Policy Analysis Paper 5

Hans Peterson

School of Cybersecurity, Old Dominion University

CYSE 425W: Cybersecurity Strategy and Policy

Professor Francis Hiser

December 5, 2025

Policy Analysis Paper 5

Considering CISA, the Cybersecurity Information Act of 2015, has been thoroughly reviewed in previous papers, the act's effectiveness can be evaluated based on its current necessity and how the act is perceived.

Starting from Policy Analysis Paper 2, which was concerned with political implications, it is apparent that CISA had striking issues. To reiterate, CISA was a policy meant to foster cooperation and cyberthreat information sharing between government agencies and private entities to bolster national defense. Although CISA was drafted as a response to frequent cyberattacks, it faced criticism. First, Heidenreich (2015) stated that CISA was tacked onto the 2016 spending bill, which was partly passed to avoid a government shutdown; this implies that CISA was underdeveloped, as it was drafted in a time of necessity. It lacked consideration of future privacy concerns. Additionally, CISA had vaguely worded language that expanded the definition of what a "cybersecurity threat" is, increasing the scope of what information government agencies could collect.

In Policy Analysis Paper 3, which was concerned with ethical implications, CISA also had several issues. CISA was widely believed to be a surveillance bill that allowed private companies to share information with intelligence agencies such as the National Security Agency; this included personal data of customers, including their names, addresses, and how they used a company's services (CISA passes Senate, threatens liberty and privacy, 2015). CISA was perceived more so as a backdoor for the NSA. Individual rights and privacy were being threatened. Additionally, Greene (2015) also criticizes the loose definitions of "cybersecurity

threat" and "cyber threat indicators," which could be interpreted as any personally identifiable information under its definition.

In Policy Analysis Paper 4, which was concerned with social implications, CISA faced the same criticisms. Despite CISA's intent to ally the private sector with the public sector through transparency and open cooperation, society hardly trusted the act and, again, perceived it as expanding mass government surveillance. Greene (2015) explains how CISA would provide easy access to the NSA, and Tran (2016) concluded that "sharing information does little to prevent successful cyberattacks, given that there have been many already in place." For example, the U.S. Computer Emergency Readiness Team collected and analyzed cyberthreat data, but its efficacy was unclear (Tran, 2016). Lastly, CISA was created in a time where the nation, even the general public, was more concerned with security rather than privacy, further entrenching its status as a surveillance bill.

Considering how several experts from different papers perceive CISA in a negative context, their assessments would not support the continuation of CISA based on privacy concerns. It is important to note that the main concern between all three papers was mass surveillance or government overreach. In fact, there is support for CISA's existence. According to Jaikaran (2025), the expiration of CISA would eliminate liability protections, disclosure protections, and antitrust protections, which would ward off private agencies from sharing. If the concern was mass surveillance, it would imply that agencies exploited the mandates provided by CISA. Personally, I believe CISA was effective from the fact that it allowed private entities to share cyberthreat information with government agencies, and if CISA were to be removed, our national defense would weaken. Less cyberthreat data would be shared; the main concern would be that private companies were less willing to cooperate with agencies. A few days ago, CISA

was renewed and extended to January 2026. Congress had realized its necessity and decided to continue its existence.

Although CISA could be considered ineffective in enforcing privacy rights, there are recommendations that could fix this issue. Jaikaran (2025) explained how risks to cyberspace have evolved, which includes operational technology and edge devices; these technologies are involved in critical infrastructure systems, such as supervisory control and data acquisition (SCADA) systems. These technologies were not defined in the act, so if the act were to be reviewed and updated, definitions of what could be considered a "cybersecurity threat" may also be revamped to include these technologies as points of concern. CISA's outdated language could be updated enough so that definitions of "cyber threat indicators" would be more accurate and concise in what it is actually trying to define. The privacy issues surrounding CISA are not set in stone. If cybersecurity experts were to revise CISA, it would be revised to avoid the same pitfalls it had before.

References:

CISA passes Senate, threatens liberty and privacy. (2015). *The New American (Belmont, Mass.)*, *31*(22), 7. https://research-ebsco-com.proxy.lib.odu.edu/c/lnv5pa/viewer/pdf/nzwh6vyirj?route=details

Greene, R. (2015). Cybersecurity Information Sharing Act of 2015 is about cyber surveillance, not cybersecurity. *Washington, DC: Open Technology Institute-New America*. https://static.newamerica.org/attachments/2741-cybersecurity-information-sharing-act-of-2015-is-cyber-surveillance-not-cybersecurity/CISA_Cyber-Surveillance.488b3a9d2da64a27a9f6f53b38beb575.pdf

Heidenreich, J. (2015). The privacy issues presented by the cybersecurity information sharing act. *NDL Rev.*, *91*, 395. https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/nordak91&id=404&men_tab=srchresults

Jaikaran. (2025). *Cybersecurity Information Sharing Act of 2015: Expiring Provisions (IF12959) [2025]* (1295th ed.). Washington: U.S. G.P.O. https://heinonline-org.proxy.lib.odu.edu/HOL/Page?collection=congrec&handle=hein.crs/cbyscinsh0001&id=2&men_tab=srchresults

Tran, J. L. (2016). Navigating the cybersecurity act of 2015. *Chap. L. Rev.*, *19*, 483. https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/chlr19&id=508&men_tab=srchresults