CENTER FOR CYBERSECURITY POLICY AND LAW

Cybersecurity Coalition

WHITEPAPER

THROUGH THE LOOKING GLASS:

An Updated Vision for the Office of the National Cyber Director

By Ari Schwartz, Inés Jordan-Zoob, and Samara Friedman

DECEMBER, 2024

Through the Looking Glass: An Updated Vision for the Office of the National Cyber Director

By Ari Schwartz, Inés Jordan-Zoob, and Samara Friedman

Executive Summary

In 2021, the Office of the National Cyber Director (ONCD) was established and statutorily charged with advising the President of the United States on matters related to cybersecurity. In the three years since, ONCD has matured into one of the several key components of the U.S. government's policymaking apparatus for cybersecurity - across both the government and the private sector. However, several changes are needed to ensure the efficacy of the office, especially as it relates to these other relevant agencies within the U.S. government.

The incoming administration has the ability to clarify and enhance ONCD's mission and resources. This paper provides five key policy and structural recommendations to support this effort, with the goal of minimizing duplication of efforts, enabling accountability, and more broadly, increasing the security and resiliency of the U.S. cyber posture. These recommendations include:

1. Update and clarify the ONCD mission statement, including a clear articulation of the policy making responsibility of the National Cyber Director (NCD) versus other key senior cyber leadership.
2. Codify the NCD's role as the U.S. Government's lead external-facing cyber official.
3. Improve collaboration between ONCD and the National Security Council (NSC) through dual-hatting a senior director. NSC/Cyber should also play more of a NSC/Intecon-like role for coordination between both entities.
4. Staff ONCD with additional agency detailees and subject matter experts from within the government.
5. Reinforce and codify the position of the Federal Chief Information Security Officer (CISO) within White House Office of Management and Budget (OMB), to be dual-hatted as a direct report to the NCD.

Introduction

On Jan. 1, 2021 the Office of the National Cyber Director (ONCD) was established under §1752 of the National Defense Authorization Act (NDAA) for FY2021.[1] The NDAA officially positioned ONCD within the Executive Office of the President (EOP) and tasked it with the responsibility of advising the President on

[1] Andrew Grotto, "How to Make the National Cyber Director Position Work," Lawfare, January 2021, https://www.lawfaremedia.org/article/how-make-national-cyber-director-position-work.

matters pertaining to cybersecurity policy and strategy.[2] Per the legal wording, ONCD's mission is "to advance national security, economic prosperity, and technological innovation through cybersecurity policy leadership."[3]

Over three years later, ONCD exists as a key component of the U.S. cybersecurity policy apparatus and is larger in size than originally envisioned. However, the exact nature of its role, and how it interacts with other governmental offices, can be ambiguous, and at times, even contested. This paper will summarize the context on the origins of ONCD and its current activities and provide recommendations on how its structure can be optimized to limit duplication, enable accountability, and maximize value.

Background

In 2019, the Cyberspace Solarium Commission (CSC) was established to develop "a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences," and recommend the policies and legislation required to implement that strategy.[4] The impactful work of the CSC materialized in their ensuing 2020 report, which featured 82 recommendations across six thematic pillars.

One of the first recommendations in the report was for Congress to create a National Cyber Director (NCD) position and a supporting office, in part to help consolidate accountability for harmonizing the executive branch's policies, budgets, and responsibilities in cyberspace.[5] This recommendation aligned with both public discourse and feedback shared with government from the private sector, academia and civil society.[6]

In its report, the CSC urged Congress to establish a Senate-confirmed NCD, which would be supported by an Office of the NCD and positioned within the EOP. Unlike the related historic role of "cyber czars" within the U.S. government, the CSC recommended that the NCD should hold formal authority and maintain an independent budget.[7] The NCD would not be responsible for directing or managing day-to-day cybersecurity policy or any singular federal agency, but would instead bear the responsibility of integrating cybersecurity policy and operations across the entirety of the EOP. As drafted in the proposal, the NCD would:

---

[2] "Office of the National Cyber Director," WH.GOV, https://www.whitehouse.gov/oncd/#:~:text=Established%20by%20Congress%20in%202021,issued%20on%20March%202%2C%202023.

[3] "Office of the National Cyber Director," WH.GOV, https://www.whitehouse.gov/oncd/#:~:text=Established%20by%20Congress%20in%202021,issued%20on%20March%202%2C%202023.

[4] United States of America Cyberspace Solarium Commission, "Introduction," https://www.solarium.gov/.

[5] Andrew Grotto, "How to Make the National Cyber Director Position Work," Lawfare, January 2021, https://www.lawfaremedia.org/article/how-make-national-cyber-director-position-work.

[6] Andrew Grotto, "How to Make the National Cyber Director Position Work," Lawfare, January 2021, https://www.lawfaremedia.org/article/how-make-national-cyber-director-position-work; United States of America Cyberspace Solarium Commission, "CSC Final Report," solarium.gov/report, March 2020, https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view?pli=1.

[7] Ellen Nakashima, "Cyber Solarium Commission proposes actions to strengthen nation's defenses against foreign threats," March 2020, https://www.washingtonpost.com/national-security/cyber-solarium-commission-proposes-actions-to-strengthen-nations-defenses-against-foreign-threats/2020/03/10/d6980218-62d2-11ea-acca-80c22bbee96f_story.html.

"(1) be the President's principal advisor on cybersecurity and associated emerging technology issues and the lead national-level coordinator for cyber strategy and policy; (2) oversee and coordinate federal government activities to defend against adversary cyber operations inside the United States; (3) with concurrence from the National Security Advisor or the National Economic Advisor, would convene Cabinet-level or National Security Council (NSC) Principals Committee–level meetings and associated preparatory meetings; and (4) would provide budgetary review of designated agency cybersecurity budgets."[8]

The NCD would be added to the list of NSC regular attendees and would serve on the NSC for issues related to cybersecurity and associated emerging technologies.[9] Furthermore, the NCD would lead the national development and coordination of cyber strategy, policy, and defensive operations, including the drafting and implementation of the U.S.'s National Cyber Strategy. Finally, the NCD would lead efforts to develop a private-public relationship to mutually defend critical infrastructure and coordinate the security challenges facing emerging technology.

The CSC specifically included a provision that established that although the NCD's responsibilities would not impinge on the responsibilities of the Department of Defense (DoD), Office of the Director of National Intelligence (ODNI), the Department of Justice (DOJ), and FBI, it would be kept informed of their efforts.[10]

In terms of resources, the CSC's proposal recommended a staff size of approximately 50 people, comparable to other EOP offices.[11] Budget-wise, the report asserted that the NCD would "have budgetary oversight over the cybersecurity community,"[12] including entities within the executive branch that are working to implement the National Cyber Strategy. Any head of a program, agency, or department must first send its cyber budget request to the NCD prior to sending it to the Office of Management and Budget (OMB). If the budget proposal is not aligned with the aims of the National Cyber Strategy, the NCD reserves the right to suggest revisions, which will eventually be sent to OMB. Finally, any significant changes that OMB makes to the cybersecurity budget of any agency or department must meet the approval of the NCD.

The passage of the FY2021 NDAA codified 25 of the CSC's recommendations, signifying the most comprehensive piece of national cybersecurity legislation in American history.[13]

ONCD as Established in the FY2021 NDAA

The NDAA declared that the NCD is subject to the authority of the President and shall:

1. Serve as the principal advisor to the President on cybersecurity policy and strategy.
2. Offer advice to the NSC, the Homeland Security Council, and the relevant Federal departments and agencies relating to the coordination of national cyber policy and strategy.
3. Lead the coordination and implementation of the national cyber policy strategy.

---

[8] United States of America Cyberspace Solarium Commission, "CSC Final Report," solarium.gov/report, March 2020, https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view?pli=1.
[9] Ibid.
[10] Ibid.
[11] Ibid.
[12] Ibid.
[13] United States of America Cyberspace Solarium Commission, "Introduction," https://www.solarium.gov/.

4. Masrshall the coordination of development and implementation by the Federal Government of integrated incident response to cyberattacks.
5. Prepare the Federal Government (across agencies and departments) to respond to cyberattacks.
6. Join the Cybersecurity and Infrastructure Security Agency (CISA) and other Federal heads to coordinate and consult with private sector leaders on cybersecurity and other emerging technology issues.
7. Submit an annual report to Congress on cybersecurity threats and issues facing the U.S.
8. Hold responsibility for other functions as the President directs.[14]

With respect to its authority, the NCD may serve as the senior representative to any organization founded by the President with the purpose of advising him or her on cybersecurity matters. Furthermore, the NCD may be included as a participant in the preparations and execution of domestic and international summits or meetings, in which cybersecurity is a main topic. The NCD also may delegate its functions, powers, and duties to other employees of ONCD. Additionally, §1752 amended the National Security Act of 1947 to allow the NCD to participate in the NSC when cybersecurity issues are a major topic.[15]

The powers allotted to the NCD include the ability to select and appoint its employees, hire experts and consultants, utilize the services of other Federal agencies, enter into contracts and agreements necessary to the work of the office. The statute allows for ONCD to hire a staff of up to 75 people outside the normal Title 5 civil service authorities. This has offered a lot of flexibility for the size and structure of ONCD staff.

The Original Vision for ONCD

The Biden administration published its Statement of Strategic Intent for ONCD in 2021, the same year the office was created.[16] The statement describes the following steps for the office:

> *"First, and above all else, the ONCD will champion federal coherence across U.S. government in cyber policy, action, and doctrine. It will improve public-private collaboration to tackle cyber challenges across sectoral lines. It will align resources to aspirations by ensuring U.S. departments and agencies are resourcing and accounting for the execution of cyber initiatives, assets, and talent entrusted to their care, and considering all possible future such requirements. And it will push forward initiatives across all available avenues in order to increase present and future resilience, ensuring our workforce, technologies, and organizations are fit for purpose today and future-proofed for tomorrow."*[17]

To adhere to its mission and achieve its goals, ONCD will work in partnership with other federal agencies, such as the NSC and OMB, and will also work through seven main lines of effort, including:

---

[14] "William M. (Mac) Thronberry National Defense Authorization Act for Fiscal Year 2021," United States Government Publishing Office, January 2021, https://www.govinfo.gov/content/pkg/PLAW-116publ283/html/PLAW-116publ283.htm.
[15] John Costello and Mark Montgomery, "How the National Cyber Director Position is Going to Work: Frequently Asked Questions," Lawfare, February 2021, https://www.lawfaremedia.org/article/how-national-cyber-director-position-going-work-frequently-asked-questions.
[16] "A Strategic Intent Statement for the Office of the National Cyber Director," WH.GOV, https://www.whitehouse.gov/wp-content/uploads/2021/10/ONCD-Strategic-Intent.pdf?utm_source=newsletter&utm_medium=email&utm_campaign=sendto_newslettertest_technology&stream=top#_ga=2.218487897.1396320975.1726082544-1664879296.1725913517
[17] Ibid, 7-8.

1. National Cybersecurity
2. Federal Cybersecurity
3. Budget Review and Assessment
4. Technology and Ecosystem Security
5. Planning and Incident Response
6. Workforce Development
7. Stakeholder Engagement

ONCD in Action

Since its creation, ONCD has accomplished several major recommendations coming out of the CSC report, including the publication of an updated U.S. Cybersecurity Strategy, as well as an associated National Strategy Implementation Plan to put the aforementioned strategy into practice. The relatively easy Senate confirmation of the first NCD, Chris Inglis, and the second and current NCD, Harry Coker, at a time when that is not guaranteed, illustrates that the existence of its office and leadership continues to have support of Congress.

The office has grown too - both in terms of the number of its employees, which is nearing 85,[18] as well as the diversity of their experiences. In the immediate aftermath of its creation, and for the sake of expediency, ONCD was primarily staffed by political appointees. Through 2024, this shifted to more appointed career civil service positions, meaning more subject matter experts from around the government, including from regulatory agencies, are getting the opportunity to work at ONCD.

Lastly, ONCD has begun to increasingly collaborate with its interagency and regulatory partners to further major initiatives, such as coordinating with CISA to establish an Internet Routing Security Working Group.[19]

Inspiration from the EOP

While ONCD has legitimized itself in 2024, there is more work to be done to improve its functionality as many observers, both inside and outside of government see the work of the office as unclear and sometimes duplicative of others in cyber policy. ONCD requires clearer authorities and additional resources.

As noted in the original CSC report, the Office of the United States Trade Representative (USTR) can serve as a useful reference and perhaps the closest parallel for ONCD. USTR is another organization that sits within the EOP, maintains a clear mandate, and collaborates efficiently with the rest of the executive branch. The Office of USTR is responsible for developing and coordinating U.S. international trade policy as well as overseeing trade negotiations.[20]

---

[18] "Congressional Budget Submission Fiscal Year 2025," WH.GOV, https://www.whitehouse.gov/wp-content/uploads/2024/03/FY-2025-Executive-Office-of-the-President-Congressional-Budget-Submission.pdf

[19] Cate Burgan, "ONCD Creates new Working Group to Bolster Internet Routing Security," MeriTalk, September 2024, https://www.meritalk.com/articles/oncd-creates-new-working-group-to-bolster-internet-routing-security/

[20] "Mission of the United States Trade Representative", USTR.GOV, https://ustr.gov/about-us/about-ustr

Like ONCD, the head of USTR, the U.S. Trade Representative, is a Cabinet-level official who serves "as the president's principal trade advisor, negotiator, and spokesperson on trade issues."[21] This public-facing position, currently filled by Katherine Tai, also requires Senate confirmation. Both offices currently sit within the EOP, both are responsible for advising the President on their respective policy domains, and both offices have to substantively collaborate with the interagency and the breadth of the U.S. government to truly achieve their mission statements.

To do this, USTR maintains a staff of over 250 professionals who work through its own interagency structure to coordinate trade policy, resolve trade disagreements, and frame relevant issues for presidential decision-making. Over a dozen other U.S. government agencies, commissions, and courts – such as the Department of Commerce, the Department of Justice, and the U.S. Court of International Trade – have authority over some element of international trade. In turn, many of these organizations work closely with USTR.[22] This is a similar situation to the complex jurisdictions for cyber policy and operations where multiple agencies need to work together to accomplish most objectives.

In 1962, Congress established a USTR-led interagency that supports the coordination of trade policy. The three tiers include: the Trade Policy Staff Committee (TPSC), which is chaired by the USTR to develop and review policy and negotiating documents; the Trade Policy Review Group (TPRG), which coordinates between the Deputy USTR and Assistant Secretary levels; and the National Economic Council (NEC), which is led by the President and coordinates Cabinet-level review.[23] Through its clear mission, well-staffed office, and robust interagency collaboration, USTR has been highly successful in its mission.

Optimizing ONCD

Using the USTR model as a reference, there are tangible next steps the incoming administration can take to strengthen ONCD.

First, the mission statement of the office should be amended to more clearly articulate its mandate and the authorities that will support this mission. This clarification should include a clear articulation of the policymaking responsibilities of the NCD versus other key senior cyber leadership within the U.S. government, including operational entities like CISA, as well as from OMB and other federal entities. By doing so, ONCD will assuage any concerns over its mandate, especially in relation to other relevant cyber offices and agencies within the government.

Second, the NCD should explicitly become the U.S. government's external-facing cyber official, just as the USTR is to trade. This would help cement the role, and specifically that the public can and should voice their concerns regarding cybersecurity and emerging technologies to the NCD and their staff. For USTR, the mission of stakeholder engagement and public-private partnership is supported by a robust and well-structured advisory committee system – including the President's Advisory Committee for Trade Policy and Negotiations, as well as policy and sectoral committees such as the Industry Trade Advisory Committees.

[21] Ibid.
[22] USTR's Relationship with Other Government Agencies
[23] U.S. Trade Policy Functions: Who Does What?

Third, ONCD must more effectively work with the NSC. This collaboration can be made difficult by concerns over executive privilege - namely, that the leadership of the NSC staff, as Title 3 employees, are not typically called to testify before Congress because of separations of powers issues, while the NCD, as a Senate-confirmed position, can and has been called to testify. Despite these tensions, cybersecurity and national security decision-making have only continued to overlap.

This nexus was illustrated in 2021 when the Biden administration created a new position on the NSC for a Deputy National Security Advisor (DNSA) for Cyber and Emerging Technology. The position was created to better coordinate the federal government's cybersecurity effort, and the efforts of current DNSA Anne Neuberger have certainly met this mandate. The DNSA is supported by the pre-existing Cyber Directorate of the NSC (NSC/Cyber). The DNSA, as well as the prior Special Assistant to the President roles that it was based on, have all featured non-typical levels of external engagement, although all of these positions existed before there was an ONCD.

The balance and boundaries between the DNSA role and the NCD remain unclear, and collaboration between the two offices lacks organization and structure. One immediate potential solution would be to dual-hat a senior official at ONCD as a Senior Director at NSC/Cyber, to serve as the primary connecting node between both offices but without the NCD's responsibility for Congressional testimony. Currently, a Deputy NCD is already dual-hatted with OMB, with successful cross-agency collaboration occurring as a result. Further structural changes are likely needed to the actual policy making apparatus to support dual-hatting.

These changes should also include making the NSC/Cyber more closely resemble the existing Directorate of International Economic Affairs (Intecon). Intecon serves as a liaison between USTR, NSC, and NEC. As noted above, NSC and NEC officials are appointed by the President, and they are not required to testify to Congress due to confidentiality, presidential records, and separation of powers concerns.

USTR, like the NCD however, is removed from the inner circle of the President and can be subpoenaed to testify in front of Congress, and the people. As such, USTR is considered to be the public-facing figure regarding trade, whereas the NSC and NEC are more insular. Intecon functions as the policy connection apparatus between these public and the private entities.

Under the Bush and Obama administrations, Intecon was responsible for overseeing "a wide range of policy issues, including macroeconomics, finance, trade, development, global health, and energy." Intecon served as the policy coordinating group to make sure that NEC, NSC, and USTR were able to work effectively with one another. The head of Intecon served as deputy to both the National Security Adviser and the Director of the NEC.

We suggest that the next President follow a similar format by clarifying the role of NSC/Cyber making it responsible for liaising and coordinating between the external-facing ONCD and internal-facing NSC and NEC. ONCD should be considered the primary advisor to the President on most unclassified

cybersecurity-related issues.[24] This would extend to any policy intended to specifically improve the cybersecurity posture of the U.S., including regulatory harmonization efforts, public-private partnerships, and coordination of domestic incident response.

NSC/Cyber would continue to coordinate all other cyber policy, including offensive cyber (of all stripes, military and intelligence-related) and cyber as a component of bilateral and multilateral relationships with foreign governments. Finally, NSC/Cyber, and the broader NSC staff), would coordinate response actions to cyber incidents – opposed to the traditional cyber incident response intended to get systems back to a state of good order – and incidents for which cyber is but a component of the whole-of-government response, for example Colonial Pipeline.

Lastly, USTR optimizes the functionality of its 250 person staff by breaking it down into policy areas.[25] ONCD currently uses policy pillars to guide its work too, and Congress should provide funding in order for it to expand its workforce beyond the current 85, while placing emphasis on hiring more detailees and subject matter experts from within the government, rather than primarily political appointees. While increasing the size of ONCD should be a priority, this may prove to be unpopular with the incoming administration.

While discussing USTR, we must acknowledge another EOP office that could serve as reference for ONCD reforms. The Office of Science and Technology Policy (OSTP) was established in 1976 to advise the President and others within the EOP on a broad array of topics under the umbrella of science and technology.[26]

As part of this, OSTP leads the interagency science and technology policy coordination efforts and assists OMB with an annual review and analysis of related federal research and development. OSTP has played a significant role in prior Democratic administrations, working closely with relevant agencies and, under Obama, growing to an organization of over 135 staff.[27] This influence has not endured to the same degree in Republican administrations. The general assessment is that OSTP does not have as effective policy making apparatus and process. Today, major positions in the office, such as their CTO role, remain unfilled. For these reasons, we found USTR a more useful model.

These examples can also inform another power conflict that has arisen with ONCD: its role in U.S. government cybersecurity spending and operations management. Within its establishing authorities from Congress, ONCD was tasked with "reviewing the annual budget proposals" and "advising the heads of such departments and agencies" to align actions with the federal cyber strategy. These taskings overlap with core authorities of OMB, which is responsible for overseeing the implementation of the President's vision

[24] We realize that saying the NCD should be the main presidential advisor on "most unclassified cyber policy matters" is not a clear delineation. It would also not be clear to say a DNSA should lead on "most national security related cyber policy matters." We believe that there is just no way to make such a clear line here. In some cases the NSC might need to take the lead on a national security policy matter with unclassified information or ONCD might need to take the lead on a non-national security policy matter that might include some classified information. While it would be ideal to make these roles work completely independent of the personalities involved and we should strive to do so, we also must recognize there will always be a need to have them cooperate and work together.

[25] Congressional Research Service, "U.S. Trade Policy Functions: Who Does What?", February 2024, https://crsreports.congress.gov/product/pdf/IF/IF11016

[26] Congressional Research Service, "Office of Science and Technology Policy (OSTP): History and Overview", March 2020, https://sgp.fas.org/crs/misc/R43935.pdf

[27] Jeffrey Mervis, "Trump's White House science office still small and waiting for leadership", Science, July 2017, https://www.science.org/content/article/trump-s-white-house-science-office-still-small-and-waiting-leadership

through federal budget development and execution, as well as management of federal information security and privacy policies.

The Federal Chief Information Officer, referred to in statute as the Director of the E-Government Office, is the primary authority for setting federal policies for federal enterprise security and advising OMB's Resource Management Offices (RMOs), which house the budgetary examiners for all federal agencies, on appropriate investments. Cybersecurity concerns have been delegated from the Federal Chief Information Officer to their Federal Chief Information Security Officer (FCISO) for the past decade.

In setting up ONCD, the Biden administration made the FCISO dual-hatted, housed at OMB, but also serving as the Deputy National Cyber Director for Federal Cybersecurity. Similarly to OSTP's collaboration with OMB to provide an annual review and analysis of related federal R&D, ONCD and OMB collaborated on an annual memorandum regarding cybersecurity priorities.

However, the Federal CISO was primarily tasked with advising ONCD on federal cybersecurity concerns, and budgetary review was delegated to others at ONCD. This risks conflicting authorities in the EOP on cybersecurity resourcing and budgets, with the potential for political maneuvering, inefficiencies and misaligned requests.

We recommend codifying the position of the FCISO, enshrining it as a formal role within OMB, and delineating that the position also be dual-hatted, with the FCISO also serving as a direct report to the NCD — equal to or directly named as a Deputy. This position should lead and maintain all authorities over budgetary matters, as well as federal information systems across both general and national security systems.

This ensures that OMB and ONCD take a collaborative approach on resourcing and the organization of the federal enterprise. Additionally, it allows for ONCD to have a direct pathway to OMB's substantial and well-defined authorities to compel agency actions and conduct oversight.

Looking Forward

Although we have outlined how to make the strategic vision and mandate of ONCD clearer, difficulty arises in how to codify our proposals. Three possible ways to formally adopt our suggestions are through:

1. Executive Order (EO)
2. Presidential Policy Directive (PPD)
3. Legislation in Congress, including potentially within a forthcoming NDAA.

Of these three options, the most immediate would be for the incoming administration to sign an EO or PPD.

In July 2024, bipartisan legislation was introduced in the Senate to establish a comprehensive framework for harmonizing cybersecurity regulations across the federal government. The draft legislation seeks to address some of the challenges associated with multiple cyber regulatory regimes by establishing an interagency harmonization committee to be chaired by ONCD. While the Peters-Lankford bill captures part of the challenge ONCD faces - unclear authorities amidst numerous relevant agencies and regulators - it does not comprehensively empower the office in the way that is outlined above.

The incoming Trump administration could address some of these issues as it nominates the next NCD and other cyber policy roles. That nominee could also spell out a structure of the Office. Finally, Congress will also need to act, working with the administration, to ensure that many of these roles and authorities are properly delineated going forward.

Recommendations

1. The White House should update and clarify the ONCD mission statement, including a clear articulation of the policy making responsibility of the NCD versus other key senior cyber leadership.
2. Congress should codify the NCD's role as the USG's lead external-facing cyber official.
3. The White House should improve collaboration between ONCD and the NSC through dual-hatting a senior director. NSC/Cyber should also play more of a NSC/Intecon-like role for coordination between both entities.
4. The NCD should staff the Directorate with more agency detailees and subject matter experts from within government along with private sector subject matter experts.
5. Congress should codify the position of the Federal CISO within OMB, to be dual-hatted as a direct report to the NCD.