

The success of the 2023 U.S. NCS will be determined by whether the objectives set by the strategy have resulted in a stronger cybersecurity. In my earlier policy papers, I have addressed the aims of the strategy as well as its political, ethical, and social effects. These areas are necessary for the evaluation of the strategy as cybersecurity impacts the government, private sector, and individuals. An evaluation of the strategy should assess whether the objectives of the strategy are being achieved, whether the risks to cybersecurity have decreased, and whether organizations and critical infrastructure are becoming more secure.

One way to measure the strategy is whether the strategy's aims are being implemented and whether this will achieve measurable gains in cybersecurity. The National Cybersecurity Strategy and the implementation plan were reviewed by the U.S. Government Accountability Office (GAO, 2024), which identified that they addressed four out of six characteristics that GAO finds desirable in a national strategy, and addressed the other two in part. A major issue is that the strategies do not contain all outcome-oriented performance measures. Furthermore, GAO found that the implementation plan does not clearly identify what resources and estimated costs are associated with carrying out its initiatives. These points matter because completing an initiative does not necessarily mean that cybersecurity has improved.

Finally, studies reveal that research on national cybersecurity strategies should be conducted periodically and each time there is a change in the cybersecurity environment. Cram and Yuan (2023) researched how national cybersecurity strategies change over time and provided reasoning why they must change over time- technology, cyber threats, and government priorities. Therefore, the 2023 National Cybersecurity Strategy should not only be assessed once but should continue to be measured.

Another aspect covered by the article by Craig et al. (2023) is the case of national cybersecurity strategies and capacity building. This article highlights the significance of considering the capacity of governments and organizations to respond to cyber security threats and this is relevant to the 2023 strategy in the sense that the impact of policies can be checked through the enhancement of cyber capacity by organizations rather than merely the creation of policies.

Another key consideration is whether cybersecurity controls reduce risk. Woods and Seymour (2024) examined the research on the efficacy of cybersecurity controls and concluded that how the control is implemented has an impact on whether the control "worked" to reduce risk. Their research supported controls like attack surface management, patching, and multi-factor authentication, while indicating that merely mandating that a security control exists will not necessarily have an impact on risk. This indicates that analysis of the National Cybersecurity Strategy should be based on cybersecurity outcomes rather than just implementation of requirements.

I would evaluate the strategy using a set of outcome measures, such as: the number of successful cyberattacks; number of ransomware attacks and ransomware losses; number of exploited vulnerabilities; time to identify and respond to cyberincidents; security and resilience of critical infrastructure; adoption of proven cybersecurity practices; information sharing among government agencies and private companies; and whether small organizations have sufficient resources to comply with cybersecurity requirements. The strategy would show that progress is being made if each outcome measure shows significant improvement over a period, rather than only showing that programs had been established or requirements had been met. This approach is

aligned with GAO's recommendation to use outcome measures to verify that the strategy is achieving its goals.

The potential political, social, and ethical implications examined in my previous paper need to be part of the 'fit' calculation. Politically, this strategy will determine levels of state intervention, regulatory decisions, public financing, roles of private actors, and international co-operation. Ethically, the gains from improved cybersecurity need to be viewed against rights and concerns of individuals and their privacy. Socially this impacts upon all who use technology, given that today we rely upon it for health care, banking, transportation, communication, education, and much more. Thus, the evaluation would need to account for improved cybersecurity along with costs, privacy impacts, public trust, and differences in resources available to both big and small organizations.

In summary, understanding the 2023 U.S. National Cybersecurity Strategy involves more than assessing whether the efforts of that strategy have concluded. A sound assessment would include consideration of measurable cybersecurity outcomes and determine whether the actions of organizations and operational environments are becoming more resilient. Empirical evidence indicates that cybersecurity strategies must evolve, as threats and technologies change. Empirically isolating the results of different strategy elements might identify areas producing measurable gains and those elements that need adjustment, added resources, or an innovative approach. Technical results, combined with political, ethical, and social considerations, will provide a better understanding of the strategy's impact.

References

- Craig, A. J. S., Johnson, R. A. I., & Gallop, M. (2023). Building cybersecurity capacity: A framework of analysis for national cybersecurity strategies. *Journal of Cyber Policy*, 7(3), 375–398. <https://doi.org/10.1080/23738871.2023.2178318>
- Cram, W. A., & Yuan, J. (2023). Out with the old, in with the new: Examining national cybersecurity strategy changes over time. *Journal of Cyber Policy*, 8(1), 26–47. <https://doi.org/10.1080/23738871.2023.2238712>
- U.S. Government Accountability Office. (2024). *Cybersecurity: National Cyber Director needs to take additional actions to implement an effective strategy* (GAO-24-106916).
- Woods, D. W., & Seymour, S. (2024). Evidence-based cybersecurity policy? A meta-review of security control effectiveness. *Journal of Cyber Policy*, 8(3), 365–383. <https://doi.org/10.1080/23738871.2024.2335461>