2022

Answering the Cyber Oversight Call

Amy Gaudion
Penn State Dickinson Law, acg14@psu.edu

Recommended Citation

Amy Gaudion, *Answering the Cyber Oversight Call*, 54 *Loyola University Chicago Law Journal* 139 (2022).

Answering the Cyber Oversight Call

Amy C. Gaudion[*]

In the past few years, a revised cyber strategy, a spate of new cyber authorities, and revamped presidential directives have significantly expanded the cyber capabilities of the U.S. military. This expansion has coincided with a weakening and dispersion of traditional congressional oversight mechanisms, creating a separation of powers mismatch. This mismatch, and the necessarily stealthy features that characterize cyber operations, inhibit Congress's ability to gain a comprehensive understanding of the use and deployment of these cyber powers, while obscuring the use of such powers from the public as well. Put bluntly, the traditional congressional oversight mechanisms are not suited to the cyber oversight task. There is a need to find alternative players able to answer the cyber oversight call. To fill this gap, scholars have proposed various "surrogates" and "intermediaries" including foreign allies, local governments, technology companies, and other private sector actors. This Article urges a different approach by examining the consequential role of the Department of Defense Office of Inspector General (DoD OIG) from the cyber oversight perspective. Although often maligned and misunderstood as the bean counters of the federal government, inspectors general serve critical functions in our constitutional scheme, both as internal checks on abuses of executive power and as conduits of information to the legislative branch. The DoD OIG is uniquely positioned and equipped to fill the gaps in the cyber oversight framework, and to ensure that the political branches are working together to appropriately limit and guide the use of these vast new cyber powers. In sum, this Article explores the DoD OIG's distinctive ability to answer the cyber oversight call.

---

* Professor of Lawyering Skills and Associate Dean for Academic Affairs, Penn State Dickinson Law. Thanks to Rebecca Crootof, Asaf Lubin, Samantha Prince, Alan Rozenshtein, Scott Shackelford, and participants at the 2021 Cybersecurity Law & Policy Scholars Conference (hosted by the University of Minnesota Law School) and 2021 National Security Law Scholars workshop (hosted by the University of Florida Levin College of Law) for their helpful comments and feedback. I am grateful to Rebekah Bronkema, Jeremy Garcia, and Maria Germanetti for their terrific research assistance.

INTRODUCTION

In March of 2018, then Lieutenant General Paul Nakasone testified before the Senate Armed Services Committee.[1] At the time, he was the head of U.S. Army Cyber Command, and a few months later he would be promoted to Commander of U.S. Cyber Command.[2] During that March 2018 hearing, senators peppered Nakasone with questions about how the U.S. should respond to nations that infiltrated government networks, stole data from contractors, or tried to influence elections.[3] Senator Dan Sullivan commented that the U.S. seemed to be the "cyber punching bag of the world."[4] In response, Nakasone agreed, stating that adversaries do not think much will happen to them if they conduct computer-based attacks against the U.S. "They don't fear us," he told senators, "[i]t is not good."[5]

That characterization of the U.S. military's cyber capabilities, as feeble and lacking bite, was about to change radically. In the past four years, a revised cyber strategy, a spate of new cyber authorities, and revamped presidential policy directives have significantly expanded the cyber capabilities of the U.S. military, as exercised most frequently by U.S. Cyber Command. Indeed, by May of 2019, only a year after the hearing, it was reported that U.S. Cyber Command had conducted "more cyberspace operations in the last few months than in the

1. Lolita Baldor, *Army Officer: China, Russia Don't Fear US Cyber Retaliation*, AP NEWS (Mar. 1, 2018), https://apnews.com/article/ae43a2aa63e2430ea67d42bae868ea8d [https://perma.cc/S8PJ-7CWA]. *See also Nominations of Paul Nakasone, Brent Park, and Anne Marie White: Hearing Before the S. Comm. on Armed Services*, 116th Cong. (2018).

2. U.S. Cyber Command, Gen. Paul M. Nakasone, https://www.cybercom.mil/About/Leadership/Bio-Display/Article/1512978/commander-uscybercom [https://perma.cc/K96H-E72L]. In addition to serving as Commander of U.S. Cyber Command, General Nakasone serves as Director of the National Security Agency and Chief of Central Security Services. *Id*.

3. Baldor, *supra* note 1.

4. *Id.*

5. *Id.*

previous ten years."[6]

The revamped approach has been applauded by many commentators for endorsing a more aggressive cyber posture and achieving an appropriate recalibration of the U.S. military's cyber capabilities to match the cyber threat.[7] Other commentators, however, have expressed

---

6. Mark Pomerleau, *New Authorities Mean Lots of New Missions at Cyber Command*, FIFTH DOMAIN (May 8, 2019), https://www.fifthdomain.com/dod/cybercom/2019/05/08/new-authorities-mean-lots-of-new-missions-at-cyber-command/ [https://perma.cc/SSN6-6RDX].

7. *See, e.g.,* Zach Dorfman et al., *Exclusive: Secret Trump Order Gives CIA More Powers to Launch Cyberattacks*, YAHOONEWS (July 15, 2020), https://www.yahoo.com/video/secret-trump-order-gives-cia-more-powers-to-launch-cyberattacks-090015219.html [https://perma.cc/SU3V-R9PQ] ("Some CIA officials greeted the new finding as a needed reform that allows the agency to act more nimbly. 'People were doing backflips in the hallways [when it was signed],' said another former U.S. official."); Eric Geller, *Trump Scraps Obama Rules on Cyberattacks, Giving Military Freer Hand*, POLITICO (Aug. 16, 2018), https://www.politico.com/story/2018/08/16/trump-cybersecurity-cyberattack-hacking-military-742095 [https://perma.cc/PWU3-8P6L] (quoting administration official who lauded the revamped presidential directive for "giving the military freer rein to deploy its advanced hacking tools without pushback from the State Department and the intelligence community"); Herb Lin, *President Biden's Policy Changes for Offensive Cyber Operations*, LAWFARE (May 17, 2022), https://www.lawfareblog.com/president-bidens-policy-changes-offensive-cyber-operations [https://perma.cc/9L5H-UGF9] ("NSPM-13 enabled faster, more agile decision-making by allowing delegations of authority and enabling the delegate (the party to whom authority was delegated) to make coordination and approval decisions that would otherwise be made by the National Security Council."); Ellen Nakashima, *White House Authorizes 'Offensive Cyber Operations' to Deter Foreign Adversaries*, WASH. POST (Sept. 20, 2018, 7:18 PM), https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html [https://perma.cc/2VW2-UWSR] ("Our hands are not tied as they were in the Obama administration," said national security adviser John Bolton when describing new cyber strategy); Hon. Paul C. Ney, Jr., DoD Gen. Couns. Remarks at U.S. Cyber Command Legal Conf. (Mar. 2, 2020), https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/ [https://perma.cc/48T3-M7Q7] (commending the new approach for responding to the "complexity and dynamism of the [cyber] domain and the threat environment, the need for persistent engagement outside U.S. networks, and the critical advantage that cyber operations provide our Armed Forces" and for recognizing the need for DoD to "develop, review, and approve military cyber operations at so-called 'warp-speed'"); Dustin Volz, *Trump, Seeking to Relax Roles on U.S. Cyberattacks, Reverses Obama Directive*, WALL ST. J. (Aug. 15, 2018) https://www.wsj.com/articles/trump-seeking-to-relax-rules-on-u-s-cyberattacks-reverses-obama-directive-1534378721 [https://perma.cc/D2AA-7ZHR] ("The change was described as an 'offensive step forward' by an administration official briefed on the decision, one intended to help support military operations, deter foreign election influence and thwart intellectual property theft by meeting such threats with more forceful responses."). For additional descriptions of the revamped approach to the military's use of cyber capabilities, *see generally* Chris Bing, *Command and Control: A Fight for the Future of Government Hacking*, CYBERSCOOP (Apr. 11, 2018), https://www.cyberscoop.com/us-cyber-command-nsa-government-hacking-operations-fight/ [https://perma.cc/N5UQ-HTBA]; Erica D. Borghard & Shawn W. Lonergan, *What Do the Trump Administration's Changes to PPD-20 Mean for U.S. Offensive Cyber Operations?*, CFR (Sept. 10, 2018), https://www.cfr.org/blog/what-do-trump-administrations-changes-ppd-20-mean-

concerns about the recent expansion of the U.S. military's cyber authorities, and advocated for more robust oversight to ensure the appropriate use of such capabilities, considering their potential for unintended escalation and catastrophic effects as well as harm to third-party entities, damage to diplomatic relationships, and the development of reciprocal state actions at odds with the goal of creating international norms in cyberspace.[8] These concerns are exacerbated by the "stealthy features" that characterize cyber operations and the weakening of congressional oversight mechanisms, leading scholars to ask whether the cyber operations occupy a legal space distinct from other military operations, such that they upset the traditional separation of powers constitutional scheme.[9]

---

us-offensive-cyber-operations [https://perma.cc/PM8X-4JL4]; Robert Chesney, *The Domestic Legal Framework for US Military Cyber Operations*, HOOVER INST. WORKING GRP. ON NAT'L SEC. TECH. & L., Aegis Series Paper No. 2003 (July 29, 2020) [hereinafter Chesney, *Domestic Legal Framework*] https://www.hoover.org/sites/default/files/chesney_webreadypdf.pdf [https://perma.cc/K27P-58MR].

8. *See, e.g.,* Patrick Barry**,** *The Trump Administration Just Threw Out America's Rules for Cyberweapons*, FOREIGN POLICY (Aug. 21, 2018), https://foreignpolicy.com/2018/08/21/the-trump-administration-just-threw-out-americas-rules-for-cyberweapons [https://perma.cc/N7YY-4RJZ] ("[T]he Trump administration has taken the United States' purported rules for using cyberweapons and thrown them out the window."); Borghard & Lonergan, *supra* note 7 ("The news about loosening some of the restrictions on Cyber Command has been met with concern in some cyber policy circles, on the grounds that making the approvals process less rigorous creates undue risks of escalation and threatens to prioritize military over intelligence requirements."); Benjamin Jensen & J.D. Work, *Cyber Civil-Military Relations: Balancing Interests on the Digital Frontier*, WAR ON THE ROCKS (Sept. 4, 2018), https://warontherocks.com/2018/09/cyber-civil-military-relations-balancing-interests-on-the-digital-frontier/ [https://perma.cc/W2PJ-92ET] (describing concerns that empowering "Cyber Command to conduct short-notice attacks without White House approval or interagency coordination" will work a dramatic shift in civil-military relations leading to "a professional military cyber force capable of autonomously protecting society absent constant civilian oversight."); *see also generally* Rebecca Crootof, *Autonomous Weapons and the Limits of Analogy*, 9 HARV. NAT'L SEC. J. 51, 82-83 (2018) (describing challenges of applying existing legal frameworks to emerging weapon technologies, noting that "[w]hile analogical reasoning allows 'most law-of-war rules [to] apply most of the time to most new technologies,' in some situations there is no way to credibly stretch existing rules to answer novel legal questions"); Ashley Deeks, *Will Cyber Autonomy Undercut Democratic Accountability?*, 96 INT'L L. STUD. 464, 465–66 (2020) [hereinafter Deeks, *Cyber Autonomy*] (describing how cyber operations could alter existing relationships between the legislative and executive branches because they "are harder to detect publicly and do not require the type of robust legislative support that large scale conflicts do"); Elad D. Gil, *Cyber Checks and Balances*, 54 CORNELL INT'L L.J. (forthcoming 2022) (manuscript at 140–54) (available on SSRN) (explaining that "exogenous forces and actors," beyond the judicial and legislative branches, are needed to constrain government actions in cyberspace).

9. Matthew C. Waxman, *Cyberattacks and the Constitution*, HOOVER INST. WORKING GRP. ON NAT'L SEC., TECH., & L., Aegis Series Paper No. 2007, 11 (Nov. 10, 2020) [hereinafter Waxman, *Cyberattacks and the Constitution*] https://www.hoover.org/sites/default/files/research/docs/waxman_webready.pdf

This Article explores the resulting separation of powers mismatch: expanding military cyber capabilities and shrinking congressional oversight instruments. Its thesis is that the mismatch inhibits Congress's ability to gain a comprehensive understanding of the use and deployment of these evolving cyber powers, while obscuring the use of such powers from the public as well. Put more bluntly, the traditional congressional oversight mechanisms are not suited to the cyber oversight task. As such, there is a need to identify alternative players to take on the oversight task usually assigned to Congress. To fill this void, scholars have proposed various "surrogates" and "intermediaries" including foreign allies, local governments, technology companies, as well as other private sector actors.[10] This Article urges a different approach, examining the consequential role of the Department of Defense Office of Inspector General (DoD OIG)[11] from the cyber oversight perspective. Although often maligned and misunderstood as the bean counters of federal government, the DoD OIG is uniquely positioned and distinctively equipped to fill the gaps in the cyber oversight framework and to ensure that the political branches are working together to appropriately limit and guide the use of these vast new cyber powers.

Part I describes the recent expansion of the U.S. military's cyber capabilities, examining the adoption of a more aggressive cyber strategy, the passage of new cyber authorities in addition to the expansion of existing authorities, and the revamping of presidential policy directives to reflect the more aggressive cyber posture. It then reviews the evolving congressional reporting structure designed to oversee the use and deployment of these new cyber authorities. While noting the need for flexibility and deference given the cyber domain's distinctive characteristics, this Part explores gaps in the current reporting structure as well as larger oversight challenges relating to military cyber operations. These include: reporting requirements that are narrow and

---

[https://perma.cc/NQ3Z-X93B] (questioning whether cyber operations form a "new constitutional category altogether, for which the respective roles of Congress and the president are not yet established").

10. *See* Ashley Deeks, *Secrecy Surrogates*, 106 VA. L. REV. 1395, 1395–96 (2020) (identifying technology companies, local governments, and foreign allies as "secrecy surrogates" with important advantages over traditional oversight mechanisms) [hereinafter Deeks, *Secrecy Surrogates*]; Gil, *supra* note 8, at 105 (explaining how "exogenous forces and actors" can serve a checking function); Alan Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 122–49 (2018) (describing potential contributions of technology companies, serving as "surveillance intermediaries," to the oversight function).

11. This Article follows the Department of Defense's labeling scheme, using the term "Department of Defense Office of Inspector General" or "DoD OIG" when referring to the entity or office, and "inspector general" or "IG" when referring to the position generally or the head of a particular office.

underinclusive, covering only a limited set of cyber operations; lack of clarity on legal interpretations and definitions; lack of information about operational partners, collateral effects, and metrics of success for cyber operations; lack of a public accountability check; a disjointed and fractured congressional committee structure for oversight of the U.S. government's cyber-related activities, the lack of technological savvy, or cyber literacy, within the congressional committees charged with oversight; and the lack of substantive prohibitive authorities governing military cyber operations. These gaps and challenges are further aggravated by the "stealthy features"[12] that characterize military cyber operations, which hinder the usual checks of public debate and congressional approval. This Part finds that the fractured nature of the congressional oversight framework is an inappropriate fit for these new cyber capabilities, creating a separation of powers mismatch. This Part wraps up by considering alternative players, both inside and outside the executive branch, able to answer the cyber oversight call.

Part II offers the DoD OIG as a corrective for the separation of powers mismatch and explains why this player is particularly well-suited to answer the cyber oversight call. This Part provides a history of the IG position, examining its legislative origins and its distinctive attributes and statutory mandates. This Part explores the role of the IG in the constitutional scheme, both as an internal check on abuses of executive power within the administrative state and as a conduit of the information necessary to the congressional oversight task. It explores the IG's congressional reporting relationship as well as the powerful investigatory and audit tools it wields. It then focuses on the distinctive features that characterize the DoD OIG, describing the office's organizational structure, authorities, and the special statutory provisions governing its work. It catalogs the distinctive attributes that place the IG in the "presidential synopticon" of executive branch watchers.[13] These include: a special perch within the Department of Defense and a powerful investigatory toolkit; the ability to balance the need for secrecy with

12. *See* Jack Goldsmith & Matthew Waxman, *The Legal Legacy of Light-Footprint Warfare*, 39 WASH. Q. 7, 18 (2016) (describing how light footprint warfare, including cyber tools, may be a "bug for U.S. democracy, since the stealthy features mean that public debate and political checks—which reduce error as well as excess, and promote legitimacy—function ineffectively").

13. *See* JACK GOLDSMITH, POWER AND CONSTRAINT: THE ACCOUNTABLE PRESIDENCY AFTER 9/11 207 (2012). Goldsmith uses the term "presidential synopticon"—in the context of the counterterrorism policies and programs developed in the wake of the September 11, 2001, attacks—to describe a group of watchers in positions where they are able to check executive branch power and hold executive branch actors accountable. According to Goldsmith, this group is comprised of courts, members of Congress and their staffs, human rights activists, journalists, lawyers and other watchers and checkers both inside and outside the executive branch. *Id*.

illumination of wrongdoing; a growing role as independent advisor and policy evaluator within the Defense Department; and the power to guide and influence congressional cyber oversight efforts. To illustrate these attributes, this Part compiles recent examples of the DoD OIG engaged in oversight activities relating to military cyber operations and capabilities. This Part concludes by considering potential limits on the DoD OIG's oversight role.

Part III, while recognizing the need for additional study, offers preliminary recommendations for strengthening the DoD OIG's cyber oversight toolkit and role as a member of the presidential synopticon. These include: amendments to the Federal Vacancies Reform Act and Inspector General Act to incentivize or require IG nominations within a certain date of a new administration; revisions to the removal provisions governing IGs, particularly in intelligence and national security agencies; and revisions to the secretary of defense's prohibition authorities. In addition, reforms to the DoD OIG should complement other reform efforts designed to improve the federal government's defensive cybersecurity initiatives,[14] including congressional committee reform, cyber literacy efforts within the legislative and executive branches.

This Article's aim is to bring attention to the gaps and challenges in the current congressional oversight framework for military cyber operations and capabilities and to highlight the DoD OIG's distinctive contributions to the cyber oversight task. As officials contemplate whether cyber operations fundamentally alter the separation of powers dynamic, they should acknowledge the contributions of the DoD OIG and its efforts to effectively shepherd the use of these new cyber powers.

I. A SEPARATION OF POWERS MISMATCH: GROWING CYBER POWERS AND INADEQUATE CONGRESSIONAL OVERSIGHT

In 2018, then Lieutenant General Paul Nakasone commented that the U.S. military's cyber operations lacked bite and that our adversaries

14. It is beyond the scope of this Article to examine the larger structural challenges stemming from the dispersion of cyber authorities and capabilities across the federal agencies responsible for identifying and assessing cyber threats and defending government networks and related private-sector infrastructure. For a discussion of the challenges in the defensive and organizational space, *see generally* Amy C. Gaudion, *Recognizing the Role of Inspectors General in the U.S. Government's Cybersecurity Restructuring Task*, 9 BELMONT L. REV. 180 (2021) [hereinafter Gaudion, *Cybersecurity Restructuring Task*]; Carrie Cordero & David Thaw, *Rebooting Congressional Cybersecurity Oversight*, CTR. NEW AM. SEC. (Jan. 30, 2020) [hereinafter Cordero & Thaw, *Rebooting Congressional Cybersecurity* Oversight] https://www.cnas.org/publications/reports/rebooting-congressional-cybersecurity-oversight [https://perma.cc/6NBS-PT7C]; U.S. CYBERSPACE SOLARIUM COMM'N, FINAL REPORT (2020) at 35–37 [hereinafter CSC REPORT 2020].

"don't fear us."[15] In the following years, a spate of new congressional authorizations and executive branch strategy and policy guidance significantly expanded the cyber capabilities of the Department of Defense, as exercised most frequently by U.S. Cyber Command. By May of 2019, it was reported that U.S. Cyber Command had deployed the new authorities "to conduct more cyberspace operations in the last few months than in the previous 10 years." [16] This Part describes the rapid expansion of the U.S. government's cyber capabilities since 2018, examining the adoption of a more aggressive cyber strategy, the passage of new cyber authorities in addition to the expansion of existing authorities, and the revamping of presidential policy directives to reflect the more aggressive cyber posture. It then reviews the evolving congressional reporting structure designed to oversee the use and deployment of these new authorities and catalogs persistent gaps in the reporting framework as well as larger oversight challenges.

A. Expanding Cyber Authorities and Capabilities

Many (although not all) commentators applauded the recent expansion of cyber authorities and capabilities for endorsing a more aggressive cyber posture, eliminating a burdensome interagency process, and authorizing a wider lens for the conduct of military cyber operations. This Section provides an overview of the strategy documents framing the need for and deployment of expanded cyber capabilities, the new and expanded statutory authorities, and the presidential policy directives that loosened the approval process for military cyber operations. Appreciating the breadth of these new authorities is critical to understanding the stakes in the cyber oversight game.

1. An Aggressive Cyber Strategy

The origins of a more expansive and offensive approach are found in a slew of executive branch strategy and policy documents. In 2018, the executive branch published the Command Vision for U.S. Cyber Command, the Department of Defense Cyber Strategy, and the White House National Cyber Strategy.[17] These documents reflected a shift from

15. Baldor, *supra* note 1.
16. Pomerleau, *supra* note 6.
17. U.S. CYBER COMMAND, ACHIEVE AND MAINTAIN CYBERSPACE SUPERIORITY: COMMAND VISION FOR US CYBER COMMAND (2018) https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf [https://perma.cc/4EKY-VL55]; U.S. DEP'T OF DEF., CYBER STRATEGY (2018) [hereinafter DOD CYBER STRATEGY 2018], https://media

a deterrence-based strategy in cyberspace to a "defend forward" concept, and the embrace of a more aggressive posture in the cyber domain. The DoD Cyber Strategy provided: "We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[18]

In a March 2020 speech to the U.S. Cyber Command Legal Conference, Department of Defense General Counsel Paul Ney commended the strategy shift for responding to the "complexity and dynamism of the [cyber] domain and the threat environment, the need for persistent engagement outside U.S. networks, and the critical advantage that cyber operations provide our Armed Forces" and for recognizing the need for DoD to "develop, review, and approve military cyber operations at so-called 'warp-speed.'"[19] General Nakasone offered a similar description, describing the strategy as one that acknowledges "that defending the United States in cyberspace requires executing operations outside the U.S. military's networks and that the country cannot afford to wait for attacks to come its way."[20]

The revised cyber strategy coincided with a significant structural change within the military. In early May 2018, U.S. Cyber Command was elevated to the status of a unified combatant command.[21] This elevation is noteworthy for several reasons. First, it formally acknowledged cyber as a new war-fighting domain. Second, it provided dedicated funding and staffing streams for the command and its operations. Third, and possibly most significantly, the command's leader now reported directly to the secretary of defense, effectively giving "cyber issues a more powerful voice within the Department of Defense."[22]

.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF [https://perma.cc/7QVD-EVC3]; THE WHITE HOUSE, NATIONAL CYBER STRATEGY (2018), https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf [https://perma.cc/B667-TWXB]. For a comprehensive history on the origins of U.S. Cyber Command and the command's jurisdiction and organizational evolution, *see generally* FRED KAPLAN, DARK TERRITORY: THE SECRET HISTORY OF CYBER WAR (2017); Michael Warner, *US Cyber Command's First Decade*, HOOVER INST. WORKING GRP. ON NAT'L SEC. TECH. & L., Aegis Series Paper No. 2008 (Dec. 3, 2020); Rebecca Slayton, *What Is a Cyber Warrior? The Emergence of U.S. Military Cyber Expertise, 1967–2018*, 4 TEX. NAT. SEC. REV. 1 (2021).

18. DOD CYBER STRATEGY 2018, *supra* note 17, at 1.

19. Ney, *supra* note 7.

20. Paul M. Nakasone & Michael Sulmeyer, *How to Compete in Cyberspace: Cyber Command's New Approach*, FOREIGN AFFS. (Aug. 25, 2020), https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity [https://perma.cc/7JDP-YMWM].

21. Lisa Ferdinando, *Cybercom to Elevate to Combatant Command*, U.S. DEP'T OF DEF. (May 3, 2018), https://www.defense.gov/Explore/News/Article/Article/1511959/cybercom-to-elevate-to-combatant-command [https://perma.cc/QR36-3RWR].

22. Nakasone & Sulmeyer, *supra* note 20.

2. Burgeoning Statutory Authorities

Expansive congressional authorizations soon followed the newly articulated executive branch cyber strategy. The National Defense Authorization Act for Fiscal Year 2019 (NDAA for FY2019), passed in August 2018, expanded existing cyber authorities and included new authorizations reflecting the more aggressive cyber posture.[23] In addition to the substantive provisions, the legislation conducted some statutory housekeeping, possibly to further signal the strategy shift, and pulled most of Title 10's cyber provisions into one chapter, Chapter 19, now labeled "Cyber and Information Operations Matters."[24] This Section will provide a brief overview of the relevant provisions.

Section 1636 of the NDAA for FY2019 best exemplifies the expansive new cyber policy. That provision sought to address the problem General Nakasone had raised several months earlier in his hearing before the U.S. Senate, during which he warned that adversaries did not fear U.S. cyber capabilities.[25] The provision provides:

> It shall be the policy of the United States, with respect to matters pertaining to cyberspace, cybersecurity, and cyber warfare, that the United States should employ all instruments of national power, including the use of offensive cyber capabilities, to deter if possible, and respond to when necessary, all cyber attacks or other malicious cyber activities of foreign powers that target United States interests with the intent to— (1) cause casualties among United States persons or persons of United States allies; (2) significantly disrupt the normal functioning of United States democratic society or government (including attacks against critical infrastructure that could damage systems used to provide key services to the public or government); (3) threaten the command and control of the Armed Forces, the freedom of maneuver of the Armed Forces, or the industrial base or other infrastructure on which the United States Armed Forces rely to defend United States interests and commitments; or (4) achieve an effect, whether individually or in aggregate, comparable to an armed attack or imperil a vital interest of the United States.[26]

In addition, the provision lays out a broad range of response options for carrying out the policy described above, noting that "the United States shall plan, develop, and, when appropriate, demonstrate response options

---

23. John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 1636, 132 Stat. 2123–24 (2018) [hereinafter NDAA for FY2019].

24. For comprehensive summaries of the evolution in U.S. cyber strategy and its legal implications, *see generally* Chesney, *Domestic Legal Framework*, *supra* note 7; Waxman, *Cyberattacks and the Constitution*, *supra* note 9.

25. Baldor, *supra* note 1.

26. NDAA for FY2019, *supra* note 23, § 1636(a) (codified in Statutory Notes to 10 U.S.C. § 394).

to address the full range of potential cyber attacks on United States interests that could be conducted by potential adversaries of the United States."[27]

Section 394(a), initially enacted in 2015 and amended in 2018 by the NDAA for FY2019, provides general authorization for military cyber operations. Specifically, it authorizes the secretary of defense to prepare for, and when appropriately authorized, to conduct "military cyber activities or operations in cyberspace, including clandestine military activities or operations in cyberspace, to defend the United States and its allies, including in response to malicious cyber activity carried out against the United States or a United States person by a foreign power."[28] Section 394(b), which was added in 2018 as part of the NDAA for FY2019, affirmed an expansive reading of these authorities, providing that the U.S. military was authorized to conduct cyber activities or operations "short of hostilities" and to conduct such operations outside areas of active hostilities.[29]

In addition, and most notably, the NDAA for FY2019 included specific pre-authorization for U.S. military cyber and information operations in response to certain types of cyber actions by certain state actors.[30] Section 1642 authorizes the secretary of defense, acting through U.S. Cyber Command, to take "appropriate and proportional action in foreign cyberspace" against Russia, China, North Korea, or Iran if the National Command Authority[31] determines that one of those states "is conducting an active, systematic, and ongoing campaign of attacks against the Government or people of the United States in cyberspace."[32] According to reports, U.S. Cyber Command has not been hesitant in deploying its capabilities pursuant to this new authority.[33]

---

27. *Id.* at § 1636(b).
28. 10 U.S.C. § 394.
29. *Id.*
30. NDAA for FY2019, *supra* note 23, § 1642.
31. Given the expansive and potentially escalatory nature of these authorities, Congress seemed to attempt a different type of limit: requiring the decision be made by the National Command Authority, rather than merely the president or further down the chain of command. Robert Chesney, *The Law of Military Cyber Operations and the New NDAA*, LAWFARE (July 26, 2018), https://www.lawfareblog.com/law-military-cyber-operations-and-new-ndaa [https://perma.cc/4JGV-XPV2].
32. NDAA for FY2019, *supra* note 23, § 1642(a)(1) (codified in Statutory Notes to 10 U.S.C. § 394).
33. *See, e.g.,* Julian E. Barnes, *U.S. Begins First Cyberoperation against Russia Aimed at Protecting Elections*, N.Y. TIMES (Oct. 23, 2018), https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html [https://perma.cc/R94R-2L5H] (reporting "Cyber Command is targeting individual Russian operatives to try to deter them from spreading disinformation to interfere in elections....."); Ellen

The NDAA for FY2019 was also notable for answering the long-debated question of whether military cyber operations constituted covert actions subject to presidential finding and congressional reporting requirements. Section 1632 answered that question in the negative and clarified that such operations fall into the exception for "traditional military activities."[34] The implications of removing military cyber operations from the jurisdiction of the covert action statute are explored in greater detail in Section I.C.[35]

In sum, the statutory updates endorsed a more aggressive cyber posture, resolved the covert action question, and authorized a significantly expanded range for the conduct of military cyber operations, beyond Department of Defense Information Networks (DoDIN) and outside areas of active hostilities. The new and expanded authorities gave the U.S. military potent, but largely unchecked, cyber capabilities.

3. Revamped Presidential Directives

The more aggressive strategy and burgeoning statutory authorities were accompanied by a revamped presidential directive that significantly loosened internal executive branch oversight of military cyber operations. No discussion of cyber power would be complete without a reminder of the discretion exercised by the president, pursuant to Article II, with regard to use of force decisions. "The domestic legal authority for the DoD to conduct cyber operations is included in the broader authorities of the President and the secretary of defense to conduct military operations in defense of the nation," and assessed in accord with the "longstanding view of the Executive Branch that this authority may include the use of

---

Nakashima, *U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms*, WASH. POST (Feb. 26, 2019), https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html [https://perma.cc/3LKC-G7VM] (reporting on "the first offensive cyber-campaign against Russia designed to thwart attempts to interfere with a U.S. election "); Nakashima, *supra* note 7 (reporting on White House authorization for offensive cyber operations against U.S. adversaries); Mark Pomerleau, *Here's How Cyber Command Is Using 'Defend Forward'*, FIFTH DOMAIN (Nov. 12, 2019), https://www.fifthdomain.com/smr/cybercon/2019/11/12/heres-how-cyber-command-is-using-defend-forward [https://perma.cc/ADT7-FJHL] (describing "defend forward," or getting as close to adversaries as possible to see their plans and inform allies).

34. NDAA for FY2019, *supra* note 23, § 1632; *see also* Ney, *supra* note 7 ("Congress also has clarified that the President has authority to direct military operations in cyberspace to counter adversary cyber operations against our national interests and that such operations, whether they amount to the conduct of hostilities or not, and even when conducted in secret, are to be considered traditional military activities and not covert action, for purposes of the covert action statute."); Chesney, *Domestic Legal Framework*, *supra* note 7, at 10–12 (providing summary of covert action/traditional military activities debate and resolution).

35. *See* discussion *infra* Section I.C.

armed force when the anticipated nature, scope, and duration of the operations do not rise to the level of 'war' under the Constitution, triggering Congress's power to declare war."[36] Given the nature of cyber conflict and operations, most cyber operations will fall easily into the less than constitutional "war" category, and thus, the president may conduct them without first seeking congressional approval. To account for the lack of external approval, presidential administrations often adopt internal guidance, in the form of presidential policy directives or presidential memoranda, that serve a vetting function and provide a level of intra-branch constraint on the decision-making process.[37]

To this end, the Obama administration implemented Presidential Policy Directive 20 (PPD 20), a classified eighteen-page memorandum, that laid out an extensive interagency process for consultation and approval of high-level cyber operations and required presidential approval for cyber operations with effects outside U.S. government networks.[38] In mid-August 2018, anticipating the new statutory authorities and reflecting the strategic shift from deterrence to a more aggressive posture, the Trump administration adopted a new policy. Known as National Security Presidential Memorandum 13 (NSPM 13), the new policy was described as an "offensive step forward."[39] Although it remains classified, media reporting indicates that the revamped

36. Ney, *supra* note 7. Under the executive branch's articulation of the president's Article II powers, the president may use force absent congressional authorization when he finds it is in the national interest to do so, and when the force used does not rise to the level of constitutional war. *See* Memorandum from U.S. Dep't of Just., Off. of Legal Couns., on January 2020 Airstrike in Iraq against Qassem Soleimani, at 12–20 (Mar. 10, 2020), https://s3.documentcloud.org/documents/21012045/redacted-olc-memo-justification-of-soleimani-strike.pdf (examining president's use of force in 2020 military airstrike targeting Qassem Soleimani); Memorandum from U.S. Dep't of Just., Off. of Legal Couns., on April 2018 Airstrikes against Syrian Chemical-Weapons Facilities, at 9–22 (May 31, 2018), https://www.justice.gov/olc/opinion/file/1067551/download (examining president's use of force in 2018 military airstrikes targeting Syrian chemical weapons facilities); Memorandum from U.S. Dep't of Just., Off. of Legal Couns., on Authority to Use Military Force in Libya, at 27–31 (Apr. 1, 2011), https://www.justice.gov/sites/default/files/opinions/attachments/2021/02/18/2011-04-01-libya-deployment.pdf, (examining president's use of force in 2011 military airstrikes and other missions in Libya).

37. *See, e.g.,* PRESIDENTIAL DIRECTIVES & EXECUTIVE ORDERS, FEDERATION OF AMERICAN SCIENTISTS, https://fas.org/irp/offdocs/direct.htm [https://perma.cc/FD8N-29HQ] (providing access to all unclassified Presidential Policy Directives (PPDs) and National Security Presidential Memoranda (NSPMs), organized by administration); *see also* Ashley Deeks, *Secret Reason-Giving*, 129 YALE L.J. 612, 666–82 (2020) (describing virtues and problems with interbranch oversight of classified national security decisions); Rebecca Ingber, *Interpretation Catalysts and Executive Branch Legal Decision-making*, 38 YALE L.J. 359, 360 (2013) (identifying concept of "interpretation catalysts" and exploring their role as an intra-branch constraint on executive branch legal analysis).

38. Volz, *supra* note 7.

39. *Id.*

directive accomplished three significant changes.[40] First, it loosened the interagency approval process for military cyber operations, as well as those conducted by the CIA, and allowed the Pentagon to override objections from other agencies (most notably the State Department) without explanation or sometimes notice.[41] Second, it shortened the approval timeline to allow for more responsive actions.[42] Third, it removed the presidential approval requirement for cyber operations that fall below the use of force (or similar) thresholds and delegated that decision-making authority to others within the chain of command.[43] While questions remain as to the contours of that delegation, Department of Defense General Counsel Paul Ney Jr. described the delegation in March 2020 as one that "allows for the delegation of well-defined authorities to the Secretary of Defense to conduct time-sensitive military operations in cyberspace."[44] Former President Trump touted the executive branch policy change as an effective response to criticism that the prior approval process had been overly burdensome and left U.S. Cyber Command looking feeble.[45] The policy remains in effect at the time of the publication of this Article, although the Biden administration reportedly has made several procedural revisions to NSPM 13.[46]

---

40. For initial media reactions to the revamped presidential directive, *see generally* Borghard & Lonergan, *supra* note 7; Geller, *supra* note 7; Nakashima (Sept. 20, 2018), *supra* note 7; Volz, *supra* note 7.

41. *See* Dorfman et al., *supra* note 7 (describing how the order "open[ed] the way for the agency to launch offensive cyber operations with the aim of producing disruption—like cutting off electricity or compromising an intelligence operation by dumping documents online—as well as destruction "); Lin, *supra* note 7 ("NSPM-13 enabled faster, more agile decision-making by allowing delegations of authority and enabling the delegate—the party to whom authority was delegated—to make coordination and approval decisions that would otherwise be made by the National Security Council.").

42. Dorfman et al., *supra* note 7; Lin, *supra* note 7.

43. Lin, *supra* note 7; Geller, *supra* note 7.

44. Ney, *supra* note 7.

45. Despite the administration's boasting of its effectiveness, it was unwilling to share NSPM 13 with Congress. After numerous requests, Congress mandated its release to the relevant congressional committees, in Section 1650 of the NDAA for FY2020. In March 2020, the White House finally permitted congressional leaders to view the memorandum. Mark Pomerleau, *After Tug-of-War, White House Shows Cyber Memo to Congress*, C4ISRNET (Mar. 13, 2020), https://www.c4isrnet.com/congress/2020/03/13/after-tug-of-war-white-house-shows-cyber-memo-to-congress/ [https://perma.cc/GHB9-CQ77].

46. Early reporting on the Biden administration's policy reveals a focus on improving deconfliction efforts (particularly between Cyber Command and the Department of State and White House) and clarifying the delegation authorities. Lin, *supra* note 7; Ellen Nakashima, *The Biden Administration is Refining a Trump-Era Cyber Order*, WASH. POST (May 13, 2022, 7:16 AM), https://www.washingtonpost.com/politics/2022/05/13/biden-administration-is-refining-trump-era-cyber-order/ [https://perma.cc/XGT5-JGZW]; Suzanne Smalley, *Biden Administration Is Studying Where to Scale Back Trump-Era Cyber Authorities at DoD*, CYBERSCOOP (Mar. 31, 2022), https://www.cyberscoop.com/biden-trump-nspm-13-presidential-memo-cyber-command-white-house/ [https://perma.cc/S5EB-4DVC].

The new strategy, in concert with expanded congressional authorities and a revamped executive branch directive, was applauded by many commentators for endorsing a more aggressive cyber posture, resolving the covert action question, eliminating a burdensome interagency process, and authorizing a wider lens for the conduct of military cyber operations.[47] Other commentators, however, expressed concern that the expansion of the U.S. military's cyber authorities necessitated more robust internal and external oversight to prevent unintended escalation and increased hostilities, harm to third-party entities (both private and governmental), damage to diplomatic relationships, and the development of reciprocal state actions at odds with the goal of creating international norms.[48] Given the initiative-taking advantage held by the president in use of force scenarios generally and in cyber operation circumstances particularly, the need for post-event congressional reporting and access to information about military cyber operations appears all the more critical. Let's turn now to a review of the mechanisms of interbranch oversight, and an assessment of whether the current congressional reporting structure is up to the cyber oversight task.

B. The Current Framework for Congressional Oversight of Military Cyber Operations

In describing the need for congressional oversight of executive branch activities, Neal Katyal writes "without that checking function, presidential administration can become an engine of concentrated power."[49] The need in the national security context is especially compelling, as oversight requirements:

> oblige executive branch actors to provide certain information to Congress . . . if not also to the public. In theory, they serve the important purpose of making it more reasonable for Congress to conduct oversight of secret, highly sensitive activities and thus to be in a reasonable position to legislate or take other actions as needed. They also have the salutary effect of ensuring that the executive branch actors understand that someone from outside their immediate sphere will to some extent be aware of what they do (thus incentivizing greater care).[50]

Although Congress has included oversight requirements with the grant

47. *See supra* note 7.

48. *See supra* note 8.

49. Neal Kumar Katyal, *Internal Separation of Powers: Checking Today's Most Dangerous Branch from Within*, 115 YALE L.J. 2314, 2318 (2006) [hereinafter Katyal, *Internal Separation of Powers*]. *Cf.* Elena Kagan, *Presidential Administration*, 114 HARV. L. REV. 2245 (2001) (describing the foundation laid by the Reagan administration that "enhanced presidential control over administration" to "serve pro-regulatory objectives" in a controlling environment lacking significant congressional and judicial review).

50. Chesney, *Domestic Legal Framework*, *supra* note 7, at 13.

of the new cyber authorities described above, significant reporting gaps remain. This Section will provide an overview of the current notice and reporting mechanisms for military cyber operations, and then catalog the gaps and areas of concern in this evolving oversight framework.

At present, there are seven mechanisms with the potential to provide oversight of military cyber operations: (i) the War Powers Resolution, (ii) the covert action statute, (iii) quarterly briefings on military cyber operations, (iv) written notice of sensitive military cyber operations, (v) written notice of cyber weapons review, (vi) written notice of delegation of cyber authorities, and (vii) a written annual cyber action report. While there are additional mechanisms at play in the larger cyber oversight context,[51] this Article focuses on those mechanisms that directly govern military cyber operations.

War Powers Resolution.[52] Congress adopted the War Powers Resolution in 1973 in an attempt to rebalance the sharing of national security powers between the executive and legislative branches after the Vietnam War and in response to the revelation that multiple presidential administrations had failed to consult or share information with Congress.[53] To accomplish this rebalancing, the War Powers Resolution requires the executive branch to consult with and report to Congress regarding use of force operations that meet certain threshold requirements.[54] Arguably, the requirements of the War Powers

---

51. Cordero & Thaw, *Rebooting Congressional Cybersecurity Oversight*, *supra* note 14.

52. War Powers Resolution, 50 U.S.C. § 1541 et seq.

53. The War Powers Resolution was designed to reassert the oversight control that Congress had lost in the wake of Watergate, Vietnam, and other abuses involving the defense and intelligence domains of the executive branch. *See generally* War Powers Resolution, 50 U.S.C. § 1541(a) ("It is the purpose of this chapter to fulfill the intent of the framers of the Constitution of the United States and insure that the collective judgment of both the Congress and the President will apply to the introduction of United States Armed Forces into hostilities, or into situations where imminent involvement in hostilities is clearly indicated by the circumstances, and to the continued use of such forces in hostilities or in such situations."). These abuses were chronicled in three notable reports. *See generally* CHURCH COMMITTEE, SENATE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES (1976) [hereinafter Church Committee Report] https://www.senate.gov/about/powers-procedures/investigations/church-committee.htm [https://perma.cc/77BZ-83NC]; HOUSE SELECT COMMITTEE ON INTELLIGENCE, PIKE COMMITTEE REPORT (1976) [hereinafter Pike Committee Report] https://archive.org/details/PikeCommitteeReportFull [https://perma.cc/6BRV-CH5G]; REPORT TO THE PRESIDENT BY THE COMM'N ON CIA ACTIVITIES WITHIN THE UNITED STATES (1975) [hereinafter Rockefeller Commission Report] https://www.fordlibrarymuseum.gov/library/document/0005/1561495.pdf [https://perma.cc/68J5-28M6].

54. 50 U.S.C. § 1542(c) ("The President in every possible instance shall consult with Congress before introducing the United States Armed Forces into hostilities or into situations where imminent involvement in hostilities is clearly indicated by the circumstances, and after every such

Resolution will apply to cyber operations conducted by the U.S. Armed Forces that meet the requisite thresholds. However, by their nature, and in many cases their design and operational objectives, few, if any, military cyber operations will trigger the oversight provisions.[55]

Covert Action Reporting.[56] This requirement's objective is to ensure executive branch accountability and thoughtful intra-branch decision-making while also providing an opportunity for Congress to check presidential abuses of power in the intelligence field.[57] The statute requires a written presidential finding for actions that meet the "covert" definition, and subsequent reporting of that finding to Congress.[58] The statute includes exceptions for certain types of operations, and a long-standing question had been whether military cyber operations qualified for one of the exceptions, known as the traditional military activities

---

introduction shall consult regularly with the Congress until United States Armed Forces are no longer engaged in hostilities or have been removed from such situations."); 50 U.S.C. § 1543 (requiring written initial and periodic reports when the president commits U.S. Armed Forces into certain types of situations).

55. Cyber operations usually fall outside the statute's reporting requirements due to the narrow definition adopted by the executive branch for "hostilities." Eric Talbot Jensen, *Future War and War Powers Resolution*, 29 EMORY INT'L L. REV. 499, 541 (2015). While beyond this Article's scope, it is worth noting that the War Powers Resolution's reporting structure may be failing as a checking mechanism for traditional uses of military force as well. This is due to executive branch legal interpretations, seemingly acquiesced to by Congress, that focus on putting U.S. troops in danger, or boots on the ground, as the key factor in determining whether the "hostilities" trigger is met. *See Testimony by Legal Adviser Harold Hongju Koh U.S. Dep't of State on Libya and War Powers before the Senate Foreign Relations Committee*, 112th Cong. (2011) (describing four factors in determining "hostilities" for reporting purposes). Indeed, one of the advantages of cyber operations is avoidance of putting troops in harm's way. This advantage, of course, is not limited to the cyber domain, and also explains the transition to lighter footprint military operations. Several scholars have suggested that shifting the focus to the "risk of escalation" factor may be necessary to right-set the constitutional checks and balances scheme with regard to uses of force. *See* Chesney, *Domestic Legal Framework*, *supra* note 7, at 7 ("Disruptive technological changes with respect to the array of capabilities for delivering kinetic attacks without placing service members in range of hostile fire, not to mention the emergence of the cyber domain in its entirety, are producing an ever-larger set of circumstances in which the United States can exercise coercion without putting troops in harm's way. To be sure, this dynamic should not change the 'war' and 'hostilities' analyses if in both cases the ultimate determining factor is indeed whether service members' lives are in immediate danger. But if instead considerations of escalation risk drive these analyses, their logical foundations are eroding."); Waxman, *Cyberattacks and the Constitution*, *supra* note 9, at 4 ("It is questionable, though, whether the vast majority of actual and plausible cyberattacks should be understood as exercises of war powers at all. In other words, it may be a category error to analyze many cyberattacks as one would the application of hostile military force abroad, either as to the scope of the president's inherent constitutional authority or as to any constitutional requirement for congressional approval.").

56. 50 U.S.C. § 3093.

57. *Id.*

58. *Id.* at § 3093(c) (defining "covert action").

exception.[59] The NDAA for FY2019 resolved that question, providing that military cyber operations constitute "traditional military activities" in most instances.[60] Accordingly, military cyber operations are not subject to the requirements of the covert action statute.

If neither the War Powers Resolution nor the covert action statute provide a mechanism for reporting on military cyber operations, how will Congress exercise its oversight function in this evolving domain? Many were concerned about this very question, and to address it, Congress started to build the architecture for a parallel, although less robust, oversight framework for military cyber operations. The components of this developing framework are described below.

Oral Quarterly Briefings on Cyberspace Operations.[61] Section 484(a) of Title 10 was initially included in the NDAA for FY2013 and has been revised several times, including with passage of the NDAA for FY2021 in January 2021.[62] The section requires the secretary of defense to provide quarterly briefings to the Armed Services committees in the House and Senate on "all offensive and significant defensive military operations in cyberspace, including clandestine cyber activities, carried out by the Department of Defense during the immediately preceding quarter."[63] The briefings cover "any military activities or operations in cyberspace, including clandestine military activities or operations in cyberspace," and each briefing shall include, among other items, the following:

> (1) An update, set forth separately for each applicable geographic and functional command, that describes the operations carried out in the area of operations of that command or by that command;
>
> (2) An update, set forth for each applicable geographic and functional command, that describes defensive cyber operations executed to protect or defend forces, networks, and equipment in the area of operations of that command;
>
> (3) An update on relevant authorities and legal issues applicable to operations, including any presidential directives and delegations of authority received since the last quarterly update;

---

59. *Id. at* § 3093(e)(2) (excluding "traditional diplomatic or military activities or routine support to such activities" from definition of "covert action"). For a summary of this long-fought definitional battle, *see* Chesney, *Domestic Legal Framework*, *supra* note 7, at 8–13.

60. NDAA for FY2019, *supra* note 23, § 1632(c) ("A clandestine military activity or operation in cyberspace shall be considered a traditional military activity for the purposes of section 503(e)(2) of the National Security Act of 1947 (50 U.S.C. 3093(e)(2)).").

61. 10 U.S.C. § 484.

62. *Id.*

63. William M. (Mac) Thornberry Nat'l Def. Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 1703, 134 Stat. 4081 (2021) [hereinafter NDAA for FY2021] (replacing current provisions in 10 U.S.C. § 484(a) and (b)).

> (4) An overview of critical operational challenges posed by major adversaries or encountered in operational activities conducted since the last quarterly update [64]

Notably, the NDAA for FY2021 added a documentation requirement to accompany the oral briefing.[65]

Written Notice of Sensitive Military Cyber Operations.[66] Section 395(a) requires the secretary of defense to submit to the armed services committees, in both chambers, written notice "of any sensitive military cyber operation conducted under this title no later than 48 hours following such operation."[67] The statute defines a "sensitive military cyber operation" as an offensive or defensive cyber operation, carried out by U.S. Armed Forces, where its effects are intended to be felt in a geographic area outside those where the U.S. is involved in current or declared hostilities, and where the operation is "determined to" meet one of the following risk levels:

> (i) have a medium or high collateral effects estimate;
>
> (ii) have a medium or high intelligence gain or loss;
>
> (iii) have a medium or high probability of political retaliation, as determined by the political military assessment contained within the associated concept of operations;
>
> (iv) have a medium or high probability of detection when detection is not intended; or
>
> (v) result in medium or high collateral effects.[68]

Written Notice of Cyber Weapons Review.[69] A less noted but important provision requires written notice to the congressional defense

---

64. 10 U.S.C. § 484(b); *see also* Chesney, *Domestic Legal Framework*, *supra* note 7, at 14–16 (describing evolution of transparency and reporting rules for military cyber operations).

65. NDAA for FY2021, *supra* note 63, § 1703 (adding subsection (c) to 10 U.S.C. § 484, which requires "classified placement" and "unclassified memorandum").

66. 10 U.S.C. § 395. This notice provision for certain cyber operations conducted by the U.S. military was introduced in the Nat'l Def. Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, § 1631(a), 131 Stat. 1736 (2017) [hereinafter NDAA for FY2018], renumbered in the NDAA for FY2019, *supra* note 23, § 1631(c), and then modified further by the NDAAs for FY2020 and FY2021. *See* Nat'l Def. Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 1701, §115a, 133 Stat. 1794 (2019) [hereinafter NDAA for FY2020]; NDAA for FY2021, *supra* note 63, § 911, §125a(e)(2). *See also* Mark Pomerleau, *Which NDAA Cyber Provisions Have the Most Impact for DoD?*, C4ISRNET (Dec. 22, 2020), https://www.c4isrnet.com/cyber/2020/12/22/which-ndaa-cyber-provisions-have-the-most-impact-for-dod/ [https://perma.cc/6LAM-GBYK] (describing significant modifications of notification requirements for sensitive military cyber operations in NDAA for FY2021).

67. 10 U.S.C. § 395. For a discussion of the definitional questions that arise under this provision, *see infra* Section I.C.

68. 10 U.S.C. § 395(c)(1)(B). The risk thresholds, contained in Section 395(c)(1)(B), were added as part of the NDAA for FY2020. *See* NDAA for FY2020, *supra* note 66, § 1632. They were not included in the statute's first iteration. *See* NDAA for FY2018, *supra* note 66, § 1631(a). For a fuller discussion of this narrowing of the reporting requirements, *see infra* Section I.C.

69. 10 U.S.C. § 396.

committees on a quarterly basis of the results of reviews under DoD Directive 5000.1 for "a cyber capability that is intended for use as a weapon."[70] In addition, the provision requires written notice to the congressional defense committees within forty-eight hours following the "use as a weapon of any cyber capability that has been approved for such use under international law by a military department."[71] While the weapons reporting provisions seem to overlap with Section 395's provisions for "special military cyber operations" (SMCOs), a closer accounting shows that "a wide swath of 'cyberspace attack' operations might be undertaken without implicating the weapon/weapon-system categories it follows, therefore, that there might be an array of SMCOs that would not also trigger Section 396(a)(2)'s 48-hour notification rule."[72]

Written Notice of Delegation of Authorities for Military Operations in Cyberspace.[73] A similarly obscure, but possibly important, reporting requirement was included in Section 1642 of the NDAA for FY2020.[74] The section requires the secretary of defense to provide written notice to the armed services committees in both chambers if the president delegates authorities "for military operations in cyberspace that are otherwise held by the National Command Authority."[75] The secretary must provide written notice no later than fifteen days after the delegation, and the notice must include a description of the authorities delegated to the secretary.[76] This provision seems to be an effort to identify instances when the president delegates certain cyber operations to the secretary of defense or

---

70. *Id.* Directive 5000.01 was overhauled in 2020. *See* Press Release, *Defense Acquisition System Directive Goes into Effect*, U.S. DEP'T OF DEF. (Sept. 9, 2020), https://www.defense.gov/Newsroom/Releases/Release/Article/2340746/defense-acquisition-system-directive-goes-into-effect/ [https://perma.cc/6M7C-R63N] ("[D]efense Acquisition System develops a more lethal force based on U.S. technological innovation and a culture of performance that yields a decisive and sustained U.S. military advantage.").

71. 10 U.S.C. § 396(a)(2). Although added as part of the NDAA for FY2018, *see* NDAA for FY2018, *supra* note 66, § 1631(a) (2017), these provisions were later renumbered and are now codified at 10 U.S.C. § 396. Exceptions to this requirement include certain training exercises and covert actions. 10 U.S.C. § 396(c).

72. Robert Chesney, *Military Cyber Operations: The New NDAA Tailors the 48-Hour Notification Requirement*, LAWFARE (Dec. 18, 2019, 9:22 AM), https://www.lawfareblog.com/military-cyber-operations-new-ndaa-tailors-48-hour-notification-requirement [https://perma.cc/4RAH-LZ4N].

73. 10 U.S.C. § 394 note (Notification of Delegation of Authorities to the Secretary of Defense for Military Operations in Cyberspace).

74. NDAA for FY2020, *supra* note 66, § 1642 (codified in Statutory Notes to 10 U.S.C. § 394 (Notification of Delegation of Authorities to the Secretary of Defense for Military Operations in Cyberspace)).

75. *Id.* at § 1642(a)(1).

76. *Id.* at § 1642(a).

a subordinate delegate.[77]

Annual Military Cyberspace Operations Report.[78] An additional oversight mechanism requires the secretary of defense to provide a written report "summarizing all named military cyberspace operations conducted in the previous calendar year" to the congressional defense committees by March 1 of each year.[79] The reports include the following information, organized by adversarial country, for each "named" operation:

> (1) An identification of the objective and purpose.
>
> (2) Descriptions of the impacted countries, organizations, or forces, and nature of the impact.
>
> (3) A description of methodologies used for the cyber effects operation or cyber effects enabling operation.
>
> (4) An identification of the Cyber Mission Force teams, or other Department of Defense entity or units, that conducted such operation, and supporting teams, entities, or units.
>
> (5) An identification of the infrastructures on which such operations occurred.
>
> (6) A description of relevant legal, operational, and funding authorities.
>
> (7) Additional costs beyond baseline operations and maintenance and personnel costs directly associated with the conduct of the cyber effects operation or cyber effects enabling operation.
>
> (8) Any other matters the Secretary determines relevant.[80]

The secretary has the discretion to provide the reports at the classification level the secretary determines appropriate.[81] There is no public analog at present.

In sum, Congress has dedicated time and effort to building an oversight structure, focused on reporting and notice, for the expansion of the military's cyber capabilities. In building this structure, Congress sought to avoid a system so onerous that it returned to the problem the new

---

77. As the legislation wound its way through the committee process, the Trump administration issued a statement strongly objecting to this provision, arguing it would "interfere with the established process for military operations in cyberspace, unduly hinder cyber operations, and contravene the President's constitutional prerogative not to disclose privileged information, including national security information." ADAM SMITH, OFF. OF MGMT. AND BUDGET OFF. OF PRESIDENT, STATEMENT OF ADMINISTRATION POLICY TO HR 2500—NDAA FOR FY2020 (July 9, 2019), at 5.

78. NDAA for FY2020, *supra* note 66, § 1644 (codified in Statutory Notes to 10 U.S.C. § 394 (Annual Military Cyberspace Operations Report)). The legislative history provides little guidance on whether or how "named" military cyberspace operations differ from the cyber operations that require reporting under the other provisions of Section 484 or 395.

79. *Id.*

80. *Id.* at § 1644(a).

81. NDAA for FY2020, *supra* note 66, § 1644(b) (codified in Statutory Notes to 10 U.S.C. § 394 (Annual Military Cyberspace Operations Report Classification)).

authorities sought to remedy: "an operational space that is far too narrow to defend national interests."[82] Appreciating that many in the Pentagon feel that the existing reporting obligations are sufficient (possibly more than sufficient) to quell any separation of powers concerns about the executive branch's use of the newly granted cyber capabilities, it is nonetheless important to explore the gaps and challenges that remain. Indeed, it seems that despite the quantity of reporting and notice provisions, there may be a lack of substantive and useful information making its way from the Pentagon to the Capitol.

C. Reporting Gaps and Other Challenges in the Current Framework

The recent expansion of the U.S. military's cyber authorities and embrace of a more aggressive cyber posture, explored above, have fueled concerns about the vigor of existing congressional oversight mechanisms.[83] Relatedly, the "stealthy features" characteristic of military cyber operations hinder the usual checks of public debate and congressional approval, exacerbating concerns about the adequacy of the current mechanisms.[84] Despite Congress's efforts to put in place reporting and notice requirements specific to military cyber operations, significant concerns remain.[85] This section will catalog the gaps in the current reporting framework governing military cyber operations and

---

82. JOHN S. MCCAIN NAT'L DEF. AUTHORIZATION ACT FOR FISCAL YEAR 2019, H.R. REP. NO. 115-874, at 1049 (2018) (Conf. Rep.).

83. For commentary on the problems associated with the fractured and disaggregated approach to congressional reporting on cyber-related issues, s*ee* Cordero & Thaw, *supra* note 14 (exploring means of improving congressional oversight of cybersecurity challenged by the current cybersecurity policymaking legal framework). Concerns about the adequacy of congressional oversight in the cyber domain reflect similar and long-standing concerns about oversight of executive branch activity in other areas requiring secrecy and stealth. *See, e.g.*, Amy B. Zegart, *The Roots of Weak Congressional Intelligence Oversight*, HOOVER INST. TASK FORCE ON NAT'L SEC. & L. 6–11 (2011) (explaining challenges of congressional oversight in intelligence operations); Deeks, *Secrecy Surrogates*, *supra* note 10, at 1413–16 (2020) (explaining why congressional committees are "less than fully effective overseers" of intelligence and defense matters); Susan Landau & Asaf Lubin, *Examining the Anomalies, Explaining the Value: Should the USA FREEDOM Act's Metadata Program be Extended?*, 11 HARV. NAT. SEC. J. 308, 350–54 (2020) (describing limitations on Congress's oversight role in national security-related operations). Congress's inability to conduct sufficient oversight of the U.S. military's cyber operations may also reflect the military's organizational divide, between its operational and administrative components. As explored by Mark Nevitt, the two-military divide incentivizes congressional focus on the administrative military at the expense of operational military oversight, among other problems. Mark P. Nevitt, *The Operational and Administrative Militaries*, 53 GA. L. REV. 905, 911 (2019).

84. Goldsmith & Waxman, *supra* note 12, at 18 (noting that light footprint warfare, including through the use of cyber tools, may be a "bug for U.S. democracy, since the stealthy features mean that public debate and political checks—which reduce error as well as excess, and promote legitimacy—function ineffectively").

85. Deeks, *Cyber Autonomy*, *supra* note 8, at 493 (noting it is not yet clear how these initial efforts "are functioning and whether Congress is receiving the information that it believes it needs to provide adequate oversight").

identify the broader challenges that limit the vitality of external oversight efforts of such operations.

Gap: Underinclusive Requirements for Operations Designed for the Gray Zone. The current reporting requirements are narrow and underinclusive, covering only a limited set of military cyber operations. Much of the activity in the cyber domain occurs in a "gray zone" below the level of armed conflict and outside the commonly adopted definition of hostilities, the triggering points where Congress usually engages its constitutional role. As such, very few cyber operations (if any) will fall within the reporting requirements of the War Powers Resolution.[86] Likewise, military cyber operations are excluded from the reporting requirements of the covert action statute.[87] The notice and reporting provisions enacted in the past three years were intended to remedy these flaws by providing a "parallel transparency rule-architecture."[88] The gaps, however, persist. Few operations, often by military design, will meet the heightened risk thresholds that would require reporting under Section 395. It is worth noting that the first iteration of this reporting requirement did not include a risk threshold; it required reporting of both offensive and defensive operations when the operation was carried out by U.S. Armed Forces and when its effects were intended to be felt in a geographic area outside those where the U.S. was involved in current or declared hostilities.[89] The risk threshold provision, Section 395(c)(1)(B), was added as part of the NDAA for FY2020.[90] The NDAA for FY2021

---

86. *See supra* Section I.B., at 117 (discussing War Powers Resolution's reporting thresholds).

87. *See supra* Section I.B., at 118 (discussing covert action reporting requirements).

88. Chesney, *Domestic Legal Framework*, *supra* note 7, at 15 (describing Congress's efforts to anticipate objections by building "a parallel transparency-rule architecture at much the same time it was endeavoring to shield military cyber operations from the covert action and intelligence legal frameworks").

89. NDAA for FY2018, *supra* note 66, § 1631(c). As initially enacted, SMCOs were defined as follows:

> (1) In this section, the term 'sensitive military cyber operation' means an action described in paragraph (2) that—
>
> (A) is carried out by the armed forces of the United States; and
>
> (B) is intended to cause cyber effects outside a geographic location—
>
> (i) where the armed forces of the United States are involved in hostilities (as that term is used in section 1543 of title 50, United States Code); or
>
> (ii) with respect to which hostilities have been declared by the United States."
>
> (2) The actions described in this paragraph are the following:
>
> (A) An offensive cyber operation.
>
> (B) A defensive cyber operation outside the Department of Defense Information Networks to defeat an ongoing or imminent threat.

Id.

90. NDAA for FY2020, *supra* note 66, § 163; *see also* Chesney, *supra* note 72 (noting risk levels

revised the risk thresholds again, further narrowing the category of cyber operations subject to the written notice requirement.[91] Another limit is placed on the annual reports for "named" military cyber operations: the statute excludes "cyber-enabled military information support operations or military deception operations."[92] The underinclusive gap means that Congress will not receive information about most cyber operations, nor be able to assess their legality or efficacy, in a timely manner. Rather, this important information will not find its way to Congress until the next quarterly oral briefing is delivered or the annual written report is due, often too late to correct or respond to operations with possibly calamitous and far-reaching effects.

Gap: Lack of Legal Interpretations. A second gap in the current reporting framework is the lack of information about operating interpretations and definitions. What legal interpretations has the executive branch adopted in exercising these new cyber authorities? Is the Defense Department interpretating its authorities under 395(a) broadly while interpreting the reporting requirements of Section 484 and 395(d) narrowly? What activities other than election interference has the military found sufficient to justify action under Section 1642?[93] The Annual Military Cyberspace Operations Report requires a "description of relevant legal, operational, and funding authorities" for each operation in the report.[94] This is a promising development, however, it is operation specific and does not get to the need for department or command-wide legal interpretations of the various authorities and reporting thresholds. These concerns harken back to the revelations that the NSA's interpretation of the term "relevant" in Section 215 was not consistent with the authority Congress thought it granted to the NSA under that provision.[95]

Gap: Lack of Information on Operational Partners, Collateral Effects, and Metrics. A related gap includes the lack of useful information about operational partners, collateral effects, and metrics of success. Specifically, it is difficult to discern when and how U.S. Cyber Command

---

were developed to align with concerns related to the purpose of reporting and that revision "will tend to eliminate relatively unimportant, low-risk operations from the scope of the notification obligation").

91. NDAA for FY2021, *supra* note 63, § 1702.

92. NDAA for FY2020, *supra* note 66, § 1644(c).

93. Chesney, *supra* note 31 (noting that because current reporting requirements do not require reporting to public, "outsiders are not often going to have a good sense of what, if any, use 1642 gets").

94. NDAA for FY2020, *supra* note 66, § 1644.

95. *See generally* PRIV. AND C.L. OVERSIGHT BD., REPORT ON TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (2014); Landau & Lubin, *supra* note 83.

partners with other U.S. military components, U.S. civilian agencies, foreign governments, as well as private sector entities to conduct cyber operations. In many ways, military cyber operations are like all other military operations in their collaboration with non-military entities, however, programs like Project Indigo[96] and news stories about the Vulnerabilities Equities Process[97] raise questions about operational command and jurisdictional boundaries as well as budgetary concerns. Relatedly, the current reporting framework fails to include any level of detailed reporting on post-operation collateral effects or metrics of operational success.[98] Although recent congressional efforts added quantitative and qualitative metrics,[99] the reporting is limited to the number of operations conducted or their initial tactical effects. Missing from the reports are measures of the "defend forward" outcomes at the strategic, operational, and tactical levels.[100]

Gap: Lack of Public Accountability Check. A final, and summative, gap in the current framework is the lack of a public accountability check. While the statutory mandates for reporting exist, there remains the challenge of determining whether the required briefings are occurring and whether the required reports are being submitted.[101] Notably, the Senate

96. *See* Chris Bing, *Inside 'Project Indigo,' the Quiet Info-Sharing Program Between Banks and U.S. Cyber Command*, CYBERSCOOP (May 21, 2018), https://www.cyberscoop.com/project-indigo-fs-isac-cyber-command-information-sharing-dhs/ [https://perma.cc/2TTK-C744] (discussing the broad purpose of Project Indigo). A related gap may be in discerning when and how the Defense Department partners with private sector entities to counter or hunt for adverse activities, and, relatedly, an understanding of the role played by the NSA's Cybersecurity Directorate. As well-documented in the recent CSC Report, significant concerns exist regarding the extent that mission creep and wasteful duplication is occurring among the three federal agencies charged with ensuring the nation's cyber defenses and cyber offensive capabilities. CSC REPORT 2020, *supra* note 14, at 36.

97. *Vulnerabilities Equities Policy and Process for the U.S. Government*, WHITEHOUSE.GOV (Nov. 15, 2017), https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF [https://perma.cc/7HW3-563H]. Of particular concern is the use of purchased vulnerabilities for use in military cyber operations, which may fall outside the interagency vetting process established by the Vulnerabilities Equities Process. Rhys Dipshan, *The Federal Policy Loophole Supporting the Hacking-for-Hire Market*, SLATE (June 20, 2018, 9:30 AM), https://slate.com/technology/2018/06/the-federal-policy-loophole-supporting-the-hacking-for-hire-market.html [https://perma.cc/NPX9-4FVE]; Andi Wilson Thompson, *Assessing the Vulnerabilities Equities Process, Three Years after the VEP Charter*, LAWFARE (Jan. 13, 2021, 8:57 AM), https://www.lawfareblog.com/assessing-vulnerabilities-equities-process-three-years-after-vep-charter [https://perma.cc/7KJJ-7WRH].

98. Deeks, *Cyber Autonomy*, *supra* note 8, at 485–86; CSC REPORT 2020, *supra* note 14, at 117.

99. *See, e.g.*, NDAA for FY2020, *supra* note 66, § 1634 (detailing quarterly assessments of the readiness of cyber mission forces).

100. CSC REPORT 2020, *supra* note 14, at 117. For example, what are the "direct and indirect costs imposed on adversaries" and how have cyber operations impacted adversary behavior?

101. *See, e.g.*, Waxman, *Cyberattacks and the Constitution*, *supra* note 9, at 12 (noting that cyber

Armed Services Committee Report accompanying the NDAA for FY2021 expressed frustration with the Defense Department's lack of compliance with the oversight provisions, stating that the committee had been "consistently frustrated by the Department's unwillingness to keep the committee apprised of cyber operations conducted to gain access to adversary systems, including those conducted pursuant to standing military plans against military targets."[102] To date, the reports do not appear to be publicly available on any government website, and there has been no media reporting on whether the secretary of defense has provided written reports or notice pursuant to Section 394 (annual report, cyber weapons review, delegation of cyber authorities), Section 395 (sensitive military cyber operations), or Section 484 (quarterly oral briefings).[103] Admittedly, these matters are classified, and thus efforts to determine whether the requirement has been complied with, and whether compliance occurred in a timely manner, will be difficult to discern. Nonetheless, the lack of an accountability check or public confirmation is problematic. Congress, in the NDAA for FY2021, took a step toward

---

operations are "especially invisible compared to other methods of international conflict, so robust congressional oversight is arguably extra-important as a stand-in for public scrutiny").

102. COMM. ON ARMED SERV., NAT'L DEF. AUTHORIZATION ACT FOR FISCAL YEAR 2021, S. REP. NO. 116-236, at 337 (2020) (Conf. Rep.). The section labeled "Modification of requirements for quarterly Department of Defense cyber operations briefings for Congress (sec. 1614)" recommended updates to the requirements for the quarterly cyber operations briefings to Congress, specifically:

> The provision would require the Under Secretary of Defense for Policy, the Commander of United States Cyber Command, and the Chairman of the Joint Chiefs of Staff, or designees from each of their offices, to provide the quarterly briefings. The provision would also require the briefings to specifically cover recent presidential directives, delegations of authority, and operational challenges and would require the briefers to present certain documentation at the briefings.
>
> Current statute dictates that the quarterly cyber operations briefings "cover all offensive and significant defensive military operations in cyberspace carried out by the Department of Defense during the immediately preceding quarter." This provision would make no changes to this requirement. However, the committee has been consistently frustrated by the Department's unwillingness to keep the committee apprised of cyber operations conducted to gain access to adversary systems, including those conducted pursuant to standing military plans against military targets. The committee believes that it is critical that the committee is informed as to what targets are being developed, at what stage these operations stand, and what cyber effects are available to combatant commanders.
>
> Therefore, the committee expects the Department to fully follow the letter of the law in providing these briefings to the Congress by supplying the congressional defense committees details as to the operational activities of the Department's offensive forces even short of effects, including, as appropriate, the specific intent of and progress made in operations targeting adversary cyber and military actors.

Id.

103. My own initial efforts to confirm the occurrence of the briefings or submission of the reports have come up short. These efforts continue and will form the basis for future research on this topic.

mitigating this problem, by adding an unclassified memorandum to accompany the quarterly briefings.[104] It remains to be seen whether the unclassified written memo will provide a meaningful level of transparency.

Challenge: Disjointed Congressional Committee Structure. Coupled with the gaps described above is an organizational one: the disjointed and fractured congressional committee structure for oversight of the U.S. government's cyber-related activities. Carrie Cordero, a former government official, calls this the "Patchwork Mismatch."[105] There are no committees focused solely or entirely on cyber matters. Rather, oversight of cyber-related responsibilities and capabilities are divided among many committees and sub-committees. While committee overlap and shared jurisdiction provide certain advantages to the oversight scheme,[106] the current structure has moved well past the beneficial tipping point. The dispersion and disjointed nature of the committee structure is causing significantly more harm than good. Each committee views the cyber issue only through the narrow lens before it, and thus, Congress is unable to distinguish the cyber forest from the trees.[107] This fractured committee structure exacerbates the gaps in the cyber reporting framework and inhibits Congress's ability to gain a comprehensive understanding of the use and deployment of these new cyber capabilities.

Challenge: Congressional Lack of Technological Expertise. The organizational problems are intensified by a lack of technological savvy, or cyber literacy, within the congressional committees charged with oversight. The lack of basic understanding, much less technological sophistication, among members of Congress and their staffers is well

104. NDAA for FY2021, *supra* note 63, § 1703 (codified as amended in 10 U.S.C. § 484) (adding subsection (c) which requires "classified placement" and "unclassified memorandum").

105. Cordero & Thaw, *Rebooting Congressional Cybersecurity Oversight*, *supra* note 14; Carrie Cordero & David Thaw, *The Cyberspace Solarium Commission's Mandate to Fix Congressional Oversight*, LAWFARE (Mar. 18, 2020, 8:00 AM), https://www.lawfareblog.com/cyberspace-solarium-commissions-mandate-fix-congressional-oversight [https://perma.cc/3TGN-3XD6].

106. *See* Katyal, *Internal Separation of Powers*, *supra* note 49, at 2324 (describing the importance of bureaucratic and agency overlap).

107. *See* Cordero & Thaw, *Rebooting Congressional Cybersecurity Oversight*, *supra* note 14 ("[T]he lack of a coordinating function among these committees limits Congress's ability to obtain a comprehensive picture of the cybersecurity problem."); Gaudion, *Cybersecurity Restructuring Task*, *supra* note 14, at 190 (illustrating the dispersion challenge by summarizing cyber-related congressional hearings held across only a four-month period); Gil, *supra* note 8, at 104 (identifying significant gaps in current congressional oversight framework for use of cyber capabilities); CSC REPORT 2020, *supra* note 14, at 35 (stating that disjointed nature of current committee structure "prevents Congress from effectively providing strategic oversight of the executive branch's cybersecurity efforts or exerting its traditional oversight authority for executive action and policy in cyberspace").

documented.[108] Research into the skill sets and expertise of the relevant committee staffs demonstrates "a serious dearth of technical expertise among the staffers" and reveals staffers who are "underwater when it comes to poking into the nitty gritty of cyber warfare."[109] This challenge manifests in various ways, ranging from ridiculous questions at committee hearings to adverse impacts on the substantive content of legislation. In addition, and relevant to this Article's proposition, the lack of understanding significantly impairs the ability of congressional committees to engage in adequate oversight of technological matters, including cyber operations, thus adding another layer to an already gnarly problem.

Challenge: Lack of Substantive Prohibitive Authorities. In addition to the preceding gaps and challenges lies a larger separation of powers problem: the lack of substantive *prohibitive* authorities governing military cyber operations. Congress enthusiastically engaged in the authorizing and reporting tasks; however, it has failed to place any meaningful constraints on the military's use of its cyber capabilities. In essence, Congress gave the president a green light for the deployment of cyber weapons, beyond a president's Article II powers, but the guard rails are not yet up on this cyber dirt road. Currently, there are no cyber-specific U.S. laws that prohibit certain actions or outcomes.[110] As the

---

108. *See, e.g.*, Deeks, *Cyber Autonomy*, *supra* note 8, at 486–88 (noting lack of technical prowess or understanding among members and staff); Zach Graves & Daniel Schuman, *The Decline of Congressional Expertise Explained in Ten Charts*, TECHDIRT (Oct. 18, 2018, 11:55 AM), https://www.techdirt.com/articles/20181018/10204640869/decline-congressional-expertise-explained-10-charts.shtml [https://perma.cc/2L8N-Q3FB] ("When Mark Zuckerberg was called to testify earlier this year, the world was shocked by Congress's evident lack of basic technological literacy."); Emily Stewart, *Lawmakers Seem Confused about What Facebook Does—and How to Fix it*, VOX (Apr. 10, 2018, 7:50 PM), https://www.vox.com/policy-and-politics/2018/4/10/17222062/mark-zuckerberg-testimony-graham-facebook-regulations [https://perma.cc/7ZMA-DF7R] ("Many of the lawmakers' questions suggested they're still trying to understand the basics of how the [Facebook] platform works."); Zegart, *Roots of Weak Congressional Oversight*, *supra* note 83, at 1 ("[M]any of Congress's oversight troubles lie with Congress and two institutional deficiencies in particular: limited expertise and weak budgetary power over the Intelligence Community."). The larger societal challenge stemming from the loss of faith in expertise is explored in TOM NICHOLS, THE DEATH OF EXPERTISE: THE CAMPAIGN AGAINST ESTABLISHED KNOWLEDGE AND WHY IT MATTERS (Oxford Univ. Press, 1st ed. 2017).

109. Jenna McLaughlin, *Congress May Lack Technical Expertise to Properly Investigate Russian Hacking*, THE INTERCEPT (Feb. 28, 2017, 9:38 AM) https://theintercept.com/2017/02/28/congress-may-lack-technical-expertise-to-properly-investigate-russian-hacking/ [https://perma.cc/FF4X-3N38] (concluding that committee staff tend to be "lawyers, policy wonks, and budget experts" not experts in "coding, information security, and attribution"); Deeks, *Secrecy Surrogates*, *supra* note 10, at 1415 ("[I]t is far from clear that members or staffers have the technological sophistication necessary to provide deep oversight over programs involving complicated electronic surveillance, cyber, or artificial intelligence technologies.").

110. Chesney, *Domestic Legal Framework*, *supra* note 7, at 16 ("There is no statute or executive

U.S. military exercises these expanded cyber powers, a key question will be whether Congress should impose constraints or cabin the use of cyber capabilities. If Congress is unable to obtain the information it needs on the use and deployment of cyber capabilities, it will be difficult for Congress to assess if the lack of prohibitive guidance should be remedied.

Challenge: The "Stealthy Features" That Characterize Cyber Operations. The reporting gaps and oversight challenges outlined above are further aggravated by the "stealthy features"[111] that characterize military cyber operations. These features hinder the usual checks of public debate and congressional approval, raising significant concerns about the vitality and adequacy of the current congressional oversight framework. In most instances, for cyber operations to be effective, the need for secrecy and concealment is high. Relatedly, operational effectiveness requires quick decision-making and the avoidance of interagency friction with its slowing effects.[112] As a result, the president, and the executive branch more broadly, exercise great discretion when engaging in cyber operations. Despite the need for secrecy and responsiveness, there is also a need to deconflict military cyber operations and intelligence operations occurring in the same networks, requiring some level of interagency exchange.[113] Finally, even the most narrowly designed cyber operation has the potential to cause catastrophic unintended effects and to lead to a violent response, armed retaliation, or escalation.[114]

This tendency toward stealth also is reflected in the manner in which many of the authorizing statutes and reporting requirements are codified: rather than be included in the text of the U.S. Code provision, many of the authorities and oversight mechanisms are listed in the statutory notes

---

order, for example, that flat out forbids the implanting of malware in industrial control systems associated with the electrical grid in a foreign country. Nor have there been any significant proposals for statutes of that kind.").

111. Goldsmith & Waxman, *supra* note 12, at 18.

112. Crootof, *supra* note 8, at 81 (describing how speed of autonomous cyber countermeasures leaves little room for oversight or debate); AMY B. ZEGART, SPIES, LIES, AND ALGORITHMS: THE HISTORY AND FUTURE OF AMERICAN INTELLIGENCE 259 (Bridget Flannery-McCoy et al. eds., 2022) ("The longer attribution takes, the weaker any threat of punishment becomes—and the more deterrence unravels. Fast attribution matters, and it is far more elusive in cyberspace than anywhere else.").

113. Chesney, *Domestic Legal Framework*, *supra* note 7, at 8; DEP'T OF DEF., JOINT PUBLICATION 3-12, CYBERSPACE OPERATIONS (2018), at IV-18 (explaining the importance of integrating cyberspace operations with other operations of U.S. government entities, and explaining "deconfliction is the act of coordinating the employment of cyberspace capabilities to create effects with applicable DOD, interagency, and multinational partners to ensure operations do not interfere, inhibit, or otherwise conflict with each other").

114. *But see* Waxman, *Cyberattacks and the Constitution*, *supra* note 9, at 5–6 (suggesting cyber operations may be less likely to lead to violent responses or escalation).

to the text. For example, the Statutory Notes to 10 U.S.C. 394 include authorizing and reporting provisions from several of the recent national defense authorization acts, most notably: "Framework for Cyber Hunt Forward Operations," "Tailored Cyberspace Operations Organizations," "Notification of Delegation of Authorities to the Secretary of Defense for Military Operations in Cyberspace," "Annual Military Cyberspace Operations Report," "Policy of the United States on Cyberspace, Cybersecurity, Cyber Warfare, and Cyber Deterrence," and "Active Defense Against the Russian Federation, People's Republic of China, Democratic People's Republic of Korea, and Islamic Republic of Iran Attacks in Cyberspace."[115] Thus, only someone who possesses familiarity with statutory structure and the legislative codification process would know to look to the statutory notes for guidance.[116] I am not suggesting this was intentional—indeed, it may have been a decision made for administrative convenience. Nonetheless, it feeds the narrative that military cyber operations operate in the shadows, with little to no external oversight.

Despite Congress's efforts to establish a notice and reporting framework for military cyber operations, the substance and scope of the current requirements are quite limited. The framework is far from complete and includes a number of gaps. These gaps and challenges require acknowledgment that many, if not most, military cyber operations will *not* be reported to congressional committees and are even less likely to come to the attention of the public. Further, the operations that are presented to congressional committees will be presented to them *after* the event, in a post hoc review manner. Moreover, the challenges associated with a disjointed congressional committee structure, lack of technological expertise among members of Congress and their staffs, and the "stealthy" nature of cyber operations call for a different approach to oversight. While affirming the need for oversight of military cyber operations, we must acknowledge that *congressional* oversight may not be the optimal mechanism to achieve this constitutional check. Because cyber operations occupy a legal and policy space distinct from other military operations, they challenge the traditional separation of powers constitutional scheme and the adequacy of existing checks.[117] Scholars

115. See Statutory Notes to 10 U.S.C. § 394.

116. *See Detailed Guide to the United States Code Content and Features*, OFF. OF THE L. REVISION COUNS., https://uscode.house.gov/detailed_guide.xhtml [https://perma.cc/8GFU-PKRG] (last visited Nov. 25, 2022) (explaining the authority of Statutory Notes and Editorial Notes).

117. *See* Waxman, *Cyberattacks and the Constitution*, *supra* note 9, at 11 (questioning whether cyber operations form a "new constitutional category altogether, for which the respective roles of Congress and the president are not yet established").

recognizing this void have identified the need for alternative players to take on the oversight task usually assigned to Congress.[118] Among these alternative players, the DoD OIG is particularly well-positioned to fill these gaps and to bring an appropriate level of oversight and review to the use and deployment of these expanding cyber capabilities. In describing the scope of the investigatory authorities and access that Congress gave to IGs in 1978, Paul Light noted that "[t]he question was not if IGs had the power, but whether they would use it."[119]

II. PLUGGING THE GAPS: THE DEPARTMENT OF DEFENSE OFFICE OF INSPECTOR GENERAL (DOD OIG) AND THE CYBER OVERSIGHT TASK

To answer that question—whether the IGs would use their power—this Part provides a primer on the IG position in our constitutional scheme, exploring the IG's congressional reporting relationship as well as the special agency perch it occupies and the powerful investigatory and audit tools it wields. This Part then focuses on the distinctive features that characterize the DoD OIG, describing the office's organizational structure, authorities, and the special statutory provisions governing its work. It catalogs the office's unique contributions to the cyber oversight ecosystem and provides contemporary examples of the office's cyber oversight activities. This Part concludes by considering potential limits on the DoD OIG's oversight role.

A. The Role of Inspectors General in the Constitutional Scheme

This Section offers a history of the IG position, examining its legislative origins and the statutory authorities that define the duties and responsibilities of the role. This Section then explains the role of the IG in the constitutional scheme. It first describes the importance of the position as an internal oversight mechanism within the executive branch and as a counterweight to the growth of the administrative state. It then shifts to explore the IG's secondary, although equally important, role in support of congressional oversight efforts, particularly with regard to

---

118. *See, e.g.,* Deeks, *Secrecy Surrogates*, *supra* note 10 (identifying technology companies, local governments, and foreign allies as "secrecy surrogates" with important advantages over traditional oversight mechanisms);; Gil, *supra* note 8, at 105 (explaining how "exogenous forces and actors" can serve a checking function); Rozenshtein, *supra* note 10, at 122–49 (describing potential contributions of technology companies to serve as "surveillance intermediaries" in support of the oversight function); *see also generally* Elena Chachko, *Administrative National Security*, 108 GEO. L.J. 1063 (2020); Kristen E. Eichensehr, *Cyberattack Attribution as Empowerment and Constraint*, HOOVER INST. WORKING GRP. ON NAT'L SEC., TECH., & L., Aegis Series Paper No. 2101 (Jan. 15, 2021).

119. PAUL C. LIGHT, MONITORING GOVERNMENT: INSPECTORS GENERAL AND THE SEARCH FOR ACCOUNTABILITY 23 (1993).

programs in the national security and intelligence spheres.

1. Watch Dogs: The Inspector General Act of 1978 and Independence

There are currently seventy-five IGs in the U.S. government, and more than 14,000 employees working in IG offices across the federal government.[120] Their task is to serve as "the principal watchdogs of the nation's major federal agencies."[121] While the concept of independent auditors within executive branch agencies has existed since the founding of the country,[122] the position was formalized and expanded in the Inspector General Act of 1978 (IGA), which created and currently governs the offices of statutory IGs.[123] The IGA fit into a group of legislative efforts, which Paul Light framed as a "busy season in the

120. COUNCIL OF THE INSPECTORS GEN. ON INTEGRITY AND EFFICIENCY, ANNUAL REPORT TO THE PRESIDENT AND CONGRESS: FISCAL YEAR 2021 1 (2021), https://www.ignet.gov/sites/default/files/files/992-011CIGIEAnnualReport-Full508.pdf [https://perma.cc/3A7V-M6ZH] ("In FY 2021, over fourteen thousand employees at seventy-five OIGs conducted audits, inspections, evaluations, and investigations."). *See also Inspector General Vacancies* [last visited Nov. 30, 2022], https://www.oversight.gov/ig-vacancies (identifying vacant IG positions).

121. HENRY A. WAXMAN, IMPROVING GOVERNMENT ACCOUNTABILITY ACT, H.R. REP. NO. 110–354, at 8 (2007) (Conf. Rep.).

122. *See* GOLDSMITH, *supra* note 13, at 99 (2012) ("Inspectors General, or inspectors general, are watchdogs that have been sprinkled around the executive branch since George Washington named Baron Frederick von Steuden to be inspector general for the Continental Army."). Although "finding the roots of the IG Act is like making a geological dig, stripping one layer of explanation off another until the underlying stratum is uncovered," LIGHT, *supra* note 119, at 39, the following sources provide able guides to tracing the history of IG-like positions in the federal government since the country's founding through the passage of the 1978 IGA: MICHAEL HENDRICKS ET. AL., INSPECTORS GENERAL: A NEW FORCE IN EVALUATION (1990); CHARLES A. JOHNSON & KATHRYN E. NEWCOMER, U.S. INSPECTORS GENERAL: TRUTH TELLERS IN TURBULENT TIMES (2020); LIGHT, *supra* note 119; MARK H. MOORE & MARGARET JANE GATES, INSPECTORS GENERAL: JUNKYARD DOGS OR MAN'S BEST FRIEND (1986); KATHRYN A. FRANCIS, CONG. RSCH. SERV., R45450, STATUTORY INSPECTORS GENERAL IN THE FEDERAL GOVERNMENT: A PRIMER (2019); John Adair & Rex Simmons, *From Voucher Auditing to Junkyard Dogs: The Evolution of Federal Inspectors General*, PUB. BUDGETING AND FIN. (1988); Margaret J. Gates & Marjorie F. Knowles, *The Inspector General Act in the Federal Government: A New Approach to Accountability*, 36 ALA. L. REV. 473 (1984); Katheryn E. Newcomer, *The Changing Nature of Accountability: The Role of the Inspector General in Federal Agencies*, 59 PUB. ADMIN. REV. 129 (1998). For detailed accounts of the role of inspectors general in national security and intelligence entities within the federal government, *see* CARMEN R. APAZA, INTEGRITY AND ACCOUNTABILITY IN GOVERNMENT: HOMELAND SECURITY AND THE INSPECTOR GENERAL (2010); Ryan M. Check & Afsheen J. Radsan, *One Lantern in the Darkest Night: The CIA's Inspector General*, 4 J. NAT'L SECURITY L. & POL'Y 247 (2010); Shirin Sinnar, *Protecting Rights from Within? Inspectors General and National Security Oversight*, 65 STAN. L. REV. 1027 (2013) [hereinafter Sinnar, *Protecting Rights from Within?*]; *see also* Margo Schlanger, *Offices of Goodness: Influence Without Authority in Federal Agencies*, 36 CARDOZO L. REV. 53, 60–62 (2014) [hereinafter Schlanger, *Offices of Goodness*] (describing need for and characteristics of "offices of goodness"—which share common traits but are distinct from inspectors general—to check executive branch conduct, as well as limits on such officers).

123. Inspector General Act of 1978, 5 U.S.C. app. 3 §§ 1–13 (1978) [hereinafter IGA].

search for government accountability."[124] The Act came about in response to executive branch abuses[125] and can be grouped with the War Powers Resolution of 1973, the Ethics in Government Act of 1978, the Civil Service Reform Act of 1978, and the Foreign Intelligence Surveillance Act of 1978, among others.[126] These statutes shared common goals: to ensure robust and accountable executive branch decision-making, to increase transparency of executive branch decision-making, and to bolster Congress's access to information in the hands of executive agencies.

While it is difficult to identify the exact mix of motivations that led Congress to enact the IGA, the act was focused on two broad objectives:

> To increase the overall scale and effectiveness of audits and investigative activities . . . and to make these activities visible by assuring that the information developed in audits and investigations reaches the highest levels of departments, the Congress, and the American public rather than being stifled at lower levels of the bureaucracy.[127]

To accomplish these objectives, Congress made independence the defining feature of the IG position. Independence is integral to the statute's objective of increasing transparency and visibility, and this feature is reflected in: the responsibilities Congress assigned to the IG, most notably the dual reporting obligation to the agency head and to Congress; the Act's appointment and removal provisions; the organizational structure and reporting lines of the position; the IG's authority to select activities and to act without interference; and the obligation to make reports available to the general public.[128] The strong emphasis on independence explains why IGs are grouped with other mechanisms and entities in what Jack Goldsmith calls the "presidential

---

124. LIGHT, *supra* note 119, at 11.

125. *See* S. REP. NO. 95-1071, at 4 (1978) (listing examples of "epidemic" levels of fraud, abuse, and waste motivating enactment of the IGA). Scholars have also taken note of the "common motivations" underlying passage of the IGA and other legislative efforts designed to reassert the oversight control that Congress had lost in the wake of Watergate, Vietnam, and other executive branch abuses. JOHNSON & NEWCOMER, *supra* note 122; *see also* LIGHT, *supra* note 119, at 48 (describing how "post-Watergate struggle over access to executive branch information" impacted passage of IGA); MOORE & GATES, *supra* note 122, at 12 (describing importance of IGA's focus on ensuring information reached Congress); *see also generally* Church Committee Report, *supra* note 53; Pike Committee Report, *supra* note 53.

126. *See* War Powers Resolution, 50 U.S.C. §§ 1541–50 (1973); Ethics in Government Act, 5 U.S.C. app. 4 § 101; Civil Service Reform Act, 5 U.S.C. § 1101; Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801.

127. MOORE & GATES, *supra* note 122, at 13; *see also* LIGHT, *supra* note 119, at 39 ("Finding the roots of the IG Act is like making a geological dig, stripping one layer of explanation off another until the underlying stratum is uncovered.").

128. *See generally* IGA, *supra* note 123.

synopticon," a group of watchers designed to check executive branch power and hold executive branch actors accountable.[129]

The emphasis on independent advice and assessment is reflected in Section 2 of the IGA, which describes the core responsibilities of the position. These include conducting and supervising audits and investigations relating to the programs and operations of their agency, department, or establishments. In addition, the IG is expected "to provide leadership and coordination and recommend policies for activities designed (A) to promote economy, efficiency, and effectiveness in the administration of, and (B) to prevent and detect fraud and abuse in, such programs and operations."[130] Most notably, the IG is tasked with "keeping the head of the establishment and the Congress fully and currently informed about problems and deficiencies relating to the administration of such programs and operations and the necessity for and progress of corrective action."[131]

This mandate places the IG in a dual reporting relationship, providing reports internally to the relevant agency head, and providing information externally to the relevant congressional committees. During passage of the IGA, Congress debated how best to ensure the independence of the IG and considered making the position independent even of the department secretary.[132] Congress eventually abandoned that idea, and instead determined that dual reporting was the wisest path. "[I]ndependence could truly be assured only if the IGs were made accountable to someone other than the Secretary—for example, the Congress."[133] Moreover, giving IGs the option of going to Congress provided a powerful incentive for agency management to consider the IG's advice and recommendations. "If management is unresponsive, the IGs can always go to Congress or the press. Indeed, this threat is implicit in much of their negotiations with management. Political support and the values they stand for allow IGs to gain a hearing from management that might otherwise be absent."[134]

The independence feature is also prominent in the provisions

---

129. GOLDSMITH, *supra* note 13, at 207.

130. 5 U.S.C. app. 3 § 2; *see also* MOORE & GATES, *supra* note 122, at 26–27 (describing challenges when efforts to prevent and detect fraud and abuse come into conflict with efforts to promote economy, efficiency, and effectiveness).

131. 5 U.S.C. app. 3 § 2.

132. *See* MOORE & GATES, *supra* note 122, at 12 (referencing conference report and noting that "for the first time however, the Congress began thinking that the OIG should be made independent even of the Secretary, lest the Secretary be tempted to quash investigations or ignore OIG recommendations").

133. *Id.*

134. *Id.* at 71.

governing the appointment and eligibility requirements for IGs. The Act provides that IGs shall be appointed "without regard to political affiliation and solely on the basis of integrity and demonstrated ability in accounting, auditing, financial analysis, law management analysis, public administration, or investigations."[135] While IGs may be appointed in several ways, the usual route is appointment by the president and confirmation by the Senate.[136]

The importance of protecting the IG's independence is also reflected in the provisions governing removal. The removal process is generally uniform across the federal government, permitting the president to remove any IG at any time.[137] To protect the IG's independence, the statute adds an accountability wrinkle to any removal activity by the president. It requires that the president communicate in writing the reasons for removal of an IG to both chambers of Congress at least thirty days before the removal or transfer.[138] Thus, the independence vein is reflected here not by limiting the president's removal power, but by requiring written notice and explanation, in advance, to Congress. More recent expressions of support for the preservation of the IG's

---

135. 5 U.S.C. app. 3 § 3(a). In addition, candidates for IG positions with the DoD, CIA and Intelligence Community must meet additional requirements or limits specific to their agencies. 5 U.S.C. app. 3 § 8(i) ("No member of the Armed Forces, active or reserved shall be appointed Inspector General of the Department of Defense."); 50 U.S.C. § 3033(c)(2)(B) (requiring nominations for IG of the Intelligence Community to be in "compliance with the security standards of the intelligence community, and [to have] prior experience in the field of intelligence or national security"); 50 U.S.C. § 3517(b) (1) (requiring nominations for CIA IG to be in "compliance with the security standards of the Agency and [have] prior experience in the field of foreign intelligence").

136. *See* 5 U.S.C. app. 3 § 3(a) (laying out this process generally). This method applies to IGs in cabinet-level departments and larger agencies, often referred to as "establishment IGs," including the Department of Defense. FRANCIS, *supra* note 122, at 12–13 (describing different methods for appointments of IGs in designated federal entities, in non-IGA authorized positions, and temporary IGs).

137. 5 U.S.C. app. 3 § 3(b). This level of discretion is consistent with the general principles governing the president's ability to remove various types of executive branch officials, and the knotty separation of powers issues that arise when Congress attempts to constrain the president's removal power. For a discussion of the legal principles governing congressional efforts to constrain the president's removal power, *see generally* Seila L. LLC v. Consumer Fin. Prot. Bureau, 140 S. Ct. 2183 (2020).

138. 5 U.S.C. app. 3 § 3(b) ("If an Inspector General is removed from office or is transferred to another position or location within an establishment, the President shall communicate in writing the reasons for any such removal or transfer to both Houses of Congress, not later than 30 days before the removal or transfer."). Certain types of IGs are subject to more stringent removal requirements. *See*, *e.g.*, 5 U.S.C. app. 3 § 8G(e)(1) (requiring written concurrence by two-thirds majority, as well as written notification to both houses of Congress at least thirty days before removal of an IG from a designated federal entity for which a board or commission is the head of the designated federal entity); *see also* 5 U.S.C. app. 3 § 8G(e)(1-2) (limiting removal to "for cause" and requiring written concurrence by seven out of nine presidentially appointed governors of IG of U.S. Postal Service).

independence can be found in a variety of legislative proposals circulating in Congress which call for limiting the president's ability to remove IGs.[139]

Independence is also reflected in the day-to-day organizational and operational aspects of the position. First, the IG reports directly to the head of the agency, or the officer next in rank below the head.[140] In addition, the IG has the authority to structure the office, selecting heads of the various departments and hiring and firing staff.[141] In some instances, the IG may also hire a general counsel dedicated to serving that IG's office.[142] The IG receives and identifies work assignments from several sources, including statutory mandate, congressional request, agency head request, or at the IG's own initiative.[143] Relatedly, the statute gives the IG authority to identify and engage in auditing, investigative, and inspection activities without interference from the department head or others. "Neither the head of the establishment nor the officer next in rank below such head shall prevent or prohibit the Inspector General from initiating, carrying out, or completing any audit or investigation, or from issuing any subpoena during the course of any audit or investigation."[144] Paul Light identifies this "full authority to undertake whatever audits and investigations deemed necessary" as one of the devices that protects the IG from administrative politics, thus

---

139. *See, e.g.,* Protecting Our Democracy Act of 2021, H.R. 5314, 117th Cong. (2021) (proposing protections for inspectors general, including limiting the president's ability to remove them without good cause); Inspectors General Independence Act, S. 3664, 116th Cong. (2020) (protecting inspectors general with a "for cause" termination requirement). *See generally* Inspectors General Independence Act, H.R. 6668, 116th Cong. (2020); Inspector General Access Act of 2019, S. 685, 116th Cong. (2019); Inspector General Access Act of 2019, H.R. 202, 116th Cong. (2019); Inspector General Protection Act, H.R. 1847, 116th Cong. (2019); Seeking Inspector General's Honest Testimony Act (SIGHT Act), S. 3766, 116th Cong. (2020); Securing Inspector General Independence Act of 2020, S. 3994, 116th Cong. (2020). Not surprisingly, many of these proposals arose in response to former President Trump's spate of IG firings, most notably from intelligence and national security agencies. The Lawfare Podcast*, Firing Inspectors General*, LAWFARE (May 19, 2020), https://www.lawfareblog.com/lawfare-podcast-firing-inspectors-general/ [https://perma.cc /QP5H-FQ55].

140. *See* 5 U.S.C. app. 3 § 3(a) (indicating that, in most instances, IGs report directly to the agency head or high-level member of the secretary's executive team).

141. *See* 5 U.S.C. app. 3 § 6 (explaining that IGs may, as necessary, appoint Assistant IGs as well as IGs to head other departments).

142. *See* 5 U.S.C. app. 3 § 3(g) at 13 (designating independent counsel for IG).

143. *See* 5 U.S.C. app. 3 § 8(c)(2) (stating that "the Inspector General of the Department of Defense shall . . . initiate, conduct, and supervise such audits and investigations in the Department of Defense (including the military departments) as the Inspector General considers appropriate"); FRANCIS, *supra* note 122 (explaining that an IG conducts reviews in response to statutory mandate, at the request of Congress or other stakeholders (e.g., the President), or upon self-initiation); JOHNSON & NEWCOMER, *supra* note 122, at 96–97, 132–35 (describing congressional requests for IG action and other interactions between congressional entities and IG offices).

144. 5 U.S.C. app. 3 § 3(a).

strengthening the IG's powers.[145] This protection from interference is a hallmark of the position's independence and fosters the officer's ability to serve public law values.[146] There are exceptions to this mandate for IGs located in national security and intelligence agencies. The agency heads in these entities may block IG activities if they relate to certain sensitive topics or national security matters.[147] It is noteworthy, however, that the norm of allowing IGs to work free from interference is so powerful that even the agency heads with a statutorily granted justification for halting or blocking IG work rarely invoke this prohibition.[148]

The statutorily mandated obligation to make reports available to the general public is another feature that supports the independence of the office. The statute requires IGs to publish their findings and recommendations, as well as their semiannual reports, for public review.[149] While IGs may not publicly disclose information that is prohibited from disclosure due to classification level or other security-based reasons, most of the IG reports are published both on the agency's website and the consortium's page.[150]

A final note on the independence of IGs is reflected by the statute's focus on giving IGs advisory roles. The IG may identify problems and recommend changes, however, the IG has no authority to take corrective action or to implement the policy changes it recommends. As Paul Light writes, IGs "are to look, not act; recommend, not implement."[151] While this can be viewed as a limit, or a bug in the statutory design, it is better viewed as a feature. Indeed, the advisor role may actually advantage the IG. Without concern for implementation remedies, the IGs do not pull their punches. They do not pre-frame the problem in a way that allows for or leans heavily toward a desired solution. Their advisory status provides for greater candor. The Senate report accompanying the 1978 IGA acknowledged the challenge of balancing the IG's need for independence with the agency's management needs, concluding:

---

145. LIGHT, *supra* note 119, at 23–24.

146. A deeper discussion of the public law values embodied by IGs can be found in Deeks, *Secrecy Surrogates*, *supra* note 10, at 1452–54.

147. 5 U.S.C. app. 3 § 8(b)(1); *see also infra* Section II.C. (exploring how this limit impacts the work of the Department of Defense Office of Inspector General).

148. The most striking example of this may be CIA IG John Helgerson's investigation into CIA detention and interrogation activities. GOLDSMITH, *supra* note 13, at 99–108.

149. 5 U.S.C. app. 3 §§ 4(e), 5(e).

150. *See generally Inspector General Reports*, OVERSIGHT.GOV, https://www.oversight.gov/reports [https://perma.cc/AJ2S-ZMW3]; *All DoD OIG Reports*, OFF. OF INSPECTOR GEN., U.S. DEP'T OF DEF., https://www.dodig.mil/reports.html/ [https://perma.cc/9CUF-NMNT].

151. LIGHT, *supra* note 119, at 16.

> If the Agency Head is committed to running and managing the agency effectively and to rooting out fraud, abuse, and waste at all levels, the Inspector and Auditor General can be his strong right arm in doing so, while maintaining the independence needed to honor his reporting obligations to Congress. The Committee does not doubt that some tension can result from this relationship, but the Committee believes that the potential advantages far outweigh the potential risks.[152]

In sum, Congress intended the position to be one of significant authority and structural independence. Scholars Margaret Gates and Marjorie Fine Knowles offer this observation: "The inspector general is the only executive branch Presidential appointee who speaks directly to Congress without clearance from the Office of Management and Budget . . . This ability to speak directly to Congress provides a potential source of substantial clout for an active inspector general."[153] The independence and clout described above gain greater reach when paired with the position's statutorily mandated perch within the executive branch entity and accompanying toolkit.

2. Junk-Yard Dogs: Oversight Perch, Activities, and Tools

IGs are often viewed as "junk yard dogs"[154] by colleagues in their agencies for their exasperating, grating, and at times, maddening pursuit of any procedural or substantive flaw, evoking the bothersome junk yard dog that follows one around and continuously digs for bones. Of course, this dogged (forgive the pun) focus is intentional. The IGs were created to provide a critical internal oversight function by identifying wasteful, wrongful, and illegal activities inside the executive branch. To accomplish this task, Congress created a special perch for the IG to occupy within the agency, allowing them to get "deep inside the presidency"[155] while providing unparalleled access and a wholistic perspective.

In addition to the special perch, Congress provided IGs with an enviable arsenal of information-gathering tools. The IG is charged with keeping the head of the establishment or agency "fully and currently informed about problems and deficiencies relating to the administration of such programs and operations and the necessity for and progress of

---

152. S. REP. NO. 95-1071, at 9 (1978).
153. Gates & Knowles, *supra* note 122, at 475.
154. *See* MOORE & GATES, *supra* note 122 (embracing junk yard dog metaphor in title of their work); GOLDSMITH, *supra* note 13, at 99 (summarizing the "junk yard dog" comparison).
155. GOLDSMITH, *supra* note 13, at 105.

corrective action."[156] To accomplish this objective, as well as the congressional notice task, IGs engage in three principal activities: investigations, audits, and evaluations/inspections.[157] Investigations generally involve criminal or civil misconduct by a government employee, contractor, or grant recipient. Audits include both performance and financial audits. Financial audits tend to be the most familiar of the IG review types (at least to outsiders) and involve the assessments of the appropriate allocation and use of federal funds. Performance audits provide programmatic analysis of an entire program or operation; they focus on compliance, efficiency and effectiveness, internal control, and prospective analysis. Inspections or evaluations are also programmatic in nature; they examine the policies, operations, regulations, or legislative implications of a specific aspect of a program or operation, or review of a specific agency facility, and involve the IG engaging in "evaluation activity."[158] "Some inspections examine the extent to which individual federal programs or installations are complying with applicable laws, regulations, and policies, while other inspections determine how entire programs might be amended or redirected."[159] These programmatic and evaluative IG activities are often missed by those outside the IG community, contributing to the common but incomplete view of IGs as bean counters.

To pursue these activities, the IGA and its subsequent amendments[160] provide IGs with broad investigatory powers. These include authority to: conduct and supervise audits, investigations, inspections and reviews into the actions of agencies without interference by agency heads; issue reports with recommendations for corrective action; receive full access to all information (i.e., records and materials) available to the agency; request materials from other executive branch agencies; issue administrative subpoenas to nonfederal entities; administer or take an oath, affidavit, or affirmation from any person; exercise the authority of law enforcement; receive employee and external complaints; appoint officers as necessary to carry out such powers; refer matters (both criminal and civil) to the United States Attorney General; hire employees, experts, and consultants and procure necessary equipment and services; obtain assistance from other agencies (federal, state and local); and enter

156. 5 U.S.C. app. 3 § 2(3).
157. *See* FRANCIS, *supra* note 122, at 7–9 (comparing the differences between the three common types of IG reviews).
158. *Id.*; *see also* APAZA, *supra* note 122, at 13 (describing types of evaluation activities in the IG portfolio).
159. APAZA, *supra* note 122, at 13.
160. *See* FRANCIS, *supra* note 122, at 3 (summarizing these amendments).

into contracts and other arrangements with public and private entities.[161] The work product that comes from the use of these tools is voluminous, even if not widely read. IGs produce statutorily mandated semiannual reports and incident-specific reports to Congress as well as reports on the implementation status of prior recommendations.[162] In addition, both Congress and the agency head can ask the IG to conduct specific investigations, audits or inspections.[163] The IG's special perch and accompanying toolkit allow those in the position to effectively disseminate information to those in policy-making positions, while also providing opportunities to "nudge the Executive toward.....public law values."[164]

Thus, on paper, Congress appears to have placed an array of investigative tools at the IG's disposal while imposing very few limits on how the tools could be deployed. Indeed, the potential scope of tools available has led some to question whether "the congressional intrusion into executive branch operations was so substantial that it violated the separation of powers doctrine," representing a usurpation of executive power by Congress.[165] This sentiment remained strong as recently as

---

161. 5 U.S.C. app. 3 §§ 4(a), 4(d), 5(a), 6(a), 6(e), 7.

162. *See* 5 U.S.C. app. 3 § 5(a) (describing semi-annual reports); 5 U.S.C. app.3 § 4(d) (describing reporting for matters involving violations of federal criminal law); 5 U.S.C. app. 3 § 5(d) (describing reporting for serious or flagrant matters). In addition, IGs are tasked with preparing an annual report as required by the Federal Information Security Modernization Act of 2014, 44 U.S.C. §§ 3554(c)(1), 3555(2)(b)(1), and a joint biennial report as required by the Cybersecurity Information Sharing Act of 2015, 6 U.S.C. § 1506(b). For a full discussion of IG congressional reporting responsibilities, *see infra* Section II.A.3.

163. *See* FRANCIS, *supra* note 122, at 7 (explaining that an IG conducts reviews in response to "a statutory mandate, at the request of Congress or other stakeholders (e.g., the President), or upon self-initiation"); JOHNSON & NEWCOMER, *supra* note 122, at 96–97, 132–35 (describing congressional requests for IG action and other interactions between congressional entities and IG offices).

164. Deeks, *Secrecy Surrogates*, *supra* note 10, at 1453. Accountability is a hallmark of democratic systems of government, and in the national-security setting, the "relevant subset of public law values includes (1) legal compliance; (2) competence and rationality; (3) holding government decision makers accountable for the decisions that they have made, including by demanding justifications for those decisions; and (4) seeking transparency about government decisions where possible." Moreover, IGs and other secrecy surrogates:

> can nudge the Executive toward those public law values by testing whether the Executive appears to be acting in a legal way (or at least not acting in a patently illegal way); whether the Executive appears to be making rational, reasoned decisions based on the secret information it possesses; and whether the Executive is being as transparent as possible, recognizing that some information and acts must necessarily remain secret.

Id. at 1452–53.

165. *See* MOORE & GATES, *supra* note 122, at 10 (citing Memorandum from Griffin Bell, Att'y Gen., to President Jimmy Carter on H.R. 2819 (Feb. 24, 1977) (enclosing and describing memorandum from John M. Harmon, Assistant Att'y Gen., Off. of Legal Couns., (Feb. 21, 1977) on the same subject)); *see also id.* at 13 (noting President Carter's concern that the IGA amounted to congressional usurpation of executive branch powers).

1998, when a group of experts labeled IGs "congressional ferrets of dubious constitutionality."[166]

3. Man's Best Friend: Answering Congress's Call for Information

While much of the IG attention and scholarship focuses on the internal oversight function, the position serves a secondary, although equally important, role in support of congressional oversight efforts, particularly with regard to programs in the national security and intelligence spheres, by serving as a conduit of information to congressional committees. One of the motivations for passage of the IGA was a "burgeoning congressional demand for information."[167] As noted above, Congress established the offices of IGs in executive branch agencies "to provide a means for keeping the head of the establishment and *the Congress* fully and currently informed about problems and deficiencies relating to the administration of such programs and operations and the necessity for and progress of corrective action."[168] The information conduit function gives IGs a lead role in the constitutional separation of powers scheme by serving as an effective counterweight to abuses in the executive branch. In contrast to agency heads and employees who may view the IG as an exasperating junk yard dog, the congressional committees have a kinder view of IGs, relying on them to provide oversight support as well as access to information that would otherwise be difficult to acquire from the executive branch, categorizing the IGs more favorably as man's—or committee's—best friend.

IGs fulfill this congressional informing task through a variety of mechanisms, some generally applicable and some specific to the agency, some routine and some urgent.[169] These mechanisms include semiannual reports mandated by the IGA, implementation updates, fast action reports for particularly egregious violations and the threat of seven-day letters, specific inquiries from Congress to investigate matters, and congressional requests for IG testimony. This Section will briefly review each of these mechanisms.

---

166. GOLDSMITH, *supra* note 13, at 106 (quoting FINAL REPORT OF THE NATIONAL COMM'N ON THE SEPARATION OF POWERS, MILLER CTR. OF PUB. AFFS. (Dec. 7, 1998)).

167. LIGHT, *supra* note 119, at 39.

168. 5 U.S.C. app. 3 § 2 (emphasis added); *see also* Schlanger, *Offices of Goodness*, *supra* note 122, at 101 ("Even if an Office's conclusions do not accord with the external users' views, if the Office does a competent job gathering and analyzing the situation, the resulting information can be highly useful to external actors, contributing to what Seth Kreimer names the 'ecology of transparency.'").

169. *See* LIGHT, *supra* note 119, at 24 (describing reporting requirements as "one ordinary, one urgent"); *see also* Schlanger, *Offices of Goodness*, *supra* note 122, at 101 (describing McCubbins and Schwarz's "fire-alarm" as compared to "police" strategies with regard to congressional oversight).

Semiannual Reports. IGs must submit semiannual reports, summarizing the activities of the IG's office during the immediately preceding six-month period, to the agency head by April 30 and October 31 of each year.[170] The list of required components is comprehensive and includes the following notable categories among a list of twenty-two other components: a description of "significant problems, abuses, and deficiencies relating to the administration of programs and operations" at the agency; a description of recommendations for "corrective action;" a summary of matters referred to prosecutive authorities and resulting prosecutions and convictions; a summary of each report made to the head of the establishment under Section 6(c)(2); statistical tables showing the total number of audit, inspection and evaluation reports, and the total dollar value of questioned costs; reports of "outstanding unimplemented recommendations;" information concerning "any significant management decision with which the Inspector General is in disagreement;" and "a detailed description of any instance of whistleblower retaliation."[171]

Upon receiving the report, the agency head must transmit the report within thirty days to the appropriate congressional committee or sub-committee, and the IG's report must be accompanied by a report of the agency head commenting on and responding to certain aspects of the IG's report.[172] Within sixty days of submitting the semiannual report to Congress, the agency head "shall make copies of such report available to the public upon request and at a reasonable cost,"[173] and in most instances, the reports are published on the website of the IG for the agency or the central IG report repository.[174]

Flagrant Incident Reports and Seven-Day Letters. The IG is subject to an additional heightened reporting requirement for "particularly serious or flagrant problems, abuses, or deficiencies relating to the administration of programs and operations" in the agency.[175] When the IG becomes aware of a matter in this category, the IG must report the

170. 5 U.S.C. app. 3 § 5.
171. 5 U.S.C. app. 3 § 5(a).
172. 5 U.S.C. app. 3 § 5(b).
173. 5 U.S.C. app. 3 § 5(c).
174. *See, e.g.*, *Inspector General Reports*, OVERSIGHT.GOV, https://www.oversight.gov/reports [https://perma.cc/AJ2S-ZMW3] (providing searchable database of IG reports); *see generally All DoD OIG Reports*, OFF. OF INSPECTOR GEN., U.S. DEP'T OF DEF., https://www.dodig.mil/reports.html/ [https://perma.cc/9CUF-NMNT]; *see also* Schlanger, *Offices of Goodness*, *supra* note 122, at 96–97 (describing how the presumption of open publication for IG reports enhances the effectiveness of IGs).
175. 5 U.S.C. app. 3 § 5(d).

matter immediately to the head of the agency.[176] The burden then shifts to the agency head to transmit such report to the appropriate committees or subcommittees of Congress within seven calendar days.[177] Referred to as "seven-day letters" in IG lingo, the potential to swing this sword provides critical leverage to the office of the IG. Indeed, that potential leverage may account for the sparing use of this tool. According to a 2011 Government Accountability Office (GAO) study, between 2008 and 2010, only one IG issued a seven-day letter, and between January 1990 and April 1998, no seven-day letters were issued.[178] Recognizing the value of the information provided by IGs, particularly with regard to issues of immediate concern, Congress has encouraged IGs to use the seven-day letter in a less sparing fashion.[179]

Annual Implementation Update Reports. In addition to the semiannual and incident-specific reports, IGs must track, and provide to Congress and the public on an annual basis, the implementation status of their prior recommendations.[180] The purpose underlying the requirement is "to ensure that the inspectors general avoid overstating the actual savings that can be attributed to their work."[181] The implementation status check also provides a useful tool for agency heads, relevant congressional committees, and the public to identify areas of persistent challenge, as well as possible foot-dragging or resistance by agencies.

Annual Top Management Challenges Reports. Pursuant to the Reports Consolidation Act of 2000, each IG is required to prepare an annual

---

176. 5 U.S.C. app. 3 § 5(d); *see, e.g.*, LIGHT, *supra* note 119, at 24 (highlighting the IG's responsibility to immediately report to the head of the department when the IG becomes aware of certain types of conduct or activities).

177. 5 U.S.C. app. 3 § 5(d). A recent example is a 2019 seven-day letter to the EPA Director reporting on the persistent refusals to cooperate by the agency's chief of staff. Letter from Charles J. Sheehan, Acting Inspector Gen., U.S. EPA, to Andrew R. Wheeler, Adm'r, U.S. Env't. Prot. Agency (Oct. 29, 2019), https://www.epa.gov/sites/production/files/2019-11/documents/_epaoig_7dayletter_11-6-19.pdf [https://perma.cc/KH8Y-RV96].

178. *See generally* U.S. GOV'T ACCOUNTABILITY OFF., GAO-11-770, INSPECTORS GENERAL: REPORTING ON INDEPENDENCE, EFFECTIVENESS, AND EXPERTISE (2011), https://www.gao.gov/new.items/d11770.pdf [https://perma.cc/KY93-K5VU].

179. *See generally* Timothy R. Smith, *Darrell Issa Wants Inspectors General to Loop in Congress on Big Investigations*, WASH. POST (Aug. 6, 2012), https://www.washingtonpost.com/blogs/federal-eye/post/darrell-issa-wants-inspectors-general-to-loop-in-congress-on-big-investigations/2012/08/06/22b53364-dfdc-11e1-a421-8bf0f0e5aa11_blog.html [https://perma.cc/RS3N-GC7D].

180. 5 U.S.C. app. 3 § 5(a)(15); *see, e.g.,* OFF. OF INSPECTOR GEN., U.S. DEP'T OF DEF., COMPENDIUM OF OPEN OFFICE OF INSPECTOR GENERAL RECOMMENDATIONS TO DEPARTMENT OF DEFENSE (2022) [hereinafter DOD COMPENDIUM 2022] (providing list of open recommendations made by DoD OIG).

181. 133 CONG. REC. S4554-01, at 7959 (daily ed. Apr. 3, 1987) (statement of Rep. Glenn) ("The bill requires more detailed statistical analysis from the inspectors general and requires periodic reporting to Congress by the agency heads on their implementation of recommended corrective action. This means savings will be realized and reported when such action is completed.").

statement that summarizes what the IG considers to be the "most serious management and performance challenges facing the agency" and to assess the agency's progress in addressing those challenges.[182] These reports are forward-looking and used by IGs to determine areas of risk in the agency's operations and to assess where to allocate the office's oversight resources.

Oversight Planning Reports. The annual oversight plan is related to the top management challenges report. It describes the specific oversight projects the office intends to conduct during the upcoming fiscal year and explains how those activities relate to the top management challenges facing the agency.[183] The plans are organized by management challenge, with each chapter providing a summary of a particular challenge, followed by an inventory of the ongoing and planned oversight projects that directly align with that challenge.[184]

Specific Investigation Requests. In addition to reports described above, members of Congress may also request specific action by IGs.[185] For example, in November 2020, members of the Senate Select

---

182. Reports Consolidation Act of 2000, Pub. L. No. 106-531, § 3, 114 Stat. 2537–38; *see, e.g.,* OFF. OF INSPECTOR GEN., U.S. DEP'T OF DEF., TOP DOD MANAGEMENT CHALLENGES FOR FISCAL YEAR 2022 (2021) [hereinafter TOP DOD MANAGEMENT CHALLENGES FY2022] (identifying top management challenges for Department of Defense).

183. *See generally* OFF. OF INSPECTOR GEN., U.S. DEP'T OF DEF., FISCAL YEAR 2021 OVERSIGHT PLAN (2020) [hereinafter DOD OVERSIGHT PLAN FY2021].

184. *See, e.g*., *id.* (describing arrangement of the Oversight Plan).

185. *See* FRANCIS, *supra* note 122, at 7 (explaining that an IG conducts reviews in response to "statutory mandate, at the request of Congress or other stakeholders (e.g., the President), or upon self-initiation'); JOHNSON & NEWCOMER, *supra* note 122, at 96–97, 132–35 (describing congressional requests for IG action and other interactions between congressional entities and IG offices). Not surprisingly, the SolarWinds hack has been the subject of several requests to agency IG offices. In December 2020, Representatives Bill Pascrell, D-N.J., and Mike Kelly, R-Pa., reached out to the IG for the Internal Revenue Service. Dave Nyczepir, *"No Evidence" IRS Taxpayer Information Exposed by SolarWinds Hack*, FEDSCOOP (Dec. 23, 2020), https://www.fedscoop.com/taxpayer-information-solarwinds-hack-irs/ [https://perma.cc/XU2S-N2R7]. Admirably, the IG responded within a few days. *See* Letter from J. Russell George, Inspector Gen. for Tax Admin., to Rep. Bill Pascrell, Chairman of the H.R. Subcomm. on Oversight, and Rep. Mike Kelly, Ranking Member of the H.R. Subcomm. on Oversight (Dec. 23, 2020), available at https://pascrell.house.gov/uploadedfiles/ways_and_means_response_final_12-23-2020.pdf [https://perma.cc/Z3J4-ZJCV] (responding to concerns with assurance that the Treasury Inspector General for Tax Administration was investigating and no exposure of taxpayer information was discovered). A slew of additional requests followed, including to the IGs of the Department of Justice and Department of Homeland Security. *See generally Senators Request Information from FBI, CISA on Reports of Russian Cyberattack against the U.S. Government*, UNITED STATES SENATOR FOR KANSAS JERRY MORAN (Dec. 15, 2020), https://www.moran.senate.gov/public/index.cfm/2020/12/senators-request-information-from-fbi-cisa-on-reports-of-russian-cyberattack-against-the-u-s-government [https://perma.cc/QY2Z-EMDV] ("How has CISA and the Federal Bureau of Investigation (FBI) organized their coordination efforts with the impacted federal agencies to support forensic analysis and investigative efforts related to unauthorized access? What role do the federal agencies or their Inspectors General play in the investigations?").

Committee on Intelligence and Senate Armed Services submitted a request to the DoD OIG, asking that office to investigate the president's selection for the general counsel position in the National Security Agency.[186] Congress also has a practice of including specific action requests to the DoD OIG in the annual national defense authorization acts.[187]

Congressional Testimony. As part of their responsibilities to keep Congress fully informed, IGs testify before Congress. Anticipating the need for congressional support, many IG offices have a division or position dedicated to legislative affairs and tasked with preparing the semiannual reports and otherwise serving as liaisons between the office and the relevant congressional committees. For example, the DoD OIG has a dedicated office of Legislative Affairs and Communications. In addition, IGs are well-positioned to complement the work of the GAO.[188] Examples of recent IG testimony include: "Oversight of the United States Capitol Police and Preparations for and Response to the Attack of January 6th" (April 21, 2021) before the House Committee on Administration;[189]

---

186. *See generally* Letter from Mark R. Warner, Vice Chairman of the S. Select Comm. on Intel., and Jack Reed, Ranking Member of the Comm. on Armed Serv., to Sean O'Donnell, Acting Inspector Gen. for U.S. Dep't of Def. (Nov. 16, 2020), https://assets.documentcloud.org/documents/20407603/dod-ig-letter.pdf [https://perma.cc/XR7T-78B8].

187. *See, e.g.*, NDAA for FY2020, *supra* note 66, § 6721 (requiring IGs of several intelligence community entities to provide reports to congressional intelligence committees on compliance and effectives of classification procedures in their entities). In June 2021, Senator Richard Blumenthal, D-Conn., announced that he planned to write a "mandatory reporting requirement" into the NDAA for FY2022. Kristin Hall et al., *Top General 'Shocked' by AP Report on AWOL Guns, Mulls Fix,* DETROIT NEWS (June 17, 2021, 10:04 PM), https://www.detroitnews.com/story/news/nation/2021/06/17/top-general-shocked-ap-report-awol-guns-mulls-fix/7741070002/ [https://perma.cc/K5SK-EAFF]. In a letter to Defense Secretary Lloyd Austin, Blumenthal also asked that the Department of Defense's Office of the Inspector General conduct "a thorough review" of policies and security procedures. *Id.*; *see also Blumenthal and Austin Discuss Challenges Facing the Defense Department during Nomination Hearing*, U.S. SENATOR RICHARD BLUMENTHAL (Jan. 19, 2021), https://www.blumenthal.senate.gov/newsroom/press/release/blumenthal-and-austin-discuss-challenges-facing-the-defense-department-during-nomination-hearing [https://perma.cc/M3KL-ZQ7S].

188. The GAO and IGs have a history of working together on various projects because both entities focus on supporting Congress's oversight efforts. Indeed, the relationship is a complicated one as the GAO also audits each agency's office of the IG to ensure it is meeting the statutory mission. A recent example of this can be found in the GAO's report on the work of the Office of Inspector General of the Department of Homeland Security. *See, e.g.,* U.S. GOV'T ACCOUNTABILITY OFF., GAO-08-751, PRELIMINARY OBSERVATIONS ON LONG-STANDING MANAGEMENT AND OPERATIONAL CHALLENGES (2021), https://www.gao.gov/assets/gao-21-452t.pdf [https://perma.cc/JZA7-GTHB].

189. *Oversight of the United States Capitol Police and Preparations for and Response to the*

"Department of Defense Inspector General and the Services Inspector Generals: Roles, Responsibilities and Opportunities for Improvement" (April 15, 2021) before the House Subcommittee on Military Personnel;[190] and "Restoring Independence of Inspectors General" (April 20, 2021) before the House Committee on Oversight and Reform.[191]

The IG's role as congressional information supplier was an integral driver in passage of the IGA and part of larger congressional efforts to expand the mechanisms and entities able to monitor the executive branch. Paul Light writes that IGs should be viewed as both "an extension and an outcome of earlier congressional reform efforts to reign in executive power. As an extension, the IGs are another tool for limiting executive branch discretion. As an outcome, they are essential suppliers of the information needed to sustain the earlier reforms."[192] This has led IGs to become a particularly desirable partner in national security matters, providing Congress with the information needed to conduct its oversight responsibilities.

B. National Security Mutts: The DoD OIG

From the early days of our nation, both military commanders and legislative bodies recognized the need for an IG position. In December 1777, Congress, by resolution, created the position of Inspector General of the Army.[193] From General Washington's perspective, such an agent was desirable because they could provide consistent discipline and ensure "tactical competence."[194] The Continental Congress also found the

---

Attack of January 6th: Hearing Before Comm. on H. Admin., 117th Cong. (2021), https://cha.house.gov/committee-activity/hearings/oversight-united-states-capitol-police-and-preparations-and-response [https://perma.cc/QYW4-BEEK].

190. *Department of Defense Inspector General and the Service Inspector Generals: Roles, Responsibilities and Opportunities for Improvement: Hearing before the Subcomm. on Mil. Pers. of the H. Comm. on Armed Serv.,* 117th Cong. (2021), https://armedservices.house.gov/hearings?ID=8B79E0CA-6761-4213-A0BA-142C740D040F [https://perma.cc/TBU8-P3X8].

191. *Restoring Independence: Rebuilding the Federal Offices of Inspectors General: Hearing before the Subcomm. on Gov't Operations of the H. Comm. on Oversight and Reform*, 117th Cong. (2021), https://oversight.house.gov/legislation/hearings/restoring-independence-rebuilding-the-federal-offices-of-inspectors-general [https://perma.cc/2RGL-PV3T]; *see also Subcommittee Committee Held Hearing on Restoring Independence of Inspectors General*, H. COMM. ON OVERSIGHT & REFORM (Apr. 20, 2021), https://oversight.house.gov/news/press-releases/subcommittee-committee-held-hearing-on-restoring-independence-of-inspectors [https://perma.cc/V576-G7EE] (summarizing key points from hearing).

192. LIGHT, *supra* note 119, at 39.

193. *History of the U.S. Army Inspector General*, U.S. MIL. ACAD. WEST POINT, https://www.westpoint.edu/about/west-point-staff/inspector-general/history [https://perma.cc/AF7E-DNMP].

194. *Id.*; *see also* LIGHT, *supra* note 119, at 25 (describing the value of an IG to the "American

position desirable as a mechanism for providing that body with important information relating to the conduct of military operations and to "help in accountability for the military investments."[195] The Continental Congress thought the position would provide "assurances the military would remain subordinate to its authority,"[196] a noteworthy consideration in the context of cyber operations as well. Indeed, as Shirin Sinnar observed, "IGs may be most significant in areas where secrecy is greatest."[197]

The Office of Inspector General within the Defense Department was established formally in 1982.[198] The DoD OIG is categorized as an "establishment" entity, signifying the IG is appointed by the president and must be confirmed by the Senate. The president may remove the IG at any time in accord with the removal procedures outlined in the Section above. There have been eight Senate-confirmed IGs since the office's inception.[199]

Army" and other "departments"); *see also* GOLDSMITH, *supra* note 13, at 99 (tracing IGs back to George Washington and the Continental Army).

195. *History of the U.S. Army Inspector General*, *supra* note 193.

196. *Id.*

197. Sinnar, *Protecting Rights from Within?*, *supra* note 122, at 1074.

198. *See* Department of Defense Authorization Act 1983, Pub. L. No. 97-252, 96 Stat. 750 (creating a place for the OIG within the DoD); *see also* U.S. DEP'T OF DEF., DOD DIRECTIVE 5106.01, OFF. OF INSPECTOR GEN. (2020) (IG is "an independent and objective unit within DoD to conduct and supervise audits, investigations, evaluations, and inspections relating to the programs and operations of the DoD."). It may seem striking that the IGA of 1978 omitted the Department of Defense from the initial group of entities receiving statutory IGs. The IGA mandated creation of IGs in twelve federal departments (Agriculture, Education, Housing and Urban Development, Interior, Labor, Transportation, Community Services, Environmental Protection, General Services, NASA, Small Business, Veterans Affairs) and joined existing statutory IG offices in the departments of Health, Education, and Welfare, and Energy. MOORE & GATES, *supra* note 122, at 9. The Department of Defense, however, was not entirely excluded from the IGA. Section 8(a) placed semiannual reporting requirements, similar to those applying to statutory IG offices in other agencies, on the Department of Defense's existing audit, investigation, and inspection offices. Pub. L. No. 95-452, § 8(a), 92 Stat. 1105. The IGs for the Department of Homeland Security (2002) and for the Intelligence Community (2010) came later, in reforms relating to the 9/11 terrorist attacks and then the Edward Snowden revelations. JOHNSON & NEWCOMER, *supra* note 122, at 30–32.

199. The office has lacked a Senate-confirmed IG since January 2016, when Jon Rymer stepped down. Glenn Fine served as the acting IG from 2016 to 2020. *See* Anne Joseph O'Connell, *Watchdogs at Large*, BROOKINGS (Aug. 6, 2020), https://www.brookings.edu/research/watchdogs-at-large/ [https://perma.cc/3LX4-XP5R] (addressing the reason behind IG vacancies and explaining the possible consequences of reform). President Trump nominated Jason Abend on Apr. 6, 2020; however, the U.S. Senate took no action on that nomination. Indeed, several sources indicated concerns about Abend's qualifications for the position. Gordon Heddell, *Abend Unqualified to Be Defense Department Watchdog*, DEFENSENEWS (Sept. 29, 2020), https://www.defensenews.com/opinion/commentary/2020/09/29/abend-unqualified-to-be-defense-department-watchdog/ [https://perma.cc/W82Y-TLBV] (article by former DoD IG). Sean O'Donnell, who is the Senate-confirmed IG for the EPA, has been the acting IG for the Department of Defense since April 2020. According to the IG vacancy tracker maintained by oversight.gov, the position of the DoD OIG has been vacant for more than 2,500 days at the time of the writing of

This Section provides an overview of the DoD OIG, paying particular attention to how that office's attributes relate to the cyber oversight task. It provides an overview of the office's organizational structure and briefly summarizes the subordinate but separate IG offices within the department. It describes the roles and responsibilities of the DoD OIG and outlines the office's statutory authorities, agency directives, and congressional reporting responsibilities, noting distinctions and differences from the provisions governing IGs in other agencies and entities. Finally, this Section describes constraints placed on the activities of the DoD OIG due to the Defense Department's national security and intelligence activities.

1. The DoD OIG Organizational Structure

The office, which went through a significant departmental reorganization in 2019,[200] has more than fifty field offices located in the United States and overseas, and employs approximately 1,800 individuals.[201] The DoD OIG submitted an aggregate budget request for

---

this Article. *Inspector General Vacancies,* https://www.oversight.gov/ig-vacancies [https://perma.cc/4EE3-CWM6];. This concerning trend seems to be continuing. Although President Biden nominated Robert Stoch in November 2021, that nomination has been stalled in the Senate. *See* Rebecca Kheel, *Biden Names Pick for Pentagon Watchdog, Filling Job That's Been Vacant for Half a Decade*, MILITARY.COM (Nov. 15, 2021), https://www.military.com/daily-news/2021/11/15/biden-names-pick-pentagon-watchdog-filling-job-thats-been-vacant-half-decade.html [https://perma.cc/D2CH-QN6S]; Bryant Harris, *Dozen Pentagon Nominees Stalled as Senate Leaves for August Recess*, DEFENSENEWS (Aug. 8, 2022), https://www.defensenews.com/congress/2022/08/08/dozen-pentagon-nominees-stalled-as-senate-leaves-for-august-recess/ [https://perma.cc/7K4J-A5YU]; Glenn Fine, *After Six Years, It's Time to Confirm a Defense Department Inspector General*, GOV'T EXECUTIVE (Oct. 20, 2022), https://www.govexec.com/management/2022/10/after-six-years-its-time-confirm-defense-department-inspector-general/378686/ [https://perma.cc/E5FT-REBK]. More troubling is a June 2022 legal opinion by the GAO concluding that the currently acting IG is serving in that role without legal authorization. U.S. Gov't Accountability Off., Decision Letter on Dept. of Def. Off. of Inspector Gen.—Legality of Serv. of Acting Inspector Gen. (June 28, 2022) https://www.gao.gov/assets/730/721336.pdf.

200. *See* OFF. OF INSPECTOR GEN., U.S. DEP'T OF DEF., FISCAL YEAR 2021 BUDGET ESTIMATES OPERATION AND MAINTENANCE, DEFENSE-WIDE OFFICE OF INSPECTOR GENERAL (2020) [hereinafter IG Fiscal Year 2021] https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2021/budget_justification/pdfs/01_Operation_and_Maintenance/O_M_VOL_1_PART_1/OIG_OP-5.pdf [https://perma.cc/7WA6-VCT8] ("During FY 2019, the DoD OIG reorganized its three components that conduct program evaluations (Intelligence and Special Program Assessments, Policy and Oversight, and Special Plans and Operations) into a single Evaluations component. This reorganization was designed to improve the efficiency and effectiveness of the OIG's evaluations function.").

201. OFF. OF INSPECTOR GEN., U.S. DEP'T OF DEF., SEMIANNUAL REPORT TO THE CONG. OCT. 1, 2021 THROUGH MAR. 31, 2022 (2022), at 3 [hereinafter DoD OIG SAR (Oct. 1, 2021–Mar. 31, 2022)].

Fiscal Year 2021 of $395.508 million.[202] The DoD OIG includes the following sub-departments and entities: Office of General Counsel, Office of the Ombuds, Office of Legislative Affairs and Communications, Office of Equal Employment Opportunity, Office of Professional Responsibility, and Military Detachment. The chief of staff and principal deputy inspector general report to the IG. The following divisions report to the principal deputy inspector general: Audit, Evaluations, Defense Criminal Investigative Service, Administrative Investigations, Overseas Contingency, and the newly created Diversity and Inclusion/Military Insider Threat Office.[203]

In addition to the department-wide DoD OIG, the Department of Defense includes separate component-specific IG offices; these include the Defense Intelligence Agency, the National Geospatial Intelligence Agency, the National Security Agency, and the National Reconnaissance Office. In addition, each of the military services (Army, Navy, Air Force, and Marine Corps) has an IG appointed by the secretary of that service.[204] Finally, each of the eleven combatant commands has a dedicated IG, appointed by the associated commander, including U.S. Cyber Command.[205] These IGs report to their commander, and ultimately the DoD OIG.[206] The responsibilities of the combatant command IGs include: reporting on the state of various aspects of the command; performing investigations, inspections, evaluations, assistance, teaching, and training; coordinating with the DoD OIG on matters of mutual concern; inspecting and reporting on intelligence oversight programs; providing investigatory findings to other military departments; maintaining records; making recommendations; and reporting allegations

---

202. *See* IG Fiscal Year 2021, *supra* note 200 (reporting "aggregate Fiscal Year 2021 budget request for base and OCO for the operations of the DoD OIG is $395.508 million").

203. *See* DoD OIG SAR (Oct. 1, 2021–Mar. 31, 2022), *supra* note 201, at 4 (charting the departments and positions in the DoD OIG). The newest position in the office, the Deputy Inspector General for Diversity and Inclusion/Military Insider Threats, was established in 2021. *See* OFF. OF INSPECTOR GEN., U.S. DEP'T OF DEF., SEMIANNUAL REPORT TO THE CONGRESS OCT. 1, 2020 THROUGH MAR. 31, 2021, at i-ii [hereinafter DoD OIG SAR (Oct. 1, 2020–Mar. 31, 2021)] (announcing establishment of new position in DoD OIG as directed by Section 554 of the NDAA for FY2021, *supra* note 63).

204. *See* 10 U.S.C. § 7020 (Army IG); 10 U.S.C. § 8014(c)(1)(E), 8020 (Navy IG); 10 U.S.C. § 9020 (Air Force IG); 10 U.S.C. §§ 8014(c)(1)(E), 8020 (Marine Corps IG). These "service IGs," as they are often called, report to their commanding officer as well as to the DoD OIG. Their responsibilities include: inquiring into and reporting "upon the discipline, efficiency, and economy" of the department; performing "other duties prescribed by the Secretary or Chief of Staff;" recommending additional inspections; and cooperating fully with the DoD OIG. For a discussion on the interactions between the DoD OIG and the service IGs, *see Hearing Before the Subcomm. on Mil. Pers. of the H. Comm. on Armed Serv.*, *supra* note 190.

205. *See* U.S. DEP'T OF DEF., DOD DIRECTIVE 5106.04, COMBATANT COMMAND INSPECTORS GEN. (2020) (detailing the organization and management of the combatant commands).

206. *Id.*

to the DoD OIG.[207] Given their connection to the military's use of cyber operations and capabilities, the following component IG offices warrant further description: the National Security Agency Office of Inspector General (NSA OIG) and the Inspector General for U.S. Cyber Command (IG USCYBERCOM).

The NSA OIG was created as part of the 2010 amendments to the Inspector General Act of 1978.[208] In 2018, the NSA OIG employed approximately ninety-seven individuals.[209] The office's responsibilities include: conducting performance audits to "evaluate the economy, efficiency, and effectiveness of entities and programs and their internal controls," and financial audits to "determine the accuracy of the agency's financial statements and controls;"[210] performing inspections to "assess the efficiency and effectiveness of components across the agency;"[211] ensuring that "intelligence and intelligence-related functions [of the National Security Agency and Central Security Service (NSA/CSS)] comply with federal law, executive orders, and DoD and NSA policies, and that Agency activities are conducted consistently with civil liberties and U.S. person privacy protections;"[212] and investigating "a wide variety of allegations of waste, fraud, abuse, and misconduct involving NSA/CSS programs, operations, and personnel."[213]

The IG USCYBERCOM is a commander-appointed position that

---

207. *Id.*

208. *See* Intelligence Authorization Act for the Fiscal Year 2010, Pub. L. No. 111-259, § 431(a), 124 Stat. 2731 (amending 5 U.S.C. app. 3 § 8G(a)(2) and defining NSA as a "designated federal entity" with IG appointed by agency head); *see also* Intelligence Authorization Act for Fiscal Year 2014, Pub. L. No. 113-126, § 402(1), 128 Stat. 1408, (amending 5 U.S.C. app. 3 §§ 8G(a)(2) & (12) and designating NSA as an "establishment" IG subject to the subsequent appointment provisions). *See* Margo Schlanger, *Intelligence Legalism and the National Security Agency's Civil Liberties Gap,* 6 HARV. NAT'L SEC. J. 112, 142–44 (2015) [hereinafter, Schlanger, *Intelligence Legalism*] (providing overview of the NSA IG office).

209. Jory Heckman, *NSA IG Looks to Make Agency "Transparent Where We Can Be",* FED. NEWS NETWORK (Nov. 19, 2018, 6:50 PM), https://federalnewsnetwork.com/agency-oversight/2018/11/nsa-ig-looks-to-make-agency-transparent-where-we-can-be/ [https://perma.cc/V4PR-M3PY].

210. *Audits,* NAT'L SEC. AGENCY OFF. OF THE INSPECTOR GEN., https://oig.nsa.gov/OIG-Divisions/Audits/ [https://perma.cc/EEM9-4595].

211. *Inspections*, NAT'L SEC. AGENCY OFF. OF THE INSPECTOR GEN., https://oig.nsa.gov/OIG-Divisions/Inspections/ [https://perma.cc/5N9K-2JKA].

212. *Intelligence Oversight*, NAT'L SEC. AGENCY OFF. OF THE INSPECTOR GEN., https://oig.nsa.gov/OIG-Divisions/Intelligence-Oversight/ [https://perma.cc/KBG4-MZPP].

213. *Investigations*, NAT'L SEC. AGENCY OFF. OF THE INSPECTOR GEN., https://oig.nsa.gov/OIG-Divisions/Investigations/ [https://perma.cc/9LNX-QXSF] ("The OIG initiates investigations based upon information from a variety of sources, including complaints made to the OIG Hotline; information uncovered during its inspections, audits, and reviews; and referrals from other Agency organizations..... The NSA OIG Hotline provides a mechanism for whistleblowers to make protected communications, and the Investigations Division carefully examines all credible claims of whistleblower reprisal.").

serves on the command staff.[214] The statute describes the position's responsibilities to include "conduct[ing] internal audits and inspections of purchasing and contracting actions through the cyber operations command and such other inspector general functions as may be assigned."[215] The website, however, offers a more expansive view of the position's responsibilities, noting the following charge to the IG USCYBERCOM: to "assess the efficiency of USCYBERCOM activities and processes, and also validate command compliance with public law and Department of Defense (DoD) requirements and policies."[216] Of particular interest in the area of cyber oversight mechanisms, the IG USCYBERCOM is tasked with coordinating and conducting inspections and audits to ensure compliance with public law, governing regulations and standards, evaluating command processes and recommending areas for improvement; and executing inspection programs to ensure command compliance with the DoD Intelligence Oversight program and Executive Order 12333.[217] As a combatant command IG, the office is not subject to the annual reporting requirements for unclassified or publicly accessible summaries of work.[218]

A final organizational note is in order to acknowledge the various interagency aspects of the DoD OIG's work, most notably in two partnership entities. The first of these is the Council of Inspectors General on Integrity and Efficiency (CIGIE).[219] The council was established in the Inspector General Reform Act of 2008 as an independent entity within the executive branch.[220] Its mission is to "address integrity, economy and effectiveness issues that transcend individual Government agencies and aid in the establishment of a professional, well-trained and highly skilled workforce in the Offices of Inspectors General."[221] CIGIE is responsible for oversight.gov, among

214. *See* 10 U.S.C. § 167b(C)(3)(C) ("The staff of the commander shall include an inspector general who shall conduct internal audits and inspections of purchasing and contracting actions through the cyber operations command and such other inspector general functions as may be assigned.").

215. *Id.*

216. *Inspector General,* U.S. CYBER COMMAND, https://www.cybercom.mil/About/Inspector-General/ [https://perma.cc/UN6Q-JTDG].

217. *Id.*

218. *See* DOD DIRECTIVE 5106.01, *supra* note 198 (listing the responsibilities and authorities of the OIG DoD); DIRECTIVE 5106.04, *supra* note 205.

219. *What Is CIGIE?*, COUNCIL OF THE INSPECTORS GEN. ON INTEGRITY AND EFFICIENCY, https://www.ignet.gov/ [https://perma.cc/598M-MJ4S].

220. Inspector General Reform Act of 2008, Pub. L. No. 110-409, 122 Stat. 4306 (codified as amended in U.S.C. app. § 11).

221. *Council of the Inspectors General on Integrity and Efficiency,* OVERSIGHT.GOV, https://www.oversight.gov/inspectors-general/council-inspectors-general-integrity-and-efficiency [https://perma.cc/L2JK-84ZM].

other tasks.[222] Each year, the council prepares a report that identifies management and performance challenges facing multiple federal agencies.[223]

The second partnership is the Intelligence Community Inspectors General Forum, which was established in 2010.[224] The forum's "mission is to promote and further collaboration, cooperation and coordination among the Inspectors General of the Intelligence Community of the United States."[225] The forum is led by the Intelligence Community Inspector General, and it includes representatives from IG offices in CIA, DHS, DIA, DoD, DOE, DOJ, State, Treasury, NGA, NRO, NSA and FBI.[226] Forum members meet quarterly and its activities focus on:

> [s]upporting the IC IG in the performance of audits, inspections, evaluations and investigations within their respective departments and agencies; strengthening the collective role and effectiveness of IG's throughout the Intelligence Community and to enhance the value of IGs' activities in support of the National Intelligence Strategy; and Achieving optimal utilization of resources, to increase efficiency and to avoid duplication of effort among the Inspectors General of the Intelligence Community.[227]

With the organizational structure of the DoD OIG and its component entities as a backdrop, albeit a complicated one, let's turn now to consideration of the office's authorities, activities, and reporting mechanisms.

2. DoD OIG Authorities, Activities and Reporting Mechanisms

The DoD OIG, often called the Pentagon's watchdog, has a broad mandate, which includes overseeing all defense spending as well as management oversight of IG offices in other defense-related components and commands. According to the semiannual report released on May 27, 2022, the mission of the DoD OIG is "to detect and deter fraud, waste, and abuse in DoD programs and operations; promote the economy, efficiency, and effectiveness of the DoD; and help ensure ethical conduct

---

222. *About Oversight.gov*, OVERSIGHT.GOV, https://www.oversight.gov/about [https://perma.cc/Y6EN-8RAY].

223. *See, e.g.*, COUNCIL OF THE INSPECTORS GEN. ON INTEGRITY AND EFFICIENCY, TOP MANAGEMENT AND PERFORMANCE CHALLENGES FACING MULTIPLE FED. AGENCIES (Feb. 2021), https://www.ignet.gov/sites/default/files/untracked/TMPC_report_02022021.pdf [https://perma.cc/A4LH-HHML] (reporting the "key areas of concern").

224. *ICIG FAQs*, OFF. OF THE DIR. OF NAT'L INTEL., https://www.dni.gov/index.php/who-we-are/organizations/icig/icig-about-us/icig-faqs [https://perma.cc/VRS3-9YWN].

225. *IC Inspectors General Forum*, OFF. OF THE DIR. OF NAT'L INTEL., https://www.dni.gov/index.php/who-we-are/organizations/icig/icig-features/367 [https://perma.cc/YZ83-FYBR].

226. *Id.*

227. *Id.*

throughout the DoD."[228] The office accomplishes this mission through a varied set of functions and responsibilities, which include to:

> Recommend policies for and conduct, supervise, or coordinate other activities for the purpose of promoting economy and efficiency, and preventing and detecting fraud, waste, and abuse in DoD programs and operations; serve as the principal advisor to the Secretary of Defense in matters of DoD fraud, waste, and abuse; provide policy direction for and conduct, supervise, and coordinate audits and investigations relating to the programs and operations of the DoD; ensure that the Secretary of Defense and the Congress are fully informed of problems in the DoD; review existing and proposed legislation and regulations relating to programs and operations of the DoD in regard to their impact on economy and efficiency and the prevention and detection of fraud, waste, and abuse in the DoD; coordinate relationships with Federal agencies, state and local government agencies, and non-governmental entities in matters relating to the promotion of economy and efficiency and detection of fraud, waste, and abuse; transmit a semiannual report to Congress that is available to the public.[229]

The DoD OIG is governed by the general provisions of the Inspector General Act of 1978 and several provisions specific to the Department of Defense as well as executive orders and agency directives.[230] Pursuant to these authorities, the DoD OIG, similar to all IGs, has the authority to conduct audits, evaluations, administrative inspections, and criminal investigations.[231] In addition, the DoD OIG has oversight responsibility for certain overseas contingency operations, reviews proposed legislation, regulations, executive orders and department directives, and conducts congressional engagement in the form of informal inquiries and hearings.[232] The semiannual reports provide a sense of the scope and scale of the DoD OIG's work. According to the semiannual report for the period from October 1, 2020, to March 31, 2021, the DoD OIG issued fifty audit reports and eighteen evaluation reports (which included 190

228. DoD OIG SAR (Oct. 1, 2021–Mar. 31, 2022), *supra* note 201, at 2.

229. *Id.*

230. *See* 5 U.S.C. app. 3 § 2 (referencing addition of Department of Defense to list of departments and agencies with an IG); § 8 (listing additional provisions specific to the DoD OIG); DOD DIRECTIVE 5106.01, *supra* note 198 (describing DoD OIG's "mission, organization and management, responsibilities and functions, relationships and authorities"); DOD DIRECTIVE 5106.04, *supra* note 205 (describing "established policy and the responsibilities and functions of Defense inspectors general").

231. *See* DOD OVERSIGHT PLAN FY2021, *supra* note 183 ("This broad mandate encompasses analysis that may be compliance based (i.e., did department comply with internal policy, statutory requirements, congressional reporting), focused on program efficiency and/or effectiveness (i.e., did program meet its objectives), or prospective (i.e., reviews of proposed legislation, regulations, executive orders, directives).").

232. *See, e.g.,* DoD OIG SAR (Oct. 1, 2020–Mar. 31, 2021), *supra* note 203.

recommendations to the DoD for improvement); completed 237 criminal investigations, some conducted jointly with other law enforcement organizations, resulting in 93 arrests, 126 criminal charges, 125 criminal convictions,"; publicly released two administrative investigation reports; and reviewed 145 existing and proposed regulations.[233] During this period, the DoD OIG also issued five quarterly reports on overseas contingency operations in accord with its lead IG responsibilities.[234] The office received more than one hundred congressional inquiries and conducted more than eighty-five engagements with members of Congress and congressional staff during the six-month reporting period.[235]

The DoD OIG is subject to various reporting requirements, some appliable to all IG offices and others specific to the DoD OIG. These include: semiannual reports; annual implementation updates; fast action reports for particularly egregious violations; joint biennial reports relating to the Cybersecurity Information Sharing Act; annual reports mandated by the Federal Information Security Modernization Act (FISMA); annual reports identifying top management challenges facing the entire Department of Defense; and annual oversight planning reports describing the OIG's anticipated activities in the upcoming year.[236]

3. Special Provisions and Restrictions on the DoD OIG

In addition to the provisions applicable to all IGs, the DoD OIG is subject to additional responsibilities and limitations on the scope of its authority. The additional responsibilities include: heightened reporting requirements, generally with regard to contract audits and external peer reviews, in the semiannual reports;[237] specific guidance on the committee recipients of the reports (Senate Armed Services Committee, the House Armed Services Committee, the Senate Homeland Security and Governmental Affairs Committee, and the House Committee on Oversight and Government Reform); specific instructions on flagrant action reports (or seven-day letters);[238] unique subpoena-related requirements;[239] and specifications on the DoD OIG's advisory role and ability to exercise discretion in initiating activities the IG "considers

233. *Id.* at i, v-vi.
234. *Id*. at i.
235. *Id*. at 48 ("The DoD OIG routinely engages with Congress to proactively share information regarding DoD OIG oversight work; participate in congressional briefings and hearings; communicate DoD OIG needs and concerns; and respond to inquiries and requests from congressional committees, individual Members of Congress, and congressional staff.").
236. For a fuller description of each of these types of reports, *see supra* Section II.A.3.
237. 5 U.S.C. app. 3 § 8(f)(1).
238. 5 U.S.C. app. 3 § 8(f)(2).
239. 5 U.S.C. app. 3 § 8(i).

appropriate."[240]

The provision also imposes two limitations on the DoD OIG. First, this provision limits who can serve as DoD OIG, prohibiting a member of the armed forces, active or reserve, from serving in the role.[241] Second, and most notably, the provision places a significant constraint on the DoD OIG, one not present in most other IG offices. Under this provision, the secretary of defense may block IG activities when they relate to certain sensitive topics or national security matters, including sensitive operational plans, intelligence matters, counterintelligence matters, ongoing criminal investigations by other administrative units, or other matters the disclosure of which would constitute a serious threat to national security."[242] Should the secretary of defense determine such action is necessary to "preserve the national security interests of the United States," the Secretary may prohibit the IG from "initiating, carrying out, or completing any audit or investigation," "accessing information," or "issuing any subpoena."[243] Importantly, however, if the secretary of defense invokes this prohibition, the secretary must report the fact of the invocation to the relevant congressional committees within thirty days, and within an additional thirty days, the secretary must submit to the committee a statement explaining the reasons for exercising the prohibition power.[244] Although this provision creates a sweeping exception to the independence provisions in Section 3(a) of the IGA, it has been rarely, if ever, invoked by the secretary of defense.[245]

Of course, each IG office is unique and, to some extent, a creature of its department or agency. Inspectors general define the mission of their offices dependent upon a variety of factors, including their understanding of congressional intent in the IGA, the direction provided by higher level IG coordinating groups and entities, the expectations of the agency head (in this case the secretary of defense), the particular challenges and problems facing the agency, and the individual IG's professional

240. 5 U.S.C. app. 3 § 8(c).
241. 5 U.S.C. app. 3 § 8(a).
242. 5 U.S.C. app. 3 § 8(b)(1)–(2).
243. 5 U.S.C. app. 3 § 8(b)(2). Similar restrictions exist on the IGs for the Department of Justice, § 8E(a), Department of Homeland Security, § 8I(a)(2), the Intelligence Community, § 8G(d)(2)(A-B), and the CIA, 50 U.S.C § 3033. For a discussion of these prohibitions, *see* Sinnar, *Protecting Rights from Within?, supra* note 122, at 1035-36.
244. 5 U.S.C. app. 3 § 8(b)(3)–(4) (listing those requiring notice as "Committees on Armed Services and Governmental Affairs of the Senate and the Committee on Armed Services and the Committee on Government Reform and Oversight of the House of Representatives and to other appropriate committees or subcommittees of the Congress.").
245. *See* Sinnar, *Protecting Rights from Within?*, *supra* note 122, at 1036 (concluding so much based on extensive interviews with IG offices through 2012); *see also* GOLDSMITH, *supra* note 13, at 99–108 (noting that CIA agency head allowed an IG investigation to go forward and did not invoke the prohibition).

background and experiences.[246] And of course, the individuals holding the position of IG often "vary in their aggressiveness, expertise, and influence."[247] This Section has summarized the unique drivers and constraints shaping the DoD OIG and provided context for understanding the office's distinctive ability to conduct oversight of the U.S. government's expanding arsenal of cyber authorities and capabilities, the topic of the next Section.

C. The DoD OIG's Contributions to the Cyber Oversight Task

As described above, the recent expansion of the U.S. military's cyber capabilities has been paired with a feeble and disjointed congressional oversight framework, creating a separation of powers mismatch with regard to military cyber operations. Recognizing Congress's inability to provide appropriate oversight of cyber operations, there is a need to identify alternative players able to answer the cyber oversight call. The DoD OIG should be among the list of top draft picks for this team of alternatives. It is well-positioned to fill the gaps and to provide the level of oversight and informed debate necessary to ensure the use of these consequential tools and capabilities complies with the relevant legal authorities as well as department policy. In the course of this work, the DoD OIG also is able to flag concerning operational and interpretative issues.

The DoD OIG is well-suited to the cyber oversight task due to a general alignment with public law values[248] and the following specific attributes unique to the office: (1) a special perch within the Department of Defense and a powerful investigatory toolkit; (2) an ability to balance the need for secrecy with illumination of wrongdoing; (3) a growing role as independent advisor and policy evaluator within the department; and (4) the ability to guide congressional oversight efforts and focus. This Section will explore these attributes in turn.

1. A Special Perch

One of the chief advantages of IGs is that they are "ideally situated to detect problems that would otherwise go undetected," and this ability derives from their special perch within the agency and the potent tools at their disposal.[249] IGs were created to provide a critical internal oversight function by identifying wasteful, wrongful, and illegal activities in their agencies. To accomplish this task, Congress crafted a special perch for

246. MOORE & GATES, *supra* note 122, at 43.
247. *See* Schlanger, *Intelligence Legalism, supra* note 208, at 144.
248. *See supra* note 164 and sources cited therein on how IGs serve public law values.
249. MOORE & GATES, *supra* note 122, at 48.

the IG to occupy within the agency. This perch provides advantages over the usual congressional oversight mechanisms, including access to information usually protected by separation of powers obstacles and at a depth and scope more comprehensive than Congress's usual efforts. By design, the agency perch allows the IG to surmount the usual separation of powers objections proffered to block congressional, judicial, or public inquiries.[250] These objections are eliminated, or minimized, when the information is sought as part of IG activity.

The special perch also enables the IG to get "deep inside the presidency," and to acquire a comprehensive and wholistic understanding of the matter under review.[251] Jack Goldsmith describes the advantages of this delegation: "Congress in effect delegates its initial oversight function to the IG, who can quickly gather a much more complete understanding of executive branch activity than Congress itself could have."[252] Put bluntly, Congress is simply not able to achieve a comparable level of access or understanding through its usual oversight mechanisms. For example, with regard to the Defense Department's use of cyber tools and capabilities, the DoD OIG is able to access information relating to relevant legal interpretations, compliance with internal policies, as well as compliance with external reporting requirements.

In addition to the special perch, Congress provided IGs with an arsenal of information-gathering tools designed to identify concerning, problematic, and abusive behavior. The IG is charged with keeping the head of the establishment or agency and Congress "fully and currently informed about problems and deficiencies relating to the administration of such programs and operations and the necessity for and progress of corrective action."[253] To accomplish this objective, as well as the congressional notice task, IGs have a bevy of investigatory powers which they deploy in three principal activities: investigations, audits, and inspections or evaluations.[254]

For the cyber oversight task, the programmatic tools (particularly

250. GOLDSMITH, *supra* note 13, at 105 (describing common objections based in claims of classified information, executive privilege, and attorney-client privilege, and obstacles presented by the state secrets and political question doctrines); *cf.* Andrew McCanse Wright, *Executive Privilege and Inspectors General*, 97 TEX. L. REV. 1295 (2019) (exploring how the ability of IGs to access agency materials can put agency executive privilege claims at risk, thus impacting effectiveness of IGs).

251. GOLDSMITH, *supra* note 13, at 104–05.

252. *Id.* at 105.

253. 5 U.S.C. app. 3 § 2(3).

254. *See supra* Section II.A. (describing IG's investigatory tools); *see also* APAZA, *supra* note 122, at 12–14 (comparing the three primary mechanisms by which OIGs accomplish their objectives); FRANCIS, *supra* note 122, at 7–9 (describing types of IG reviews and comparing differences in terms of quality standards, scope of analysis, and type of analysis).

inspections and evaluations) may be the most relevant. These tools examine the policies, operations, regulations, or legislative implications of a given program. These evaluative activities tend to fall into two categories: those that assess compliance with applicable laws, regulations, and internal policies and those that assess "how entire programs might be amended or redirected."[255] For example, IG inspections in the cyber context could assess whether the department's use of its cyber authorities conforms to the congressional text, whether such operations comply with the approval requirements of the relevant presidential and agency/command directives, whether they comply with the relevant rules of engagement, and whether the congressional reporting, notices and briefings are occurring as required by statute. These inspections also could evaluate whether the use of cyber capabilities and operations are in alignment with the national cyber strategy endorsed by the president and/or Congress. In addition to identifying compliance, accountability, or transparency problems, the OIG also has the ability to recommend corrective action, including whether additional guardrails on the use of cyber capabilities may be desirable or necessary. The ability to issue not only findings, but also recommendations based on those findings allows IGs to offer "broad proposals for change."[256]

The special perch and accompanying toolkit statutorily allocated to the DoD OIG provide a unique capacity to identify challenges and problems in the military's use of its cyber capabilities. In addition, they provide mechanisms for gathering and disseminating important information to those in policy-making positions, including the relevant congressional committees and the agency leadership. The access provided by the IG's perch within the agency is comparable to that of other entities seen as substitutes for the checking function generally provided by Congress and the courts. The value of what Ashley Deeks calls "surrogates" is that they have access to highly classified and secret information by virtue of their position or status, and thus are able to highlight abusive executive branch actions that otherwise would go unchecked.[257] In some circumstances, these surrogates may actually be better positioned than the traditional interbranch checking mechanisms to shape executive branch behavior.

---

255. APAZA, *supra* note 122, at 13.

256. LIGHT, *supra* note 119, at 19.

257. Deeks, *Secrecy Surrogates*, *supra* note 10, at 1403, 1413–14, 1417. For a review of current instances where the DoD OIG is utilizing this perch and designated toolkit in support of the oversight task for military cyber operations, *see infra* Section II.D.

2. Ability to Balance Secrecy with Illumination

The second characteristic that makes the DoD OIG well-suited to the cyber oversight task is the office's ability to balance the government's legitimate need for secrecy with the public's interest in identifying wrongdoing, abuse of power, or compliance failures. The challenge of appropriately aligning the government's interest in secrecy with democratic norms and values is not new.[258] Military cyber operations highlight this dilemma in stark terms. In almost every instance, military cyber operations require speed, concealment, and secrecy to achieve the intended effects. As such, pre-approval from Congress is not desirable, and possibly constitutionally suspect.[259]

Similarly, an elaborate pre-approval interagency process, another common mechanism for providing internal oversight and vetting of executive branch decision-making, is also undesirable and unworkable. Indeed, many officials and commentators heralded the policy changes included in NSPM 13 for eliminating a cumbersome interagency process they saw as inhibiting the U.S. government's ability to respond effectively to cyber threats.[260] Thus, the government's interest in secrecy is strong in the area of cyberspace operations. However, the need for oversight is equally compelling given the potential for a cyber operation to cause catastrophic effects (whether intended or unintended), escalation of a conflict, as well as significant adverse impacts on intelligence and diplomatic efforts. Thus, "IGs may be most significant in areas where secrecy is greatest."[261]

The DoD OIG is able to provide oversight of military cyber operations in a manner that appropriately protects secrecy. The statute governing the DoD OIG expressly acknowledges the need for secrecy given the agency's responsibilities and crafts the DoD IG's responsibilities accordingly. Section 8 provides additional responsibilities and places special limits on the DoD OIG.[262] The statute requires the DoD OIG to report directly to the secretary of defense when the IG's activities seek access to information that involves "sensitive operational plans; intelligence matters; counterintelligence matters; ongoing criminal investigations by other administrative units of the Department of Defense related to national security; or other matters the disclosure of which

258. *See, e.g.,* Deeks, *Secrecy Surrogates*, *supra* note 10, at 1399–1400, 1411, 1454, 1466 (describing value that surrogates bring as they are "positioned to 'promote[] responsible executive action' without revealing the secrets themselves").
259. *See supra* Section I.C. (discussing challenges in current reporting framework).
260. *See supra* Section I.A.3. (summarizing responses to NSPM 13).
261. Sinnar, *Protecting Rights from Within?*, *supra* note 122, at 1074.
262. 5 U.S.C. app. 3 § 8.

would constitute a serious threat to national security."[263] In addition, the secretary of defense may limit or prohibit IG access to information and may prohibit the entire investigation, audit, or inspection if the matter falls into one of the categories listed above and "if the secretary determines that such prohibition is necessary to preserve the national security interests of the United States."[264] At first glance, this prohibition authority appears to give the secretary of defense a fairly big club to block IG activities.[265] However, the statute includes two checks on potential abuses of this authority. First, the statute requires the IG for the Defense Department to notify Congress within thirty days if the secretary halts or prohibits any IG activity under the prohibition provision.[266] Significantly, the statute then requires that the notice to Congress be followed, within thirty additional days, by an explanation of the reasons for so doing by the secretary.[267] Second, the threat of a seven-day letter also provides a mechanism for preventing abuses of this provision.[268] Thus, the statutory requirements provide mechanisms for bringing to Congress's attention matters of significant oversight concern while appropriately respecting the department's legitimate need for secrecy. The effectiveness of these mechanisms may be best observed in noting how rarely the power has been used by the secretary of defense.[269]

The DoD OIG works comfortably within secrecy-imposed constraints while fulfilling its statutorily mandated duty of shining a light on areas of concern and wrongdoing through the use of investigations, audits, and inspections. Thus, the DoD OIG is uniquely positioned to identify problems, and to then bring them to the attention of those entities—the agency head or Congress—that have the capacity and authority to rectify and correct. In many ways, one of the purposes of the IGA was to give internal executive branch agents, through the offices of IGs, a mandate to identify problems that fall beyond Congress's oversight abilities. This ability to effectively balance the secrecy-transparency scale is especially critical in the context of military cyber operations.

---

263. 5 U.S.C. app. 3 § 8(b)(1).
264. 5 U.S.C. app. 3 § 8(b)(2).
265. *See infra* Section II.E (discussing potential limits on the DoD OIG's cyber oversight role).
266. 5 U.S.C. app. 3 § 8(b)(3) (identifying the "Committees on Armed Services and Governmental Affairs of the Senate . . . the Committee on Armed Services and the Committee on Government Reform and Oversight of the House of Representatives and . . . other appropriate committees or subcommittees of the Congress").
267. 5 U.S.C. app. 3 § 8(b)(4).
268. *See supra* notes 175–179 and accompanying text (describing seven-day reporting requirement and practices).
269. *See* Sinnar, *Protecting Rights from Within?*, *supra* note 122, at 1035–36 (reporting on infrequent use of prohibition authority).

3. Growing Role as Policy Evaluator and Independent Advisor

A third reason the DoD OIG is well-positioned to check the U.S. military's use of its cyber capabilities is due to the growing role of evaluative work in the IG portfolio. IGs are moving—indeed have moved—well beyond the tasks of identifying fraud, waste, and abuse and instead are more often engaged in reviewing emerging policy areas. The 1978 IGA anticipated such a role, and the report accompanying the IGA looked favorably upon IG involvement in "reviewing the existing legislation and proposed regulations in order to offer guidance concerning their likely impact on fraud and abuse control as well as economy and efficiency."[270] The conference report notes that the "committee believes that this is a particularly vital role for the inspector and auditor general to play. The inspector and auditor general should not simply investigate fraud and waste after they have occurred. Rather, this preventative and deterrent function . . . should be crucial."[271] Only a few years after passage of the IGA, scholars were commenting on the growth in this aspect of the IG role. "The IGs are no longer simply observing program operations to detect isolated problems. Instead, they are proposing changes in procedures that will alter the character of the product or service being delivered, and therefore the value of the program."[272] The intended impact of IG-related work covers a spectrum, from controlling costs to holding employees accountable to shaping agency policy to improving processes and policies and, finally, to supporting achievement of the agency mission. The corelating signs of achievement for these impact objectives run the gambit from cost savings to strengthened internal controls to changes in law, policy, and regulations.[273] The evaluative nature of IG work is best reflected in inspections that "examine the extent to which individual federal programs or installations are complying with applicable laws, regulations, and policies, while other inspections determine how entire programs might be amended or redirected."[274]

The policy evaluator and advisor role is particularly critical in national security, law enforcement, and intelligence entities. As chronicled in the work of Shirin Sinnar, IGs in these entities are uniquely positioned to influence internal executive branch policy in a way that Congress is not.

---

270. S. REP. NO. 95-1071, at 8 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 2676, 2683.

271. *Id.*

272. MOORE & GATES, *supra* note 122, at 29.

273. *See* JOHNSON & NEWCOMER, *supra* note 122, at 164–65 fig. 6-1.

274. APAZA, *supra* note 122, at 13; *see also* LIGHT, *supra* note 119, at 19 (noting that ability of IGs to issue not only findings, but recommendations for resolution and improvement based on those findings leads to "broad proposals for change that emerge from audits, investigations, and evaluations.").

She explains that the role of IGs in national security and intelligence community entities has evolved since 9/11 from a focus on mismanagement, waste, and audits to inspections of privacy and civil rights abuses, and evaluation of internal policies and guidelines.[275] The expansion of the IG's role in these areas is credited to the comprehensive and independent nature of the IG reports, the public release of the IG reports (even if in redacted form), and the subsequent media coverage of IG findings and recommendations in those reports.[276]

Examples of IGs influencing internal rules and policies include: changes made to the FBI's Foreign Intelligence Surveillance Act (FISA) warrant application process after the DOJ IG's report on the Carter Page/Crossfire Hurricane Investigation;[277] changes made to the CIA's rendition and interrogation programs after the CIA IG's report identified abuses in the program's administration, questioned its efficacy, and doubted the legal basis offered for the program;[278] changes made to the Defense Department's use of Threat and Local Observation Notice (TALON) reports after a DoD IG investigation into whether the reports complied with intelligence laws and department regulations;[279] changes to the Justice Department's "hold until cleared" detention policy after a DOJ IG investigation into individual allegations of detainee abuse;[280] and

---

275. Sinnar, *Protecting Rights from Within?*, *supra* note 122, at 1032.

276. *See id.* at 1043 ("The reports drew tremendous media attention, including front-page coverage in major national newspapers, and Congress held several hearings questioning Justice Department officials on the detentions, with members of both parties praising the OIG report").

277. *See, e.g.*, OFF. OF INSPECTOR GEN., U.S. DEP'T OF JUST., REVIEW OF FOUR FISA APPLICATIONS AND OTHER ASPECTS OF THE FBI'S CROSSFIRE HURRICANE INVESTIGATION (2019); Elizabeth Goitein, et al., *Top Experts Analyze Inspector General Report Finding Problems in FBI Surveillance*, JUST SECURITY (Apr. 27, 2020), https://www.justsecurity.org/69879/top-experts-analyze-inspector-general-report-finding-problems-in-fbi-surveillance/ [https://perma.cc/U2L9-6RX5]; David Kris, *Further Thoughts on the Crossfire Hurricane Report,* LAWFARE (Dec. 23, 2019, 4:19 PM), https://www.lawfareblog.com/further-thoughts-crossfire-hurricane-report [https://perma.cc/A5EF-GW7A]; Garret M. Graff, *So Much for the Deep State Plot against Donald Trump,* WIRED (Dec. 9, 2019, 3:44 PM), https://www.wired.com/story/ig-report-fbi-trump-deep-state/ [https://perma.cc/PQ8Y-FQYA]; Natasha Bertrand & Darren Samuelson, *Inspector General's Report on Russia Probe: Key Takeaways,* POLITICO (Dec. 9, 2019, 1:17 PM), https://www.politico.com/news/2019/12/09/inspector-generals-report-russia-key-takeaways-079030 [https://perma.cc/VV9P-GGZQ].

278. *See* Sinnar, *Protecting Rights from Within?*, *supra* note 122, at 1047–49 ("Despite the renewed legal authority for enhanced interrogations, the CIA claims that it has not waterboarded any detainees since 2003, and some commentators have credited the inspector general investigation for the cessation of the practice.").

279. OFF. OF INSPECTOR GEN., U.S. DEP'T OF DEF., THE THREAT AND LOCAL OBSERVATION NOTICE (TALON) REPORT PROGRAM (2007); Sinnar, *Protecting Rights from Within?*, *supra* note 122, at 1053.

280. OFF. OF INSPECTOR GEN., U.S. DEP'T OF DEF., THE SEPTEMBER 11 DETAINEES: A REVIEW OF THE TREATMENT OF ALIENS HELD ON IMMIGRATION CHARGES IN CONNECTION WITH THE INVESTIGATION OF THE SEPTEMBER 11 ATTACKS 195 (2003); Sinnar, *Protecting Rights from Within?*, *supra* note 122, at 1043.

the establishment of tighter cybersecurity standards for supply chain vendors after a DoD IG report on vulnerabilities.[281] More recent examples of IG reviews likely to lead to changes in department policy and legal interpretation include an IG review of the use of federal law enforcement personnel in responding to protest activity and civil unrest during the summer of 2020 in Washington, D.C., and in Portland, Oregon,[282] an IG review of the DOJ's use of subpoenas at the end of the Trump administration to collect data on members of Congress and the media,[283] and a recent request for an IG investigation into the DHS's surveillance of money transfers by U.S. citizens.[284] These examples reveal the key role IGs play in initiating and supporting reform efforts at the governance, managerial, policy, and legal levels.

Not surprisingly, this shift from IGs assessing whether the agency followed the applicable legal or regulatory requirement to a scenario where the IG assesses the content of the applicable law, policy, or agency regulation is not a welcome development in all corners.[285] Nonetheless, this shift has occurred and it is critical to appreciate how this shift in responsibility—from identifying waste and mismanagement to being the "fount of accountability inside the presidency's secretive national security bureaucracy"[286]—signifies a larger role for IGs in evaluating the efficacy and substance of various policies relating to the use of and constraints on cyber operations. This shift, and the examples above, reveal that IGs constitute a rich resource for illuminating the policies in need of change. As such, they will be able to effectively focus the defense secretary's attention on cyber topics and programs in need of review and reform.

---

281. OFF. OF INSPECTOR GEN., U.S. DEP'T OF DEF., DODIG-2021-034, SUMMARY OF REPORTS ISSUED REGARDING DEPARTMENT OF DEFENSE CYBERSECURITY FROM JULY 1, 2019 THROUGH JUNE 30, 2020 (2020); Lucas Truax, *The Department of Defense Is Serious about Cybersecurity*, LINKEDIN PULSE (Mar. 25, 2020), https://www.linkedin.com/pulse/department-defense-serious-cybersecurity-lucas-truax/ [https://perma.cc/U9UF-8UBE]; Dawn E. Stern & Ryan Carpenter, *Into the Unknown: DOD's Long-awaited Cybersecurity Rule Leaves Critical Questions Unanswered,* LEXOLOGY (Oct. 5, 2020), https://www.lexology.com/library/detail.aspx?g=fbf41783-86c9-456e-8418-9241ccf5fa46 [https://perma.cc/PK73-979Y].

282. *DOJ OIG Announces Initiation of Work*, DEP'T OF JUST. (July 23, 2020), https://oig.justice.gov/news/doj-oig-announces-initiation-work [https://perma.cc/YS8E-5GYF].

283. Charlie Savage, *Justice Dept. Will Toughen Rules for Seizing Lawmakers' Data, Garland Says*, N.Y. TIMES (June 14, 2021), https://www.nytimes.com/2021/06/14/us/politics/leak-investigations-justice-department.html [https://perma.cc/LVB8-ZKKE].

284. Max Jaeger, *DHS Surveilled US Citizens' Money Transfers Senator Says*, LAW 360 (Mar. 8, 2022, 11:56 AM), https://www.law360.com/articles/1471737/dhs-surveilled-us-citizens-money-transfers-sen-says [https://perma.cc/LYA8-ZZBG].

285. *See* Schlanger, *Intelligence Legalism*, *supra* note 208, at 144 n.134 (describing efforts to limit NSA IG's portfolio).

286. GOLDSMITH, *supra* note 13, at 104.

4. Ability to Guide Congressional Committee Attention

The final characteristic that makes the DoD OIG well-suited to the cyber operations oversight task is the office's ability to draw a road map for congressional committee attention and action. As noted above, Congress is struggling to grasp the scope and scale of the executive branch's use of cyber operations.[287] The legislative branch's difficulties stem from a number of institutional challenges, including a lack of cyber literacy or comprehensive understanding of the technologies that allow the use of cyber operations as well as a lack of time to focus deeply on the intricate nature of cyber operations and their ability to avoid neat categorization. The DoD OIG is able to gap fill for Congress through the reports it provides. The paragraphs below describe the IG's annual reporting tasks best suited to offer insight and guidance into the Defense Department's use of its offensive cyber capabilities.

Top DoD Management Challenges Report (Annual). Pursuant to the Reports Consolidation Act of 2000, each IG is required to prepare an annual statement that summarizes what the IG considers to be the "most serious management and performance challenges facing the agency" and to assess the agency's progress in addressing those challenges.[288] These annual reports align with the office's dual reporting role, and provide Congress and the DoD's civilian and military leaders an independent assessment of the management and performance challenges confronting the Defense Department in the year ahead. The DoD OIG identifies the top challenges based on a variety of factors, including DoD OIG oversight work, research, and judgment; oversight work done by other DoD components; oversight work conducted by the Government Accountability Office; and input from DoD officials.[289] The resulting reports are forward-looking, and used by the DoD OIG to determine areas of risk in the agency's operations and to allocate effectively the office's oversight resources. In the Top DoD Management Challenges for Fiscal Year 2021, the OIG identified "enhancing cyber operations and capability and securing the DoD's Information Systems, Network and Data" as one of the top ten management and performance challenges."[290] The reports

287. *See supra* Section II.A.

288. OFF. OF INSPECTOR GEN., U.S. DEP'T OF DEF., TOP DOD MANAGEMENT CHALLENGES FISCAL YEAR 2021 (2020), at i [hereinafter TOP DOD MANAGEMENT CHALLENGES FY2021].

289. *Id.* at 1.

290. *Id*. For FY 2021, the DoD OIG identified the following management and performance challenges:

> 1. Maintaining the Advantage While Balancing Great Power Competition and Countering Global Terrorism

submitted for Fiscal Year 2020, Fiscal Year 2019, and Fiscal Year 2018 included similar calls for improving cyber operations and related support programs.[291]

Oversight Plans (Annual). The annual oversight plan is related to the top management challenges report. It describes the specific oversight projects the DoD OIG intends to conduct during the upcoming fiscal year and explains how those activities relate to the top management challenges facing the DoD. The plans are organized by management challenge, with each chapter providing a summary of a particular challenge, followed by an inventory of the ongoing and planned oversight projects that directly align to that challenge. To prepare the plan, the IG considers the top management challenges, and then:

> reviews and considers its own research and previous oversight work; key strategic documents, such as the National Security Strategy, the National Defense Strategy, and the DoD's President's Budget Request; oversight work from other oversight organizations, including the Government Accountability Office and DoD Components; and congressional hearings, legislation, and feedback from Members of Congress.[292]

Semiannual Reports. The DoD OIG is tasked with preparing semiannual reports summarizing the activities of the department during the immediately preceding six-month period.[293] The reports are to be submitted by the secretary of defense to the Senate Committees on Armed

---

2. Building and Sustaining the DoD's Technological Dominance
3. Strengthening Resiliency to Non-Traditional Threats
4. Assuring Space Dominance, Nuclear Deterrence, and Ballistic Missile Defense
5. Enhancing Cyberspace Operations and Capabilities and Securing the DoD's Information Systems, Network, and Data
6. Transforming Data Into a Strategic Asset
7. Ensuring Health and Safety of Military Personnel, Retirees, and Their Families
8. Strengthening and Securing the DoD Supply Chain and Defense Industrial Base
9. Improving Financial Management and Budgeting
10. Promoting Ethical Conduct and Decision Making.

Id. ("[The challenges] are not listed in order of priority, importance, or magnitude").

291. OFF. OF INSPECTOR GEN., U.S. DEP'T OF DEF., TOP DOD MANAGEMENT CHALLENGES, FISCAL YEAR 2020 (2019), at 1, 3 [hereinafter TOP DOD MANAGEMENT CHALLENGES FY2020] (identifying "Enhancing DoD Cyberspace Operations and Capabilities" as a top management challenge); OFF. OF INSPECTOR GEN., U.S. DEP'T OF DEF., TOP DOD MANAGEMENT CHALLENGES, FISCAL YEAR 2019 (2018), at 44 [hereinafter TOP DOD MANAGEMENT CHALLENGES FY2019] (identifying "Improving Cyber Security and Cyber Capabilities" as a top management challenge); OFF. OF INSPECTOR GEN., U.S. DEP'T OF DEF., TOP DOD MANAGEMENT CHALLENGES, FISCAL YEAR 2018 (2017), at 28 [hereinafter TOP DOD MANAGEMENT CHALLENGES FY2018] (identifying "Increasing Cyber Security and Cyber Capabilities" as a top management challenge).

292. DOD OVERSIGHT PLAN FY2021, *supra* note 183, at 1.

293. 5 U.S.C. app. 3 § 5.

Services and Homeland Security and Governmental Affairs and to the House Committees on Armed Services and Oversight and Government Reform, as well as to other appropriate committees or subcommittees of Congress.[294] In addition to the standard components, Congress has added special required categories for the reports prepared by the DoD OIG; these include: "information concerning the numbers and types of contract audits conducted by the Department during the reporting period;" and "information concerning any Department of Defense audit agency that, during the reporting period, has either received a failed opinion from an external peer review or is overdue for an external peer review required to be conducted in accordance with subsection (c)(10)."[295]

Compendium of Unimplemented Recommendations (Annual). The DoD OIG compendium is a lengthy document, often running more than 500 pages, which lists the number, type, age, and status of all open recommendations.[296] It also identifies high-priority recommendations made in earlier DoD OIG reports. The summaries on each open recommendation include the implementation status of the recommendations and a description of information required to close each recommendation. In addition, the report identifies recommendations that have been open for at least five years. A review of these compendium reports shows Congress where to direct its sparse energy, in essence creating a road map for future legislative and oversight efforts relating to cyber operations and capabilities. For example, the July 2021 compendium identified twenty high-priority open recommendations, nearly half of which related to cyberspace operations and capabilities, as well as securing DoD information systems, network, and data.[297] These reports provide a means for "Congress, acting in its traditional surrogate role, [to] draw on the unsung surrogates' [here, the DoD OIG] exposure to executive operations to increase its own visibility into executive cyber, election, and counterterrorism operations."[298]

As demonstrated in the paragraphs above, the work of the DoD OIG is an important component in the cyber oversight ecosystem. The office is

294. 5 U.S.C. app. 3 § 8(f)(1).
295. 5 U.S.C. app. 3 § 8(f)(1)(A)–(B).
296. *See, e.g.,* OFF. OF INSPECTOR GEN., U.S. DEP'T OF DEF., COMPENDIUM OF OPEN OFFICE OF INSPECTOR GENERAL RECOMMENDATIONS TO DEPARTMENT OF DEFENSE (2021) [hereinafter DOD COMPENDIUM 2021] (describing the list of open recommendations to the Department of Defense). For a list of all published annual compendium reports, s*ee Compendium of Open Recommendations*, OFF. OF INSPECTOR GEN., U.S. DEP'T OF DEF., https://www.dodig.mil/Reports/Compendium-of-Open-Recommendations/ [https://perma.cc/W6GL-WZPB].
297. DOD COMPENDIUM 2021, *supra* note 296, at 23.
298. Deeks, *Secrecy Surrogates supra* note 10, at 1467.

particularly well-positioned to address the separation of powers mismatch problem—that the unique nature of cyber capabilities is upsetting the usual constitutional separation of powers balance. As scholars and government officials continue to assess whether cyber operations form a "new constitutional category altogether, for which the respective roles of Congress and the president are not yet established,"[299] internal oversight, as conducted by the DoD OIG, becomes all the more critical. To better understand and assess the DoD OIG's contributions to the cyber oversight ecosystem, the next Section explores the extent to which the DoD OIG is already engaged in this effort.

D. Current DoD OIG Activities Focused on Cyber Operations

Recent activities by the DoD OIG reveal a substantial uptick in work focused on the department's military cyber operations. The office appears fully engaged in the cyber oversight mission and is filling the gaps in congressional oversight caused by the unique attributes of military cyber operations. A review of recent DoD OIG reports illuminates the breadth and scope of DoD OIG activities focused on U.S. military cyber operations. The DoD OIG's most recent reports[300] identify the following completed and anticipated inspections, evaluations, and audits of the Defense Department's cyber-related programs:

Audit of U.S. Combatant Command Offensive Cyber Operations.[301] This audit is referenced in the oversight plans for Fiscal Years 2020, 2021 and 2022, and the objective of the audit is "to determine whether U.S. combatant commands planned and executed offensive cyberspace operations within the scope of their operational plans and contingency plans."

Audit of the Department of Defense's Deconfliction of Cyberspace Operations.[302] This audit was referenced in the oversight plans for Fiscal

299. Waxman, *supra* note 9, at 11.

300. The list of reports in the text is gathered from semiannual reports, oversight plans, top management challenges reports, and annual compendium reports prepared by the DoD OIG from January 2019 to June 2022. It does not include reports prepared by the IGs for the National Security Agency, Defense Intelligence Agency, or National Geospatial Intelligence Agency. Although these entities are DoD components, they have separate inspector general offices.

301. OFF. OF INSPECTOR GEN., U.S. DEP'T OF DEF., FISCAL YEAR 2020 OVERSIGHT PLAN (2019), at 42 [hereinafter DOD OVERSIGHT PLAN FY2020]; DOD OVERSIGHT PLAN FY2021, *supra* note 183, at 24; OFF. OF INSPECTOR GEN., U.S. DEP'T OF DEF., FISCAL YEAR 2022 OVERSIGHT PLAN (2021), at 14 [hereinafter DOD OVERSIGHT PLAN FY2022].

302. FISCAL YEAR 2021 OVERSIGHT PLAN, *supra* note 183, at 25; FISCAL YEAR 2022 OVERSIGHT PLAN, *supra* note 301, at 14.

Years 2021 and 2022 with the following objective: "to determine whether U.S. Cyber Command implemented processes to deconflict offensive and defensive cyberspace operations in accordance with policy to prevent compromise of DoD Component and interagency missions and operations."[303]

U.S. European Command Efforts to Integrate Cyberspace Operations into Contingency Plans.[304] This report is dated March 30, 2018; the report is classified.

Audit of Combatant Command Training in a Contested Cyberspace Environment.[305] This audit was referenced in the oversight plans for Fiscal Years 2021 and 2022 with the following objective: "to determine to what extent the combatant commands are conducting training exercises that include evaluation of the DoD's ability to conduct operations in a contested cyberspace environment."[306]

Evaluation of U.S. Special Operations Command Joint Military Information Support Operations Web Operations Center.[307] This evaluation was referenced in the Fiscal Year 2022 Oversight Plan with the following objective: to "determine whether the U.S. Special Operations Command's Joint Military Information Support Operations Web Operations Center meets the combatant commander's requirements to support the geographic and functional combatant commander's ability to counter adversary messaging and influence in the information environment."[308]

Audit of the DoD's Implementation of the Memorandums between the DoD and the Department of Homeland Security regarding Cybersecurity and Cyberspace Operations.[309] This audit was referenced in the Fiscal Year 2020 Oversight Plan and its objective is "to determine whether the

303. DOD OVERSIGHT PLAN FY2021, *supra* note 183, at 25; DOD OVERSIGHT PLAN FY2022, *supra* note 301, at 14.
304. OFF. OF INSPECTOR GEN., U.S. DEP'T OF DEF., DODIG-2018-097, U.S. EUROPEAN COMMAND EFFORTS TO INTEGRATE CYBERSPACE OPERATIONS INTO CONTINGENCY PLANS (2018) (full report is classified).
305. DOD OVERSIGHT PLAN FY2021, *supra* note 183, at 25; DOD OVERSIGHT PLAN FY2022, *supra* note 301, at 14.
306. DOD OVERSIGHT PLAN FY2021, *supra* note 183, at 25; DOD OVERSIGHT PLAN FY2022, *supra* note 301, at 14.
307. DOD OVERSIGHT PLAN FY2022, *supra* note 301, at 14.
308. *Id.*
309. DOD OVERSIGHT PLAN FY2020, *supra* note 301, at 44.

DoD planned and executed activities to implement memorandums between the DoD and the Department of Homeland Security regarding cybersecurity and cyberspace operations."[310]

Audit of Cybersecurity Requirements for Weapon Systems in Operations and Support of Phase of Development of Defense Acquisition in Life Cycle.[311] This audit was completed in February 2021, and it assessed "whether DoD Components took action to update cybersecurity requirements for weapon systems in the Operations and Support (O&S) phase of the acquisition life cycle, based on publicly acknowledged or known cybersecurity threats and intelligence-based cybersecurity threats."[312]

Follow-up Audit on Corrective Actions Taken by DoD Components in Response to DoD Cyber Red Team-Identified Vulnerabilities and Additional Challenges Facing DoD Cyber Red Team Missions.[313] This audit was completed in March 2020; it is classified.

Combat Mission Teams and Cyber Protection Teams Lacked Adequate Capabilities and Facilities to Perform Missions.[314] The report was completed in 2015; it is redacted in part.

In addition, the DoD OIG has undertaken a number of activities and issued reports, some classified and some publicly available, related to the department's defensive cyber operations and cyber workforce development.[315] These include:

- Follow-up Audit on Staffing, Equipping, and Fielding the

---

310. *Id.*

311. OFF. OF INSPECTOR GEN., U.S. DEP'T OF DEF., DODIG-2021-051, AUDIT OF CYBERSECURITY REQUIREMENTS FOR WEAPON SYSTEMS IN THE OPERATIONS AND SUPPORT PHASE OF THE DEPARTMENT OF DEFENSE ACQUISITION LIFE CYCLE (2021).

312. *Id.*

313. OFF. OF INSPECTOR GEN., U.S. DEP'T OF DEF., DODIG-2020-067, FOLLOW-UP AUDIT ON CORRECTIVE ACTIONS TAKEN BY DOD COMPONENTS IN RESPONSE TO DOD CYBER RED TEAM-IDENTIFIED VULNERABILITIES AND ADDITIONAL CHALLENGES FACING DOD CYBER RED TEAM MISSIONS (2020) (full report is classified).

314. OFF. OF INSPECTOR GEN., U.S. DEP'T OF DEF., DODIG-2016-026, COMBAT MISSION TEAMS AND CYBER PROTECTION TEAMS LACKED ADEQUATE CAPABILITIES AND FACILITIES TO PERFORM MISSIONS (2015) (redacted).

315. OFF. OF INSPECTOR GEN., U.S. DEP'T OF DEF., DODIG-2021-034, SUMMARY OF REPORTS ISSUED REGARDING DEPARTMENT OF DEFENSE CYBERSECURITY FROM JULY 1, 2019 THROUGH JUNE 30, 2020 at ii (2020), https://media.defense.gov/2020/Dec/15/2002552095/-1/-1/1/DODIG-2021-034.PDF [https://perma.cc/FV78-XX7Z]; *see also* DOD OVERSIGHT PLAN FY2022, *supra* note 301, at 14–17 (listing planned and ongoing oversight projects).

Cyber Mission Force;[316]

- Audit of U.S. Coast Guard Operated DoD Information Network Systems;[317]
- Audit of the DoD's Vulnerability Identification and Mitigation Programs;[318]
- Follow-up Audit on the DoD's Implementation of Cybersecurity Controls and Incident Response Procedures for Industrial Control Systems Supporting the Defense Critical Infrastructure;[319]
- Audit of the DoD's Information Technology Modernization Protection of DoD Information Maintained on Contractor Systems and Networks;[320]
- Audit of the DoD's Recruitment and Retention of the Civilian Cyber Workforce;[321]
- Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems;[322] and
- Cyberspace Operations Audit of Cybersecurity Controls Over the Air Force Satellite Control Network (results are classified).[323]

The office's top management plans reveal the DoD OIG's focus on cyber operations as well. As noted above, each IG is required to prepare an annual statement that summarizes what the IG considers to be the "most serious management and performance challenges facing the agency"[324] and to assess the agency's progress in addressing those challenges. In its report on Top DoD Management Challenges for Fiscal Year 2022, the DoD OIG identified "Strengthening DoD Cyberspace Operations and Securing Systems, Networks, and Data" as the

316. DOD OVERSIGHT PLAN FY2021, *supra* note 183, at 25.
317. *Id.*
318. *Id.*
319. *Id.* at 26.
320. *Id.*
321. DOD OVERSIGHT PLAN FY2021, *supra* note 183, at 27.
322. OFF. OF INSPECTOR GEN., U.S. DEP'T OF DEF., DODIG-2019-105, AUDIT OF PROTECTION OF DOD CONTROLLED UNCLASSIFIED INFORMATION ON CONTRACTOR-OWNED NETWORKS AND SYSTEMS (2019).
323. OFF. OF INSPECTOR GEN., U.S. DEP'T OF DEF., DODIG-2021-054, CYBERSPACE OPERATIONS AUDIT OF CYBERSECURITY CONTROLS OVER THE AIR FORCE SATELLITE CONTROL NETWORK (assessing whether U.S. Space Force implemented cybersecurity controls to protect the Air Force Satellite Control Network against potential threats) [classified].
324. TOP DOD MANAGEMENT CHALLENGES FY2021, *supra* note 288, at ii.

department's number three challenge.[325] The reports for prior years included the following as top management and performance challenges: "enhancing cyber operations and capability and securing the DoD's Information Systems, Network and Data;"[326] "Enhancing DoD Cyberspace Operations and Capabilities;"[327] and "Improving Cyber Security and Cyber Capabilities."[328]

Finally, recent reports prepared by the NSA IG further illustrate the IG's contributions to the cyber oversight mission, particularly with regard to interpretative questions. The semiannual report for the NSA IG, filed in February 2021, referenced two activities focused on identifying interpretative disagreements in how entities within the IG were applying statutory constraints and reporting incidents. The first report assessed overhead signals intelligence (SIGINT) compliance at a joint facility. The IG found "differing interpretations of SIGINT compliance governing documents and conflicting viewpoints regarding authorities and application of compliance procedures, and lack of an escalation process to bring issues to the attention of top-level management."[329] The second review examined incidents of "reported over collect compliance" that involved "unauthorized collection by overhead satellite systems."[330] The IG determined that "inconsistencies in interpretation of incident reporting standards and incomplete guidance to the workforce raise a significant risk of less than complete incident reporting by NSA."[331]

As illustrated by the examples above, the DoD OIG is already robustly engaged in the oversight task with regard to military cyber operations. Synthesizing these reports uncovers valuable insight into the following aspects of the military's use of cyber capabilities: the effectiveness (or

---

325. TOP DOD MANAGEMENT CHALLENGES FY2022, *supra* note 182, at 25. The Defense Department "faces challenges in having the capabilities, interoperable systems, defined roles and responsibilities, and inter- and intragovernmental information sharing to coordinate and conduct effective cyber operations." *Id.* The report then concludes that "[w]ithout developing and modernizing its command and control infrastructure to coordinate and conduct operations, the DoD will not be able to maintain a competitive advantage over adversaries in cyberspace." *Id.* at 27. To address this challenge, the DoD OIG plans to perform an audit to determine the extent to which the DoD has modernized its command, control, communications, and computer infrastructure and systems to support enterprise-wide missions and priorities. *Id.*

326. TOP DOD MANAGEMENT CHALLENGES FY2021, *supra* note 288, at 47.

327. TOP DOD MANAGEMENT CHALLENGES FY2020, *supra* note 291, at 73.

328. TOP DOD MANAGEMENT CHALLENGES FY2019, *supra* note 291, at 6; TOP DOD MANAGEMENT CHALLENGES FY2018, *supra* note 291, at 28.

329. OFF. OF THE INSPECTOR GEN., NAT'L SEC. AGENCY, SEMIANNUAL REP. TO CONG., 1 APR. 2020 TO 20 SEPT. 2020 (2021), at 1–2 (describing audit report on interpretation discrepancies regarding collection authorities). The report also noted "a persistent lack of understanding of the partners' respective missions, cultures, and perspectives, combined with the lack of joint operating instructions, integration of SIGINT experts, and tailored training." *Id.*

330. *Id.*

331. *Id.*

lack thereof) of information sharing agreements between various government agencies and agreements with private sector entities; revealing after-action reports on cyber incidents or data breaches; effectiveness of cyber workforce development programs; identification of vulnerabilities in defense industrial base and other NSS information systems; documentation of interpretative challenges, both legal and policy-based, regarding the application of authorities and reporting requirements; and a cataloging of unimplemented cyber-related recommendations from years past. While the contributions of the DoD OIG have gone unnoticed by most observers, the employees of the Pentagon's watchdog have continued with their work, quietly but thoroughly assessing and evaluating the military's cyber programs, capabilities, and operations and contributing to the oversight mission, while also making recommendations for improvements at the programmatic and policy levels.

E. Potential Limitations on the DoD OIG's Cyber Oversight Role

In assessing the contours and depth of the DoD OIG's contributions to the cyber oversight framework, it is important to identify potential limits and obstacles. This Section explores potential critiques specific to the ability of the DoD OIG to provide adequate oversight of the U.S. military's cyber operations and capabilities.[332] These include concerns that the DoD OIG may be constrained in the following ways: (1) limited to an advisory role, and unable to take corrective or remedial action; (2) limited by the special rules that allow the secretary of defense to prohibit certain inspector general activities that implicate national security interests; (3) limited by persistent constitutional separation of powers concerns; and (4) limited by the contours of the individual inspector general's character and working relationship with the secretary of defense. This Section will briefly review each of the limits and then explain how in practice these potential limits do not actually inhibit the work of the DoD OIG to any significant extent.

1. Limited to an Advisory Role

The primary knock on the DoD OIG with regard to its oversight activities is that the inspector general is limited to an advisory role, and

---

332. For other critiques relating to effectiveness of the IG position, *see* LIGHT, *supra* 119, at 203–23; MOORE & GATES, *supra* 122, at 77–80; Peter Tyler, *Rating the Watchdogs: Are Our Inspectors General Effective?*, POGO (Aug. 10, 2018), https://www.pogo.org/analysis/2018/08/rating-watchdogs-are-our-inspectors-general-effective [https://perma.cc/P5XH-S4HM]; *Partnership for Public Service, The Forward-Looking Inspector General*, P'SHIP FOR PUB. SERV. 1, 2 (2017) https://ourpublicservice.org/wp-content/uploads/2017/11/4ed423645dfcc8c0fba0be1b9d25964e-1510540855.pdf [perma.cc/VKZ5-BAJN]; JOHNSON & NEWCOMER, *supra* note 122, at 195–206.

unable to take corrective or remedial action. However, this knock misunderstands the role Congress intended for inspectors general while also ignoring the larger oversight ecosystem. Let's start by understanding the critique. Certainly, it is correct to say that inspectors general serve in an advisory role. The inspector general may identify problems and recommend changes, however, the inspector general has no authority to take corrective action or to implement the policy changes it recommends. As Paul Light writes, IGs "are to look, not act; recommend, not implement."[333] The purely advisory status can be admittedly frustrating at times, particularly when IGs identify wrongful or wasteful conduct, and the bad conduct is left uncorrected or unaddressed by those tasked with remedial action.[334] A related concern highlights the timing and durability of inspector general activities, because inspector general work product is often ex post.[335]

These critiques, however, are misplaced for several reasons. First, while the purely advisory status can be viewed as a limit, or a bug in the statutory design of the Act of 1978, it is better seen as a feature. Indeed, the advisor role may actually advantage the inspector general. Without concern for the implementation of particular remedies, inspectors general do not pull their punches. They do not pre-frame the problem in a way that allows for, or leans heavily toward, a desired solution. Their advisory status provides for blunt assessment and candor. The Senate report accompanying the 1978 Act acknowledged the challenge of balancing the inspector general's need for independence with the agency head's management needs, which may on occasion lead to a failure to follow the inspector general's recommendation. The Committee "does not doubt that some tension can result from this relationship, but the Committee believes that the potential advantages far outweigh the potential risks."[336]

Second, the critique has been addressed by recent legislative efforts to

---

333. LIGHT, *supra* note 119, at 16; *see also* 5 U.S.C. App. §§ 8G(b), 9(a)(2) (prohibiting IGs from taking on "program operating responsibilities," including the responsibility of enforcing recommendations or implementing their advice).

334. *See, e.g.,* OFF. OF INSPECTOR GEN., U.S. DEP'T OF DEF., COMPENDIUM OF OPEN OFFICE OF INSPECTOR GENERAL RECOMMENDATIONS TO THE DEPARTMENT OF DEFENSE 9 (2022) [hereinafter DOD COMPENDIUM 2022] (stating eighty DoD OIG recommendations are currently "unresolved").

335. The critique is that the ex-post or "stochastic" nature of an inspector general's work lacks durability and will not accomplish lasting change. Neal Kumar Katyal, *Stochastic Constraint,* 126 HARV. L. REV. 990, 1000 (2013) (critiquing ex post scrutiny as inadequate, noting that "given these expanded powers, there is a deep risk that Presidents may, in the interim between the exercise of power and the ex post check, work grave harm—to peace, to civil liberties, and to the image of the United States abroad.").

336. S. REP. NO. 95-1071, at 9 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 2676, 2684.

shine a light on agency failures to take corrective action. In early 2019, Congress passed the Good Accounting Obligation in Government Act, with the objective of shining a light on agencies' failures to act on recommendations of the OIG.[337] The act requires that affected agencies report on open IG recommendations (and other matters) and provide explanations for not implementing each recommendation in their annual budget justification statements.[338] These reports, often labeled something like "Compendium of Open Office of Inspector General Recommendations to the Department of Defense,"[339] are made available to the public on an annual basis. The most recent Compendium, released publicly in July 2022, identified 1,425 open recommendations.[340] In addition to the list of open recommendations, the Compendium reports identify high priority open recommendations, summarize the potential monetary benefits of open recommendations, and list recommendations that have been open for more than five years. Both Congress and the media rely on these reports to highlight unheeded recommendations or instances where agency heads failed to follow the counsel of their advisors.[341]

Third, and finally, the critique misunderstands how the IGs fit into the larger oversight ecosystem. Their ability to illuminate and identify wrongdoing or abuse is sufficient in itself to serve the larger constitutional checking scheme. By highlighting the problematic conduct, the inspector general shifts responsibility for enforcement or remedial action to the appropriate entities: the relevant congressional committees, the secretary of defense, or other actors (such as the Department of Justice). For example, in a study that asked inspectors general to identify the mechanisms they use to get open recommendations implemented, the following activities, among others, were identified: informal conversations with agency staff in offices affected by the

---

337. Good Accounting Obligation in Gov't Act (GAO-IG Act), Pub. L. No. 115-414, 132 Stat. 5430–32 (2019) (codified as amended in 31 U.S.C. §§ 1105, 720), accompanied by S. REP. NO. 115-331, at 2 (2018) (stating that "[b]y disclosing open recommendations and being required to explain the lack of implementation in an agency's budget request, agencies will be held more accountable for unimplemented recommendations.").

338. *See* GAO-IG Act, *supra* note 337, at § 2(b)(3) (describing common procedure when IG recommendations are not implemented).

339. *See, e.g.*, discussion *supra* Section II.C.4.

340. DOD COMPENDIUM 2022*, supra* note 334, at 2.

341. *See, e.g.*, *Implementing Solutions: The Importance of Following through on GAO and OIG Recommendations: Hearing before the Subcomm. on Regul. Aff. & Fed. Mgmt. of the S. Comm. on Homeland Sec. & Governmental Affs*., 114th Cong. 2–3 (2015) (statement of Sen. Heidi Heitkamp) (noting importance of ensuring recommendations do not remain unimplemented or delayed); *see also* Schlanger, *Offices of Goodness*, *supra* note 122, at 94–95 (noting power of "advice-giving" or recommendations because it can highlight or spot issues that "might otherwise be insufficiently noticed or valued" while also increasing the political cost of not taking the advice).

recommendation; raising the issue with agency leadership; raising the issue in testimony and/or written reports to Congress; and informal conversation with relevant congressional staff, among others.[342] Moreover, the concerns about the durability of IG work seems to be countered by numerous examples, particularly in the last fifteen years, indicating that the work of inspectors general can have lasting impact on both the legal and policy levels.[343]

2. Limited by the Prohibitions in Section 8(b)

A second critique in the area of oversight of cyber operations is that the DoD OIG is limited by the special rules that allow the secretary of defense to prohibit or block DoD OIG activities when the activities relate to certain sensitive topics or national security matters.[344] As noted above, Section 8(b) allows the secretary of defense to prohibit IG activities if the matter involves sensitive operational plans, intelligence matters, counterintelligence matters, ongoing criminal investigations by other administrative units, or other matters the disclosure of which would constitute a serious threat to national security.[345]

This potential critique, however, is blunted by procedural requirements and practice. Let's start with the process and notice requirements. If the secretary of defense invokes this prohibition, the secretary must report the fact of the invocation to the relevant congressional committees within thirty days, and within an additional thirty days, the secretary must submit to the committees a statement explaining the reasons for exercising the prohibition power.[346] This reporting mechanism puts Congress on notice that the independence of the IG's office may be on a collision course with an agency's priority or mission. In many instances, the relevant congressional committees may agree with the secretary's exercise of the prohibition power. In those instances, however, where the agency's use of the power seems questionable or possibly wrongful, Congress has the ability to illuminate the conflict and draw attention to its contours, the precise oversight task that is required in such scenarios and that is appropriately exercised by Congress once armed with the knowledge that the agency is blocking certain IG activity. Second, and likely related to

342. JOHNSON & NEWCOMER, *supra* note 122, at 113 (indicating frequency with which IGs use the various activities).
343. *See supra* Section II.C.3 (describing DoD OIG's growing role as independent advisor and policy evaluator); *see also* Sinnar, *Protecting Rights from Within, supra* note 122, at 1031–32 (describing IG's potential to influence executive branch policy and decision-making, as well as limits on that ability).
344. *See supra* notes 242–244 and accompanying text (describing § 8(b) provision and use).
345. 5 U.S.C. app. 3 § 8(b)(1), (2).
346. *See supra* Section II.C.

the first point, is the use of the prohibition power in practice. The prohibition power has been rarely, if ever, invoked by the secretary of defense.[347] Even in arguably legitimate uses of the prohibition power, agency heads are reluctant to exercise it.[348] This reluctance may stem from the ability of agency leaders to appreciate the transparency and accountability value gained—in the eyes of Congress and the public—by giving the inspector general a wide berth. Put in starker institutional power terms, the secretary of defense and agency heads in other intelligence and defense entities recognize that "the institution of the inspector general has empowered the presidency by constraining it."[349]

3. Limited by Persistent Separation of Powers Concerns and Turf Battles

A third potential limit on the ability of IGs to serve as effective oversight mechanisms is a lingering concern about the constitutionality of inspectors general within the separation of powers scheme. During legislative debates regarding the IGA, Department of Justice lawyers went so far as to question whether "the congressional intrusion into executive operations was so substantial that it violated the separation of powers doctrine."[350] Within the Defense Department, this separation of powers concern, while muted, may be expressed as a potential turf battle between the Office of the Inspector General (DoD OIG) and the Office of General Counsel (DoD OGC). In the Office of the Secretary of Defense, both the DoD inspector general and the General Counsel of the Department (GC) are considered "component heads" and provide immediate staff assistance and advice to the secretary of defense. However, they have different responsibilities and priorities within the department's operational and administrative organizations.[351] The GC serves as the chief legal officer for the Department of Defense, where the primary responsibility is to provide advice to the secretary and deputy

---

347. *See* Sinnar, *Protecting Rights from Within*, *supra* note 117, at 1049 (concluding so much based on extensive interviews with inspector general offices through 2012).

348. *See* GOLDSMITH, *supra* note 13, at 108–10 (noting that the CIA director allowed an inspector general investigation of the CIA's detention and interrogation to go forward and did not invoke the prohibition although there likely were statutory grounds to do so).

349. *Id.* at 108.

350. MOORE & GATES, *supra* note 122, at 10 (citing Memorandum from Griffin Bell, Att'y Gen., to President Jimmy Carter on H.R. 2819 (Feb. 24, 1977) (enclosing and describing memorandum from John M. Harmon, Assistant Att'y Gen., Off. of Legal Couns., (Feb. 21, 1977) on the same subject)).

351. *See* EXEC. SERVS. DIRECTORATE, DOD AND OSD COMPONENT HEADS (Feb. 22, 2022), https://www.esd.whs.mil/Potals/54/Docments/DD/iss_process/coordination/DoD_OSD_Component%20Heads.pdf [https://perma.cc/2LG9-SMRD] (defining DoD "component heads" as the "leaders of [their] organizations"). *See also* U.S. DEP'T OF DEF., ORGANIZATION & MANAGEMENT OF DEPARTMENT OF DEFENSE (2019) (outlining organizational structure of the OSD).

secretary of defense regarding all legal matters and services performed within, or involving, the Department of Defense.[352] A related responsibility of the GC includes overseeing legal services performed within the DoD. A notable exception to this authority is the Office of the General Counsel to the DoD IG, where the head of that office reports to the IG, not the GC.[353]

The IG is the head of "an independent and objective unit" within the department, and is charged with conducting and supervising audits, investigations, evaluations, and inspections relating to the programs and operations of the Defense Department.[354] The primary responsibilities of the IG include: serving as the principal advisor to the secretary of defense on all audit and criminal investigative matters and for matters relating to the prevention and detection of fraud, waste, and abuse in the programs and operations of the DoD; initiating, conducting, supervising, and coordinating such audits, investigations, evaluations, and inspections; and providing policy and direction for audits, investigations, evaluations, and inspections relating to fraud, waste, abuse, program effectiveness, and other relevant areas within OIG DoD responsibilities.[355]

Thus, the question becomes whether the IG intrudes on the GC's turf in the performance of the office's audit, evaluation, and inspection activities. Areas of potential overlap with regard to cyber operations include: review of existing and proposed legislation and regulations relating to DoD programs and operations; coordinating congressional requests for information and testimony; managing the whistleblower protection program; receiving and evaluating "urgent" concern information; and reviewing and assessing compliance with DoD operational policy or compliance with congressional reporting provisions regarding various cyber operations.[356]

These turf battle concerns regarding oversight of cyber operations are overstated. First, the timing of each office's activities differs. The GC

352. 10 U.S.C. § 140(b); *See* U.S. DEP'T OF DEF., DOD DIRECTIVE NO. 5145.01, GEN. COUNS. OF DEP'T OF DEF. (2015) (outlining GC DoD position responsibilities); *see also* U.S. DEP'T OF DEF., DOD DIRECTIVE NO. 5145.04, DEF. LEGAL SRVS. AGENCY (2020). The General Counsel also serves as the Director of the Defense Legal Services Agency (DLSA), which provides legal advice and services for the Defense Agencies, DoD Field Activities, and other assigned organizations. For a breakdown of responsibilities within these roles, see *About Us,* U.S. DEP'T OF DEF., OFF. OF GEN. COUNS., (last visited Sept. 14, 2022) https://ogc.osd.mil/About/ [https://perma.cc/C4Z9-PM7H].

353. DOD DIRECTIVE NO. 5145.01, *supra* note 352, at § 3.c. (2015).

354. U.S. DEP'T OF DEF., DOD DIRECTIVE NO. 5106.01, INSPECTOR GEN. OF DEP'T OF DEF. (2020).

355. *Id.*

356. *Compare* DOD DIRECTIVE 5145.01, *supra* note 352, at § 3 (h, n, v, w), *with* DOD DIRECTIVE 5106.01, *supra* note 354, at § 5 (n, s, u, ad) to examine how position overlap may occur.

primarily provides legal advice in the planning and pre-operation stages, whereas the IG primarily provides post-operation review and evaluation, including legal and policy assessments as well as recommendations on correcting failures and preventing future errors. Ideally, the GC and other DoD leadership will consider the IG's recommendations when engaged in future operational planning efforts, however, there is no conflict or confusion as to which office's legal advice governs the operation.

Second, the focus of each office's reviews differs: while the GC focuses on evaluating the legal propriety of the operation with international law or domestic legal authorities (both constitutional and statutory)[357], the IG's review focuses on identifying interpretative discrepancies, de-confliction problems, a failure to comply with department policy or ROEs, or a failure to comply with congressional reporting requirements.

Third, in areas where overlap between the IG and GC may exist, that overlap is best viewed as supporting the larger oversight task by pairing two internal watchers with complementary skills aimed at a common objective: ensuring compliance, accountability, and transparency for the military's cyber operations.

In sum, inspectors general are not the proper entity to make decisions when interests (whether between branches of the federal government, between executive branch agencies, or within an executive department) are in conflict. Rather, such political-normative judgments must be made by political actors and will continue to be the purview of political actors with regard to policy judgments affecting the cyber domain and the military's role in it. Inspectors general, however, contribute to such decisions—and the discussions that lead up to the normative judgments—by "revealing questionable actions by program officials and forcing debate among congressional overseers, program managers, and those representing clients to determine how the balance should be struck."[358] Rather than inhibiting the work of the general counsel or intruding on the actions of Defense Department actors, the inspector general's contribution is initiating the discussion and providing context for the contours of the debate. Ideally, the illumination of the issue by the IG will lead to "new policies enacted in legislation, administrative rulings, or agency practices that balance the competing interests more precisely."[359]

---

357. *See* DOD DIRECTIVE 5145.01, *supra* note 352, at § 3.n.(3)(c) (2015) (specifying that the GC has responsibility for reviewing the legality of the department's cyber capabilities).
358. MOORE & GATES, *supra* note 122, at 69.
359. *Id.*

4. Limited by the Individual Inspector General's Working Relationship with the Secretary of Defense

A final potential constraint is the individual inspector general's character, working relationship with the secretary of defense, and related concerns about agency capture. Not surprisingly, the IG's impact on the agency (or the office's effectiveness) is influenced by that inspector general's personality traits, management style, agenda, and of course, the inspector general's relationship with the agency head. As previously stated, IG offices "vary in their aggressiveness, expertise, and influence."[360] Let's break this concern into two components: one focused on the IG's individual strengths and weaknesses, and one that considers the relationship between the IG and the agency head and the related "agency capture" concern.

IGs, of course, are not perfect. Their individual motives and actions do not always align with the public values envisioned by the drafters of the legislation that created the position. Examples abound of IGs or their staff members behaving badly or with less than appropriate motivations.[361] This concern, while important to record, seems true of any office and individual charged with oversight, whether the check comes from external sources, another branch of the federal government, within the executive branch, or within that very agency. Indeed, most humans are flawed, and most working relationships are challenging, but this hardly seems a limit that would impact the Department of Defense IG more so than other players in the oversight ecosystem. Moreover, the mechanisms[362] currently in place to watch the watchers seem to be

---

360. Schlanger, *Intelligence Legalism*, *supra* note 208, at 144.

361. *See, e.g.*, Danielle Brian & Jana Persky, *Watching the Watchdogs: The Good, the Bad, and What We Need from the Inspectors General*, POGO (Jan. 14, 2014), https://www.pogo.org/report/2014/01/watching-watchdogs-good-bad-and-what-we-need-from-inspectors-general/ [https://perma.cc/847F-3GDG]; s*ee also* U.S. GEN. ACCT. OFF., OSI-95-9, INSPECTORS GEN.: ALLEGED MISCONDUCT BY NASA INSPECTOR GEN. (1995); U.S. GOV'T ACCOUNTABILITY OFF., GAO-10-63R, INTEGRITY COMM.'S PROCESS TO ADDRESS ALLEGATIONS OF WRONGDOING BY INSPECTORS GEN. (2009). Recent examples include Laura Wertheimer, the former IG for FHFA, and Joseph Cuffari, the current IG of DHS. Rachel Siegel, *Inspector General Resigns,* WASH. POST, (June 30, 2021) https://www.washingtonpost.com/us-policy/2021/06/30/fhfa-inspector-general-resigns-laura-wertheimer/ [https://perma.cc/K3AK-JU3A]; Adam Zagorin & Nick Schwellenback, *Homeland Security's Embattled Watchdog Faces Probe*, POGO (Feb. 11, 2022) https://www.pogo.org/investigation/2022/02/homeland-securitys-embattled-watchdog-faces-probe [https://perma.cc/S4F4-4MTK]; Geneva Sands, *Watchdog Finds DHS Identified Threats Prior to Jan. 6, but Did Not Widely Share Intelligence until After Attack,* CNN, https://www.cnn.com/2022/03/08/politics/dhs-ig-report-threats-intelligence-january-6 [https://perma.cc/CE5Z-SZJ9] (last updated Mar. 8, 2022).

362. These mechanisms include the president's removal power, congressional oversight, agency approval or commentary, DOJ decisions whether to prosecute individuals or others flagged by the OIG for misconduct, as well as the Committee of Inspectors General on Integrity and Efficiency,

effective, at least to the extent that improper conduct of an individual IG is usually identified in short order.

The second component presents a potentially more significant concern—that the IG is "captured" by the agency mission or "assimilated" as a result of loyalty to the agency head, and thus unwilling or unable to exercise the required independence or conduct the oversight role with sufficient candor and robustness.[363] "Scholars of bureaucracy and administration have long explained that agencies have difficulty simultaneously internalizing a mission and its constraints,"[364] which means that internal oversight offices—like IGs—face "continual pressure to slide into disempowered irrelevance or to be tamed by capture or assimilation."[365] IGs, however, are better suited than other internal separation of power entities due to their statutorily mandated autonomy, budgetary independence, and the various channels of congressional reporting. These characteristics strengthen the IG's ability to resist capture or assimilation in most, although not all, instances. As noted throughout this Article, IGs are not a perfect or exclusive answer to the cyber oversight problem.

While this Article urges recognition of the role to be played by the DoD OIG, it readily acknowledges that the office is an incomplete solution on its own to the cyber oversight challenge. Rather, the contributions of the DoD OIG should be seen as one part of a wider oversight framework involving Congress, the courts, the media, and other surrogates within and outside the federal government.[366] As such, the potential constraints described above, while limited or non-existence in practice, are further muted by the other actors in the cyber oversight ecosystem.

III. INITIAL RECOMMENDATIONS FOR STRENGTHENING THE DOD OIG'S CYBER OVERSIGHT ROLE

This Article's aim was two-fold: to bring attention to the gaps and challenges in the current congressional oversight framework for military cyber operations and to highlight the DoD OIG's unique contributions to the cyber oversight task and its ability to fill some of the most problematic gaps. Further study is needed to assess whether reforms to the DoD

known as the federal government's "watchdog of the watchdogs" which is charged with monitoring allegations of wrongdoing by inspectors general and high-level staff members. JOHNSON & NEWCOMER, *supra* note 122, at 157–60.

363. Schlanger, *Officers of Goodness*, *supra* note 122, at 104.

364 *Id.*

365. *Id.*

366. *See* JOHNSON & NEWCOMER, *supra* note 122, at 152–59 (describing other entities and mechanisms contributing to the oversight ecosystem).

OIG's cyber oversight toolkit or authorities are warranted, as well as additional analysis of the interactions between the various IG offices with jurisdiction over the government's cyber capabilities. Accordingly, the recommendations offered here are preliminary and are provided to generate further consideration and study. These recommendations focus on strengthening the DoD OIG's role as a member of the presidential synopticon charged with watching—and providing oversight of—the U.S. military's use and deployment of cyber operations and capabilities.

The first bucket of reforms focuses on executive branch policies and practices. As a preliminary matter, the president should submit timely nominations for the position of IG in the Department of Defense, which has been sitting vacant for more than 2,500 days at the time of the writing of this Article.[367] Relatedly, Congress should consider amendments to the Federal Vacancies Reform Act and Inspector General Act to incentivize or require nominations of statutory IGs within a certain date of a new administration. These adjustments to the appointment process will combat concerns of stochasticity and the durability of the IG's oversight tools. In addition, the executive branch directives and policies governing cyber operations, reportedly contained in classified NSPM 13 as revised by the Biden administration, should be clarified with regard to the delegation authority. As described more fully above, the policy currently allows the president to delegate authority for the approval of certain offensive cyber operations to the secretary of defense or others within the department or military. The revisions should clarify the types of operations that require presidential approval and specify the characteristics that influence the delegation decision. Relatedly, the policy should identify the nature of the offensive cyber activities that DoD can undertake within these delegated authorities. Ideally, the distinctions between the operations requiring presidential approval and those within the delegated authority would track the relevant domestic and international legal frameworks and may also contribute to the development of norms. The goal of the policy revisions should be to maintain the agility and speed gained by the 2018 revamp while adding appropriate guardrails for the military's use of its cyber capabilities.

The second bucket of reform focuses on congressional actions. Congress should consider revisions to the removal provisions governing IGs, particularly in intelligence and national security agencies, to allow for greater independence and more structured succession paths.[368]

---

367. *Inspector General Vacancies,* OVERSIGHT.GOV (last visited Nov. 30, 2022) https://www.oversight.gov/ig-vacancies [https://perma.cc/7GG6-LBGR].

368. For a variety of recent legislative efforts to reform IG removal provisions, *see supra* note 139 and accompanying text.

Relatedly, Congress should amend the national security prohibition on the DoD OIG by adding an opportunity for the agency's IG to provide formal commentary to Congress when the secretary of the defense invokes the prohibition power. There is a model for this proposal in the provisions governing IGs in other national security and intelligence entities.[369] Congress should task the current DoD OIG, via the National Defense Authorization Act, with specific projects relating to military cyber operations. These projects should include requests to determine how the Department of Defense is interpretating its authorities and reporting requirements under the relevant provisions of Chapter 19 of Title 10, which governs cyber and information operations, as well as audits to ensure the Defense Department is complying with the reporting and notice provisions of that chapter. Congress should amend the quarterly briefing requirements in Section 484 of Chapter 19 in Title 10 to define department-specific metrics (and provide data) that measure defend forward outcomes across strategic, operational, and tactical levels.[370]

The legislative proposals and executive branch reforms listed above should occur in parallel with two other efforts. First, the DoD OIG's activities and role should develop in concert with the oversight activities of other players tasked with checking cyber operations: these include foreign states, courts, technology companies, and other "good offices."[371] The interaction of these entities, which have "overlapping, but non-identical incentives" to check executive branch exercises of power,

---

369. *See, e.g.*, 5 U.S.C. app. 3 § 8G(d)(2)(A-C) (describing exercise of prohibition authority process when secretary of defense prohibits activities of the DIA, NGIA, NRO, and NSA IGs, stating that these IGs may "submit to such committees of Congress any comments on a notice or statement received by the inspector general under this subparagraph that the inspector general considers appropriate"); 5 U.S.C. app 3 § 8I(a)(3) (establishing parallel authority for the secretary of homeland security and the DHS IG, stating that the DHS IG shall provide a written statement to Congress "regarding whether the Inspector General agrees or disagrees with such exercise, and the reasons for any disagreement"); 50 U.S.C. § 3033(f)(4) (conveying parallel instruction for the director of national intelligence and the IC IG, stating that IC IG "may submit to the congressional intelligence committees any comments on the statement of which the Inspector General has notice under paragraph (3) that the Inspector General considers appropriate").

370. CSC REPORT 2020, *supra* note 14, at 117 ("In light of DoD's expanding mission set, it is imperative to assess the extent to which cyber campaigns and operations conducted in support of the defend forward strategy are achieving their intended effects."). The report suggested measurement outcome metrics including "direct and indirect costs imposed on adversaries, the impact of defend forward operations and campaigns on adversary behavior, how adversary cyber operations have quantifiably affected DoD's ability to conduct or succeed across cyber and non-cyber missions, and DoD's assessment of the ability of adversary cyber operations to impact future campaigns." *Id*.

371. *See generally* Schlanger, *Offices of Goodness, supra* note 122 (proposing internal mechanisms tasked with furthering "goodness" in ensuring executive branch behavior); *see also supra* note 83 and accompanying text (describing alternatives to congressional oversight).

strengthens the oversight function.[372] In addition, reforms to the DoD OIG should complement other reform efforts designed at improving the federal government's defensive cybersecurity initiatives. These efforts include congressional committee reform, cyber literacy efforts within the legislative and executive branches, the establishment of the National Cyber Director and related office, as well as reforms to the U.S. government's vulnerabilities equities process.[373]

While wary of creating a burdensome oversight structure that undercuts the need for speed and flexibility in the cyber environment, there is no doubt the current framework could bear improvement. The recommendations above are offered to initiate conversations about striking that balance appropriately, and correctly calibrating the role of the DoD OIG in that effort.

CONCLUSION

The recent expansion of the U.S. government's cyber authorities and capabilities has coincided with a weakening and dispersion of the traditional congressional oversight mechanisms. This combination inhibits Congress's ability to gain a comprehensive understanding of the use and deployment of these new cyber capabilities and obscures the use of such powers from the public as well. In considering the proper oversight mechanisms for cyber operations, due regard must be given to the government's legitimate need for concealment and secrecy while also acknowledging justifiable concerns about the potential catastrophic consequences of such operations. As explained above, the DoD OIG, due to its distinctive mandate, authorities, perch, and tools, is well-suited to

372. Deeks*, Secrecy Surrogates*, *supra* note 10, at 1466; *see also* Gillian E. Metzger, *The Interdependent Relationship between Internal and External Separation of Powers*, 59 EMORY L.J. 423, 426 (2009) (noting the link between the internal constraints and external legal doctrine of the executive branch).

373. *See, e.g.*, RICHARD A. CLARKE & ROBERT KNAKE, THE FIFTH DOMAIN: DEFENDING OUR COUNTRY, OUR COMPANIES, AND OURSELVES IN THE AGE OF CYBER THREATS 144–53, 172 (2019) (proposing re-establishment of Office of Technology Assessment in Congress, as well as detailing national security lawyers from executive branch entities to congressional committees); Sharon Bradford Franklin & Andi Wilson Thompson, *Rules of the Road: The Need for Vulnerabilities Equities Legislation*, LAWFARE (Nov. 22, 2017, 7:00 AM), https://www.lawfareblog.com/rules-road-need-vulnerabilities-equities-legislation [https://perma.cc/UQ8M-ZEPE] (identifying the work that Congress must take to codify the VEP); Gaudion, *Cybersecurity Restructuring Task* , *supra* note 14, at 181 (describing need to reform the U.S. government's cybersecurity organizations and mechanisms); CSC REPORT 2020, *supra* note 14, at 35 (describing need for congressional committee reform); Cordero & Thaw, *Rebooting Congressional Cybersecurity* Oversight *supra* note 14 (describing need for congressional committee reform); Andrew J. Grotto, *How to Make the National Cyber Director Position Work*, LAWFARE (Jan. 15, 2021, 2:40 PM), https://www.lawfareblog.com/how-make-national-cyber-director-position-work [https://perma.cc/7URM-NBFY] (noting concerns where the national cyber director's responsibilities may be challenged).

the demands of the cyber oversight task. The DoD OIG, coupled with the checking mechanisms of other entities and in accord with rigorous legal guidance from the department's Office of General Counsel, presents the most effective way to appropriately limit and guide the use of the military's formidable powers in the cyber domain. This Article joins others in recognizing that Congress's usual tools are not well-suited to the cyber oversight task. As we ponder whether cyber operations form a "new constitutional category,"[374] we should take note of the distinctive contributions of the DoD OIG to the oversight ecosystem, contributions that acknowledge the government's interest while appropriately limiting and guiding the use of these vast, untested, and consequential capabilities.

374. Waxman, *Cyberattacks and the Constitution*, *supra* note 9, at 11.