wiley

NEWSLETTER

Office of the National Cyber Director Remains Nascent, Evaluations to Come as Efforts Mature

September 2022

Privacy In Focus®

In 2021, Congress created a new cyber leadership position within the White House, enacting a suggestion from the Cyberspace Solarium Commission, to develop a new Office of the National Cyber Director (ONCD). This new office added to an array of federal leadership offices with interests in cyber, and recently the U.S. Government Accountability Office (GAO) released a short overview of it as part of its ongoing work to "evaluate the administration's efforts to develop and implement a comprehensive national cybersecurity strategy."

By way of background, the William M. (Mac) Thornberry National Defense Authorization Act (NDAA) for Fiscal Year 2021 established the Office of the National Cyber Director within the Executive Office of the President. It created this office and authorized staffing of up to 75 full-time employees. This is more than the expectations of the Solarium Commission that the office would be "staffed at a size similar to that of comparable EOP institutions (approximately 50 persons)."

This GAO product summarizes the ONCD's strategic statement and its intentions regarding a national cybersecurity strategy, which remains forthcoming. The jury is still out on whether the ONCD will fulfill the role envisioned by the Solarium Commission. The Commission wrote that "[t]he NCD would not direct or manage day-to-day cybersecurity policy or the operations of any one federal agency, but instead will be responsible for the integration of cybersecurity policy and operations across the executive branch."

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Cyber and Privacy Investigations, Incidents & Enforcement

Privacy, Cyber & Data Governance

The ONCD is headed by Director Chris Inglis and last month announced an array of new hires. The role and influence of this office on many existing federal cyber workstreams remains unclear.

GAO described several areas of ONCD focus, in seven "lines of effort" that may impact the private sector, and which have yet to be fully developed. Some examples are:

- Protect and defend state, local, and private sector networks.
- Ensure the federal government serves as a model for the private sector actors to follow.
- Encourage collaboration between the public and private sectors to develop a more secure digital supply chain.

Directional uncertainty about the priorities of the Administration may cast a pall on ongoing efforts, given the multiplicity of efforts on cyber that have been directed by Congress and invigorated by agencies. Just by way of example, recent legislation, the Cyber Incident Reporting For Critical Infrastructure Act of 2022 (CIRCIA), directs the creation of a Cyber Incident Reporting Council, which is chaired by DHS Under Secretary for Policy Robert Silvers and includes the Office of the National Cyber Director, Federal Bureau of Investigation, Securities and Exchange Commission, Federal Trade Commission, Federal Communications Commission (FCC), and Departments of the Treasury, Defense, Justice, Agriculture, Commerce, Health and Human Services, Transportation, Energy, and Homeland Security. At the same time, the Chairwoman of the FCC in February 2022 announced that she would lead a reinvigorated Federal Interagency Cybersecurity Forum.

As federal work on cyber expands, Congress, the White House, and agencies should carefully consider the landscape of existing work and how to deconflict. Private organizations should watch these efforts and consider how to engage, but also how to encourage streamlining and harmonization. GAO found that the ONCD "needs to fully develop and implement a comprehensive national strategy in order to have a clear roadmap for overcoming the cyber challenges facing our nation."