**Strengthening U.S. Cybersecurity through Private Sector Collaboration, from a Red and Blue Team perspective**.

**Introduction**

As the modern cyber world increasingly moves at the speed of light (fiber networks), borders that once took days or months to cross are now traversed instantaneously. That being said, protecting sovereignty and citizens has emerged as a broad yet important challenge in an interconnected world. In 2015, Barack Obama said, “The cyber world is sort of the Wild, Wild West, and to some degree, we’re asked to be the sheriff.” [1] Just a few years later, U.N. Secretary-General Guterres illustrated the importance of changing this when he made the statement about ushering in order, to the Wild West of cyberspace in 2020 [2]. Recognizing the emerging challenges, before Guterres’s call for order, the U.S. had begun working towards this before the speech by establishing the Cyberspace Solarium Commission (CSC). The CSC was established in 2019 by the National Defense Authorization Act. The Act recognized that, in a sense, the government and citizens must unite and act together to battle what Admiral Mike Gilday stated was a conflict that occurs day in and day out in the cyber realm. This paper focuses on Pillar 5, Operationalize Cybersecurity Collaboration with the Private Sector. It examines the key recommendations within this category, evaluating their successes, shortcomings, and essential role through the dual perspectives of Red Team (offensive) and Blue Team (defensive) cybersecurity operations.

**Overview of the CSC Pillar 5: Private Sector Collaboration**

The CSC recognizes that most of what is considered critical infrastructure is owned by the private sector [3]. Because of this, the government is not the primary actor. Private companies (finance, healthcare, energy, and transportation) are often the first to detect and defend against these attacks. The CSC mentioned that success in countering malicious actors depends highly on how the private sector responds with their underlying efforts [3]. Admiral Mike Gilday made two statements that said it best. “We are not fighting an enemy that people can see,” and “we’re not fighting a war where international norms exist. But make no mistake, we are in a conflict day-in and day-out in the cyber realm, and you are all on the front lines.” [4] This is recognized in the CSC report, also stating in the executive summary, “We are not the Chinese Communist Party.” [5]. There needs to be a balance between saddling the private sector with onerous and counterproductive regulations and forcing companies to hand over their data to the federal government [5]. Instead, the government must work to accomplish this through support (legislative policy and unique assets), therefore enabling the private sector [3]. This Pillar has three major parts:

Creating a framework for improving and prioritizing governmental cybersecurity support to critical elements in the private sector [3]. It recognizes that the government is limited in its ability, so it works to focus on what could cause a cascading, destabilizing effect on national security and economically, and on public health and safety [3]. To accomplish this, the CSC wants to offer governmental resources, such as intelligence, military, and law enforcement capabilities, to the private sector [3].

Focus the governmental abilities where they can add the most value [3]. All those abilities can aid in achieving better situational awareness, providing combined knowledge from places like the intelligence community [3]. Behind the scenes, the government can also impose costs to deter further malicious behavior by bringing all instruments of power to the defense of cyberspace, acting against the adversaries [5]. Lastly, lowering barriers to collaboration between the government and the private sector. The CSC also recommends that Congress should direct the executive branch to strengthen CISA to support infrastructure security and resilience, and establish a Joint Cyber Planning Cell under CISA [5]. In addition, the CSC also recommends improving legal protections to facilitate collaboration and joint exercises [3].

**Analysis of Recommendations**

The Joint Cyber Defense Collaborative under CISA openly states that “No one entity can secure cyberspace alone.” [6]. Bad actors are increasingly adopting a “crime-as-a-service” model [7]. With this, there are four points that the JCDC uses to facilitate this. These are [6]:

* Synchronization of National Cyber Incident Management & Campaigns
* Exchange of unique threat and vulnerability information
* Creation of world-class cybersecurity guidance
* Execution of plans that counter adversaries and reduce risk

As a Red Teamer, the JCDC helps better prepare companies’ defenses by aiding in simulating attacks. This guidance provides both red and blue teams with advanced planning. Some criticisms of information sharing are that some say that it is too slow. The newest rules have changed to giving information sharing as 30 days for the upper limit [7]. It is known that the NSA will withhold certain zero-day vulnerabilities for potential use in cyberoperations, which gives an exception to the 30-day rule. A version of this withholding is called the NOBUS Doctrine [8]. A concern from this approach was given standing with the real-world example of the EternalBlue exploit [8].

The JCDC shows progress forward with operational collaboration, other recommendations, though it has faced slower adoption with potentially even more controversy. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). It was made to help improve cybersecurity by requiring reporting of cyber incidents and ransomware payments to CISA [9]. A requirement of CIRCIA was that CISA develop and implement regulations for entities to report covered cyber incidents and ransomware payments [10]. There are four aspects of this for CISA [10]:

* Mandatory Reporting
* Rapid Response
* Rulemaking Process
* Public Input

Blue Teams will like the list of information that CISA requests from critical infrastructure, so they can better prepare their defenses. The activity criteria set forth by CISA are:

* Unauthorized access to your system
* DoS attacks that last more than 12 hours
* Malicious code on your systems, including variants if known
* Targeted and repeated scans against services on your systems
* Repeated attempts to gain unauthorized access to your system
* Email or mobile messages associated with phishing attempts or successes
* Ransomware against Critical infrastructure, including variant and ransom details if known

A criticism of CIRCIA is that the rules are still not set and are being worked on with potential dates in 2026, even though this was enacted in 2022 [11]. This has been because of legal complexities and resistance from certain sectors like the ABA. A concern has been brought up by the American Bankers Association that CIRCIA imposes excessive reporting obligations and takes the time away from critical responders occupied by reporting [12]. Yet a real-world example of the need for information sharing in a timely manner is the SolarWinds attack. In the case of SolarWinds, they never reported the incident to CISA. The report was given to the FBI, which chose to forward it to CISA.

In June of 2023, CSC 2.0 released a report stating that information and Guidance are either inconsistent or missing [13]. This underscores the importance of the recommendation of the Systemically Important Critical Infrastructure (SICI) concept. For Red Teams, this is important because they help to focus on who needs assessments prioritized for, and for Blue Teams, it helps identify what the biggest targets. The key aspect of SICI is identifying critical infrastructure so it can be prioritized. In 2023, the Homeland Security Operational Analysis Center published a proposal on how to identify what a critical entity is [14]. A way to identify the critical of the critical as power grids, financial systems, and telecommunications networks, as examples, but not expressly listed in the report. SISI has had some criticisms. One large criticism is that Presidential Policy Directive 21 (PPD-21) is about 10 years old, even though the requirement is that it is updated every four years [13]. Then there is the debate about whether defining a list would help or hurt. There is a potential that having a list of critical infrastructure could lead to it being used as a target list for adversaries.

The pillar of Cybersecurity through Private Sector Collaboration is illustrated through these three initiatives. There have been many challenges and successes, though about 70% of the recommendations from the CSC have been fully or partially implemented [13]. But the criticisms highlight the need for continued adaptation and commitment.

**Conclusion**

The CSC’s pillar on operationalizing public-private cybersecurity collaboration shows the shift in policy from having passive partnerships to having active, real-time coordination between the government and the private sector managing critical infrastructure. As a Red Team member, the JCDC exercises help simulate attacks, leading to better-prepared networks. As a Blue Team member, CIRCIA reporting helps to improve detection and response speeds through information sharing. The SICI concept underscores the difficulties in advancing more public-private cybersecurity collaboration.

**Future Considerations**

Tackling the frontier of the cyber world has had and will have more challenges in the future. The CSC has made advancements in this area, but getting more private sector buy-in has remained a challenge. Perhaps, working to streamline policies and laws could help in this area. That and along with the potential of expanding real-time cyber defense operations. These could be the first steps to address future threats. The challenges are clear, but with sustained efforts from both the government and private industry, we can protect our nation’s digital future.

# References

|  |  |
| --- | --- |
| [1] | The White House, Office of the Press Secretary, "Remarks by the President at the Cybersecurity and Consumer Protection Summit," 13 February 2015. [Online]. Available: https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit. [Accessed 2025]. |
| [2] | United Nations, Secretary-General, "Remarks to the General Assembly on the Secretary-General's priorities for 2020," United Nations, 22 Janurary 2020. [Online]. Available: https://www.un.org/sg/en/content/sg/speeches/2020-01-22/remarks-general-assembly-priorities-for-2020. |
| [3] | United States of America Cyberspace Solarium Commission, "Final Report," U.S. Cyberspace Solarium Commission, 2020. |
| [4] | P. O. 1. C. N. VanDuser, "NCWDG Celebrates Opening of Cyber Foundry," Defense Visual Information Distribution Service, 18 February 2020. [Online]. Available: https://www.dvidshub.net/news/363356/ncwdg-celebrates-opening-cyber-foundry#.Xkx8I44ONeo.twitter. |
| [5] | Cyberspace Solarium Commission, "Executive Summary," U.S. Cyberspace Solarium Commission, 2020. |
| [6] | Cybersecurity & Infrastructure Security Agency, "Joint Cyber Defense Collaborative," 2025. [Online]. Available: https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative. |
| [7] | R. M. G. Senator Angus King, "United States Of America Cyberspace Solarium Commission," U.S. Cyberspace Solarium Commission, 2020. |
| [8] | B. Buchanan, "Nobody But Us: The Rise And Fall Of The Golden Age Of Signals Intelligence," *Hoover Working Group on National Security, Technology, and Law,* no. Aegis Series Paper No 1708, 2017. |
| [9] | Cybersecurity & Infrastructure Security Agency, "Sharing Cyber Event Information Fact Sheet," April 2022. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/Sharing\_Cyber\_Event\_Information\_Fact\_Sheet\_FINAL\_v4\_0.pdf. |
| [10] | Cybersecurity & Infrastructure Security Agency, "CIRCIA FAQs," CISA, [Online]. Available: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/circia/faqs. |
| [11] | T. Temin, "New comprehensive Homeland Security cyber incident reporting rules," Federal News Network, 3 June 2024. [Online]. Available: https://federalnewsnetwork.com/cybersecurity/2024/06/new-comprehensive-homeland-security-cyber-incident-reporting-rules/. |
| [12] | American Banking Association, "ABA, associations urge officials to rethink cybersecurity reporting rule," ABA Banking Journal, 28 February 2025. [Online]. Available: https://bankingjournal.aba.com/2025/02/aba-associations-urge-officials-to-rethink-cybersecurity-reporting-rule/. |
| [13] | A. F. R. (. M. M. Mary Brooks, "Revising Public-Private Collaboration to," CSC 2.0, 2023. |
| [14] | J. W. W. S. R. B. B. A. S. S. P. C. K. M. J. W. J. W. P. M. J. D. V. Z. W. JOHN BORDEAUX, "Identifying and Prioritizing Systemically Important Entities," Rand, 2023. |
| [15] | T. Starks, "National Cyber Director Harry Coker looks back (and ahead) on the Cyber Director office," Cyberscoop, 7 January 2025. [Online]. Available: https://cyberscoop.com/national-cyber-director-harry-coker-looks-back-and-ahead-on-the-cyber-director-office/. |