

**CISA Rulemaking Process**

CISA is expected to publish a Notice of Proposed Rulemaking (NPRM) soon and must issue a final rule by September 15, 2025.[[6]](#footnote-6) As CISA develops these proposals, it should focus on the scope of the proposed regulations: which “covered entities” will be required to report cyber incidents?[[7]](#footnote-7)

Comments from around the business community emphasize two primary adverse consequences of an overly broad definition of “covered entities.” First, Business Roundtable warns that requiring too many entities to report cyber incidents could result in “uncertainty” and an “undue burden on private sector entities,” especially those that do not operate critical infrastructure.[[8]](#footnote-8) Experts project that “58,000 additional active satellites could be launched by 2030,” more than ten times as are currently in orbit.[[9]](#footnote-9) CISA may stifle commercial space innovations should all entrants in the New Space economy be required to comply with stringent reporting requirements even if they do not enable critical infrastructure missions, such as research and localized monitoring satellites. Second, the U.S. Chamber of Commerce cautions that requiring too many entities to report cyber incidents “could risk creating unintended noise in the system that detracts from protecting critical infrastructure.”[[10]](#footnote-10) If CISA required all satellite operators to disclose cyber incidents, it would need to process and respond to potentially thousands of breaches on commercial satellites. An overly broad reporting regime could stretch the agency too thin and risk deprioritizing responses to the most significant incidents. Similar concerns have been raised by the Cybersecurity Coalition, CTIA (a trade association representing the wireless industry), and other industry groups.[[11]](#footnote-11)

Additionally, CIRCIA required that the Secretary of the Department of Homeland Security (DHS) issue a report on duplicative federal cyber incident reporting standards.[[12]](#footnote-12) DHS found that there are “45 different federal cyber incident reporting requirements created by statute or regulation currently in effect or final agency guidance.”[[13]](#footnote-13) These standards impact varying sectors, have different reporting standards, and impose differing penalties for failure to comply.

**Considerations for the Space Sector**

The catastrophic potential impacts of cyber incidents on space infrastructure are well documented.[[14]](#footnote-14) Beyond the strategic threats of hacking Global Positioning Systems that are crucial to global military operations, disruptions of commercial satellites could have rippling effects that impede all functions of the global economy from shipping to electronic financial transactions.[[15]](#footnote-15) According to expert analyses, a global shutdown of satellite networks through massive cyber-attacks would immediately ground flights, stop trains, delay emergency response services, and make cash-dispensers inoperable; soon after, global financial transactions would halt and blackouts would be widespread.[[16]](#footnote-16) While this scenario is extremely unlikely, it is important to recognize the myriad of ways that modern life relies on space infrastructure. Indeed, Sam Costa, a counterintelligence officer, noted that “while space is not designated technically as critical infrastructure, I think we can all agree that all of the critical infrastructure sectors rely on space.”[[17]](#footnote-17)

While satellites are essential to all critical infrastructure operations, not all satellites enable critical infrastructure functions. For example, some weather monitoring satellites are necessary for the operation of critical infrastructure systems, while others may not be. A satellite monitoring for hurricane activity that could impact energy and chemical facilities in the Gulf Coast may be essential to prevent catastrophic societal impacts, whereas a research satellite monitoring the earth’s poles may not be considered as essential. CISA should not require the latter satellite operator to disclose cyber incidents, or else CISA may be inundated with responding to breaches that do not directly impact critical infrastructure.

However, experts from the Cyberspace Solarium Commission 2.0, the Information Sharing and Analysis Center, and the Space Foundation have called for space to be designated as the seventeenth critical infrastructure sector.[[18]](#footnote-18) Rep. Ted Lieu recently introduced bipartisan legislation on this matter, albeit with only four cosponsors.[[19]](#footnote-19) While legislative action is unlikely and the Biden administration is reportedly not pursuing this route, CISA should not require all satellite operators to comply with the same reporting standards as the established sixteen critical infrastructure sectors.[[20]](#footnote-20)

CISA must scope these rules properly to cover space assets that enable critical infrastructure operations without imposing overly burdensome requirements across the entire space industry. The Aerospace Industries Association has cautioned that deeming space as a critical infrastructure sector is unnecessary and unwise, for “many space-based capabilities and their enabling infrastructure are already considered within critical infrastructure sectors, such as the critical manufacturing, communications, defense industrial base, government infrastructure, and transportation systems sectors.”[[21]](#footnote-21) Experts have thus cautioned that designating space as the seventeenth critical infrastructure sector and imposing additional cybersecurity requirements across the entire sector may stifle commercial innovation and impose unnecessary bureaucratic burdens, especially when stacked on top of existing cyber risk disclosure rules.[[22]](#footnote-22)

As CISA finalizes its rulemaking efforts, it should focus on the specific type of space assets that should be subject to the cybersecurity reporting requirements instead of requiring that all actors in the space domain disclose cyber incidents. A properly scoped rulemaking will avoid excessive bureaucratic complexity and ensure that entities are not subject to confusing and duplicative requirements. The methodology defining covered entities should focus on the severity and scale of cyber incidents, not simply the sector that was targeted.[[23]](#footnote-23) Cyber incident disclosure rules can dramatically reduce the ensuing impacts of hacks on critical infrastructure, but they must be scoped effectively to properly ensure compliance by private industry and to enable effective responses by the government.

1. 6 U.S.C. §§ 681-681g. [↑](#footnote-ref-1)
2. Senator Gary Peters, *Senate Passes Peters Landmark Legislative Package to Strengthen Public and Private Sector Cybersecurity* (Mar. 2, 2022), <https://www.peters.senate.gov/newsroom/press-releases/senate-passes-peters-landmark-legislative-package-to-strengthen-public-and-private-sector-cybersecurity->; Senate Homeland Security & Governmental Affairs Committee, *Peters and Portman Introduce Bipartisan Legislation Requiring Critical Infrastructure Entities to Report Cyber-Attacks* (Sept. 28, 2021), <https://www.hsgac.senate.gov/media/dems/peters-and-portman-introduce-bipartisan-legislation-requiring-critical-infrastructure-entities-to-report-cyber-attacks/>. [↑](#footnote-ref-2)
3. Jen Easterly, *The Attack on Colonial Pipeline: What We’ve Learned & What We’ve Done Over the Past Two Years*, Cybersecurity & Infrastructure Security Agency(May 7, 2023), <https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years>. [↑](#footnote-ref-3)
4. *See* *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA),* Cybersecurity & Infrastructure Security Agency,<https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia>; *Presidential Policy Directive -- Critical Infrastructure Security and Resilience*, Presidential Policy Directive 21, (Feb. 12, 2013), <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>. The sixteen sectors are as follows. Chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; water and wastewater systems. [↑](#footnote-ref-4)
5. 6 U.S.C. § 681b(c)(1). [↑](#footnote-ref-5)
6. Justin Doubleday, *CIRCIA, CMMC inch closer with rulemaking marathons nearing crucial stage,* Federal News Network (Sept. 7, 2023), <https://federalnewsnetwork.com/cybersecurity/2023/09/circia-cmmc-inch-closer-with-rulemaking-marathons-nearing-crucial-stage/>; 6 U.S.C. § 681b(b)(2). [↑](#footnote-ref-6)
7. *See generally* *The 2022 Cyber Incident Reporting Law: Key Issues to Watch*, Lawfare (Mar. 25, 2022), <https://www.lawfaremedia.org/article/2022-cyber-incident-reporting-law-key-issues-watch> (discussing how CISA can “increase the quantity and quality of cyber incident reporting” by properly scoping regulations). [↑](#footnote-ref-7)
8. Bus. Roundtable, Comment on Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (Nov. 14, 2022), <https://www.regulations.gov/comment/CISA-2022-0010-0115>. [↑](#footnote-ref-8)
9. *Large Constellations of Satellites: Mitigating Environmental and Other Effects,* United States Government Accountability Office (Sept. 2022),https://www.gao.gov/assets/gao-22-105166.pdf. [↑](#footnote-ref-9)
10. U.S. Chamber of Com., Comment on Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (Nov. 14, 2022), <https://www.regulations.gov/comment/CISA-2022-0010-0075>. [↑](#footnote-ref-10)
11. Cybersecurity Coal., Comment on Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (Nov. 14, 2022), <https://www.regulations.gov/comment/CISA-2022-0010-0105>; CTIA, Comment on Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (Nov. 14, 2022), <https://www.regulations.gov/comment/CISA-2022-0010-0070>. [↑](#footnote-ref-11)
12. Cybersecurity Reporting for Critical Infrastructure Act of 2022, Pub. L. No. 117-103, 136 Stat. 1058. [↑](#footnote-ref-12)
13. U.S. Dep’t of Homeland Sec., *Harmonization of Cyber Incident Reporting to the Federal Government* (Sept. 19, 2023), <https://www.dhs.gov/sites/default/files/2023-09/DHS%20Congressional%20Report%20-%20Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf>. [↑](#footnote-ref-13)
14. *See generally* CIGI, *Cybersecurity and Outer Space* (Jan. 29, 2023), <https://www.cigionline.org/cybersecurity-and-outer-space/> (discussing perspectives on global governance for the “space-cyber nexus”). [↑](#footnote-ref-14)
15. *See, e.g.,* Walter Peeters, *Cyberattacks on Satellites: An Underestimated Political Threat*, London School of Economics (2023), <https://www.lse.ac.uk/ideas/projects/space-policy/publications/Cyberattacks-on-Satellites>. [↑](#footnote-ref-15)
16. Charlotte Van Camp and Walter Peeters, *A World without Satellite Data as a Result of a Global Cyber-Attack*, 59 Space Policy, 7 (Feb. 2022), https://doi.org/10.1016/j.spacepol.2021.101458. [↑](#footnote-ref-16)
17. Stew Magnuson, *ANALYSIS: Acknowledging Space Systems as ‘Critical Infrastructure’,* National Defense Magazine (May 10, 2022), <https://www.nationaldefensemagazine.org/articles/2022/5/10/acknowledging-space-systems-as-critical-infrastructure>. [↑](#footnote-ref-17)
18. Frank Ciullufo, et al., *Time to Designate Space Systems as Critical Infrastructure*, CSC 2.0 (Apr. 14, 2023),

    <https://cybersolarium.org/csc-2-0-reports/time-to-designate-space-systems-as-critical-infrastructure/>; Sandra Erwin, *Space industry group turns up volume on satellite vulnerabilities*, Space News (Oct. 17, 2023), <https://spacenews.com/space-industry-group-turns-up-volume-on-satellite-vulnerabilities/>; Shelli Brunswick, *The Cyber-Space Connection: Why It’s Imperative For Our Future*, Forbes (Oct. 31, 2023), <https://www.forbes.com/sites/forbestechcouncil/2023/10/31/the-cyber-space-connection-why-its-imperative-for-our-future/?sh=538c65d91087>. [↑](#footnote-ref-18)
19. Space Infrastructure Act, H.R. 5017, 118th Cong. (2023). [↑](#footnote-ref-19)
20. John Sakellariadis, *Interagency council takes wind out of push to make space critical infrastructure*, POLITICO Pro (Oct. 4, 2023), <https://subscriber.politicopro.com/article/2023/10/interagency-council-takes-wind-out-of-push-to-make-space-critical-infrastructure-00119886>. [↑](#footnote-ref-20)
21. Rachel Jewett, *AIA Takes Stance Against Space as a Critical Infrastructure Sector*, Via Satellite (Sep. 20, 2023), <https://www.satellitetoday.com/government-military/2023/09/20/aia-takes-stance-against-space-as-a-critical-infrastructure-sector/>. [↑](#footnote-ref-21)
22. *See* Brian Cavanaugh, *The Race for More Space: The flawed logic behind making space a 17th Critical Infrastructure*, Space News (Sep. 26, 2023), <https://spacenews.com/the-race-for-more-space/>. [↑](#footnote-ref-22)
23. Danielle Jablanski, *Critical infrastructure cybersecurity prioritization: A cross-sector methodology for ranking operational technology cyber scenarios and critical entities*, Atlantic Council (Apr. 19, 2023), <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/critical-infrastructure-cybersecurity-prioritization/>. [↑](#footnote-ref-23)