2021

# Recognizing the Role of Inspectors General in the U.S. Government's Cybersecurity Restructuring Task

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

# RECOGNIZING THE ROLE OF INSPECTORS GENERAL IN THE U.S. GOVERNMENT'S CYBERSECURITY RESTRUCTURING TASK

AMY C. GAUDION*



## INTRODUCTION

Months prior to the 2015 public disclosure of a data breach at the U.S. government's Office of Personnel and Management (OPM), the Office of the Inspector General for OPM issued a report that identified significant deficiencies and material weaknesses in a number of the agency's information systems and IT security programs.[1] In response to the 2020

* Associate Dean for Academic Affairs and Professor of Lawyering Skills, Penn State Dickinson Law.  This article benefited greatly

SolarWinds supply chain[2] hack, attributed to Russia, calls are underway for inspectors general to conduct audits and inspections and to review prior inspector general assessments of information systems and vulnerabilities at federal agencies.[3] The use of inspectors general to assess information system vulnerabilities and to conduct post-breach evaluations, as illustrated by the OPM and SolarWinds cyber incidents, reflect a shift in the work undertaken by inspectors general and hint at their ability to fill an important role in efforts to reform the U.S. government's cybersecurity architecture. This article examines the unheralded and unrecognized work of inspectors general and the special role they are poised to play in the U.S.

---

from the feedback of my fellow participants at the Belmont Law Review Symposium, held in January 2021. I am grateful to Emily Kortright for her excellent research assistance and the good humor she brings to every task, and I want to thank the staff of the *The Belmont Law Review* for their terrific editorial work.

1. U.S. OFF. OF PERSONNEL AND MGMT., OFF. OF THE INSPECTOR GEN., FINAL AUDIT REPORT: FEDERAL INFORMATION SECURITY MANAGEMENT ACT AUDIT FY 2014, (Nov. 14, 2014), https://www.opm.gov/our-inspector-general/publications/reports/2014/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016.pdf [https://perma.cc/9BFC-ZQW7]; Brendan I. Koerner, *Inside the Cyberattack that Shocked the US Government*, WIRED (Oct. 23, 2016, 5:00 PM), https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/ [https://perma.cc/5DNL-QYF9]; Brian Krebs, *Catching Up on the OPM Breach*, KREBS ON SECURITY (June 15, 2015, 11:25 AM), https://krebsonsecurity.com/2015/06/catching-up-on-the-opm-breach/ [https://perma.cc/F8BN-C952].

2. I will use the label "SolarWinds" to describe this incident, while recognizing that SolarWinds is only one of several attack vectors used by the threat actors. *See, e.g.*, *Risky Business #611 -- MalwareBytes the latest "Holiday Bear" victim*, RISKY BUS. (Jan. 20, 2021), https://risky.biz/RB611/ [https://perma.cc/ZUZ8-G6T5]; *Supply Chain Compromise*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/supply-chain-compromise [https://perma.cc/L4MU-XBJU] (last visited Jun. 13, 2021).

3. Naomi Jagoda, *Lawmakers Ask IRS if Its Systems Were Compromised in SolarWinds Hack*, THE HILL (Dec. 18, 2020), https://thehill.com/policy/finance/530935-lawmakers-ask-irs-if-its-systems-were-compromised-in-solarwinds-hack [https://perma.cc/YL7B-Y3EE]; 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/Q8UP-6FZT]; Dustin Volz & Richard Rubin, *Senators Press IRS for SolarWinds Hack Briefing,* WALL ST. J. (Dec. 17, 2020, 11:00 AM), https://www.wsj.com/articles/senators-press-irs-for-solarwinds-hack-briefing-11608220822 [https://perma.cc/KA5G-2RX4]; Eric White, *Senators Want Answers Regarding SolarWinds Cyber Attack*, FED. NEWS NETWORK (Dec. 16, 2020, 11:41 AM), https://federalnewsnetwork.com/federal-newscast/2020/12/senators-want-answers-regarding-solarwinds-cyber-attack/ [https://perma.cc/ERN5-SLFT].

government's cybersecurity-[4]related work in the coming years. Inspectors general serve critical but little-understood functions in our constitutional system, both as internal checks on executive power within the administrative state and as conduits of the information necessary to the congressional oversight task. In light of continuing calls for reform of the U.S. government's cybersecurity architecture, this article examines the consequential position of the inspector general from a new perspective and considers the unique contributions of inspectors general to these reform efforts.

Part I identifies flaws in the current organization of the U.S. government's cybersecurity efforts. It describes the current fractured structure as reflected by more than twenty-three executive branch entities responsible for cybersecurity-related tasks, a disjointed congressional committee structure, and inadequate coordination with private sector partners. Part II explores the common solutions offered to remedy the government's cybersecurity organizational challenges. These include calls for revising the national cyber strategy, establishing a new cyber director, strengthening the Cybersecurity and Infrastructure Security Agency and increasing its funding, revamping the congressional committee structure, and building a cyber workforce. Notably absent from these calls is recognition that inspectors general have been examining these very issues and offering recommendations. Part III calls attention to the oft-ignored contributions of inspectors general, and examines why inspectors general across the U.S. government are uniquely prepared to support a re-alignment of the government's cybersecurity-related programs and entities. Part IV catalogs examples of inspectors general already engaged in the work of identifying and evaluating cybersecurity challenges. In conclusion, Part V considers how to effectively engage inspectors general in future re-organizational efforts and suggests avenues for further research.

## I. THE U.S. GOVERNMENT'S CYBERSECURITY ORGANIZATIONAL PROBLEM

In describing the current cybersecurity organization of the U.S. government, the March 2020 report of the Cyberspace Solarium Commission offered this warning:

4. This Article focuses on the role that inspectors general play in the allocation of *defensive* cyber responsibilities, or cybersecurity, across the U.S. government. Different considerations and dynamics are involved in examining the role of inspectors general in assessing the U.S. government's organization of its *offensive* cyber capabilities, spread predominantly across intelligence, defense, and law enforcement entities. Of course, the line between cyber offense and defense is a blurry one and there will be areas of overlap.

> While cyberspace has transformed the American economy and society, the government has not kept up. Existing government structures and jurisdictional boundaries fracture cyber policymaking processes, limit opportunities for government action, and impede cyber operations.[5]

Of course, the Commission is not the first entity to note this problem nor the first to call for a government restructuring in response. Many commentators have examined the roots of the U.S. government's inability to effectively address cyber-related threats and risks.[6] The SolarWinds hack is only the most recent illustration of this defect. This section describes failings in the current cybersecurity architecture and explains how the current organization is an inappropriate fit for the cybersecurity task at hand. The challenges fall into three buckets: the dispersion of cybersecurity responsibilities and tasks across twenty-three executive branch entities; a disjointed congressional committee structure; and the persistent problem of inadequate coordination and information sharing with the private sector.

### A. The Dispersion of Cybersecurity Responsibilities Across the Executive Branch

The first and most common explanation offered for the overall level of disorganization of U.S. cybersecurity is the dispersion of cybersecurity responsibilities across the executive branch.[7] This dispersion leads to a lack

---

5. U.S. CYBERSPACE SOLARIUM COMM'N, CSC FINAL REPORT (2020) https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view [https://perma.cc/GMK2-3H7R] [hereinafter CSC FINAL REPORT].

6. CSC FINAL REPORT, *supra* note 5; U.S. GOV'T ACCOUNTABILITY OFF., GAO-20-629, CYBERSECURITY: CLARITY OF LEADERSHIP URGENTLY NEEDED TO FULLY IMPLEMENT THE NATIONAL STRATEGY (2020), https://www.gao.gov/assets/710/709555.pdf [https://perma.cc/FZF4-NT4D] [hereinafter GAO-20-629]; U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-157SP, HIGH RISK SERIES: SUBSTANTIAL EFFORTS NEEDED TO ACHIEVE GREATER PROGRESS ON HIGH RISK AREAS (2019), https://www.gao.gov/assets/700/697245.pdf [https://perma.cc/RW8D-9NEV]; OFF. OF MGMT. AND BUDGET, EXEC. OFF. OF THE PRESIDENT, FEDERAL CYBERSECURITY RISK DETERMINATION REPORT AND ACTION PLAN 6 (May 2018), https://www.whitehouse.gov/wp-content/uploads/2018/05/Cybersecurity-Risk-Determination-Report-FINAL_May-2018-Release.pdf [https://perma.cc/3TEU-HV5G] ("Agencies do not understand and do not have the resources to combat the current threat environment."); MICHAEL CHERTOFF, EXPLODING DATA: RECLAIMING OUR CYBER SECURITY IN THE DIGITAL AGE (2018); RICHARD A. CLARKE & ROBERT KNAKE, THE FIFTH DOMAIN: DEFENDING OUR COUNTRY, OUR COMPANIES, AND OURSELVES IN THE AGE OF CYBER THREATS (2019) [hereinafter CLARKE & KNAKE].

7. GAO-20-629, *supra* note 6, at 34.

of clarity as to who is responsible for leading and coordinating the various cyber defense tasks within the federal government.[8] Bluntly put, it is unclear who answers calls to the U.S. government's cyber help desk. The title of a September 2020 report, prepared by the Governmental Accountability Office frames the challenge in stark terms: "CYBERSECURITY: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy."[9] The report painstakingly catalogs the twenty-three federal entities that have "roles and responsibilities for developing policies, monitoring critical infrastructure protection efforts, sharing information to enhance cybersecurity across the nation, responding to cyber incidents, investigating cyberattacks, and conducting cybersecurity-related research."[10] The executive branch entities can be grouped into the following categories: executive offices of the President, departments, agencies, commissions, and other offices. The following list gives a sense of the scale of the dispersion:

- Executive Offices of the President[11]
- Presidential Advisory Committees[12]
- Central Intelligence Agency[13]
- Department of Agriculture[14]
- Department of Commerce[15]
- Department of Defense[16]

8. *Id.* at 33.

9. *See generally id.*

10. *Id.* at 17.

11. *Id.* at 42. The cybersecurity-related components in the Executive Offices of the President include the National Security Council, Office of Management and Budget, and Office of Science and Technology Policy.

12. *Id.* at 42–43. The cybersecurity-related presidential committees include the National Science and Technology Council, President's Council of Advisors on Science and Technology, and President's National Security Telecommunications Advisory Committee.

13. *Id.* at 43. The cybersecurity-related roles and responsibilities of the Central Intelligence Agency include providing expertise in collaboration with other federal agencies for analysis and warning, information sharing, vulnerability reduction, mitigation, and critical infrastructure information systems' incident recovery activities.

14. *Id.* at 56. The cybersecurity-related component in the Department of Agriculture is the Office of Homeland Security.

15. *Id.* at 43. The cybersecurity-related components in the Department of Commerce include the National Institute of Standards and Technology, and the National Telecommunications and Information Administration.

16. *Id.* at 44–45. The cybersecurity-related components in the Department of Defense include the Chairman of the Joint Chiefs of Staff, Defense Information Systems Agency, DoD Chief Information Officer, DoD Components, DoD Cyber Crime Center, Geographic Combatant Commands, National Guard Bureau,

- Department of Energy[17]
- Department of Health and Human Services[18]
- Department of Homeland Security[19]
- Department of Justice[20]
- Department of State[21]
- Department of Transportation[22]
- Department of the Treasury[23]
- Environmental Protection Agency[24]
- Federal Chief Information Officers Council[25]

---

National Security Agency, Office of the Under Secretary of Defense for Acquisition and Sustainment, Office of the Under Secretary of Defense for Policy, Principal Cyber Advisor, and U.S. Cyber Command.

17. *Id.* at 46. The cybersecurity-related components in the Department of Energy are the National Laboratories, and the Office of Cybersecurity, Energy Security, and Emergency Response.

18. *Id.* The cybersecurity-related components in the Department of Health and Human Services are the Office of the Assistant Secretary for Preparedness and Response, Food and Drug Administration, Office of the Chief Information Officer, and Office for Civil Rights.

19. *Id.* at 47–49. The cybersecurity-related components in the Department of Homeland Security are the Cybersecurity and Infrastructure Security Agency, Federal Emergency Management Agency, Transportation Security Administration, U.S. Coast Guard, U.S. Immigration and Customs Enforcement, and U.S. Secret Service.

20. *Id.* at 49–50. The cybersecurity-related components in the Department of Justice are the Criminal Division, Drug Enforcement Agency, Federal Bureau of Investigation, INTERPOL Washington, and National Security Division.

21. *Id.* at 50. The cybersecurity-related components in the Department of State are the Bureau of Counterterrorism, Bureau of Democracy, Human Rights, and Labor, Bureau of Economic and Business Affairs, Bureau of Intelligence and Research, Bureau of International Narcotics and Law Enforcement Affairs, Bureau of International Organization Affairs, Office of the Coordinator for Cyber Issues, Office of the Legal Advisor, and Regional Bureaus.

22. *Id.* at 51. The cybersecurity-related components in the Department of Transportation are the Federal Aviation Administration, Federal Highway Administration, Maritime Administration, National Highway Traffic Safety Administration, Office of the Assistant Secretary for Research and Technology, and Office of Intelligence, Security and Emergency Response.

23. *Id.* The cybersecurity-related components in the Department of Treasury are the Office of Cybersecurity and Critical Infrastructure Protection, and the Office of Intelligence and Analysis.

24. *Id.* at 52. The cybersecurity-related components in the Environmental Protection Agency are the Office of Homeland Security, Office of Research and Development, and the Office of Water.

25. *Id*. The cybersecurity-related roles and responsibilities of the Federal Chief Information Officers council are leveraging the Federal Information Security

- Federal Communications Commissions[26]
- General Services Administration[27]
- National Science Foundation[28]
- Office of the Director of National Intelligence [29]

A more granular view of the challenges created by the dispersion of cyber responsibilities across the executive branch can be found in the variety of reports prepared by inspectors general.[30]

There have been prior efforts to lessen the confusion and improve coordination among executive branch entities, and two deserve mention here. First, President Obama issued Presidential Policy Directive 41[31] in 2016. The directive outlines the federal government's response plan for cyber incidents involving either the government or the private sector.[32] For certain types of incidents, those designated as "significant cyber incidents," the directive establishes "lead Federal agencies and an architecture for coordinating the broader Federal Government response."[33] Second, Congress passed the Cybersecurity and Infrastructure Security Agency Act

---

Modernization Act (2014) quarterly reporting and cybersecurity budget enhancements to meet federal cybersecurity priorities.

26. *Id.* at 52–53. The cybersecurity-related components in the Federal Communications Commission are the Communications Security, Reliability and Interoperability Council, International Bureau, Public Safety and Homeland Security, Wireline Competition Bureau, and Wireless Telecommunications Bureau.

27. *Id.* at 53. The cybersecurity-related components in the General Services Administration are the Federal Acquisition Service – Office of Information Technology Category, Office of Government-Wide Policy, and Office of Mission Assurance.

28. *Id.* at 54–55. The cybersecurity-related components in the National Science Foundation are Computer and Information Science and Engineering, Education and Human Resources, Engineering, and Mathematical and Physical Sciences.

29. *Id.* at 55. The cybersecurity-related components in the Office of the Director of National Intelligence are the Cyber Threat Intelligence Integration Center; Intelligence Community Chief Information Officer, Intelligence Community – Security Coordination Center, National Aviation Intelligence – Integration Office, National Counterintelligence and Security Center, National Intelligence Manager for Cyber, National Intelligence Manager for Space and Technical Intelligence, National Intelligence Officer for Cyber, and National Maritime Intelligence – Integration Office.

30. *See infra* Part IV.

31. Presidential Policy Directive 41 on United States Cyber Incident Coordination, 2016 DAILY COMP. PRES. DOC., DCPD No. 00495 (July 26, 2016), https://www.govinfo.gov/content/pkg/DCPD-201600495/pdf/DCPD-201600495.pdf [https://perma.cc/63EN-P6VE] [hereinafter PPD-41].

32. *Id.*

33. *Id.* at 1.

of 2018[34], which President Trump signed into law in November 2018. The Act established the Cybersecurity and Infrastructure Security Agency (CISA) as a new entity within the Department of Homeland Security, although drawn from prior entities within the department. While these efforts helped to clarify who answers the calls to the "cyber help desk," at least for most U.S. government networks,[35] the problems persist.

Cybersecurity defense in practice remains piecemeal across the executive branch, systems lack integration, and threat information is often not effectively distributed within federal agencies or with the private sector.[36] In a February 2021 hearing before the Committee for Homeland Security in the House of Representatives, former CISA Director Chris Krebs offered a sobering assessment of the continuing impacts of the executive branch's disorganization:

> At the governance level, roles and responsibilities across the Federal government are unclear, potentially further complicated by the newly authorized National Cyber Director (NCD) created by Section 1752 of the NDAA. Regardless of the organizational structure, the Executive branch must establish a comprehensive strategy and vision for Federal network modernization and security, drawing in the Budget side of the Office of Management and Budget (OMB) to coordinate and consolidate budgetary oversight, the Federal CISO as the policy framer, CISA as the tool provider and enforcer of security policy. The respective roles and responsibilities of the Federal CISO and CISA should also be examined. [37]

Thus, the dispersion of cybersecurity responsibilities across the executive branch remains a challenge without an easy solution.

---

34. Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. 115-278, 132 Stat. 4168 (codified as amended in scattered sections of Title 6 of the United States Code).

35. CISA's mandate is limited to federal civilian agencies, while the defense and intelligence agency networks are excluded from CISA's jurisdiction. *See CISA Gateway Consolidated Help Desk*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/cisa-gateway-consolidated-help-desk#:~:text=The%20CISA%20Gateway%2FPCIIMS%20Help,and%207%20PM%20(ET) [https://perma.cc/7679-PLCG] (last visited Jun. 15, 2021).

36. CSC FINAL REPORT, *supra* note 5, at 31.

37. *Homeland Cybersecurity: Assessing Cyber Threats and Building Resilience: Hearing Before the H. Comm. on Homeland Sec.*, 116th Cong. (2021), https://homeland.house.gov/activities/hearings/homeland-cybersecurity-assessing-cyber-threats-and-building-resilience [https://perma.cc/JBB5-UEK5] [hereinafter *Homeland Cybersecurity*].

### B. A Disjointed Congressional Committee Structure

A second problem is the disjointed congressional committee structure for oversight of the U.S. government's cyber-related activities, both defensive and offensive. Carrie Cordero, former government official, calls this the "Patchwork Mismatch."[38] There are no committees focused solely or entirely on cybersecurity matters.[39] Rather, oversight of cyber-related responsibilities and capabilities are divided among many committees and sub-committees.[40]

The House and Senate committees on the judiciary consider issues relating to surveillance, cybercrime, and privacy.[41] The armed services committees in each chamber consider the military's use of cyber capabilities, for both offensive and defensive purposes.[42] The intelligence committees focus on the use of cyber capabilities for intelligence gathering, covert action operations, and counterintelligence activities, as well as considering the ability of foreign adversaries to use cyber tools in support

---

38. Carrie Cordero & David Thaw, *Rebooting Congressional Cybersecurity Oversight*, CTR. FOR NEW AM. SEC. (Jan. 30. 2020), https://www.cnas.org/publications/reports/rebooting-congressional-cybersecurity-oversight [https://perma.cc/G8U5-G4ET] [hereinafter *Rebooting Oversight*]; 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/L6N9-SC3K] [hereinafter *Cyberspace Mandate*].

39. *Rebooting Oversight*, *supra* note 38; *Cyberspace Mandate*, *supra* note 38.

40. *Rebooting Oversight*, *supra* note 38; *Cyberspace Mandate*, *supra* note 38.

41. *Rebooting Oversight*, *supra* note 38. Recent examples of hearings before the judiciary committees include: *The EARN IT Act: Holding the Tech Industry Accountable in the Fight Against Online Child Sexual Exploitation: Hearing Before the S. Comm. on the Judiciary*, 116th Cong. (2020), https://www.judiciary.senate.gov/meetings/the-earn-it-act-holding-the-tech-industry-accountable-in-the-fight-against-online-child-sexual-exploitation [https://perma.cc/HF9B-2W4M]; *Oversight of the Federal Bureau of Investigation: Hearing Before the H. Comm. on the Judiciary*, 116th Cong. (2020), https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=2780 [https://perma.cc/7SRA-78ML].

42. *Rebooting Oversight*, *supra* note 38. Recent examples of hearings before the armed services committees include: *Interim Review of the National Security Commission on Artificial Intelligence Effort and Recommendations: Hearing Before the Subcomm. on Intel. and Emerging Threats and Capabilities of the H. Comm. on Armed Serv.*, 116th Cong. (2020), https://armedservices.house.gov/hearings?ID=70C87ECC-DF3E-4B34-A8C7-CA9EE8B70B3A [https://perma.cc/EJJ2-WZ8Q]; *Department of Defense Cyber Operations: Hearing Before the Subcomm. on Cybersecurity of the S. Comm. on Armed Serv.*, 116th Cong. (2020), https://www.armed-services.senate.gov/hearings/20-03-03-department-of-defense-cyber-operations [https://perma.cc/9VUP-TDPJ].

of election interference efforts.[43] The committees on homeland security and governmental affairs consider cybersecurity issues relating to critical infrastructure, incident response, election security, and private sector coordination.[44] For example, the SolarWinds hack featured prominently in a February 2021 hearing before the House Committee on Homeland Security.[45] And the list goes on as the committees focused on agriculture, commerce, energy, and transportation also come into regular contact with cybersecurity-related matters in their purview.[46] Moreover, this brief summary does not include the numerous subcommittees that have jurisdiction over cybersecurity-related matters.[47]

This trend toward committee overload is not slowing. The most recent addition to the cybersecurity congressional committee list was announced in February 2021, when the 117th Congress formally convened the Subcommittee on Cyber, Innovative Technologies, and Information Systems (CITI)[48] under the House Armed Services Committee. The new

---

43. *Rebooting Oversight*, *supra* note 38. Recent examples of hearings before the intelligence committees include: *Misinformation, Conspiracy Theories, and "Infodemics": Stopping the Spread Online: Hearing Before the H. Permanent Select Comm. on Intelligence*, 116th Cong. (2020), https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=111087 [https://perma.cc/34K7-RRPB]; *Worldwide Threats: Hearing Before the S. Select Comm. on Intel.*, 116th Cong. (2019), https://www.intelligence.senate.gov/hearings/open-hearing-worldwide-threats [https://perma.cc/RW3F-39GU].

44. *Rebooting Oversight*, *supra* note 38. Recent examples of hearings before the homeland security and governmental oversight committees include: *Secure, Safe, and Auditable: Protecting the Integrity of the 2020 Elections: Hearing before the Subcomm. on Cybersecurity, Infrastructure Protection, & Innovation of the H. Comm. on Homeland Sec.*, 116th Cong. (2020), https://homeland.house.gov/activities/hearings/secure-safe-and-auditable-protecting-the-integrity-of-the-2020-elections [https://perma.cc/ULL9-36Z2]; *Evolving the U.S. Cybersecurity Strategy and Posture: Reviewing the Cyberspace Solarium Commission Report: Hearing Before the S. Comm. on Homeland Sec. & Gov't Affairs*, 116th Cong. (2020), https://www.hsgac.senate.gov/evolving-the-us-cybersecurity-strategy-and-posture-reviewing-the-cyberspace-solarium-commission-report [https://perma.cc/W7W9-QLHF].

45. The 2021 hearing featured Chris Krebs, Former Director of the Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security, Sue Gordon, Former Principal Deputy Director of National Intelligence, Office of the Director of National Intelligence, Michael Daniel, President & CEO, Cyber Threat Alliance, and Dmitri Alperovitch, Executive Chairman, Silverado Policy Accelerator. *Homeland Cybersecurity*, *supra* note 37.

46. GAO-20-629, *supra* note 6, at 41, 43, 51, 56.

47. Simon Handler, *The 5x5—Cybersecurity and the 117th Congress,* ATLANTIC COUNCIL (Oct. 7, 2020), https://www.atlanticcouncil.org/content-series/the-5x5/cybersecurity-and-the-117th-congress/ [https://perma.cc/5ZKD-AKYG].

48. Press Release, House Armed Services Committee, Smith, Langevin Announce New Subcommittee for the 117th Congress (Feb. 3, 2021),

subcommittee holds jurisdiction over: cybersecurity, operations, and forces; information technology, systems, and operations; science and technology programs and policy; defense-wide research and development (except missile defense and space); artificial intelligence policy and programs; electromagnetic spectrum policy; electronic warfare policy; and computer software acquisition policy.[49]

Committee overlap and shared jurisdiction provide certain advantages to the congressional oversight scheme.[50] However, the current structure has moved well past the beneficial tipping point. The dispersion and disjointed nature of the committee structure for cybersecurity is causing significantly more harm than good.[51] Each committee views the cybersecurity issue only through the narrow lens before it, and thus, Congress is unable to distinguish the cybersecurity forest from the trees. As stated by Carrie Cordero, "the lack of a coordinating function among these committees limits Congress' ability to obtain a comprehensive picture of the cybersecurity problem."[52] The Cyberspace Solarium Commission (CSC) Final Report offers a similarly blunt assessment, noting that the disjointed nature of the 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."[53]

A summary of congressional hearings held across only a four-month period (February to May 2021) reveals the current fractured congressional structure. On February 10, 2021, the House Committee on Homeland Security held a hearing on "Assessing Cyber Threats and Building Resilience."[54] On February 23, 2021, the Senate Select Committee on Intelligence held a hearing on "Hack of U.S. Networks by a Foreign Adversary,"[55] the House Armed Services Subcommittee on Cyber,

---

https://armedservices.house.gov/press-releases?ID=283E9BE0-65B6-4C61-880A-40E0C7CBD521&utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202 [https://perma.cc/9RWN-6QBJ].

49. *Id.*

50. CHRISTOPHER M. DAVIS ET AL., CONG. RESEARCH SERV., RL30240, CONGRESSIONAL OVERSIGHT MANUAL, at 5; 39–40 (Mar. 31, 2021), https://fas.org/sgp/crs/misc/RL30240.pdf [https://perma.cc/TF55-C28E] (describing shared yet independent authority of committees in both chambers to conduct oversight); *see also* Neal Kumar Katyal, *Internal Separation of Powers: Checking Today's Most Dangerous Branch from Within*, 115 YALE L. REV. 2314, 2324–27 (2014) (describing benefits of bureaucratic overlap and agency redundancy).

51. *Rebooting Oversight*, *supra* note 38; Handler, *supra* note 47.

52. *Cyberspace Mandate*, *supra* note 38.

53. CSC FINAL REPORT, *supra* note 5, at 35.

54. *Homeland Cybersecurity*, *supra* note 37.

55. *Hearing on the Hack of U.S. Networks by a Foreign Adversary: Hearing Before the Select Comm. on Intel.*, 117th Cong. (2021), https://www.intelligence.

Innovative Technologies and Information Systems held a hearing on "Innovation Opportunities and Vision for the Science and Technology Enterprise,"[56] and the Senate Armed Services Committee held a hearing on "Emerging Technologies and their Impact on National Security."[57] On February 26, 2021, the House Homeland Security Committee held a hearing on "The Role of Private Tech in the SolarWinds Breach and the Ongoing Campaign."[58] On March 10, 2021, the House Committee on Appropriations, Subcommittee on Homeland Security held a hearing on "Modernizing the Federal Civil Approach to Cybersecurity."[59] On March 12, 2021, the House Armed Services Subcommittee on Cyber, Innovative Technologies and Information Systems and the House Oversight and Reform Subcommittee on National Security held a joint hearing on the "Recommendations of the National Security Commission on Artificial Intelligence." [60] On April 21, 2021, the House Energy and Commerce Subcommittee on Communications and Technology held a hearing on "Securing American Network Technology"[61] and the Senate Armed Services Committee held a hearing on "The Current and Future Cyber

---

senate.gov/hearings/open-hearing-hearing-hack-us-networks-foreign-adversary [https://perma.cc/KN5H-E8AK].

56. *Innovation Opportunities and Vision for the Science and Technology Enterprise: Hearing Before the Subcomm. on Cyber, Innovative Techs., and Info. Sys.,* 117th Cong. (2021), https://armedservices.house.gov/hearings?ID=706C682F-ECFC-40CD-B0D9-87A46C7BD3B3 [https://perma.cc/M2AL-FG6K].

57. *Emerging Technologies and Their Impact on National Security, Hearing Before the Comm. on Armed Serv.,* 117th Cong. (2021), https://www.armed-services.senate.gov/hearings/21-02-23-emerging-technologies-and-their-impact-on-national-security [https://perma.cc/YR2Y-JC59].

58. *Weathering the Storm: The Role of Private Tech in The SolarWinds Breach and the Ongoing Campaign, Hearing Before the Comm. on Homeland Sec.,* 117th Cong. (2021), https://homeland.house.gov/weathering-the-storm-the-role-of-private-tech-in-the-solarwinds-breach-and-the-ongoing-campaign [https://perma.cc/9QU9-V4ZW].

59. *Modernizing the Federal Civilian Approach to Cybersecurity: Hearing Before the H. Subcomm. on Homeland Sec.,* 117th Cong. (2021), https://appropriations.house.gov/events/hearings/modernizing-the-federal-civilian-approach-to-cybersecurity [https://perma.cc/EPG8-64U4].

60. *Final Recommendations of the National Security Commission on Artificial Intelligence: Hearing Before the Subcomm. on Cyber, Innovative Techs., and Info. Sys. and H. Comm. on Oversight & Reform's Subcomm. on Nat'l Sec.,* 117th Cong. (2021), https://armedservices.house.gov/hearings?ID=32A667CD-578C-4F65-9F4F-1E26EE8F389A [https://perma.cc/MB8W-JTN6].

61. *Leading the Wireless Future: Securing American Network Technology: Hearing Before Subcomm. on Comm'ns and Tech. of the Comm. on Energy and Com.,* 117th Cong. (2021), https://energycommerce.house.gov/committee-activity/hearings/rescheduled-hearing-on-leading-the-wireless-future-securing-american [https://perma.cc/JXV7-RXPQ].

Workforce of the Defense Department and the Military Services."[62] On April 30, 2021, the House Armed Services Subcommittee on Cyber, Innovative Technologies and Information Systems held a hearing on "Technology and Information Warfare: The Competition for Influence and the Department of Defense."[63] On May 3, 2021, the House Homeland Security Committee, Subcommittee on Cybersecurity, Infrastructure Protection and Innovation held a hearing on "Responding to Ransomware: Exploring Policy Solutions to a Cybersecurity Crisis."[64]

The number of committees and subcommittee hearings in this short period, and the variety of cyber-related topics addressed in the hearings, illustrate the "patchwork mismatch" currently plaguing congressional oversight efforts. This fractured congressional committee structure, demonstrated above, exacerbates the problems stemming from the executive branch's dispersion of cybersecurity responsibilities. Both problems then contribute to the third challenge created by the U.S. government's disorganized cyber architecture: inadequate collaboration with the private sector.

### C. Inadequate Collaboration with the Private Sector

No summary of the U.S. government's cyber disorganization problem would be complete without noting the lack of effective collaboration with the private sector. Authors Richard Clarke & Robert Knake note the "collective groan from those in the industry" that meets calls for public-private partnerships and shared responsibility for cybersecurity.[65] Complaints abound from all directions, and this may be one of the knottiest challenges facing the U.S. government as it considers reforms to the cybersecurity organizational chart. While it is beyond the scope of this to provide a full accounting of the private sector collaboration

---

62. *Hearing to Receive Testimony on the Current and Future Cyber Workforce in the Department of Defense and the Military Services: Hearing Before the Subcomm. on Pers. of the Comm. on Armed Serv.,* 117th Cong. (2021), https://www.armed-services.senate.gov/hearings/to-receive-testimony-on-the-current-and-future-cyber-workforce-of-the-department-of-defense-and-the-military-services [https://perma.cc/63M3-FW3E].

63. *Technology and Information Warfare: The Competition for Influence and the Department of Defense: Hearing Before the Subcomm. on Cyber, Innovative Techs., and Info. Sys.,* 117th Cong. (2021), https://armedservices.house.gov/hearings?ID=142102B1-A2F8-44E5-B000-CB328CDFE196 [https://perma.cc/642M-WCPJ].

64. *Responding to Ransomware: Exploring Policy Solutions to a Cybersecurity Crisis: Hearing Before Subcomm. on Cybersecurity, Infrastructure, & Innovation of the Comm. on Homeland Sec.,* 117th Cong. (2021), https://homeland.house.gov/activities/hearings/responding-to-ransomware-exploring-policy-solutions-to-a-cybersecurity-crisis [https://perma.cc/RSU6-NWH3].

65. CLARKE & KNAKE, *supra* note 6, at 89.

problem, it is helpful to group the challenges into three categories: hesitancy to seek federal assistance; confusion on which federal agencies to contact; and distrust over sharing cyber threat and vulnerability information.

The first challenge involves hesitancy about alerting the federal government when a company encounters a cyber incident. This hesitancy stems in part from concerns about the government overstaying its welcome and investigating matters unrelated to the cyber incident, potentially exposing the company to antitrust and FTC enforcement actions.[66] During the Obama administration, the government initiated several efforts to alleviate these concerns by providing assurances and codifying liability protections for sharing certain types of cyber-related information.[67] Despite these efforts, few companies participate in the mechanisms provided and the hesitancy to alert the government remains.[68]

A second challenge is that many companies remain confused as to which federal government agency to contact–the FBI, CISA, US-CERT? This confusion stems from the "who sits at the cyber help desk" problem noted above. The severity and type of cyber incident may lead a company

---

66. *Id.* at 113; Jill Rhodes & Robert S. Litt, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 219-42 (2d ed. 2019).

67. *See* Cybersecurity Information Sharing Act of 2015, 6 U.S.C. §§ 1501–10 (2015); U.S. DEP'T OF JUST. AND FED. TRADE COMM'N, ANTITRUST POLICY STATEMENT ON SHARING OF CYBERSECURITY INFORMATION (Apr. 10, 2014), https://www.ftc.gov/system/files/documents/public_statements/297681/140410ftcdojcyberthreatstmt.pdf [https://perma.cc/5E8P-G4QX]; Exec. Order No. 13691, Promoting Private Sector Cybersecurity Information Sharing, 80 Fed. Reg. 9,349 (Feb. 20, 2015); *Information Sharing and Analysis Organizations (ISAOS)*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/information-sharing-and-analysis-organizations-isaos (last visited Feb. 23, 2021) [https://perma.cc/SK9X-TD88]. For a summary of why these efforts are so difficult, see Robert Knake, S*haring Classified Cyber Threat Information with the Private Sector*, COUNCIL ON FOREIGN RELATIONS (May 15, 2018), https://www.cfr.org/report/sharing-classified-cyber-threat-information-private-sector [https://perma.cc/J6NV-9Z73].

68. Joseph Marks, *Only 6 Non-Federal Groups Share Cyber Threat Info with Homeland Security*, NEXTGOV (Jun. 27, 2018), https://www.nextgov.com/cybersecurity/2018/06/only-6-non-federal-groups-share-cyber-threat-info-homeland-security/149343/ [https://perma.cc/8MCK-K7C9]. While CISA has increased the overall number of AIS program participants by 142 percent since the program's inception in 2016, "only 2 of 188 AIS participants (1 percent) shared cyber indicators with CISA in 2017, and only 9 of 252 participants (3 percent) shared indicators in 2018." OFF. OF THE INSPECTOR GEN. FOR HOMELAND SEC., DHS MADE LIMITED PROGRESS TO IMPROVE INFORMATION SHARING UNDER CYBERSECURITY ACT IN CALENDAR YEARS 2017 AND 2018 8, 12 (2020), https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-74-Sep20.pdf [https://perma.cc/YPS2-YSPW].

in different directions, and by design[69] will determine the level of government support. Of course, many large companies with well-financed IT departments have detailed incident response plans and decision trees that identify the appropriate federal agency.[70] But then, most companies, regardless of size, simply do not have the resources to do so.[71] Thus, the perception of a disorganized federal responses may be more harmful than actually warranted. Nonetheless, it persists.

A third problem in this area is that the U.S. government has a reputation for failing to share the cyber-related information it possesses. The Vulnerabilities Equities Process and Policy[72] is an executive branch policy that guides the decision-making process when the government discovers exploitable weaknesses, or vulnerabilities, in information systems. This interagency mechanism seeks to balance the private sector's (and the public's) interest in disclosure with the government's need to keep such vulnerabilities secret for national security, intelligence, or law enforcement purposes.[73] Since its inception, scholars and companies have criticized the policy for being biased in favor of defense and intelligence interests.[74] Specifically, the lack of private sector representation on the

69. PPD-41, *supra* note 31. PPD-41 offers important guidance on which federal entities have lead responsibility for responding to various types of cyber incidents. In practice, however, the directive poses almost as many questions as it resolves.

70. CLARKE & KNAKE, *supra* note 6 at 33–61.

71. Kate Polit, *Majority of Organizations Lack a Cybersecurity Incident Response Plan*, MERITALK (Apr. 11, 2019, 11:29 AM), https://www.meritalk.com/articles/majority-of-organizations-lack-a-cybersecurity-incident-response-plan/ [https://perma.cc/2TKP-MBAN].

72. WHITE HOUSE, VULNERABILITIES EQUITIES POLICY AND PROCESS FOR THE UNITED STATES GOVERNMENT (2017), https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF [https://perma.cc/ZZ4N-2BJY].

73. *Id.*

74. Sharon Bradford Franklin, *The Need for Countries to Establish Robust and Transparent Vulnerabilities Equities Processes*, 6 FLETCHER SEC. REV. 45 (2019); SVEN HERPIG, GOVERNMENTAL VULNERABILITY ASSESSMENT AND MANAGEMENT: WEIGHING TEMPORARY RETENTION VERSUS IMMEDIATE DISCLOSURE OF 0-DAY VULNERABILITIES (2018), https://www.stiftung-nv.de/sites/default/files/vulnerability_management.pdf [https://perma.cc/BSE5-HFEN]; Ari Schwartz & Rob Knake, *Discussion Paper 2016-04*, *Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process*, 2016 HARV. KENNEDY BELFER CTR. 8, https://www.belfercenter.org/sites/default/files/files/publication/Vulnerability%20Disclosure%20Web-Final4.pdf [https://perma.cc/HA6H-Y9LE]; Brad Smith, *The Need for Urgent Collective Action to Keep People Safe Online: Lessons from Last Week's Cyberattack,* MICROSOFT (May 14, 2017), https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/ [https://perma.cc/Z9SM-EK87].

decision-making body has fomented distrust within the private sector. For example, the National Security Agency's (NSA) decision to retain knowledge of the Eternal Blue vulnerability in Microsoft operating systems for five years after discovering it (and using it for intelligence exploits) badly damaged its relationship with private sector entities.[75] Despite the NSA's recent efforts[76] to rebuild that trust, the residue from that failure to share has cast a long shadow. Even when the government would like to share cyber information, a number of challenges relating to classified information and the protection of sources and methods, inhibits the ability to quickly disseminate the information to partners in the private sector.[77]

The SolarWinds hack provides a compelling reminder that government and private sector networks are intimately connected and interdependent, and that effective coordination and timely information sharing are critical to the cybersecurity task.[78] While this observation seems obvious, attempts to remedy this problem have been met with little success. The much-heralded CSC Final Report highlighted the need to "operationalize cybersecurity collaboration with the private sector" as one of six pillars supporting a strategy of layered deterrence.[79] The report urged the U.S. government and industry to develop "a new social contract of

---

75. Ellen Nakashima & Craig Timberg, *NSA Officials Worried About the Day Its Potent Hacking Tool Would Get Loose. Then it Did*, WASH. POST (May 16, 2017), https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html [https://perma.cc/N92N-X528]; *see also* Lily Hay Newman, *The Leaked NSA Spy Tool that Hacked the World*, WIRED (Mar. 7, 2018, 8:00 AM), https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/ [https://perma.cc/2XEN-AW7B]. For a detailed history of this episode, see NICOLE PERLROTH, THIS IS HOW THEY TELL ME THE WORLD ENDS: THE CYBER WEAPONS ARMS RACE (2020), 308-09, 340-41, 347–49; BEN BUCHANAN, THE HACKER AND THE STATE: CYBER ATTACKS AND THE NEW NORMAL OF GEOPOLITICS (2020), 253–54.

76. Ellen Nakashima, *The Cybersecurity 202: Here's Why NSA Rushed to Expose a Dangerous Computer Bug,* WASH. POST (Feb. 6, 2020), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/02/06/the-cybersecurity-202-here-s-why-nsa-rushed-to-expose-a-dangerous-computer-bug/5e3b0f41602ff15f8279a52e/ [https://perma.cc/H2DL-BHGV].

77. Robert K. Knake, S*haring Classified Cyber Threat Information With the Private Sector*, COUNCIL ON FOREIGN RELS. (May 15, 2018), https://www.cfr.org/report/sharing-classified-cyber-threat-information-private-sector [https://perma.cc/74M9-ZWR5].

78. *See SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (Infographic)*, U.S. GOV'T ACCOUNTABILITY OFF.: GAO@100 BLOG (Apr. 22, 2021), https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic [https://perma.cc/Z7KD-376K].

79. CSC FINAL REPORT, *supra* note 5, at 30.

shared responsibility to secure the nation in cyberspace."[80] The new arrangement must include better information sharing mechanisms to achieve "truly shared situational awareness" of cyber threats.[81]

As of February 2021, nine U.S. government entities have been identified as victims of the SolarWinds hack, as well as over 100 private companies.[82] The U.S. government's detection systems, including many that were heralded, failed to detect, identify, or halt the breach.[83] Rather, a private sector company, FireEye, alerted the U.S. government to the breach.[84] At least one private company identified the breach several months before FireEye, but decided not to share that cyber threat intelligence with other companies or the federal government.[85] The lack of coordination impacted the U.S. government's response to the incident as well, as each

80. *Id.* at 96.

81. *Id.*

82. White House Press Release, Press Briefing by Press Secretary Jen Psaki and Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger (Feb. 17, 2021), https://www.whitehouse.gov/briefing-room/press-briefings/2021/02/17/press-briefing-by-press-secretary-jen-psaki-and-deputy-national-security-advisor-for-cyber-and-emerging-technology-anne-neuberger-february-17-2021/ [https://perma.cc/WL6R-86R6].

83. Justin Katz, *Does Einstein Need a Post-SolarWinds Makeover*, FCW (Feb. 1, 2021), https://fcw.com/articles/2021/02/01/einstein-rethink-supply-chain-hack.aspx [https://perma.cc/HA49-SWZT]; Craig Timberg & Ellen Nakashima, *The U.S. Government Spent Billions on a System for Detecting Hacks. The Russians Outsmarted It,* WASH. POST (Dec. 15, 2020, 9:48 PM), https://www.washingtonpost.com/national-security/ruusian-hackers-outsmarted-us-defenses/2020/12/15/3deed840-3f11-11eb-9453-fc36ba051781_story.html [https://perma.cc/S766-4TNY]. As of the writing of this article, debates continue as to the scope of the hack and whether it was more akin to espionage or a use of force. *See, e.g.*, Dmitri Alperovitch, Erica Borghard, Jason Healey & Ryan Evans, *Great Power Cyber Party*, WAR ON THE ROCKS (Apr. 19, 2021), https://warontherocks.com/2021/04/great-power-cyber-party/ [https://perma.cc/BL49-FX7W]. Debates also continue on whether the EINSTEIN detection system was intended to or designed to detect this type of activity. *See* Katz, *supra*.

84. *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor,* FIREEYE: THREAT RESEARCH BLOG (Dec. 13, 2020), https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html [https://perma.cc/X87G-F9WN].

85. Nikesh Arora, *Palo Alto Networks Rapid Response: Navigating the SolarStorm Attack,* PALO ALTO NETWORKS, (Dec. 17, 2020, 6:03 PM), https://blog.paloaltonetworks.com/2020/12/solarwinds-statement-solarstorm/ [https://perma.cc/YNL3_2XGT]; Robert K. Knake, *Most Tools Failed to Detect the SolarWinds Malware. Those That Did Failed Too,* COUNCIL ON FOREIGN RELS. (Jan. 28, 2021, 11:07 AM), https://www.cfr.org/blog/most-tools-failed-detect-solarwinds-malware-those-did-failed-too [https://perma.cc/A9N2-Y9EC].

agency sought to conduct its own post-event review.[86] In addition, congressional committees are battling for the spotlight as each committee seeks to demonstrate its commitment to cybersecurity, and to holding executive branch officials to account for the SolarWinds episode.[87] In sum, SolarWinds is only the most recent of many incidents that have exposed the government's cybersecurity organization problem. It may however prove to be the episode that incentivizes meaningful reform.

## II. CONVENTIONAL SOLUTIONS TO THE U.S. GOVERNMENT'S CYBERSECURITY ORGANIZATIONAL PROBLEM

The section above examined the most vexing aspects of the government's disorganized cyber architecture. Taking account of those aspects, this section profiles the solutions currently being proffered to reorganize the U.S. government's approach to its cyber-related responsibilities. Calls for reform of the U.S. government's cybersecurity

86. A letter to administration officials dated February 9, 2021 from Senators Mark Warner and Marco Rubio, Chair and Vice Chair of the Senate Intelligence Committee, criticized the executive branch for a "disjointed and disorganized response" to the SolarWinds breach. Letter from Mark Warner, Chairman of the S. Select Comm. on Intel., and Marco Rubio, Vice Chairman of the S. Select Comm. on Intel., to Avril Haines, Dir. of Nat'l Intel., Paul Nakasone, Dir. of Nat'l Sec. Agency, Christopher Wray, Dir. of the Fed. Bureau of Investigation, and Brandon Wales, Acting Dir. of the Cybersecurity and Infrastructure Sec. Agency (Feb. 9, 2021), https://www.warner.senate.gov/public/_cache/files/f/2/f26e92ba-2b05-4e65-bbda-10d3a8dc1c81/0CE82FCBF5172B642C7B6F9C2440B778.hainesnakasonewraywales-ssci-09feb21.pdf [https://perma.cc/L84N-BGLS]. In response, the White House insisted that Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger was leading response efforts. Julian E. Barnes & David E. Sanger, *White House Announces Senior Official Is Leading Inquiry Into SolarWinds Hacking*, N.Y. TIMES (Feb. 10, 2021), https://www.nytimes.com/2021/02/10/us/politics/biden-russia-solarwinds-hacking.html [https://perma.cc/Q58C-SVFA].

87. Maggie Miller, *Hearings Examine Consequences of Massive SolarWinds Breach*, THE HILL (Feb. 23, 2021, 6:00 AM), https://thehill.com/policy/cybersecurity/539981-hearings-examine-consequences-of-massive-solarwinds-breach [https://perma.cc/DX92-UEYV]; Corinne Reichart, *SolarWinds Hearing Announced by House Committees*, CNET (Feb. 22, 2021, 12:44 PM), https://www.cnet.com/news/solarwinds-hearing-announced-by-house-committees/ [https://perma.cc/5G33-MQVJ]; Alyza Sebenius & Kevin Cirilli, *SolarWinds Hack Grabs Senate Spotlight with CEO in the Hot Seat*, BLOOMBERG (Feb. 23, 2021, 6:00 AM), https://www.bloomberg.com/news/articles/2021-02-23/key-lawmaker-prepares-for-first-public-hearing-on-major-hack [https://perma.cc/G365-FR96]; *U.S. House Committees to Hold Feb. 26 Hearing on 'SolarWinds' Hack*, REUTERS (Feb. 22, 2021, 10:54 AM), https://www.reuters.com/article/usa-cyber-solarwinds/us-house-committees-to-hold-feb-26-hearing-on-solarwinds-hack-idUSL1N2KS1QC [https://perma.cc/6KF2-P7EH].

architecture have been numerous and have been around for a quite a while.[88] The most comprehensive of the recent calls for organizational reform is contained in the March 2020 report of the Cyberspace Solarium Commission (CSC Final Report).[89] The report tackles the cyber disorganization problem head-on and focuses its foundational pillar on the need to reform the U.S. government's structure and organization for cyberspace.[90] Missing from the CSC Final Report and other calls for reform, however, is recognition of the important contributions that inspectors general can make–and indeed have already made–in addressing the government's cyber disorganization problem. This section will provide an overview of the most common recommendations and briefly highlight the intersection points for contributions by inspectors general.

Synthesizing the various calls for organizational reform reveals recommendations that fall into five categories and that focus on remedying two types of defects. The first category focuses on calls for the White House to update the national cyber strategy.[91] The most recent strategy[92]

---

88. *See* GAO-20-629*, supra* note 6; CLARKE & KNAKE, *supra* note 6; David H. Petraeus & Kiran Sridhar, *The Case for a National Cybersecurity Agency*, POLITICO (Sept. 5, 2018, 5:18 AM), https://www.politico.com/agenda/story/2018/09/05/cybersecurity-agency-homeland-security-000686/ [https://perma.cc/CS4E-YZNQ]; *Cyberspace Mandate*, *supra* note 38.

89. CSC FINAL REPORT, *supra* note 5, at 2. The CSC was a congressionally-created commission that was tasked with developing "a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences." John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, 132 Stat. 1636, 2141–46 (2018) (codified in scattered sections of 5 U.S.C., 10 U.S.C., 14 U.S.C., 41 U.S.C., 47 U.S.C., and 50 U.S.C.). The Commission's efforts were contained in a 180-page report issued in March 2020. The CSC Final Report calls for a cohesive U.S. cyber strategy of layered cyber deterrence, with the objective of reducing the probability and impact of cyberattacks of significant consequence. The report is structured along six pillars, and each pillar includes key recommendations as well as enabling recommendations.

90. CSC FINAL REPORT, *supra* note 5, at 1–7. The report's recommendations provide an important roadmap in this reorganization exercise because they incorporate the suggestions and observations of earlier critics, while adding valuable insights from the interagency, interbranch, and private sector perspectives.

91. Handler, *supra* note 47; U.S. CYBERSPACE SOLARIUM COMM'N, TRANSITION BOOK FOR THE INCOMING BIDEN ADMINISTRATION: CSC WHITE PAPER #5 (2021), https://www.solarium.gov/public-communications/transition-book [https://perma.cc/ZX24-RNQH] [hereinafter CSC WHITE PAPER #5]; Richard J. Harknett, *SolarWinds: The Need for Persistent Engagement,* LAWFARE (Dec. 23, 2020 4:41 PM), https://www.lawfareblog.com/solarwinds-need-persistent-engagement [https://perma.cc/867G-ZHQD].

92. Terri Moon Cronk, *White House Releases First National Cyber Strategy in 15 Years*, DOD NEWS (Sept. 21, 2018), https://www.defense.gov/Explore/News/

was published in 2018, and the prior strategy was last updated in 2003. The calls for a revamp of the national cyber strategy focus on ensuring alignment with a strategy of layered cyber deterrence[93], and providing mechanisms for better engagement with the private sector.[94] The CSC Final Report urged the executive branch to issue a new national cyber strategy designed to bring "coherence to the federal government's efforts" and to better integrate the "various departments and agencies [that] constitute critical but separate components of an effective national cyber strategy."[95]

The second recommendation category, tied closely to the first, seeks the establishment of a National Cyber Director, and accompanying office, within the executive branch. The goal of this position is to provide an executive branch that is "more agile and effective in cyberspace."[96] While some worry the position will only create more bureaucracy[97], Congress endorsed the establishment of a National Cyber Director (NCD) in the National Defense Authorization Act for FY 2021.[98] Among the

---

Article/Article/1641969/white-house-releases-first-national-cyber-strategy-in-15-years/ [https://perma.cc/5CD6-MM9H].

93. CSC FINAL REPORT, *supra* note 5, at 32; CSC WHITE PAPER #5, *supra* note 91, at 4.

94. Handler, *supra* note 47; CSC WHITE PAPER #5, *supra* note 91, at 4; Brad Smith, *A Moment of Reckoning: the Need for a Strong and Global Cybersecurity Response*, MICROSOFT (Dec. 17, 2020), https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/ [https://perma.cc/YB9C-4ADK].

95. CSC FINAL REPORT, *supra* note 5, at 31–32.

96. *Id.* at 37.

97. James N. Miller & Robert Butler, *Making the National Cyber Director Operational With a National Cyber Defense Center*, LAWFARE (Mar. 24, 2021, 10:48 AM), https://www.lawfareblog.com/making-national-cyber-director-operational-national-cyber-defense-center [https://perma.cc/2237-V72N]; 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/2ZE2-794U]; Philip Reitinger, *Establishing a National Cyber Director Would Be a Mistake*, LAWFARE (Jul. 17, 2020, 8:31 AM), https://www.lawfareblog.com/establishing-national-cyber-director-would-be-mistake [https://perma.cc/69RS-K3MZ].

98. WILLIAM M. (MAC) THORNBERRY NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2021, Pub. L. No. 116-283, 134 Stat. 3388 (2021) (codified in scattered sections of 6 U.S.C., 12 U.S.C., 15 U.S.C., 16 U.S.C., 22 U.S.C., 24 U.S.C., 33 U.S.C., 34 U.S.C., 42 U.S.C., 43 U.S.C., 47 U.S.C., 48 U.S.C., 50 U.S.C., and 52 U.S.C.). In 2021, President Biden nominated and the Senate confirmed Chris Inglis as the first National Cyber Director. In addition, the Senate confirmed President Biden's nominations of Anne Neuberger to the post of deputy national security advisor for cyber and emerging technology on the National Security Council, and Jen Easterly as the Director of the Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security. *See* Natasha Bertrand, *Biden taps intelligence veteran for new White House*

NCD's duties are serving as the principal advisor to the president on cybersecurity policy and strategy, leading coordination efforts for national cyber policy and strategy, reporting annually to Congress, and coordinating and consulting with private sector leaders on cybersecurity and emerging technology issues.[99] While the establishment of the position represents a critical step in preparing the architecture needed to adopt a whole of government approach to cyber threats, questions remain as to the NCD's ability to affect meaningful change[100] and the position's relationship with the National Security Council.[101]

The third category calls for streamlining the congressional committee structure. Specifically, the CSC recommends the establishment of two new cybersecurity-focused committees in Congress "to consolidate budgetary and legislative jurisdiction over cybersecurity issues, as well as traditional oversight authority."[102] As noted above, the current congressional committee structure can be described kindly as disjointed and, more accurately, as dysfunctional. Nonetheless, reforming entrenched committee power is a difficult task.[103] Substantive reform efforts with the legislative branch may have to wait for the executive branch to first put its cyber house in order, and to then build a committee structure that is responsive to the executive's organizational scheme.

A fourth category includes recommendations to strengthen the Cybersecurity and Infrastructure Security Agency (CISA). CISA serves as the "[n]ation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future," and its mission is "to understand and manage cyber and

---

*cybersecurity role*, POLITICO (Jan. 6, 2021, 2:56 PM), https://www.politico.com/news/2021/01/06/biden-white-house-cybersecurity-neuberger-455508 [https://perma.cc/LXQ3-69UT]; Bridget Johnson, *Jen Easterly Confirmed as New CISA Director*, HOMELAND SECURITY TODAY (July 12, 2021), https://www.hstoday.us/people-on-the-move/jen-easterly-confirmed-as-new-cisa-director/ [https://perma.cc/6NH5-2XZM]. While questions remain about each position's ability to affect meaningful change and the relationship between the positions, their formation prepares the architecture needed to adopt a whole of government approach to cyber threats. Grotto, *supra* note 97; Joshua Rovner, *A Lower Bar for the Cyber Czar*, WAR ON THE ROCKS (Jan. 26, 2021), https://warontherocks.com/2021/01/a-lower-bar-for-the-cyber-czar/ [https://perma.cc/E73G-H5MZ].

99. *See* WILLIAM M. (MAC) THORNBERRY NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2021, Pub. L. No. 116-283, 134 Stat. 3388 (2021) (codified in scattered sections of 6 U.S.C., 12 U.S.C., 15 U.S.C., 16 U.S.C., 22 U.S.C., 24 U.S.C., 33 U.S.C., 34 U.S.C., 42 U.S.C., 43 U.S.C., 47 U.S.C., 48 U.S.C., 50 U.S.C., and 52 U.S.C.).

100. Grotto, *supra* note 97.

101. Rovner, *supra* note 98.

102. CSC FINAL REPORT, *supra* note 5, at 35.

103. *See, e.g.*, Andrew McCanse Wright, *Constitutional Conflict and Congressional Oversight*, 98 MARQ. L. REV. 881 (2014).

physical risk to our critical infrastructure"[104] Recommendations in this category focus on increasing CISA's budget and staffing,[105] growing CISA's role as the go to agency for other federal civilian government agencies on cybersecurity-related matters,[106] growing CISA's private sector outreach efforts,[107] and providing CISA with certain administrative subpoena powers.[108]

A fifth category includes the ever present calls for developing "a stronger federal cyber workforce."[109] The CSC's Transition Memo[110] offers the following assessment of the enduring workforce challenge:

> At present, the public sector needs to fill more than 37,000 cybersecurity jobs. Given that the sector currently employs more than 56,000 cybersecurity professionals, this shortfall means that about one in three public-sector cybersecurity jobs sits unfilled. Meanwhile firms are confronted with the challenge of filling almost half a million cybersecurity jobs. To address unfilled federal cyber jobs in 2009, experts called for the White House cybersecurity coordinator to develop a federal cyber workforce strategy. Twelve years later, the U.S. federal government still does not have an effective cyber workforce strategy or any clear leader responsible for developing and implementing such a strategy.[111]

---

104. *About CISA*, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/about-cisa [https://perma.cc/PH97-RD9R] (last visited Aug. 22, 2021).

105. *See* CSC FINAL REPORT, *supra* note 5, at vi, 3, 39–40; CSC WHITE PAPER #5, *supra* note 91, at 5.

106. *See* CSC FINAL REPORT, *supra* note 5, at 31–33, 35, 37–41, 45.

107. *Id.* at v– vi,1– 7, 14, 16– 19, 23– 26, 29– 33, 39– 40, 45, 50– 51; CSC WHITE PAPER #5, *supra* note 91, at 1, 3–5.

108. WILLIAM M. (MAC) THORNBERRY NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2021, H.R. 6395, 116th Cong. § 1716 (2021) (enacted) (allowing CISA to issue subpoenas to internet service providers to release vulnerability information from the networks of critical infrastructure organizations).

109. CSC FINAL REPORT, *supra* note 5, at 43.

110. CSC WHITE PAPER #5, *supra* note 91, at 7.

111. *Id.* (citing "Cybersecurity Supply/Demand Heat Map," CYBERSEEK, https://www.cyberseek.org/heatmap.html [https://perma.cc/8C9V-5BE9] (last visited Oct. 5, 2021)); Partnership for Public Service & Booz Allen Hamilton, *Cyber In-Security: Strengthening the Federal Cybersecurity Workforce* (2009) https://ourpublicservice.org/wp-content/uploads/2018/09/Cyber_In-Security__Strengthening_the_Federal_Cybersecurity_Workforce-2009.07.22.pdf [https://perma.cc/WEP3-GV8Q]. In comparison, CLARKE & KNAKE, *supra* note 6, at 144–153,

The solutions proffered to address the federal government's cyber workforce shortage are plentiful and include expanding CyberCorps Scholarship for Service Program,[112] establishing a centralized workforce leadership and coordination structure for the federal cyber workforce,[113] and ensuring the availability of special hiring authorities and pay flexibilities for cyber talented employees.[114]

The five recommendations outlined above reveal efforts to tackle two types of organizational defects. The first centers on agency waste and duplication within the executive branch. As the CSC report notes, "[m]any departments and agencies, with different responsibilities for and interests in securing cyberspace, compete for resources and power, resulting in conflicting efforts sometimes carried out at cross-purposes."[115] The second defect focuses on the lack of accountability or clarity as to who has ultimate responsibility—in either the executive or legislative branches—for cybersecurity policy and oversight. In many instances, the lack of clarity is due to the overly dispersed reporting lines and committee structures described above. Both concerns fall squarely into the type of work that inspectors general perform: identification of waste and duplication, and evaluation of organizational and programmatic effectiveness.

The reform recommendations described above are well-intended efforts toward a better organizational framework for the U.S. government's cybersecurity. These recommendations, however, neglect the role that inspectors general play in supporting new governance structures and illuminating the structural defects that remain. Reform efforts will be significantly enhanced by the work of inspectors general across the executive branch, and particularly by the work of inspectors general in the Department of Homeland Security, the Department of Defense, and the Inspector General for the Intelligence Community. A few examples of recent inspector general activities illustrate their unique ability to flag points of duplication, waste, and inefficiency in the government's cybersecurity efforts.[116] For example, the annual reports required by the

---

167–178, suggest that the cyber workforce talent problem is not as dire as portrayed, and offer two programs designed to create a better pipeline.

112. CLARKE & KNAKE, *supra* note 6, at 172 (suggesting a professional cadre of federal cybersecurity officers); CSC WHITE PAPER #5, *supra* note 91, at 8 (prioritizing program in budgetary requests to Congress "in order to (1) increase the number of colleges and universities that participate in the program and (2) increase the number of scholarships awarded at participating institutions.").

113. CSC WHITE PAPER #5, *supra* note 91, at 6–7.

114. *Id.* at 8.

115. CSC FINAL REPORT, *supra* note 5, at 37.

116. OFF. OF THE INSPECTOR GEN., DHS NEEDS TO IMPROVE CYBERSECURITY WORKFORCE PLANNING, 12–13 (2019), https://www.oig.dhs.gov/reports/2019/dhs-needs-improve-cybersecurity-workforce-planning/oig-19-62-sep19 [https://perma.cc/UE7B-U5XE] [hereinafter DHS OIG REPORT]; TRANSCRIPT OF HEARING TO

Federal Information Security Management Act (FISMA),[117] prepared by inspectors general in every agency, provide critical insight into how the U.S. government is meeting its cybersecurity requirements, including red flagging those agencies with persistently weak cybersecurity. Similarly, the Department of Homeland Security's inspector general reports evaluating the effectiveness of CISA's efforts to effectively disseminate information within the federal government and to effectively partner with the private sector, provide critical insights that can shape revisions to CISA's programs and budget.[118] Finally, there are numerous reports evaluating how federal agencies are meeting the cyber workforce challenge.[119] Drawing insights and lessons learned from these reports will prevent the recreation of the wheel problem that continually stymies workforce development efforts. The next section explores these examples in greater depth, and considers the attributes that make inspectors general uniquely well-positioned to support the U.S. government's cybersecurity reorganization effort.

## III. LOOKING PAST THE CONVENTIONAL SOLUTIONS: UNDERSTANDING AND EMBRACING THE WORK OF INSPECTORS GENERAL

The work of inspectors general will be critical to the cybersecurity reorganization mission, and particularly the task of developing a coordinated and cohesive cyber strategy that avoids duplication and waste. Inspectors general are well positioned to support a whole-of-government approach due to the following attributes: their legislative mandate allows them to serve as independent advisors; they occupy a special perch within their agencies and wield tools designed for the task of assessing waste and duplication; their role as policy evaluators is growing; Congress is increasingly reliant on inspectors general for information and evaluation;

---

RECEIVE TESTIMONY ON THE CURRENT AND FUTURE CYBER WORKFORCE IN THE DEPARTMENT OF DEFENSE AND THE MILITARY SERVICES BEFORE THE SUBCOMMITTEE ON PERSONNEL 26 (2021).

117. *See* Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (requiring each agency inspector general or independent external auditor to conduct an annual independent evaluation to determine effectiveness of information security programs and practices of its respective agency); *see also* Fiscal Year 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.1 (2021).

118. DEPARTMENT OF HOMELAND SECURITY BUDGET-IN-BRIEF FISCAL YEAR 2021, 3–4, 7, 49–54; DEPARTMENT OF HOMELAND SECURITY BUDGET-IN-BRIEF FISCAL YEAR 2022, at 3–4, 7-8, 55–60, 80.

119. DHS OIG REPORT, *supra* note 116, at 5, 7, 10–11; TRANSCRIPT OF HEARING TO RECEIVE TESTIMONY ON THE CURRENT AND FUTURE CYBER WORKFORCE IN THE DEPARTMENT OF DEFENSE AND THE MILITARY SERVICES BEFORE THE SUBCOMMITTEE ON PERSONNEL, *supra* note 116, at 4, 11–12, 14, 24–26.

and inspectors general have established an interagency mechanism for exchange between inspector general offices that could provide a framework for cybersecurity-related issues. This section examines each attribute in turn.

### A. Independent Advisors by Design

There are currently seventy-five inspectors general in the U.S. government[120] and more than 13,000 employees working in inspector general offices across the federal government.[121] Their task is to "serve as the principal watchdogs of the nation's major federal agencies."[122] While the concept of independent auditors within executive branch agencies has existed since the founding of the country,[123] the position was formalized and expanded in the Inspector General Act of 1978 (IGA), which created and currently governs the offices of statutory inspectors general.[124] The IGA fit into a group of legislative efforts, which Paul Light framed as a

120. COUNCIL OF THE INSPECTORS GEN. ON INTEGRITY AND EFFICIENCY, TOP MANAGEMENT AND PERFORMANCE CHALLENGES FACING MULTIPLE FEDERAL AGENCIES 1 (2021), https://www.ignet.gov/sites/default/files/untracked/TMPC_report_02022021.pdf [https://perma.cc/95BN-WWG9]; *see also Inspector General Vacancy Tracker*, POGO (Feb. 23, 2021), https://www.pogo.org/database/inspector-general-vacancy-tracker/ [https://perma.cc/DN4V-RLMD] (identifying 16 vacancies in federal inspector general offices as of June 25, 2021, meaning the top position in office is either vacant or filled by an acting inspector general).

121. CHARLES A. JOHNSON & KATHRYN E. NEWCOMER, U.S. INSPECTORS GENERAL: TRUTH TELLERS IN TURBULENT TIMES, 2 (2020) ("The number of officials working in OIGs has increased to over 13,000 federal employees, with a combined budget of $2.7 billion in 2016.").

122. H.R. REP. NO. 110-354, at 8 (2007).

123. JACK GOLDSMITH, POWER AND CONSTRAINT: THE ACCOUNTABLE PRESIDENCY AFTER 9/11, at 99 (2012) [hereinafter GOLDSMITH] ("Inspectors General, or IGs, 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.")

124. Inspector General Act of 1978, Pub. L. No. 95-452, 92 Stat. 1101, reprinted as amended in 5 U.S.C. app. (2021). For comprehensive works on the role of the inspectors general in U.S. government, see JOHNSON & NEWCOMER, *supra* note 121; CARMEN R. APAZA, INTEGRITY AND ACCOUNTABILITY IN GOVERNMENT: HOMELAND SECURITY AND THE INSPECTOR GENERAL (Tom Payne & Tom Lansford eds., 2010); INSPECTORS GENERAL: A NEW FORCE IN EVALUATION (MICHAEL HENDRICKS ET AL. EDS., 1990); PAUL C. LIGHT, MONITORING GOVERNMENT: INSPECTORS GENERAL AND THE SEARCH FOR ACCOUNTABILITY (1993); MARK H. MOORE & MARGARET JANE GATES, INSPECTORS-GENERAL: JUNKYARD DOGS OR MAN'S BEST FRIEND? (1986); Margaret J. Gates & Marjorie Fine Knowles, *The Inspector General Act in the Federal Government: A New Approach to Accountability*, 36 ALA. L. REV. 473, 473–74 (1984).

"busy season in the search for government accountability."[125] The act came about in particular response to executive branch abuses[126] and can be grouped with the War Powers Resolution of 1973,[127] the Ethics in Government Act of 1978,[128] the Civil Service Reform Act of 1978,[129] and the Foreign Intelligence Surveillance Act of 1978.[130] These statutes shared common goals: to ensure robust and accountable executive branch decision-making, to strengthen congressional oversight of executive branch agencies, and to increase Congress's access to information in the hands of executive branch agencies.[131]

To accomplish these goals, the defining feature of the inspector general position is independence. The core responsibilities outlined in Section 2 of the Act reflect this feature:

> (1) to conduct and supervise audits and investigations relating to the programs and operations of the establishments listed in section 12(2);
>
> (2) 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; and
>
> (3) 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

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

126. *See* S. REP. NO. 95-1071, at 4 (1978) (listing examples of "epidemic" levels of fraud, abuse and waste motivating enactment of the IGA).

127. War Powers Resolution, Pub. L. No. 93-148, 87 Stat. 555 (1973).

128. Ethics in Government Act of 1978, Pub. L. No. 95-521, 92 Stat. 1824.

129. Civil Service Reform Act of 1978, Pub. L. No. 95-454, 92 Stat. 1111.

130. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436.

131. *See supra* notes 124, 127, 128, 129, 130 (identifying purposes for enactment); KATHRYN FRANCIS, CONGRESSIONAL RSCH. SERV., STATUTORY INSPECTORS GENERAL IN THE FEDERAL GOVERNMENT: A PRIMER 2-3 (Jan 3, 2019), https://sgp.fas.org/crs/misc/R45450.pdf [https://perma.cc/9YVV-CCZJ] [hereinafter FRANCIS, A PRIMER] (describing history and tenets of Inspector General Act of 1978). For a broader overview of the history of federal inspectors general, see KATHRYN FRANCIS & MICHAEL GREENE, CONGRESSIONAL RSCH. SERV., FEDERAL INSPECTORS GENERAL: HISTORY, CHARACTERISTICS, AND RECENT CONGRESSIONAL ACTION, (Jul. 20, 2016), https://www.everycrsreport.com/files/20160720_R43814_c8b393d645313cc24a2b7a1bb8c1cb4abe072ccd.pdf [https://perma.cc/TC3E-ULN3] [hereinafter FRANCIS & GREENE].

> administration of such programs and operations and the necessity for and progress of corrective action . . . ."[132]

The independence feature also is prominent in the provisions governing the appointment and eligibility requirements for inspectors general. Section 3 states that inspectors general 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."[133] While inspectors general may be appointed in several ways, the usual route, dictated by § 3 of the IGA, is appointment by the President and confirmation by the Senate.[134] This method applies to inspectors general in the cabinet-level departments and larger agencies.[135]

The importance of protecting the independence of inspectors general is also reflected in the provisions governing removal, although Congress had to address the knotty separation of powers issues involving constraints on the President's removal power. The removal process for statutory inspectors general is generally uniform.[136] The President may remove an inspector general from office, so long as the president communicates in writing the reasons for removal or transfer to both Houses of Congress at least thirty days before the removal or transfer.[137] The courts have adopted a broad interpretation of this power, consistent with the President's removal powers of other executive officers, and the legislative history of the IGA indicates the President may "remove any Inspector General at any time."[138] The independence vein is reflected here not by limiting the President's removal power, but by requiring notice to Congress of the removal and the reasons for it.[139]

---

132. 5 U.S.C. app. 3 § 2; *see also* MOORE & GATES, *supra* note 124, at 15.

133. 5 U.S.C. app. 3 § 3(a). Candidates for the CIA inspector general and the Intelligence Community Inspector General (IC IG) must also have prior experience in the field of foreign intelligence or national security and be in compliance with the relevant security standards (50 U.S.C. §3517(b) and §3033(c), respectively, for the CIA inspector general and the IC IG). FRANCIS & GREENE, *supra* note 131, at 7.

134. 5 U.S.C. app. 3 § 3(a) ("There shall be at the head of each Office an Inspector General who shall be appointed by the President, by and with the advice and consent of the Senate, 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. *See* FRANCIS & GREENE, *supra* note 131, at 3–5, 7–8 (describing different methods of appointing federal inspectors general).

136. *See* FRANCIS, A PRIMER, *supra* note 131, at 12–13 (describing common removal methods, and noting special removal procedures for inspectors general in Designated Federal Entities (DFEs), U.S. Postal Service, and U.S. Capitol Police).

137. 5 U.S.C. app. 3 § 3(b).

138. H.R. REP. NO. 95-584, at 2, 9, 12 (1997).

139. *See generally* LIGHT, *supra* note 124.

More recent expressions of support for the preservation of the inspectors general's independence can be found in a variety of legislative proposals currently circulating in Congress which call for reforming the President's ability to remove inspectors general.[140] Many of these proposals, of course, were in response to former President Trump's spate of inspector general firings, most notably from intelligence and national security agencies.[141] Independence is also reflected in the day-to-day operational aspects of the position, including the selection process for work assignments,[142] the agency reporting structures,[143] and the budgetary mechanisms and process for inspector general funding.[144]

Despite the vast powers noted above, there are two important limits on the inspectors general's authority. First, the role is advisory only.[145] 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.[146] Indeed, this advisor role may actually be an advantage.[147] Without concern for implementation of remedies, the inspectors general do not pull their punches.[148] In other words, they do not pre-frame the problem in a way that allows for or leans heavily toward a desired solution.[149] The advisory status provides for

---

140. *See* Inspectors General Independence Act, S. 3664, 116th Cong. (2020); Inspectors General Independence Act, H.R. 6668, 116th Cong. (2020); 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); 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).

141. *See The Lawfare Podcast: Firing Inspectors General*, LAWFARE (May 19, 2020), https://www.lawfareblog.com/lawfare-podcast-firing-inspectors-general [https://perma.cc/93BC-YBSH].

142. 5 U.S.C. app. 3 § 4. Work assignments come from several sources, including congressional request, agency request, or at the initiation of the inspector general.

143. *Id.* § 3(a), (d). In most instances, inspectors general report directly to the agency head (or high-level member of the secretary's executive team). In addition, inspectors general report to the relevant congressional committees. While this dual reporting structure is not without its challenges, it has proven a workable arrangement. *See infra* Section III.D.

144. Inspector General Reform Act of 2008, 5 U.S.C. app. 3 §§ 1–13, § 8 (2008); H.R. REP. NO. 110-354, at 11 (2007).

145. 5 U.S.C. app. 3 §§ 2–4.

146. *Id.* § 4.

147. Glenn Fine, *Seven Principles of Highly Effective Inspectors General*, CTR. FOR THE ADVANCEMENT OF PUB. INTEGRITY 2 (2017), http://inspectorsgeneral.org/files/2017/06/Seven-Principles-of-Highly-Effective-Inspectors-General.pdf [https://perma.cc/KA7F-CRUK].

148. *Id.* at 3.

149. *Id.* at 3–4.

greater candor. The Senate report accompanying the 1978 IGA acknowledged the challenge of balancing the inspectors general's need for independence with the agency's management needs, concluding:

> 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."[150]

Second, and not surprisingly, this independence is somewhat constrained for inspectors general in national security agencies.[151] The statute includes additional provisions governing the inspectors general for the departments of defense, homeland security, and justice. The agency heads in these entities may block inspector general investigations or reports if they relate to certain sensitive topics or national security matters.[152] As such, these provisions carve away a large swath of inspector general independence 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.[153] In such situations, the inspector general "shall be under the authority, direction, and control" of the agency head, thus creating a sweeping exception to independence provisions in Section 3(a) of the IGA.[154] If the agency head determines such action is necessary to "preserve the national security interests of the United States,"[155] they may prohibit the inspector general from "initiating, carrying out, or completing any audit or investigation, from accessing information [relating to matters described above], or from issuing any subpoena."[156] The statutes and regulations governing the inspector general for the CIA, as well as inspectors general for several other intelligence community entities, include similar clauses allowing for national security exceptions to the

150. S. REP. NO. 95-1071, at 10–11 (Westlaw) (1978).

151. 5 U.S.C. app. 3 §§ 3(d), 5(e)(1)(B), 6(e)(7), 8(b).

152. *Id.* §§ 5(e)(B), 8(b)(1)(D), (b)(2), 8D(a)(1)(F), 8E(a)(1)(E), 8G(d)(2)(A), 8I(a)(1)(F).

153. *Id.* §§ 8(b)(1) (DoD), 8E(a)(1)-(2) (DOJ), 8I(2) (DHS).

154. *Id.* §§ 8(b)(1) (DoD), 8E(a)(1) (DOJ), 8I(a)(1) (DHS).

155. *Id.* §§ 8(b)(2) (DoD), 8E(a)(2) (DOJ), 8I(a)(2) (DHS).

156. *Id.*

usual inspector general independence.[157] Importantly, if an agency head invokes this prohibition, they must report the fact of the invocation to the relevant congressional committees.[158]

Despite these limits on the independence of inspectors general, there is no doubt the position was intended to be one of significant authority and structural clout. 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."[159] The independence and clout described above gain greater reach when paired with the position's unique and statutorily-mandated agency perch and accompanying tool kit.

### B. Special Perch and Effective Tools

Inspectors general are often viewed as "junkyard dogs"[160] by colleagues in their agencies for their exasperating, and at times, maddening pursuit of any procedural or substantive flaw, evoking the bothersome junkyard dog that follows you everywhere and continually digs for bones.[161] Of course, this dogged (forgive the pun) focus is intentional. The inspectors general were created to provide a critical internal oversight function by identifying wasteful, wrongful, and illegal activities in their agencies.[162] To accomplish this task, Congress created a special perch for the inspector general to occupy within the agency.[163] This perch allows the inspector general to get "deep inside the presidency,"[164] and provides unparalleled access and a wholistic perspective. The inspector general is able to access information relating to relevant legal interpretations, compliance with internal policies, as well as compliance with external

157. *Id.* §§ 8G(a)(1)(D), 8G(f)(3)(A); *see also generally* Shirin Sinnar, *Protecting Rights from Within? Inspectors General and National Security Oversight,* 65 STAN. L. REV. 1027 (2013).

158. 5 U.S.C. app. 3 §§ 8(b)(3)-(4) (Department of Defense), 8E(a)(3) (Department of Justice), 8I(3) (Department of Homeland Security).

159. Gates & Knowles, *supra* note 124, at 475.

160. MOORE & GATES, *supra* note 124 (title of the authors' work embraces the junkyard dog metaphor).

161. GOLDSMITH, *supra* note 123, at 108; MOORE & GATES, *supra* note 124.

162. MOORE & GATES, *supra* note 124, at 3.

163. GOLDSMITH, *supra* note 123, at 107.

164. *Id.* at 105. *But see* Andrew McCanse Wright, *Executive Privilege and Inspectors General*, 97 TEX. L. REV. 1295, for (exploring how ability of inspectors general to access agency materials can put agency executive privilege claims at risk, thus impacting effectiveness of inspectors general).

reporting requirements.[165] This special perch also allows the inspector general to acquire a comprehensive and in-depth understanding of the matter being studied.[166] Jack Goldsmith describes the advantages of this delegation: "Congress in effect delegates its initial oversight function to the inspector general, who can quickly gather a much more complete understanding of executive branch activity than Congress itself could have."[167] By giving inspectors general a "perch" inside executive agencies, Congress is able to surmount the usual separation of powers objections offered to block congressional or public inquiries (e.g., classified information, executive privilege, attorney privilege, state secrets, political question doctrine).[168] To put it bluntly, Congress is not able to achieve a comparable level of access or understanding through its usual oversight mechanisms.

In addition to the special perch, Congress provided inspectors general with an arsenal of information gathering tools. As noted in Section 2 of the IGA, the inspector general 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 corrective action."[169] To accomplish this objective, as well as the congressional notice task, inspectors general engage in three principal activities: investigations, audits, and inspections or evaluations.[170] Investigations generally involve criminal or civil misconduct by a government employee, contractor, or grant recipient.[171] Audits include both performance and financial audits.[172] Financial audits tend to be the most familiar of the inspector general review types (at least to outsiders), and involve the assessments of the appropriate allocation and use of federal money.[173] Performance audits provide programmatic analysis of an entire program or operation; they focus on compliance, efficiency and effectiveness, internal control, and prospective analysis, and they follow the Generally Accepted Government Auditing Standards (or Yellow Book).[174] Inspections or evaluations are also programmatic in nature; they examine the policies, operations, regulations, or legislative implications of a specific

---

165. *See* JOHNSON & NEWCOMER, *supra* note 121, at 39–47 (describing authorities and evolution of responsibilities); Sinnar, *supra* note 157, at 1034–39, 1057–58.

166. GOLDSMITH, *supra* note 123, at 105.

167. *Id.*

168. *Id.*

169. 5 U.S.C. app. 3 § 2(3).

170. For a comparison of the differences between the three common types of inspector general reviews, see FRANCIS, A PRIMER, *supra* note 131, at 7–9.

171. APAZA, *supra* note 124, at 13.

172. *Id.* at 13–14.

173. *Id.* at 13.

174. *See generally* FRANCIS, A PRIMER, *supra* note 131, at 7.

aspect of a program or operation, or review of a specific agency facility.[175] This third activity–inspections and evaluations–is often missed by those outside the inspector general community and contributes to the common but incomplete view of inspectors general as bean counters.

To pursue these three activities, the IGA and its subsequent amendments[176] provide inspectors general 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;[177] issue reports with recommendations for corrective action;[178] receive full access to all information (i.e. records and materials) available to the agency;[179] request materials from other executive branch agencies;[180] issue administrative subpoenas to nonfederal entities;[181] administer or take an oath, affidavit, or affirmation from any person;[182] exercise the authority of law enforcement;[183] receive employee and external complaints;[184] appoint officers as necessary to carry out such powers;[185] refer matters (both criminal and civil) to the United States Attorney General;[186] hire employees, experts, and consultants and procure necessary equipment and services; obtain assistance from other agencies (federal, state and local);[187] and enter into contracts and other arrangements with public and private entities.[188]

The work product that comes from the use of these tools is voluminous, even if not widely read. Inspectors general produce statutorily mandated semi-annual reports[189] and incident-specific reports[190] to

175. APAZA, *supra* note 124, at 13.

176. Inspector General Act of 1978, Pub. L. No. 95-452, 92 Stat. 1101; Inspector General Act Amendments of 1988, Pub. L. No. 100-504, 102 Stat. 2531; Inspector General Reform Act of 2008, Pub. L. No. 110-409, 122 Stat. 4302; Inspector General Empowerment Act of 2016, Pub. L. No. 114-317, 130 Stat. 1595. For a summary of the various legislative enactments, see FRANCIS, A PRIMER, *supra* note 131, at 2-3.

177. 5 U.S.C. app. 3 § 4(a)(1).

178. *Id.* § 4(a)(5).

179. *Id.* § 6(a)(1)(A).

180. *Id.* § 6(a)(3).

181. *Id.* § 6(a)(4) (providing the power to subpoena documents but not testimony).

182. *Id.* § 6(a)(5).

183. *Id.* § 6(a)(4), (e).

184. *Id.* § 7.

185. *Id.* § 6(a)(7).

186. *Id.* § 4(d).

187. *See generally id.*

188. 5 U.S.C. app. 3 § 6(a)(9).

189. *See, e.g.*, OFF. OF THE INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., SEMIANNUAL REP. TO THE CONG.: APR. 1, 2020–SEPT. 30, 2020 (2020),

Congress, as well as reports on the implementation status[191] of prior recommendations. In addition, inspectors general provide a joint biennial report as required by the Cybersecurity Information Sharing Act of 2015[192], and annual reports as required by the Federal Information Security Modernization Act of 2014.[193] In addition, both Congress and the agency head can ask the inspector general to conduct specific investigations, audits, or inspections.[194] The special perch and accompanying tool kit statutorily allocated to inspectors general provide a unique capacity to identify cybersecurity organizational successes and failures, and to disseminate such information to those in policy-making positions.

### C. Growing Role as Policy Evaluator and Valued Advisor to Agency Head

The third reason inspectors general are well-positioned to support the U.S. Government's efforts to a build a more cohesive structure for cybersecurity matters is due to the growing role of evaluative work in the inspector general portfolio. Inspectors general 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.[195] Indeed the 1978 IGA anticipated such a role and the report accompanying the act looked favorably upon the inspector general involvement in "reviewing of existing legislation and proposed regulations in order to offer

---

https://www.oig.dhs.gov/sites/default/files/assets/SAR/2020/oig-sar-apr20-sep20.pdf [https://perma.cc/57F9-ADZ5].

190. *See, e.g.*, OFF. OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, REVIEW OF FOUR FISA APPLICATIONS AND OTHER ASPECTS OF THE FBI'S CROSSFIRE HURRICANE INVESTIGATION (2019), https://www.justice.gov/storage/120919-examination.pdf [https://perma.cc/U2HR-7CGJ] [https://perma.cc/BGW2-8CV6].

191. *Id.* OFF. OF THE INSPECTOR GEN., U.S. DEP'T OF HEALTH AND HUMAN SERVICES, OIG'S TOP UNIMPLEMENTED RECOMMENDATIONS: SOLUTIONS TO REDUCE FRAUD, WASTE AND ABUSE IN HHS PROGRAMS (2021), https://oig.hhs.gov/reports-and-publications/compendium/files/compendium2021.pdf [https://perma.cc/WZV7-97DE]

192. *See, e.g.*, OFF. OF THE INSPECTOR GEN., INTELLIGENCE COMMUNITY, JOINT REPORT ON THE IMPLEMENTATION OF THE CYBERSECURITY INFORMATION SHARING ACT OF 2015 (2017), https://oig.justice.gov/reports/2018/AUD-2017-005.pdf [https://perma.cc/26TH-ZWGU] [hereinafter Joint Report on CISA].

193. Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073, 3081-82; The most recent FISMA report for DHS is OFF. OF THE INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG-20-77, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FISCAL YEAR 2019 (REDACTED) (2019), https://www.oig.dhs.gov/sites/default/files/assets/2020-10/OIG-20-77-Sep20.pdf [https://perma.cc/NC2F-Z9VW] [hereinafter OIG-20-77].

194. 5 U.S.C. app. 3 § 2, 4.

195. Sinnar, *supra* note 157, at 1079.

guidance concerning their likely impact on fraud and abuse control as well as economy and efficiency."[196] 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."[197] The evaluative nature of inspector general 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."[198]

Inspectors general, particularly in national security, law enforcement, and intelligence entities, may be uniquely positioned to influence internal executive branch policy in a way that Congress may not.[199] As chronicled in the work of Shirin Sinnar,[200] the role of inspectors general in national security entities has evolved since 9/11 from a focus on mismanagement, waste, and audits to one of inspections of privacy and civil rights abuses, and evaluation of internal policies and guidelines.[201] This growing role as policy evaluator and valued advisor to agency head is the result of the comprehensive and independent nature of the inspector general reports, the public release of the inspector general reports (even if in redacted form), and the subsequent media coverage.[202] Examples of inspectors general influencing internal rules and policies include: changes made to the FBI's FISA warrant application process after publication of a Department of Justice Inspector General's report on the Carter Page/Crossfire Hurricane investigation;[203] changes made to the CIA's

196. S. REP. NO. 95-1071, at 8 (1978).

197. *Id.*

198. *Id.*

199. Sinnar, *supra* note 157, at 1034.

200. *Id.*

201. This evolution, according to Sinnar, led to inspectors general in national security and intelligence agencies exercising a critical individual rights oversight function. This individual rights oversight function has five dimensions: (i) increasing transparency; (ii) identifying rights violations; (iii) providing relief for victims of violations; (iv) holding government officials accountable; and (v) revising internal rules and policies to prevent future abuses. *Id.* at 1033.

202. *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.").

203. OFF. OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, REVIEW OF FOUR FISA APPLICATIONS AND OTHER ASPECTS OF THE FBI'S CROSSFIRE HURRICANE INVESTIGATION 428 (2019), https://www.justice.gov/storage/120919-examination.pdf [https://perma.cc/U2HR-7CGJ]; Natasha Bertrand & Darren Samuelson, *Inspector General's Report on Russia Probe: Key Takeaways*, POLITICO (Dec. 9,

rendition and interrogation programs after a CIA Inspector General report identified abuses in the program's administration, questioned its efficacy, and doubted the legal basis offered for the program;[204] changes made to the Defense Department's use of Threat and Local Observation Notice reports, or TALON reports, after a Department of Defense Inspector General investigation into whether the reports complied with intelligence laws and department regulations;[205] changes to the Justice Department's "hold until cleared" detention policy after an inspector general investigation into individual allegations of detainee abuse;[206] and the establishment of tighter cybersecurity standards for supply chain vendors after a Department of Defense inspector general report on vulnerabilities.[207] Ongoing Department

---

2019, 1:17 PM), https://www.politico.com/news/2019/12/09/inspector-generals-report-russia-key-takeaways-079030 [https://perma.cc/E4S9-58H9]; 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/3F3F-YHDL]; 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/5D9V-98LU]; 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/82B5-CGQZ].

204. OFF. OF THE INSPECTOR GEN., CENT. INTEL. AGENCY, COUNTERTERRORISM DETENTION AND INTERROGATION ACTIVITIES (SEPTEMBER 2001 - OCTOBER 2003) 1–2 (2004) https://fas.org/irp/cia/product/ig-interrog.pdf [https://perma.cc/48AW-YSV8]; Sinnar, *supra* note 157, 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.").

205. OFF. OF THE INSPECTOR GEN., U.S. DEP'T OF DEF., THE THREAT AND LOCAL OBSERVATION NOTICE (TALON) REPORT PROGRAM 8–9 (2007), https://www.dodig.mil/reports.html/Article/1118727/the-threat-and-local-observation-notice-talon-report-program-redacted/ [https://perma.cc/5S5N-EG27]; Sinnar, *supra* note 157, at 1043.

206. OFF. OF THE INSPECTOR GEN., U.S. DEP'T OF JUST., 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), https://oig.justice.gov/sites/default/files/legacy/special/0306/full.pdf [https://perma.cc/GJJ4-W8GR]; Sinnar, *supra* note 157, at 1043.

207. OFF. OF THE INSPECTOR GEN., U.S. DEP'T OF DEF., 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/XA73-DBTV]; OFF. OF THE UNDER SECRETARY OF DEF. FOR ACQUISITION & SUSTAINMENT CYBERSECURITY MATURITY MODEL CERTIFICATION, https://www.acq.osd.mil/cmmc/ [https://perma.cc/66KE-CMNK] (last visited Aug. 28, 2021); HEIDI M. PETERS, DEFENSE ACQUISITIONS: DOD'S CYBERSECURITY MATURITY MODEL

of Justice inspector general reviews of the use of federal law enforcement personnel in responding to protest activity and civil unrest during the summer of 2020 in Washington, DC and in Portland, Oregon[208] are likely to lead to policy revisions as well. Further evidence of this growing role can be found in the ability of inspectors general to impact management and strategic funding decisions.[209]

It bears noting of course, that this shift from inspectors general assessing whether the agency followed the applicable legal requirement to a scenario where the inspector general assesses the content of the applicable law, policy, or agency regulation, is not a welcome development in all corners.[210] However, inspectors general are not policymakers, so there is a limit to their influence. As noted above, inspectors general serve only in an advisory role and they must rely on their agency heads or Congress to take corrective action for any violations or problematic conduct they identify.[211] Nonetheless, this shift has occurred and it is critical to appreciate how this shift in responsibility – from identifying waste and misstatement to being the "fount of accountability" – will affect the potential for a larger role for inspectors general in evaluating the efficacy and substance of various cybersecurity policies. This shift, and the illustrations above, reveal that inspectors general are a good resource for illuminating the policies in need of change, and thus, may be able to provide a roadmap for effective organizational reform in the area of cybersecurity.

---

CERTIFICATION FRAMEWORK (2020), https://www.everycrsreport.com/reports/R46643.html [https://perma.cc/7P5D-BGXE]; Dawn E. Stern, *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/98FG-KMZC]; 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/E2DM-2VSW].

208. Press Release, U.S. Dep't of Just., DOJ OIG Announces Initiation of Work (July 23, 2020), available at https://oig.justice.gov/news/doj-oig-announces-initiation-work [https://perma.cc/R6A3-B5J9].

209. Memorandum from Patrick E. McFarland, Inspector Gen., U.S. Off. of Pers. Mgmt., to Beth F. Cobert, Acting Director, U.S. Off. of Pers. Mgmt., at 1 (July 22, 2015), https://www.opm.gov/our-inspector-general/publications/special-reports-and-reviews/serious-concerns-regarding-the-office-of-the-chief-information-officer.pdf [https://perma.cc/2RAM-37WT].

210. *See* Margo Schlanger, *Intelligence Legalism and the National Security Agency's Civil Liberties Gap,* 6 HARV. NAT'L SEC. J. 112, 113–14 (2015) (arguing that inspectors general should focus on compliance, not content).

211. 5 U.S.C. app. 3 §§ 2, 3, 4.

### D. Congressional Information Conduit

Finally, inspectors general are well positioned to support reform efforts due to their statutorily-mandated congressional reporting requirements. While much of the inspector general attention and scholarship focuses on the internal oversight function, the inspector general position serves a secondary, although equally important, role in support of congressional oversight efforts by serving as a conduit of information to congressional committees.[212] As noted above, Congress established the offices of inspectors general in each of the 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. . . ."[213] As such, in contrast to agency employees who often view the inspector general as an exasperating junkyard dog, the congressional committees have a kinder view of inspectors general, 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 inspectors general more as man's–or committee's–best friend.

Inspectors general fulfil this informing task through a variety of mechanisms, some generally applicable and some specific to the agency's cybersecurity and information security responsibilities. These mechanisms include semi-annual reports mandated by the IGA, implementation updates, fast action reports for particularly egregious violations and the threat of seven-day letters, joint biennial reports relating to the Cybersecurity Information Sharing Act, annual reports mandated by Federal Information Security Management Act (FISMA), requests for inspector general testimony, and by responding to specific inquiries from Congress. While the inspector general may not publicly disclose information that is prohibited from disclosure due to classification level or for other reasons,[214] most of the inspector general reports are published both on the agency website and the consortium's page.[215] This section will briefly review each

212. *Id.* § 2.

213. *Id.* (emphasis added).

214. 5 U.S.C. app. 3 § 5(e); *see also* 5 U.S.C. app. 3 § 4(e).

215. OVERSIGHT.GOV, https://www.oversight.gov/ [https://perma.cc/NYH4-QFJJ] (last visited Feb. 28, 2021); *Reports*, OFF. OF THE INSPECTOR GEN., U.S. DEP'T OF DEF., https://www.dodig.mil/reports.html/ [https://perma.cc/GY5B-TCME] (last visited Feb. 28, 2021); *Audits, Inspections, and Evaluations,* OFF. OF THE INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., https://www.oig.dhs.gov/reports/audits-inspections-and-evaluations [https://perma.cc/BG2U-TNUQ] (last visited Feb. 28, 2021); *Reports*, OFF. OF THE INSPECTOR GEN., U.S. DEP'T OF JUST., https://oig.justice.gov/reports [https://perma.cc/8YXJ-3NHH] (last visited Feb. 28, 2021).

of these mechanisms, taking particular note of each mechanism's ability to provide information relating to the U.S. government's cybersecurity practices.

*1. Semi-Annual Reports*

Section 5 of the IGA requires semi-annual reports "summarizing the activities of the Office during the immediately preceding six-month periods ending March 31 and September 30."[216] The reports must be submitted to the agency head by April 30 and October 31 of each year.[217] 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."[218]

Upon receiving the report, the agency head must transmit the report within thirty days to the appropriate congressional committees or sub-committees 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.[219] Within sixty days of submitting the semi-annual report to Congress, the agency head "shall make copies of such report available to the public upon request and at a reasonable cost,"[220] and in most instances the reports are published on the website of the inspector general or the agency or the central inspector general report repository at oversight.gov.

*2. Flagrant Incident Reports and Seven-Day Letters*

The inspector general 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.[221] When the inspector general becomes aware of a matter in this

216. 5 U.S.C. app. 3 § 5.
217. *Id.*
218. *Id.* § 5(a).
219. *Id.* § 5(b).
220. *Id.* § 5(c).
221. *Id.* § 5(d).

category, the inspector general must report the matter immediately to the head of agency.[222] The burden then shifts to the agency head to transmit such report to the appropriate committees or subcommittees of Congress within seven calendar days.[223] Referred to as "seven-day letters" in inspector general lingo, the potential to swing this sword provides critical leverage to the office of the inspector general.[224] Indeed, that potential leverage may account for the sparing use of this tool. According to a 2011 GAO study, between 2008 and 2010, only one inspector general issued a seven-day letter, and between January 1990 and April 1998, no seven-day letters were issued.[225] Recognizing the value of the information provided by inspectors general, particularly with regard to issues of immediate concern, Congress has encouraged inspectors general to use the seven-day letter in a less sparing fashion.[226]

*3. Implementation Updates*

In addition to the semi-annual and incident-specific reports, inspectors general must now track and provide to Congress and the public on an annual basis the implementation status of their prior recommendations.[227] The purpose underlying the requirement is "to ensure that the inspectors general avoid overstating the actual savings that can be attributed to their work."[228] The implementation status check provides a

222. *Id.*

223. *Id.*

224. U.S. GOV'T ACCOUNTABILITY OFF., GAO-11-770, INSPECTORS GENERAL: REPORTING ON INDEPENDENCE, EFFECTIVENESS, AND EXPERTISE 8 (2011).

225. *Id.*

226. 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/KVK5-G3RP]. *See, e.g.*, Letter from Charles J. Sheehan, Acting Inspector Gen., U.S. Env't Prot. Agency, 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/2CST-72UT].

227. U.S.C. app. 3 § 5(a)(15) (resulting from the 1988 amendments); *see e.g.*, OFF. OF THE INSPECTOR GEN., U.S. DEP'T OF HEALTH AND HUMAN SERVICES, OIG'S TOP UNIMPLEMENTED RECOMMENDATIONS: SOLUTIONS TO REDUCE FRAUD, WASTE AND ABUSE IN HHS PROGRAMS (2021), https://oig.hhs.gov/reports-and-publications/compendium/files/compendium2021.pdf [https://perma.cc/CZB8-KY5C].

228. 133 CONG. REC. S4554-01, at 7958–59 (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

useful tool for agency heads, relevant congressional committees, and the public to identify areas of persistently weak cybersecurity as well as possible foot dragging by agencies.

*4. Cybersecurity Information Sharing Biennial Reports*

The Cybersecurity Information Sharing Act of 2015 requires inspectors general of the "appropriate Federal entities," defined as the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and the Treasury, and the Office of the Director of National Intelligence (ODNI), "in consultation with the Inspector General of the Intelligence Community and the Council of Inspectors General on Financial Oversight," to provide joint biennial reports to Congress by December 18 of every other year.[229] The reports include an assessment of each agency's implementation of the act's statutory requirements.[230] The Office of the Inspector General of the Intelligence Community compiles the results in a report, an unclassified version is published,[231] and a separate, classified report[232] is provided to the appropriate congressional committees and officials. These annual reports offer a rich assessment of cybersecurity issues, some of which are agency or program specific, but many that cross agencies.[233] As such, these reports provide a roadmap rich with guidance on the problem spots and areas in need of urgent attention. Far from a mere compliance exercise, these reports provide a helpful prioritization tool for revamping the government's cybersecurity framework.

---

on their implementation of recommended corrective action. This means savings will be realized and reported when such action is completed.").

229. 6 U.S.C. §§ 1501, 1506(b).

230. *Id.* § 1506(b); *see, e.g.*, OFF. OF THE INSPECTOR GEN., INTEL. CMTY., UNCLASSIFIED JOINT REPORT ON THE IMPLEMENTATION OF THE CYBERSECURITY INFORMATION SHARING ACT OF 2015 (2019), https://www.oversight.gov/sites/default/files/oig-reports/Unclassified%2020191219_AUD-2019-005-U_Joint%20Report.pdf [https://perma.cc/DXU2-2983].

231. The most recent version of the joint report was submitted in December 2019. Joint Report on CISA, *supra* note 192.

232. OFF. OF THE INSPECTOR GEN., INTEL. CMTY., JOINT REPORT ON THE IMPLEMENTATION OF THE CYBERSECURITY INFORMATION SHARING ACT OF 2015 (2019), https://www.dodig.mil/Reports/Audits-and-Evaluations/Article/2048074/unclassified-joint-report-on-the-implementation-of-the-cybersecurity-information/ [https://perma.cc/JXX8-5GJH].

233. *Id.*; *see, e.g.*, OFF. OF THE INSPECTOR GEN., INTEL. CMTY., UNCLASSIFIED JOINT REPORT ON THE IMPLEMENTATION OF THE CYBERSECURITY INFORMATION SHARING ACT OF 2015 (2019), https://www.oversight.gov/sites/default/files/oig-reports/Unclassified%2020191219_AUD-2019-005-U_Joint%20Report.pdf [https://perma.cc/DXU2-2983].

*5. Federal Information Security Act (FISMA) Annual Reports*

An annual reporting requirement also stems from the Federal Information Security Modernization Act of 2014 (FISMA), which requires the inspector general for each affected agency to review their agency's information security program for compliance with the act's requirements.[234] FISMA requires the agency inspector general to perform an annual independent evaluation of the agency's information security programs and practices.[235] The evaluation includes testing the effectiveness of information security policies, procedures, and practices of a representative subset of agency systems.[236] These reports are a rich source of insight, identifying agencies with persistently weak cybersecurity while also providing a standard for comparative analysis. Recent reports show continuing challenges in the areas of supply chain controls, upgrades, employee training, and workforce development.[237]

*6. Specific Investigation Requests*

In addition to the reports described above, members of Congress may also request specific action by inspectors general.[238] This authority is described in 5 U.S.C. § App. 3 § 5(e)(4).[239] An example from November 2020 can be found in a request to the Department of Defense inspector general from members of the Senate Select Committee on Intelligence and the Senate Armed Services Committee to investigate then-President Trump's recent appointment to the position of general counsel for the

234. 44 U.S.C. § 3555(b)(1) ("for each agency with an Inspector General appointed under the Inspector General Act of 1978, the annual evaluation required by this section shall be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the agency").

235. *Id.*

236. 44 U.S.C. § 3555(a).

237. *See, e.g.*, OFF. OF THE INSPECTOR GEN., U.S. DEP'T OF HOMELAND SECURITY, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FISCAL YEAR 2020, (2021), https://www.oig.dhs.gov/sites/default/files/assets/2021-10/OIG-21-72-Sep21.pdf [https://perma.cc/5JPZ-TXNV]; OFF. OF THE INSPECTOR GEN., U.S. DEP'T OF THE TREASURY, FISCAL YEAR 2021 IRS FEDERAL INFORMATION SECURITY MODERNIZATION ACT EVALUATION (2021), https://www.oversight.gov/sites/default/files/oig-reports/TIGTA/202120072fr.pdf [https://perma.cc/R86R-CUVJ]; OFF. OF THE INSPECTOR GEN., U.S. DEP'T OF VETERAN'S AFFAIRS, FEDERAL INFORMATION SECURITY MODERNIZATION ACT AUDIT FOR FISCAL YEAR 2020 (2021), https://www.oversight.gov/sites/default/files/oig-reports/VA/VAOIG-20-01927-104.pdf [https://perma.cc/6A6K-J27Y].

238. 5 U.S.C. app. 3 § 5(e)(4).

239. *Id.*

National Security Agency.[240] Additional examples are found arising from the SolarWinds hack, which has been the subject of several specific requests to agency inspector general offices, including one from Representatives Bill Pascrell and Mike Kelly who reached out to the inspector general for the Internal Revenue Service.[241] Admirably, the inspector general responded within a few days.[242] A slew of additional requests followed, including to the inspectors general of the Department of Justice and Department of Homeland Security.[243]

240. Letter from Mark R. Warner, Vice Chairman of the Senate Select Comm. on Intel., and Jack Reed, Ranking Member of the Comm. on Armed Servs., to Sean O'Donnell, Acting Inspector Gen. for the Dep't of Def. (Nov. 16, 2020), https://assets.documentcloud.org/documents/20407603/dod-ig-letter.pdf [https://perma.cc/9FND-RGKX]. Another example of requests from members is an October 28, 2021 letter from Senators Rob Portman, James Lankford, and M. Michael Rounds. They ask the Department of Homeland Security Inspector General Joseph Cuffari to investigate reports that the TSA and CISA "failed to give adequate consideration to feedback from stakeholders and subject matter experts" in announcing new cybersecurity directives and in the process of drafting new regulations. Letter from Rob Portman, Ranking Member of the Comm. On Homeland Sec. and Governmental Affs., James Lankford, Ranking Member of the Subcomm. on Gov't Operations and Border Mgmt., and M. Michael Rounds, Senator, to Joseph Cuffari, Inspector General (Oct. 28, 2021), https://www.hsgac.senate.gov/imo/media/doc/2021-10-28%20RP%20Lankford%20Rounds%20to%20Cuffari%20re%20TSA%20Security%20Directives.pdf?utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202 [https://perma.cc/55YD-U8BR].

241. 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/T495-J5C3].

242. 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), https://pascrell.house.gov/uploadedfiles/ways_and_means_response_final_12-23-2020.pdf [https://perma.cc/KZ6K-367Q].

243. Press Release, Jerry Moran, Senator, Senators Request Information from FBI, CISA on Reports of Russian Cyberattack Against the U.S. Government (Dec. 15, 2020), https://www.moran.senate.gov/public/index.cfm/2020/12/senators-request-information-from-fbi-cisa-on-reports-of-russian-cyber-attack-against-the-u-s-government [https://perma.cc/X266-W36P] ("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?").

*7. Congressional Testimony*

Anticipating the need for congressional support, many offices of inspector general have a division or position dedicated to legislative affairs and tasked with preparing the semi-annual reports and otherwise serving as liaisons between the office and the relevant congressional committees.[244] In addition, inspectors general are well-positioned to complement the work of the Governmental Accountability Office, which serves as a resource to congressional staffers and members.[245] Recent testimony by inspectors general include the following: "Oversight of the United States Capitol Police and Preparations for and Response to the Attack of January 6th" (April 21, 2021);[246] "Department of Defense Inspector General and the Services Inspector Generals: Roles, Responsibilities and Opportunities for

244. *See e.g.*, *Legislative Affairs and Communications*, OFF. OF THE INSPECTOR GEN., U.S. DEP'T OF DEF., https://www.dodig.mil/About/Offices/Legislative-Affairs-and-Communications/ [https://perma.cc/LX8X-4M69] (last visited July 17, 2021).

245. The GAO and inspectors general have a history of working together on various projects, as both focus on supporting Congress' oversight efforts. Indeed, the relationship is a complicated one as the GAO also audits each agency's office of inspector general to ensure they are 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. U.S. GOV'T ACCOUNTABILITY OFF., GAO-21-452T, DHS OFFICE OF INSPECTOR GENERAL: PRELIMINARY OBSERVATIONS ON LONG-STANDING MANAGEMENT AND OPERATIONAL CHALLENGES (2021), https://www.gao.gov/assets/gao-21-452t.pdf [https://perma.cc/6SXP-KTJ7]; *see also Oversight of the Department. of Homeland Security's Office of Inspector General: Hearing Before the Comm. On Homeland Sec.,* 117th Cong. (Apr. 21, 2021), https://homeland.house.gov/activities/hearings/oversight-of-the-department-of-homeland-securitys-office-of-inspector-general [https://perma.cc/CRU7-U939]; Nick Schwellenbach & Adam Zagorin, *Pulling Punches: Trump-Appointed Watchdog Suppressed White House-Related Probes*, POGO (Apr. 20, 2021), https://www.pogo.org/investigation/2021/04/pulling-punches-trump-appointed-watchdog-suppressed-white-house-related-probes/ [https://perma.cc/4M2Q-GFP8].

246. *Oversight of the United States Capitol Police and Preparations for and Response to the Attack of January 6th: Hearing Before the Comm. on House Admin.*, 117th Cong. (Apr. 21, 2021), https://cha.house.gov/committee-activity/hearings/oversight-united-states-capitol-police-and-preparations-and-response [https://perma.cc/YE8J-NN5H].

Improvement" (April 15, 2021);[247] and "Restoring Independence of Inspectors General" (April 20, 2021).[248]

### E. Interagency Models (CIGIE, ICIG Forum, and FIORC)

Finally, there are three IG-established partnership entities that can provide insight on the U.S. government cybersecurity organizational reform efforts. The first of these is the Council of Inspectors General on Integrity and Efficiency (CIGIE).[249] The council was established in the Inspector General Reform Act of 2008 as an independent entity within the executive branch.[250] 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."[251] CIGIE is responsible for operating and maintaining oversight.gov, a "publicly accessibly, searchable website containing the latest public reports" from inspectors general across the federal government.[252] Of interest to the cybersecurity organizational task is the entity's ability to look across agencies and to offer insight on cross-cutting challenges. Each year, the council prepares a report that identifies management and performance challenges facing multiple federal agencies.[253]

---

247. *Department of Defense Inspector General and the Services Inspector Generals: Roles, Responsibilities and Opportunities for Improvement: Hearing Before the Subcomm. on Mil. Personnel, H. Comm. on Armed Servs.,* 117th Cong. (2021), https://armedservices.house.gov/hearings?ID=8B79E0CA-6761-4213-A0BA-142C740D040F [https://perma.cc/A2PE-GYTT].

248. Press Release, H. Comm. on Oversight and Reform, Subcomm. Comm. Held Hearing on Restoring Indep. of Inspectors Gen. (Apr. 20, 2021), https://oversight.house.gov/news/press-releases/subcommittee-committee-held-hearing-on-restoring-independence-of-inspectors [https://perma.cc/955Z-LWU8].

249. *What is CIGIE?*, COUNCIL OF THE INSPECTORS GEN. ON INTEGRITY AND EFFICIENCY, https://www.ignet.gov/ [https://perma.cc/MV9P-YD4R] (last visited July 17, 2021).

250. Inspector General Reform Act of 2008, Pub. L. No. 110-409, 122 Stat. 4306 (codified as amended at 5 U.S.C. app. § 11).

251. *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/6NGD-BW4Q] (last visited May 12, 2021).

252. *About Oversight.gov*, OVERSIGHT.GOV (last visited July 17, 2021), https://www.oversight.gov/about [https://perma.cc/S764-V9KU].

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

The second partnership is the Intelligence Community Inspectors General Forum, which was established in 2010.[254] 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."[255] The forum is led by the Inspector General of the Intelligence Community (commonly referred to as the IC IG), and it includes representatives from inspector general offices in the Central Intelligence Agency, Department of Homeland Security, Defense Intelligence Agency, Department of Defense, Department of Energy, Department of Justice, Department of State, Department of the Treasury, National Geospatial Agency, National Reconnaissance Office, National Security Agency, and Federal Bureau of Investigation.[256] Forum members meet quarterly and its activities focus on:

> Supporting the IC IGs in the performance of audits, inspections, evaluations and investigations within their respective departments and agencies; [s]trengthening 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 [a]chieving optimal utilization of resources, to increase efficiency and to avoid duplication of effort among the Inspectors General of the Intelligence Community.[257]

The third entity is the Five Eyes Intelligence Oversight and Review Council (FIORC). This partnership builds on the existing Five Eyes relationship, an alliance among the intelligence entities in Australia, Canada, New Zealand, the United Kingdom, and the United States. It includes the following oversight entities: the Office of the Inspector-General of Intelligence and Security of Australia; the National Security and Intelligence Review Agency of Canada; the Office of the Intelligence Commissioner of Canada; the Commissioner of Intelligence Warrants and the Office of the Inspector-General of Intelligence and Security of New Zealand; the Investigatory Powers Commissioner's Office of the United Kingdom; and the Office of the Inspector General of the

254. *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#:~:text=The%20statutory%20ICIG%20Forum%20was,oversight%20responsibilities%20for%20IC%20elements [https://perma.cc/66PZ-WPN9] (last visited May 12, 2021).

255. *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/6EE9-BJCG] (last visited May 12, 2021).

256. *Id.*

257. *Id.*

Intelligence Community of the United States.[258] According to the council's charter signed in 2017, it was established to provide a forum for council members to: "exchange views on subjects of mutual interest and concern; compare best practices in review and oversight methodology; explore areas where cooperation on reviews and the sharing of results is permitted where appropriate; encourage transparency to the largest extent possible to enhance public trust; and maintain contact with political offices, oversight and review committees, and non-Five Eyes countries as appropriate."[259]

As demonstrated in the paragraphs above, the work of inspectors general is essential to the cybersecurity reorganization mission and of particular importance to the task of developing a cohesive cybersecurity strategy that avoids duplication and waste. Inspectors general are well positioned to support the cybersecurity reorganizational effort due to their roles as independent advisors; their ability to occupy a special perch within their agencies; their evolving capacity as policy evaluators; Congress's increasing reliance on inspectors general for information; and existing interagency models that anticipates the need for cross-agency coordination in addressing cybersecurity challenges. To better understand the role of inspectors general and their contributions to the U.S. government's cybersecurity reform efforts, the next section will catalog the recent activities of inspectors general in support of these efforts.

## IV. UTILIZING INSPECTOR GENERAL WORK PRODUCT TO SUPPORT THE CYBERSECURITY REORGANIZATION PROJECT

While few have noticed the contributions of inspectors general in this space, the inspectors general have continued with their work, quietly but thoroughly assessing and evaluating the cybersecurity accomplishments and failings of their agencies, and making recommendations for improvements both at the programmatic and larger structural levels. To get a sense of the breadth and scope of inspector general activities in assessing the U.S. government's cybersecurity mission, a review of recent inspector general reports proves illuminating. The table below, which is pulled from recent semiannual or other summary reports and focuses on inspector general offices in agencies with significant cyber responsibilities, provides a revealing roadmap of the organizational work ahead:

---

258. CHARTER OF THE FIVE EYES INTELLIGENCE OVERSIGHT AND REVIEW COUNCIL (FIORC) (Oct. 2, 2017) https://www.dni.gov/files/ICIG/Documents/Partnerships/FIORC/Signed%20FIORC%20Charter%20with%20Line.pdf [https://perma.cc/9DYR-8ZG9].

259. *Id.* ¶ 2.

| **Agency** | **Selected Inspector General Reports**[260] |
|---|---|
| **Office of the Inspector General of the Intelligence Community**[261] | Cyber Threat Intelligence Integration Center (January 2020)<br><br>ODNI's Oversight of Intelligence Community Major Systems Acquisition Cybersecurity Risks (November 2019)<br><br>Assessment of IC Information System Deterrence, Detection, and Mitigation of Insider Threats (March 2018)<br><br>Audit of the Office of the Director of National Intelligence Implementation of the Cybersecurity Information Sharing Act, section 107(b), Oversight of Government Activities for Calendar Years 2019 and 2020[262] (date to be determined)<br><br>Joint Project on the Implementation of the Cybersecurity Information Act, Section 107(b), Oversight of Government Activities for Calendar Years 2019 and 2020[263] (date to be determined) |

260. The reports referenced in the table are collected primarily from the semi-annual reports provided to Congress, the annual work plans prepared for agency heads, and from the inspector general report database available at OVERSIGHT.GOV, https://www.oversight.gov/reports [https://perma.cc/JWM6-G8JK]. Excluded from this table are the annual FISMA audits conducted by each agency's inspector general office.

261. The reports listed for the Office of the Inspector General of the Intelligence Community were gathered from semi-annual reports, annual work plans, and other reports available on OVERSIGHT.GOV, https://www.oversight.gov/reports [https://perma.cc/JWM6-G8JK].

262. This report is described as a "required" project in OFF. OF THE INSPECTOR GEN., INTEL. CMTY, ANNUAL WORKPLAN FOR THE FISCAL YEAR 2021, at 4 (2021), https://www.dni.gov/files/ICIG/Documents/Publications/Annual%20Work%20Plan/IC%20IG%20Annual%20Work%20Plan%20FY21.pdf [https://perma.cc/N2DR-6NN2].

263. This report is described as a "required" project in OFF. OF THE INSPECTOR GEN., INTEL. CMTY, ANNUAL WORKPLAN FOR THE FISCAL YEAR 2021, at 4 (2021), https://www.dni.gov/files/ICIG/Documents/Publications/Annual%20Work%20Plan/IC%20IG%20Annual%20Work%20Plan%20FY21.pdf [https://perma.cc/N2DR-6NN2].

| | |
|---|---|
| | Evaluation of the Intelligence Communities' Information Technology Supply Chain[264] Fiscal Year 2020 Independent Evaluation of the Office (date to be determined) |
| **Office of Inspector General for the Department of Homeland Security[265]** | Evaluation of DHS's Information Security Program for Fiscal Year 2019 (September 2020)<br><br>DHS Made Limited Progress to Improve Information Sharing Under the Cybersecurity Act in CYs 2017 and 2018 (September 2020)<br><br>DHS Faces Challenges in Meeting the Responsibilities for the Geospatial Data Act of 2018 (September 2020)<br><br>Review of CBP's Major Cybersecurity Incident During a 2019 Biometric Pilot (September 2020)<br><br>Modernization Act Requirements for Intelligence Systems for Fiscal Year 2019 – Secret (September 2020)<br><br>Progress and Challenges in Modernizing DHS' IT Systems and Infrastructure (August 2020)<br><br>DHS Needs to Improve Cybersecurity Workforce Planning (September 2019)<br><br>DHS Can Strengthen Its Cyber Mission Coordination Efforts (September 2015) |
| **Office of the Inspector General for the** | Audit of Maintaining Cybersecurity in the Coronavirus Disease – 2019 Telework Environment (March 2021)<br><br>Audit of Cybersecurity Requirements for Weapon |

264. This report is described as a "discretionary" project in OFF. OF THE INSPECTOR GEN., INTEL. CMTY, ANNUAL WORKPLAN FOR THE FISCAL YEAR 2021, at 7 (2021), https://www.dni.gov/files/ICIG/Documents/Publications/Annual%20Work%20Plan/IC%20IG%20Annual%20Work%20Plan%20FY21.pdf [https://perma.cc/N2DR-6NN2].

265. The reports listed for the Office of Inspector General for the Department of Homeland Security were gathered from semi-annual reports, annual work plans, and other reports available on OVERSIGHT.GOV, https://www.oversight.gov/reports [https://perma.cc/JWM6-G8JK].

| | |
|---|---|
| **Department of Defense**[266] | Systems in Operations and Support of Phase of Development of Defense Acquisition in Life Cycle (February 2021)<br><br>Summary of Reports Issued Regarding Department of Defense Cybersecurity from July 1, 2019, through June 30, 2020 (December 2020)<br><br>Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems (July 2019)<br><br>Audit of the DoD's Management of the Cybersecurity Risks for Government Purchase Card Purchases of Commercial Off-the-Shelf Items (July 2019) (full report is classified)<br><br>DoD Actions Taken to Implement the Cybersecurity Information Sharing Act of 2015 (November 2018) (full report is FOUO)<br><br>Control Systems Supporting Tier I Task Critical Assets Lacked Basic Cybersecurity Controls (June 2017) (full report is classified) |
| **Office of the Inspector General for the Department of Commerce**[267] | Failures in the Department's Security Program Resulted in Exposure of Sensitive Trade Information to Unvetted Foreign Nationals (February 2020)<br><br>The Department Needs to Improve Its Capability to Effectively Share Cyber Threat Information (September 2019)<br><br>Inadequate Management of Active Directory Puts USPTO's Mission at Significant Cyber Risk (June 2019)<br><br>The Census Bureau Must Improve Its Implementation of |

266. The reports listed for the Office of Inspector General for the Department of Defense were gathered from semi-annual reports, annual work plans, and other reports available on OVERSIGHT.GOV, https://www.oversight.gov/reports [https://perma.cc/JWM6-G8JK].

267. The reports listed for the Office of Inspector General for the Department of Commerce were gathered from semi-annual reports, annual work plans, and other reports available on OVERSIGHT.GOV, https://www.oversight.gov/reports [https://perma.cc/JWM6-G8JK].

| | |
|---|---|
| | the Risk Management Framework (October 2018)<br><br>Review of IT Security Policies, Procedures, Practices, and Capabilities in Accordance with the Cybersecurity Act of 2015 (August 2016)<br><br>Successful Cyber Attack Highlights Longstanding Deficiencies in NOAA's IT Security Program (August 2016) |
| **Office of the Inspector General for the Department of Energy**[268] | Management Letter on the Department of Energy's Unclassified Cybersecurity Program for Fiscal Year 2019 (March 2020)<br><br>Management of Cybersecurity over Selected Information Systems at Department of Energy Headquarters (September 2019)<br><br>Management of Cybersecurity Activities at a Department of Energy Site (August 2019)<br><br>Management of a Department of Energy Site Cybersecurity Program (July 2019) |

As shown in the table above, the inspector general offices in the agencies with the most regular contact with cybersecurity issues already are addressing the most pressing of the government's organizational issues. Synthesizing these reports uncovers valuable insight into the following aspects of the need for cybersecurity reorganization: the effectiveness (or lack thereof) of information sharing agreements between government agencies and with the private sector (including the sharing of cyber threat information); assessments of cybersecurity coordination efforts among federal civilian agencies; after-action reports on cyber incidents or data breaches; effectiveness of cyber workforce development programs; identification of vulnerabilities in federal information systems; and a cataloging of unimplemented cybersecurity recommendations from years past. Indeed, this last item may be the most helpful takeaway as it provides a list of cybersecurity tasks to be done. When paired with the FISMA audits, the observations and recommendations included in the inspector

268. The reports listed for the Office of Inspector General for the Department of Energy were gathered from semi-annual reports, annual work plans, and other reports available on OVERSIGHT.GOV, https://www.oversight.gov/reports [https://perma.cc/JWM6-G8JK].

general reports offer a roadmap for the U.S. government's cybersecurity organizational reform efforts.

## CONCLUSION

This article examined the unheralded and unrecognized work of inspectors general, and the special role they are poised to play in the U.S. government's cybersecurity-related work in the coming years. This role will build on their ability to serve as key advisors to the agency head, their role as conduits of information to Congress, their already-established interagency mechanisms for flagging cross-cutting programs, and their special perch within the agency's day to day transactions which provides an operational understanding of the strengths and weakness of the government's cybersecurity architecture.

While it is beyond the scope of this article to identify the exact contours and curves of the future role to be played by inspectors general in the government's cybersecurity organization reforms, the following observations provide considerations for additional study. Future work should consider the mechanisms for taking advantage of the unique contributions of the inspectors general, the optimal ways to channel the contributions of inspectors general, and to assess the extent to which inspectors general should be engaged in organizational change. Options may include the creation of a special cybersecurity-focused inspector general, focused on a temporary and single task relating to the government's cybersecurity programs and efforts, or the establishment of an inspector general forum focused on cybersecurity mandates, and building on the model established by the IC IG Forum or CIGIE partnerships. While the newly-established National Cyber Director will have plenty of suggestions for cybersecurity organizational reform, that individual would do well to consider the contributions of the inspectors general to future reform efforts. Indeed, a review of the most recent inspector general reports on cybersecurity-related matters will provide an effective roadmap for sorting and prioritizing reform efforts, and for accomplishing substantive and sustainable reform.