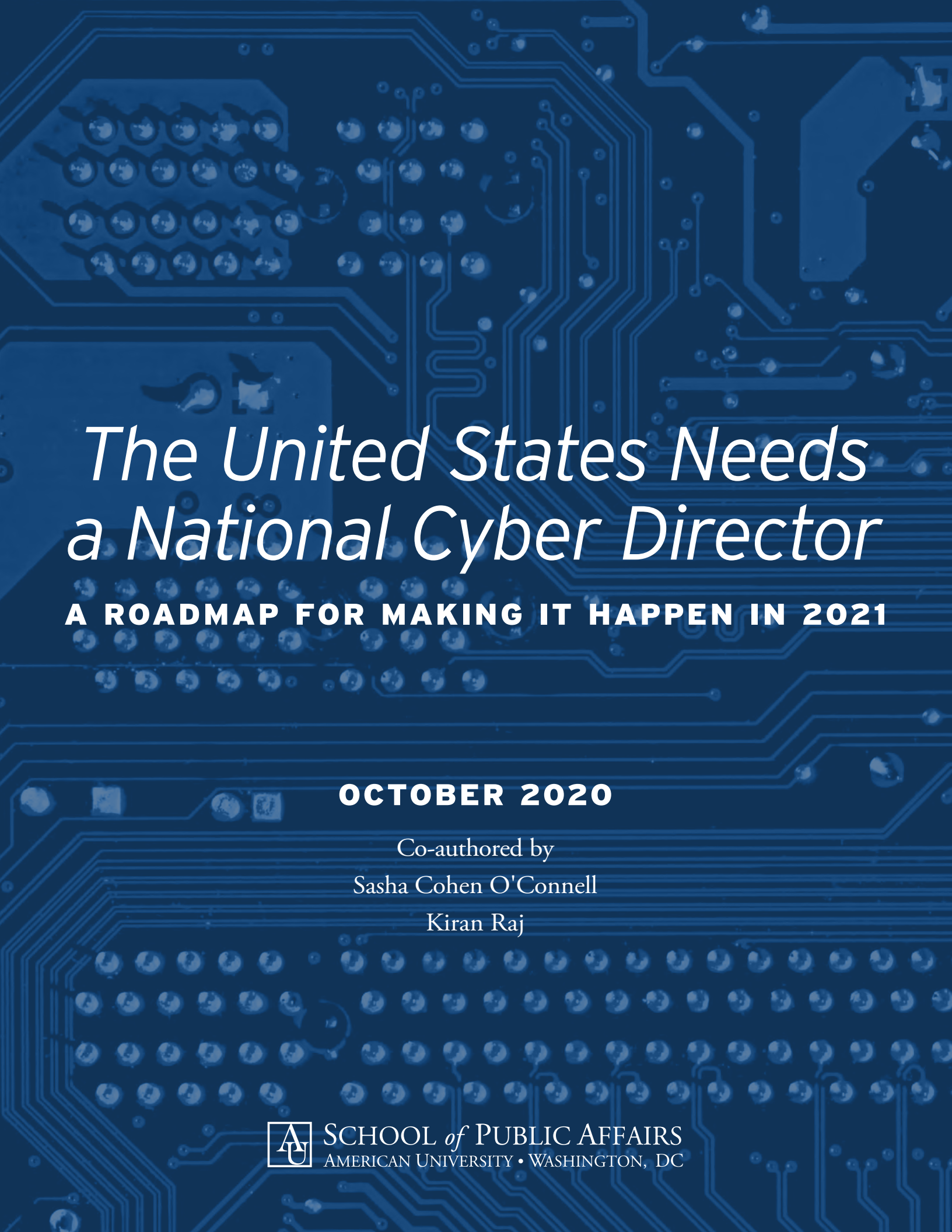


The United States Needs a National Cyber Director

A ROADMAP FOR MAKING IT HAPPEN IN 2021

OCTOBER 2020

Co-authored by
Sasha Cohen O'Connell
Kiran Raj

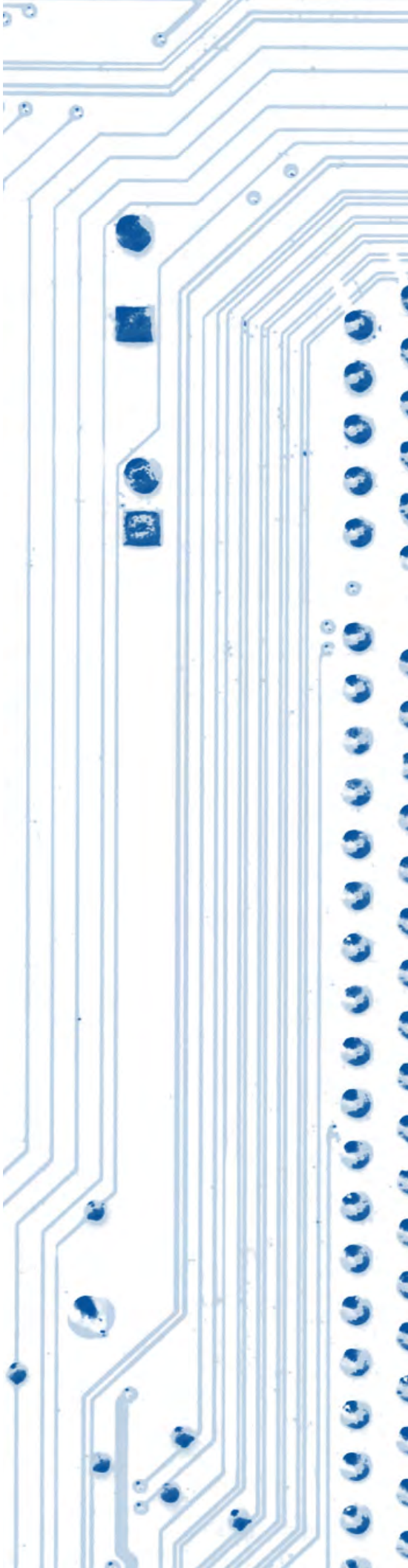
SCHOOL *of* PUBLIC AFFAIRS
AMERICAN UNIVERSITY • WASHINGTON, DC

The United States Needs a National Cyber Director

A ROADMAP FOR MAKING IT HAPPEN IN 2021

OCTOBER 2020

CONTENTS



FOREWORD

There is an overwhelming consensus that the U.S. government (USG) is not optimally organized to coordinate its response to the significant and growing cyber threat. Despite this consensus, there has been sustained resistance to implementing necessary structural reforms. The current impasse is not due to lack of serious review and study of the issue. To the contrary, as the reader of this guide will see, the literature demonstrates that options for addressing this gap have been studied, reviewed, and reported on extensively.

We took on the development of this guide to help move forward the process of creating a National Cyber Director (NCD) by summarizing the current thinking on the issue and providing concise recommendations and implementation priorities. Ever the optimists, we believe that it is not too late to adopt these changes. We see the upcoming election as an opportunity for either a Biden or second-term Trump Administration to take a fresh look at governmental reforms to address the cyber threat. It is not simple nor is it without tradeoffs; but it is doable.

What we are proposing here, as others have before us, is not a new cyber agency. We are also not suggesting a replacement for any of the existing departments and agencies that are working in this space. Rather, we are advocating for the creation of a White House entity that not only coordinates disparate interest and expertise across the entire federal government but also can represent the USG with one voice with external stakeholders on these issues. This role is critically needed and does not exist today.

This document includes a review of the literature on this topic to-date along with our recommendations for (1) what structural changes are needed and (2) the steps required to get there during the November to January 2021 timeframe and in the first 100 days of a Biden or second-term Trump Administration. Most of our recommendations align with the current language in H.R. 6395- the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, passed by the House on July 21, 2020, with four critical additions summarized below:

1. Provided specificity regarding the background expertise and skills for the NCD to include national security, technical/engineering, and leadership and stakeholder engagement experience in both the government and the private sector.
2. Recommended organizational changes regarding the Office of the National Cyber Director (ONCD), including details about how the staff should be structured.
3. Added details regarding the roles and relationship between the NCD and other key elements of the Executive Office of the President (EOP) and heads of other Executive Branch Departments and Agencies including the NCD's role in developing, implementing and leading a government-wide National Cyber Strategy.
4. Clarifying the NCD's scope as it relates to both offensive and defensive cyber operations.

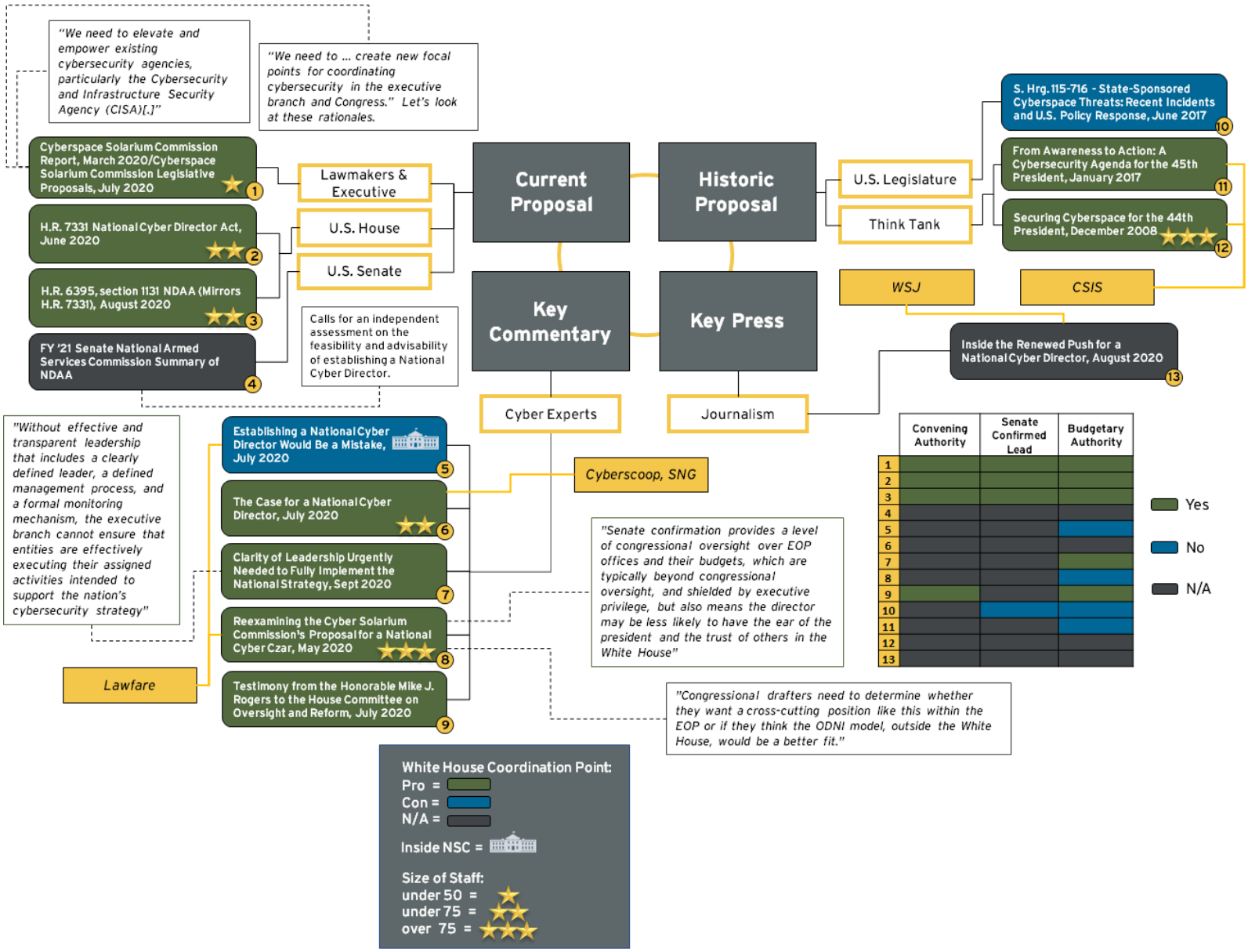
We believe these additions are critical for two important reasons:

First, for the NCD to be successful, he or she must have the required expertise. Without the correct background, there is significant risk that the NCD will not be successful and the potential benefits of an ONCD may not be realized. As such, we believe it is important to be as detailed as possible regarding the ideal background and experience required for this position. Similarly, based on our collective experience, we wanted to provide more information regarding the structure of the ONCD staff and how it should interact with relevant departments and agencies. This interaction is particularly important as it, if done correctly, will help to empower departments and agencies that are already working on these issues.

Second, we wanted to avoid artificial distinctions that have previously caused confusion and created friction within the USG and ensure a whole of government response to cyber threats. In particular, we propose that the NCD have a role in the coordination of both offensive and defensive cyber operations. Given that offensive and defensive cyber operations are often related or inexorably linked, it follows that the President's primary advisor on cyber should have visibility and coordination capacity across these issues. This is not a significant departure from the role the National Security Council plays in both offensive and defensive cyber operations today. Indeed, the natural consequence of allowing the NCD to participate in all NSC and Principal meetings regarding cyber operations, strategy, threats, responses, and remediation is to elevate the work done previously by the NSC Cyber Directorate on both offensive and defensive cyber operations to the ONCD.

We believe that adopting these recommendations will strengthen our cybersecurity capabilities and enhance the government's ability to secure America from cyber threats. The time to act is now.

LITERATURE HIGHLIGHTS MAP



LITERATURE HIGHLIGHTS CHART

			Key Rationale
CURRENT PROPOSAL	Cyberspace Solarium Commission	Cyberspace Solarium Commission Report, March 2020/Cyberspace Solarium Commission Legislative Proposals, July 2020 ★	First, "We need to elevate and empower existing cybersecurity agencies, particularly the Cybersecurity and Infrastructure Security Agency (CISA)[.]" Second, "We need to … create new focal points for coordinating cybersecurity in the executive branch and Congress."
	U.S. House of Representatives	H.R. 7331 National Cyber Director Act, June 2020 ★★	not outlined--see cyber solarium report.
	U.S. House of Representatives	H.R. 6395, section 1131 NDAA (Mirrors H.R. 7331), Aug 2020 ★★	not outlined--see cyber solarium report.
	U.S. Senate	FY 21 Senate National Armed Services Committee Summary of NDAA, June 2020	Calls for an independent assessment on the feasibility and advisability of establishing a National Cyber Director.
HISTORIC PROPOSAL	U.S. Senate Committee on Foreign Relations	S. Hrg. 115-716 - State-Sponsored Cyberspace Threats: Recent Incidents and U.S. Policy Response, June 2017	The transcript from the Senate hearing on state-sponsored cyberspace threats discusses who oversees U.S. cyber policy.
	Center for Strategic and International Studies	From Awareness to Action: A Cybersecurity Agenda for the 45th President, January 2017	Streamlining is needed within the White House regarding cybersecurity.
	Center for Strategic and International Studies	Securing Cyberspace for the 44th President, December 2008 ★★★	The national cyber coordinator needs to be in the White House so that they have the necessary authority and oversight.
KEY COMMENTARY	Michael Daniel (Cyberscoop, SNG)	The Case for a National Cyber Director, July 2020 ★★	Cybersecurity is crosscutting across the U.S. Government and departments and agencies need more incentive to sustain coordination. The current lack of central leadership hinders effective incident response. The EOP is a neutral, interagency hub for that leadership.
	U.S. Government Accountability Office	Clarity of Leadership Urgently Needed to Fully Implement the National Strategy, Sept 2020	"Without effective and transparent leadership that includes a clearly defined leader, a defined management process, and a formal monitoring mechanism, the executive branch cannot ensure that entities are effectively executing their assigned activities intended to support the nation's cybersecurity strategy."
	Philip Reitinger (Lawfare)	Establishing a National Cyber Director Would Be a Mistake, July 2020	A NCD would create confusion over roles and responsibilities and redundant layers of bureaucratic review. It would also undercut CISA.
	Anisha Hindocha, Mieke Eoyang (Lawfare)	Reexamining the Cyber Solarium Commission's Proposal for a National Cyber Czar , May 2020 ★★★	Discusses the comparisons between Cyberspace Solarium Commission-proposed cyber director and other executive offices. This article lays out various structural considerations.
	Mike Rogers	Testimony from the Honorable Mike J. Rogers to the House Committee on Oversight and Reform, July 2020	"If we do not get our national-level policy sorted now, and if we do not empower the right person and the right office with the responsibility today, I fear we will have a different type of Commission soon—one that looks at why a national cyber incident happened at the hands of China, Russia, or North Korea, and what could have been (or should have been) done to prevent it in the first place."
KEY PRESS	David Uberti and James Rundle (WSJ)	Inside the Renewed Push for a National Cyber Director, August 2020	Notes that a NCD within the White House creates an issue with separation of powers.

White House Coordination Point:
Pro = Con = N/A = Inside NSC =

Size of Staff:
< 50 = ★ < 75 = ★★ > 75 = ★★★

ADDITIONAL PRESS

			Key Rationale
2020	Lucas Ropek (GovTech.com)	Will CISA be the Savior of State and Local Cyber Security?, July	CISA is taking over the role of coordinating national and state cyber capabilities and strengthening its ability to coordinate.
	Mike Rogers (TheHill.com)	America Needs National Cyber Director to Fortify Our Security, July	A National Cyber Director would be the head of defense, coordinate with the private sector, and provide a clear mission set.
	Mariam Baksh (NextGov.com)	Bipartisan Concerns Arise Over Cyber Director Legislation, July	This article covers Rep. Langevin's legislation and other Representatives' responses to it.
	Sasha O'Connell (Politico.com)	We Don't Need a Separate Cybersecurity Agency, January	Calls for the reestablishment of a Cyber Czar, along with other coordination and collaboration mechanisms.
2018	Clip Block (PULSE, LinkedIn)	Why the Next White House Cyber Czar should be an Economist, July	Economists understand the continued growth of the cyber threat, so the new Cyber Czar should be an economist.
	Eric Geller (Politico.com)	Trump's Lack of Cyber Leader May Make U.S. Vulnerable, June	Establishing leadership at the top creates a priority for every level of government.
	Paul Rosenzweig and Megan Reiss (Lawfare)	Bolton's Magnificent Idea: Nix the White House Cyber Czar, May	Cyber coordination is needed between U.S. departments and agencies. A National Cyber Director addresses the increased need for protection of critical infrastructure and will signal that the U.S. has a strong cyber strategy.
2012	Kevin Newmeyer (PRISM Journal, NDU)	Who Should Lead US Cybersecurity Efforts?, January	Recommends the establishment of Director of Cybersecurity, modeled after the Director of National Intelligence with clear budget and operational authority.
2009	Stanton Sloane (Armed Forces Journal)	The Role of a 'Cyber Czar', September	We are experiencing a "cyber-Pearl Harbor" - i.e. the problem is underestimated and misunderstood. The Cyber Czar needs diplomatic authority and inside access in the White House to be successful.
	Andy Greenberg (Forbes)	Obama's Unwilling Cyber Czars, July	Stresses the importance of the NCD position being designed with significant and clear responsibility and authority in order to attract exemplary candidates.

Pro N/A

Our Recommendation for The National Cyber Director

Recommendations in black reflect the language in the NDAA, either verbatim or in intent, and refer specifically to NDAA DRAFT H.R. 6395, passed by the House on July 21, 2020

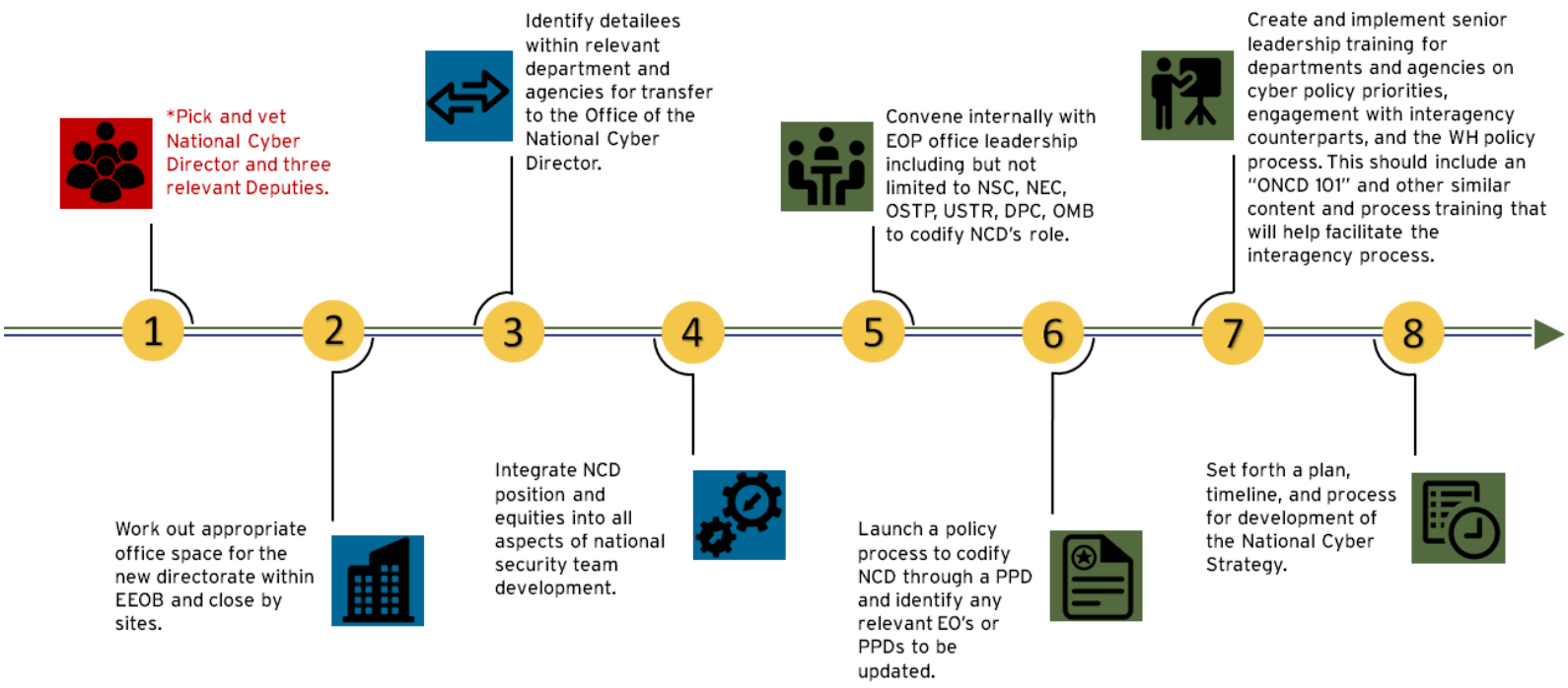
Recommendations in green are culled from other sources and are consistent with the overall posture of creating a strong, effective NCD position.

Position	Organization	Scope
The National Cyber Director (NCD) shall be an Assistant to the President. NCD has the seniority and authority to engage directly with heads of U.S. departments and agencies, and other senior officials in the Executive Branch. NCD should oversee and manage the Office of the National Cyber Director (ONCD). The ONCD shall have three deputy positions with the following responsibilities: (1) Strategy, Policy and Capabilities,(2) Budget, and (3) Plans and Operations. *While not necessary for the structural reforms proposed, Senate confirmation of the NCD is not objectionable.*	NCD will be a senior leader with national security, technical/engineering, and leadership and stakeholder engagement experience who has spent time both in the government and in the private sector. ONCD shall be staffed with approximately 75 full-time employees, a size similar to that of existing, comparable Executive Office of the President Organizations. NCD's staff should maintain a significant number of rotating detailees from other federal departments and agencies to complement a core group of direct-hire, full-time employees of the Office. NCD deputies positions should not be dual hatted but could be staffed by detailees from departments and agencies or from the private sector rotation. It is expected that the NCD Deputies should be SES-level or have at least 15 years of relevant experience. For non-deputy staff, at the discretion of the NCD, they may either be fully detailed to the ONCD (ONCD must have detailees from DHS, DOJ/FBI, IC & DOD at a minimum), dual hatted with a role in the NCD but remaining in their home agency, or from the private sector on rotation. The ONCD will absorb the Cyber Directorate of National Security Council.	NCD is the primary presidential advisor on issues involving cyber, cybersecurity, and emergent technologies. NCD is the joint coordinator of federal information security with the Federal CIO. NCD is the joint coordinator of telecommunications cyber issues, including cyber security elements of 5G, with the head of NTIA. Specific Responsibilities Include but not Limited to: Organize the coordination, integration, and planning of defensive cyber operations and maintain situational awareness of all offensive cyber operations, including all relevant Title 10 and Title 50 matters. Participate in all National Security Council and Principals meetings regarding cyber strategy, policy, operations, threats, responses, and remediation. Coordinate closely with the National Security Advisor and relevant components of the NSC such as the Resiliency Directorate. Consult within the Executive Office of the President (EOP) early and often for all policy and operational issues where the NCD's scope is implicated directly or indirectly. Develop a National Cyber Strategy and oversee its implementation by the various U.S. departments and agencies, including any classified annex that governs Intelligence Community policy and operations. Conduct budget and oversight responsibilities in the implementation of the National Cyber Strategy in coordination with the Head of OMB, including any classified annex, such as the power to review annual budgets of departments and agencies to determine whether their budgets are consistent with the National Cyber Strategy. Coordinate with Congress, the private sector, and international partners on cyber cybersecurity, and emergent technologies on behalf of the White House and EOP. Work with departments and agencies to ensure consistent messaging throughout the USG on all cyber and emergent technology related issues.

TIMELINE

Election through January 2021

First 100 days of Administration



***Identifying, recruiting and vetting the first NCD is the number one implementation priority. The NCD will be a senior leader with national security, technical/engineering, and leadership and stakeholder engagement experience who has spent time both in the government and in the private sector.**

ACRONYMS GLOSSARY

5G	Fifth Generation Global Wireless Network Standard
CIO	Federal Chief Information Officer
CSIS	Center for Strategic and International Studies
DHS	Department of Homeland Security
DOD	Department of Defense
DOJ	Department of Justice
DPC	Domestic Policy Council
EEOB	Eisenhower Executive Office Building
EO	Executive Order
EOP	Executive Office of the President
FBI	Federal Bureau of Investigation
IC	Intelligence Community
NCD	National Cyber Director
NDAA	National Defense Authorization Act
NDU	National Defense University
NEC	National Economic Council
NSC	National Security Council
NTIA	National Telecommunications and Information Agency
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
ONCD	Office of the National Cyber Director
OSTP	Office of Science and Technology Policy
PPD	Presidential Policy Directive
SES	Senior Executive Service
SNG	Scoop News Group
USG	U.S. Government
USTR	United States Trade Representative
WH	White House
WSJ	Wall Street Journal

ACKNOWLEGEMENTS AND CONTACTS

PROJECT TEAM

School of Public Affairs
Phone: 202-885-2940
spa@american.edu
4400 Massachusetts Avenue NW
Washington, DC 20016
AMERICAN.EDU/SPA

Sasha Cohen O'Connell	Executive in Residence
Kiran Raj	Adjunct Faculty
Amber Smoyer	AU SPA Graduate Candidate 2021
Moriah Kairouz Batza	AU SPA 2016 Alumna
Bailey Fillinger	AU SPA Graduate Candidate 2021
Nina Enagonio	AU SPA Graphic Design Coordinator

This project could never have come to fruition without the amazing help of the project team of Amber Smoyer, Bailey Fillinger, Moriah Kairouz Batza, and Nina Enagonio. A better team cannot be found.

In addition, the early and thorough assistance from the School of Public Affairs communications team of Chay Rao, Tony Harvin and Nina Enagonio was critical to getting this to press. We would also like to thank our early external readers for their feedback and input, your insights greatly improved the finished product.

@sco_connell
sashaoc@american.edu

Sasha Cohen O'Connell, PhD is an Executive in Residence in the Department of Justice, Law & Criminology, School of Public Affairs (SPA), American University where she currently teaches cyber policy at the graduate and undergraduate levels. Additionally, she serves as the Director of the Terrorism and Homeland Security Policy Master's program at SPA.

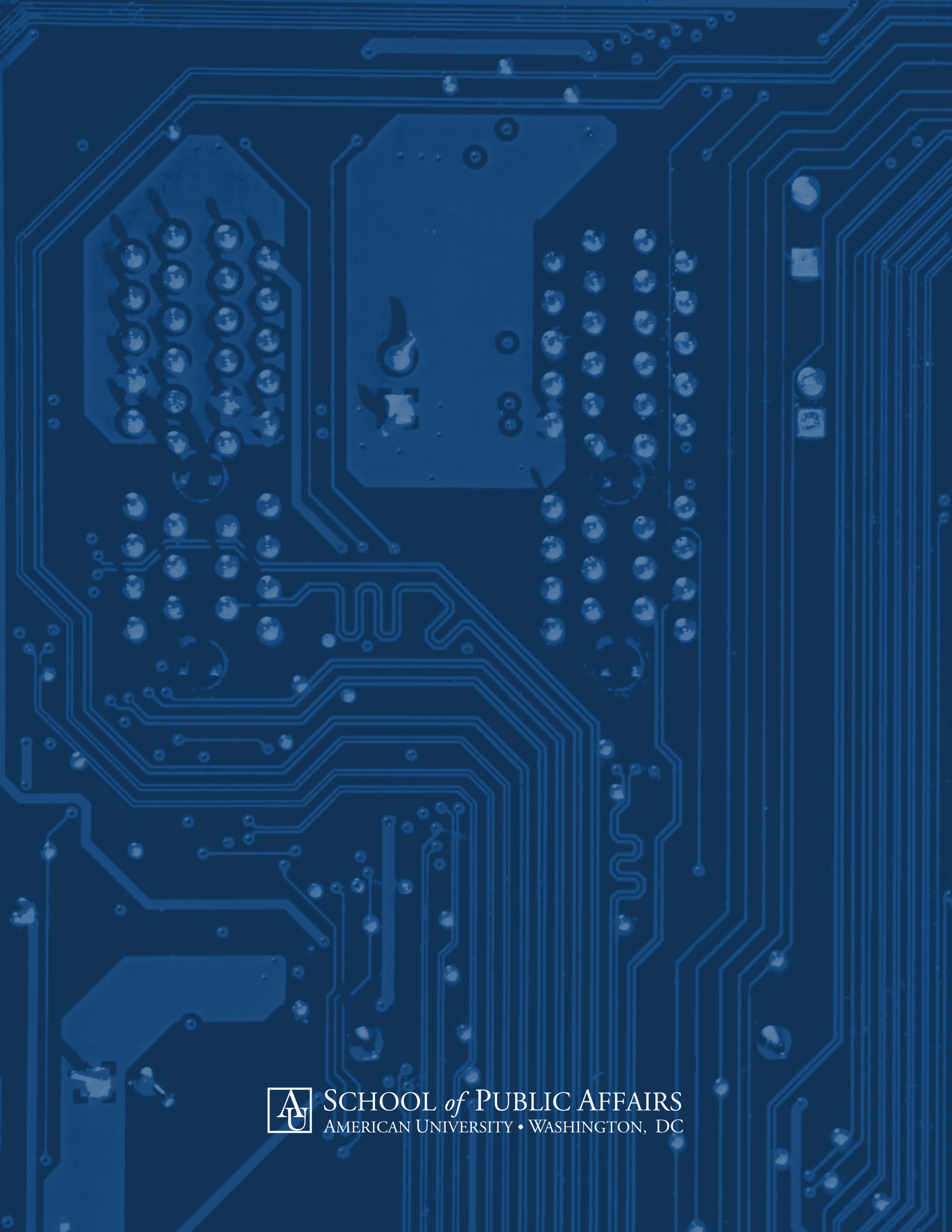
O'Connell's career in public service includes time in the executive branch. She has spent the majority of her career at the FBI where she served most recently as the organization's Chief Policy Advisory, Science and Technology and as the Section Chief of Office of National Policy for the FBI's Deputy Director where she led policy engagement with the National Security Council on a wide breadth of issues.

Among other roles, O'Connell ran the FBI's Strategy Management Office where she led implementation of the Balanced Scorecard for the FBI's Director and served as Chief of the Executive Staff for the FBI's Criminal Investigative Division where she led strategic planning, performance evaluation, training, and communications for the Bureau's criminal programs.

@kraj33
raj@american.edu

Kiran Raj, JD is a senior executive in a financial technology company. Prior to working in the fintech space, Kiran worked in private legal practice as a partner at O'Melveny & Myers in Washington DC. Before private practice, Kiran served as Deputy General Counsel at the Department of Homeland Security, working directly with leaders of corporate America on the intersection of cybersecurity and privacy with law, policy, and technology. He held a similar role at the U.S. Department of Justice as Senior Counsel to the Deputy Attorney General.

Before entering the legal profession, Kiran was a lead program manager at Microsoft Corporation where he had responsibility for developing and deploying software tools and technologies that improved the security, compatibility, and overall application experience of the Windows operating system.



SCHOOL *of* PUBLIC AFFAIRS
AMERICAN UNIVERSITY • WASHINGTON, DC