NATIONAL ACADEMY OF PUBLIC ADMINISTRATION®

Data Privacy and Security: An Agenda for 2021

Academy Election 2020 Project
Working Group:
Ensure Data Security and Privacy Rights of Individuals

ABOUT THE ACADEMY

The National Academy of Public Administration (the Academy) is an independent, nonprofit, and nonpartisan organization established in 1967 to assist government leaders in building more effective, accountable, and transparent organizations. Chartered by Congress to provide nonpartisan expert advice, the Academy's unique feature is its over 950 Fellows—including former cabinet officers, Members of Congress, governors, mayors, and state legislators, as well as prominent scholars, business executives, and career public administrators. The Academy helps the federal government address its critical management challenges through in-depth studies and analyses, advisory services and technical assistance, congressional testimony, forums and conferences, and online stakeholder engagement. Under contracts with government agencies, some of which are directed by Congress, as well as grants from private foundations, the Academy provides insights on key public management issues, as well as advisory services to government agencies.

ABOUT THE ELECTION 2020 PROJECT

The Academy formed a series of Working Groups of its Fellows to address Grand Challenges in Public Administration. These Groups were charged with producing one or more papers to advise the Administration in 2021 (whether reelected or newly elected) on the key near-time actions that should be taken to begin addressing Grand Challenges. This is a paper of the Ensure Data Security and Privacy Rights of Individuals Working Group. It includes these Fellows' recommendations for new opportunities to engage American citizens in a dialogue on data security and privacy issues and to develop the IT Workforce.

DATA PRIVACY AND SECURITY: AN AGENDA FOR 2021

A REPORT OF AN ACADEMY WORKING GROUP

NATIONAL ACADEMY OF PUBLIC ADMINISTRATION
ELECTION 2020 WORKING GROUP:
ENSURE DATA SECURITY AND PRIVACY RIGHTS OF INDIVIDUALS

Working Group Members
Costis Toregas, Chair
Jane Fountain
Nick Hart
James Hendler
Mark Reger
Priscilla Regan
Peter Winokur

THE CHALLENGE

In the digital age, the American people knowingly and unknowingly produce huge amounts of data on a daily basis, and governments at all levels increasingly rely on digital systems to manage their internal operations and deliver public services. Through widespread e-commerce, ubiquitous GPS maps, and regular social media interactions, the public transmits their sensitive financial, health, and other personal information through online platforms.

Americans need assurance that all sectors will keep their personal data private and safeguarded from abuse, but our data security infrastructure in both the public and the private sectors is vulnerable to exploitations, hacks, and breaches. With malevolent foreign intelligence entities, the hacking of public agencies, the infiltration of hostile agents in private organizations, and other dangers, the threat of data insecurity and exposure to breaches is real and immediate for governments, companies, and individuals.

Nonstate cyber actors and nation-states have developed sophisticated mechanisms for exploiting the vulnerabilities of government systems. Not only do they steal information and money; they increasingly disrupt, destroy, or threaten the delivery of essential public services. For example, hackers have been targeting local governments for ransomware attacks, with important systems and data being blocked until a ransom payment is made. In the summer of 2019, a host of local governments—including Baltimore, MD; Albany, NY; Laredo, TX; and 22 small Texas towns—had their operations disrupted by such attacks. The City of Baltimore experienced a hack that prevented the locality from issuing health alerts and delayed water bill delivery. Similarly, the City of Atlanta's systems for police reports and employment applications were down for days due to a March 2018 cyberattack. State and county governments, school districts, hospitals, and court systems have also become common targets of ransomware attacks.

The emerging threats to data privacy and security from the increasing use of digital technology are widely recognized but have gone largely unaddressed as the pace of technological change has surpassed government's modernization efforts.[1] Advances in information technologies have created situations where U.S. citizens are largely unaware of the extent and scope to which their personal data is collected, how it is being used, and who is applying that data to influence their, or others', actions. Over the next decade, technology will continue to evolve, and data privacy and security programs in both the public and the private sectors will inevitably face new vulnerabilities for which they will be unprepared.

From a somewhat different perspective, the coronavirus pandemic has brought privacy and security issues into sharp focus for most Americans. Not only are more Americans reliant on digital platforms to conduct their professional and personal lives and thus more aware of privacy and security risks, but an effective, longer-term response to the pandemic appears to necessitate tracing the spread of the virus. All citizens will be forced to decide about the necessary tradeoffs between privacy and security in attempts to reduce the spread of the coronavirus. Will Americans tolerate tracking the movement of individuals for the greater public good? Are Americans willing to sacrifice privacy for security to mitigate the coronavirus and/or terrorist threats?

[1] Security and privacy in law enforcement, defense and intelligence are critical issues but are largely beyond the scope of this white paper. Security and privacy each are quite broad areas. In some cases, security and privacy are positively correlated in the sense that strengthening one strengthens the other. In other cases, the two outcomes are traded off, when, for example, some dimension of privacy is traded off for increased security. Decision makers are challenged to craft administrative and legislative rules that optimize both privacy and security.

RECOMMENDATIONS

The Administration in 2021 (whether reelected or newly elected) has an opportunity to act quickly and strategically on these issues by leveraging the policy and administrative work that has been done over the last several years and the expertise that exists in the federal and state governments, as well as in the private sector and in academia. In this white paper, the Working Group on Data Security and Privacy recommends a number of actions that should be taken next year. Some are new, while others build upon efforts currently underway.

Create a Presidential Commission on Privacy and Security

The Working Group recommends that the Administration in 2021 engage the US population in a long-term dialogue on data privacy and security through the creation of a presidential commission.

- **Who should serve?** Primary participants should be federal policy makers at the Assistant Secretary level or higher, and corporate officials at the Executive Vice President level or higher, ensuring action orientation and a strategic perspective. Academic, research community and accreditation/service delivery organizations may be included but only after a first defining meeting to ensure laser focus on results.

- **What should its powers be?** Review and coordinate existing frameworks, recommendations and requests; develop an action plan; and facilitate implementation either through administrative reforms or legislation.

- **Why would it succeed? (critical success factors):** A public-private membership, engagement of the White House, and brevity of output will be key. In addition, a road map to accomplish practical steps forward will guarantee action orientation.

- **How will it be resourced?** It needs to be staffed by a team of competent and subject matter experts.

Create a Workforce Advisory Commission on Cybersecurity and Privacy

The Working Group recommends that the next administration address the urgent and growing skills crisis in the IT workforce for data privacy and security and for federal and private sector entities alike by creating a Workforce Advisory Commission on cybersecurity and privacy:

- **Why is this needed?** A pipeline strategy organized by synchronizing efforts of agencies such as the Office of Personnel Management (OPM), U.S. Department of Labor (DOL), the National Science Foundation (NSF), and academic and training organizations in a comprehensive, coordinated approach help to prepare the cybersecurity and privacy workforce of the future. The Administration in 2021 can build on several key initiatives in the federal government and on the recommendations of the recent Cybersecurity Solarium Commission report to develop programs to foster cybersecurity and privacy skills. The technology has been defined by technical experts, but the administrative, policy and leadership dimensions required for success have not yet received adequate attention.

- **Who should serve?** Senior HR leaders, career advisors, and educators should serve in order to determine skills needed to provide a workforce for the future that is both security and privacy aware at all levels of the organization.

- **What should its powers be?** To not only review existing frameworks, recommendations, and requests, but also design new frameworks, talent management strategies, and career paths.

- **Why would it succeed (critical success factors)?** A public-private membership, engagement of the White House and brevity of output.

- **How will it be resourced?** It needs to be staffed by a team of competent and subject matter experts.

Develop and Implement a Policy Framework to Protect Data Security and Individual Privacy

The Working Group recommends that the Administration in 2021:

- Work with Congress to craft and enact a policy framework and standards to protect consumer online data.
- Work with Congress to complete and enact a comprehensive national data privacy law to protect consumers and to foster innovation and economic growth for American companies.
- Build on the large-scale initiative, the Cyberspace Solarium Commission, a bipartisan congressional commission, to implement its recently released recommendations.

As an independent, nonpartisan, and nonprofit organization chartered by the U.S. Congress to improve government performance, the National Academy of Public Administration stands ready to assist the Administration in 2021 in implementing these recommendations. The Academy can foster multi-stakeholder dialogues that lead to actionable plans.

LEVERAGING EXISTING ACTIVITIES

The Administration in 2021 has an opportunity to act quickly and strategically to advance data privacy and security, and to build the workforce in these areas by leveraging administrative and policy initiatives that have already been successfully undertaken and that already incorporate the expertise that exists in the federal and state governments, as well as in the private sector and in academia. Privacy and security concerns pervade every federal agency and policy domain of the government. This section identifies some of the related key initiatives ongoing in the federal government to provide a starting point for the next administration.

In this paper, the Working Group focuses on two dimensions of privacy in addition to security and related workforce needs: (1) strengthening individual and corporate privacy with respect to government datasets and their use; and (2) strengthening consumer online data privacy.

A number of important initiatives have been undertaken in the area of data security and privacy.

President's Cross-Agency Priority Goals

The GPRA Modernization Act of 2013 mandates that each presidential administration develop a set of Cross-Agency Priority (CAP) Goals These are meant to prioritize areas of the President's agenda that require government-wide or cross-agency collaboration. The current CAP goals include two goals directly related to privacy and security: IT Modernization and Data, Accountability and Transparency. The Working Group recommends that the next administration build on current efforts in these CAP goals. Just as the current administration continued several CAP goals from the previous administration while putting their own stamp on them, the next administration should continue to build on previous work in priority areas.

The CAP goal titled Data, Accountability, and Transparency focuses on leveraging data as a strategic asset by developing a Federal data strategy. To do so, the data strategy must respect and maintain privacy and confidentiality, as noted in the CAP goal team's action plans, while leveraging the value of the federal government's data to serve the public. This CAP goal represents a whole-of-government effort, not surprisingly, and is led by data experts from the Office of Management and Budget (OMB), U.S. Department of Commerce (DOC), the Office of Science and Technology Policy (OSTP), and other departments and agencies.

Protecting Confidentiality While Leveraging Data

A critical issue in using data strategically is confidentiality protection, which is growing in importance in a data rich environment. The more data that becomes available in private or public settings, the more difficult are the challenges of ensuring individual-level confidentiality and anonymity. This is a fundamental element of the federal statistical system's work (Census, Bureau of Economic Adjustment, Bureau of Labor Statistics, etc.). Recommendations of the U.S. Commission on Evidence-Based Policymaking on applying privacy-preserving approaches/technologies are currently being examined.

That Commission outlined a vision for a National Secure Data Service, including the role it would play to balance transparency and data security. OMB established an advisory committee in March 2020 to plan development of the Federal Data Service with $5 million awarded to the Census Bureau and $2 million to the Bureau of Economic Analysis. An advisory committee with nonfederal members will assist in building tools to facilitate data sharing and data linkage while also preserving and enhancing privacy. As statistical and other agencies integrate, analyze and release data, they must be sure that data reconstruction and other methods cannot be used to disclose personal information.[2]

[2] See https://federalnewsnetwork.com/big-data/2019/10/where-does-the-federal-data-strategy-go-from-here-evidence-panel-members-revisit-ideas/

Student Privacy

Student privacy has gained visibility and urgency as education has moved online in the wake of the COVID-19 pandemic. This issue falls under the jurisdiction of the Department of Education (ED), the Federal Trade Commission (FTC), state legislatures (several of which have recently passed laws in this area) and state departments of education. Student privacy has become an issue for two primary reasons: the need to reconcile the requirements and accountability frameworks of the Family Educational Rights and Privacy Act (FERPA) of 1974 and the Children's Online Privacy Protection Act (COPPA) of 1998 with the increasing use of educational technology at all levels of education and for a variety of purposes. Both have been topics of FTC and ED workshops and requests for public comment, and Congress has considered multiple bills on the topic. Much of the policy groundwork has been laid with developing consensus on the steps needed to protect student privacy in technologically-mediated educational settings. But action needs to follow. The focus of the Commission should include endorsement of a bill that reconciles FERPA and COPPA, as well as the jurisdictions of the FTC and ED, and addresses the accountability of educational technology providers.

Authentication & Unique Identifiers

A recent National Academy of Sciences report notes: "As authentication becomes ever more ubiquitous, understanding its interplay with privacy is vital."[1] There are important trade-offs to be debated concerning convenience, personal and data privacy, and data security across a wide range of applications including medical records, fraud detection, public transactions and services ranging from tax filing to benefits transfers. Companies often share data with each other that identifies customers allowing the industries not just to gather their personal information for marketing but also to prevent fraud and to provide better and faster service.

[3]Who Goes There? Authentication Through the Lens of Privacy. https://www.nap.edu/read/10656/chapter/1

Government policies and administrative procedures in the areas of authentication and identity protection face a higher standard than do entities in the private sector because they are obligated to protect democracy and privacy while also seeking to modernize government services and information provision. Any comprehensive government data privacy policy will require exploring the trade-offs inherent in cross dataset and cross agency sharing of personal data and authentication.

CONSUMER ONLINE DATA PRIVACY PROTECTION

In 2018, responding to increasing public concern and serious breaches of consumer data, the Commerce Department's National Telecommunications and Information Administration (NTIA) began stakeholder meetings to build shared understanding and to develop broad principles for data privacy. The White House National Economic Council working with Congress stated at that time that it "aims to craft a consumer privacy protection policy that is the appropriate balance between privacy and prosperity."[3] **The Working Group recommends that the Administration in 2021 move quickly and purposefully to work with Congress to craft and enact a policy framework and standards to protect consumer online data.**

These initiatives follow massive data breaches in some of the largest companies in the U.S. Facebook announced in 2018 that the information of approximately 70 million U.S. users was shared improperly with Cambridge Analytica and, more generally, that Facebook has shared consumer data with four Chinese companies prompting congressional inquiries. In 2017, Yahoo reported a data theft in 2013 that hacked the personal information of all of its three billion accounts. Other large-scale breaches that have compromised consumer personal data have been reported by Target Corp., Equifax Inc., and Home Depot, Inc., among other firms. As a result, citizens have expressed increasingly growing concerns about privacy protections.

[3] See https://www.reuters.com/article/us-usa-internet-privacy/trump-administration-

working-on-consumer-data-privacy-policy-idUSKBN1KH2MK ;
https://www.washingtonpost.com/technology/2018/07/27/trump-administration-is-working-new-proposal-protect-online-privacy/

The federal government currently lacks federal rules or laws that protect consumer online privacy by regulating how firms gather and monetize Web data. In 2018, the European Union (EU) developed a set of standards called the General Data Protection Regulation (GDPR) that took effect on May 25, 2018 and is expected to have far-reaching impacts on how business is conducted worldwide with respect to the collection and use of personal data. For example, the Institute of Electrical & Electronic Engineers (IEEE), a global organization incorporated in New York with 400,000 members in more than 160 countries has been carefully reviewing the GDPR. Among the steps IEEE has taken is the formation of a cross-organizational task force that is working to ensure consistency in how volunteers, members, and professional staff worldwide collect and use personal data.

Moreover, the State of California, the world's sixth largest economy, adopted the California Consumer Privacy Act in June 2018 to protect consumer rights regarding "access to, deletion of, and sharing of personal information that is collected by businesses." If other states follow California's lead, business would be faced with a patchwork of fragmented regulatory environments domestically and internationally that would be unworkable.

In light of these developments, in September 2019 more than 50 Business Roundtable CEOs from several industries wrote to Congressional leaders urging them to enact, "as soon as possible," a comprehensive national data privacy law to protect consumers and to foster innovation and economic growth for American companies. They noted the urgency of restoring consumer trust and the importance of a national policy framework to guide corporate behavior. They included a Framework for Consumer Privacy Legislation to provide a roadmap of issues for the law to address in requiring businesses to protect consumers by holding firms responsible for "collection, use and sharing of personal information."

The Working Group recommends that the Administration in 2021 move quickly and purposefully to **work with Congress to complete and enact this legislation. Given the difficulties experienced by the EU in monitoring and enforcing their new regulations, the federal government should strengthen existing monitoring and enforcement mechanisms.**

CYBERSECURITY

The IT Modernization CAP goal is co-led by the federal Chief Information Officer and OMB, and is meant to increase productivity and security while also building a modern IT workforce, thus aligning squarely with the Academy's Grand Challenge. Among the problems it is meant to address are limited federal agency accountability for reducing cybersecurity risks, acquisition and authorization processes that hinder adoption of current commercial technologies, and reliance on legacy IT systems and a patchwork of network architectures that are difficult to modernize and secure. This cross-agency network already has developed cybersecurity KPIs, is working on several initiatives to build the federal IT workforce, and has worked to protect networks and data. It is a whole-of-government effort led by the OMB CIO in coordination with General Services Administration (GSA), the Office of Personnel Management (OPM), related units in the Office of Management and Budget (OMB), Department of Homeland Security (DHS) and other key partners including the U.S. Digital Service and the NSC Cybersecurity Directorate. **The Working Group recommends that the Administration in 2021 continue and accelerate these efforts.**

The Working Group also recommends that the Administration in 2021 build on the large-scale initiative, the Cyberspace Solarium Commission, a bipartisan congressional commission, to move its recently released recommendations to action. The Commission issued its final report in March 2020. It includes 75 recommendations for the public and private sectors meant to address not only the threat of a major cyberattack but also the "millions of daily intrusions disrupting everything from financial transactions to the inner workings of our electoral system."[4] The report includes several draft bills for Congress in an appendix, one indication of the urgency for action in security. The Chairman's letter introducing the report reads:

> The reality is that we are dangerously insecure in cyber. Your entire life—your paycheck, your health care, your electricity—increasingly relies on networks of digital devices that store, process, and analyze data. These networks are vulnerable, if not already compromised. Our country has lost hundreds of billions of dollars to nation-state-sponsored intellectual property theft using cyber espionage.

[4] Final report, p. v.

The report recommends that "deterrence requires government reform" (p. vii). It calls for the elevation of existing cyber agencies, noting the Cybersecurity and Infrastructure Security Agency (CISA) as the lead agency for the federal government and the "preferred partner" for the private sector. The report also stresses the need to improve the coordination of cybersecurity across the executive branch and Congress; to make election security a priority (Academy Grand Challenge 1); and to make CISA a preferred employer for young professionals on a par with the NSA, Google and the FBI. The report recommends that Congress establish House Permanent Select and Senate Select Committees on Cybersecurity to integrate oversight of efforts currently fragmented across the federal government. Further, Congress should establish a Senate-confirmed National Cyber Director (NCD) supported by an Office of the NCDG in the Executive Office of the President to advise the President and lead national coordination of cybersecurity strategy and policy for the government and with the private sector.

To address the critical need for workforce development, the report recommends that Congress and the executive branch pass legislation and implement policies to recruit, retain and develop "cyber talent" and to expand "the pool of candidates for cyber work in the federal government." The report recommends that Congress create an Assistant Secretary of State in a new Bureau of Cyberspace Security and Emerging Technologies to develop and lead promotion of international norms in cyberspace. Several other recommendations bear directly on this paper, including strengthening the Election Assistance Commission to secure elections by supporting state and local entities and the recommendation to "promote digital literacy, civics education, and public awareness."

Reiterating the urgency of privacy protection, the report also recommends that Congress "pass a national data security and privacy protection law … establishing and standardizing requirements for the collection, retention, and sharing of user data."

BUILDING THE IT WORKFORCE FOR PRIVACY AND SECURITY

The Administration in 2021 can draw from several current federal initiatives. By coordinating these efforts and driving toward an actionable strategic plan, the next administration can take material steps toward building the workforce needed to ensure security and privacy in the federal government and in related workforces. What is needed is a workforce strategic plan that will produce the numbers and quality of experts required to enhance data privacy and security. The next administration should revisit the idea and results of the Chief Information Officer Council's Federal Cyber Reskilling Academy, which provided hands-on training and reskilling in cybersecurity for Federal employees who do not work in IT. The pilot project trained two cohorts and is evaluating the program. The CIO Council includes in its focus areas the federal cybersecurity workforce strategy; federal information security; and several priorities related to privacy, security and related workforce strategies.

The U.S. Department of Commerce, National Institute of Standards and Technology houses the National Initiative for Cybersecurity Education (NICE), whose mission is "to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development." It is a partnership among public, private and nonprofit stakeholders. NICE heads an interagency coordinating council with members from 17 departments and agencies. The National Initiative for Cybersecurity Careers and Studies (NICCS) is "managed by the Cybersecurity Defense Education and Training (CDET) subdivision within the Cybersecurity and Infrastructure Security Agency's (CISA) Cybersecurity Division. CDET promotes cybersecurity awareness, training, education and career structure, with the added goal of broadening the Nation's volume of cybersecurity workforce professionals." Related initiatives include the National Centers of Academic Excellence (CAE) and the National Cybersecurity Workforce Framework.

In addition to the initiatives just described, one of the CAP goals is Developing a Workforce for the 21st Century. Its focus is alignment of personnel processes to serve agency missions. This goal might be expanded to focus on the data privacy and security workforce requirements of the federal government. Although the salary differential for IT professionals between the public and private sectors is typically cited as the key limiting factor in building an IT government workforce, there are tools available to overcome these limitations that could be designed into OPM's processes.

OTHER ACTIONS DURING THE FIRST 100 DAYS OF 2021

In addition to the recommendations identified above, the Working Group recommends that the following series of steps be taken in the first 100 days of the Administration in 2021 so that clear and effective pathways can be laid down for all agencies in the volatile and priority fields of data privacy and security:

1. Develop two Presidential Commissions populated by experts drawn from multiple fields: a Privacy and Security Commission and a Workforce Development Commission. Data privacy and security are issues with well-elaborated nonprofits, think tank activities, lobbying and interest groups and university research. Most experts in these areas are likely to be ready to engage because of the shared sense of the importance of these challenges and their growing urgency in increasingly data-intensive environments
2. Appoint a bipartisan group of experts to the Commissions within 30 days of taking office, within the following guidelines:
    a. Privacy and Security: the 15-20 members must have expertise that cuts across several dimensions and be weighted towards the policy, not the technology, domain. These dimensions should include law, human rights, technology, business management, risk management, cybersecurity and affiliated fields.
    b. Workforce: the 15-20 members must have expertise that cuts across several dimensions and be weighted towards the

policy, not the human resource field alone. These dimensions should include academia, certification industry, human resource professionals from public and private sector, risk management, relevant federal agencies including OPM and Department of Labor, and affiliated fields

3. The two Commissions should be provided staff resources from involved government agencies and be given a 60-day roadmap along the guidelines of this report.
4. All efforts should be made to use existing federal structures to assist the Commissions and prepare implementation roadmaps that can be quickly deployed. For example, the next administration can elevate and draw from the achievements, staffing and resources of the Modernizing IT CAP goal, and build on CAP goals using the teams already in place. OMB and the President's Management Council can also play key roles including the sharing of knowledge, experience of what works and what doesn't, and be prepared for new names, new appointees, and new teams.

OMB guidance is critical to shaping agency actions and understanding of new initiatives. Using existing CAP goal structure and methodology, each CAP goal group should (1) draw up a plan to enhance data security and privacy or to contribute to the workforce recommendation; (2) summarize their key initiatives that contribute to the plan; (3) describe the key next steps, resources needed and any additional authorities required to advance toward these goals. Using the quarterly meetings with OMB, GSA and other Executive Office of the President staff that have been so successful in moving cross-agency initiatives forward, the next administration should build privacy, security and workforce recommendations into the next set of CAP goals. In the first 90 days, OMB should direct agencies to specify in their Agency Performance Goals how their Chief Privacy Officers and others with responsibility for data privacy and security are taking steps toward strengthening privacy and security.

CONCLUSION

In the digital age, the American people knowingly and unknowingly produce huge amounts of data on a daily basis, and governments at all levels increasingly rely on digital systems to manage their internal operations and deliver public services. Americans need assurance that all sectors will keep their personal data private and safeguarded from abuse, but our data security infrastructure in both the public and the private sectors is vulnerable to exploitations, hacks, and breaches.

The Administration in 2021 (whether reelected or newly elected) has an opportunity to build on existing activities and take additional actions to protect data security and individual privacy. The leadership challenge for new appointees will be great; new appointees should be prepared to quickly be brought up to speed by their staff and interagency groups on these issues, particularly where action steps have already been deliberated, drafted and advanced. If new appointees are selected and confirmed relatively quickly, they will be able to lead more quickly. Career federal executives who have been leaders in these challenge areas should be ready to move forward and support the Administration in 2021 as it seeks to address this Grand Challenge.

Ensure Data Security and Privacy Rights of Individuals: Working Group:

Costis Toregas, Working Group Chair
Director, Cyber Security Policy and Research Institute, George Washington University; County Council IT Advisor, Montgomery County MD; Board Member and Treasurer, Ecocity Builders; Board Member and Treasurer, Women in Cybersecurity; Board Member and Finance Director, National Cyber League. Former Content Manager, Abu Dhabi Global Environmental Data Initiative; Adjunct Associate Professor, Department of Public Administration and Policy, American University; Lead Research Scientist, Department of Computer Science, George Washington University; President Emeritus, Public Technology Institute. Former positions with Public Technology, Inc.: President, Vice President, Program Director. Former Consultant, Doxiadis Systems Development Corporation.

Jane Fountain
Distinguished University Professor of Political Science and Public Policy, School of Public Policy and Department of Political Science; Distinguished Adjunct Professor, College of Information and Computer Science; University of Massachusetts Amherst; Director, National Center for Digital Government, University of Massachusetts Amherst. Former positions at John F. Kennedy School of Government, Harvard University: Associate Professor, Public Policy; Assistant Professor; Instructor. Former: Research Associate, Wesleyan University; Radcliffe Institute Fellow; Massachusetts Governor's Innovation Council of Advisors; American Bar Association Blue Ribbon Committee on the Status and Future of Electronic Rulemaking; Chair, Vice Chair, Member, World Economic Forum, Global Agenda Council on the Future of Government.

Nick Hart
Chief Executive Officer, Data Coalition. Adjunct Faculty, Trachtenberg School, George Washington University; Director, Evidence Project, Policy and Research Director, Senior Program Examiner, Education, Income Maintenance, and Labor, White House Office of Management and Budget; Special Assistant, Program Examiner, Natural Resources, White House Office of Management and Budget; Economic Research Analyst,

James Hendler
Professor, Computer Science, Rensselaer Polytechnic Institute; Professor, Computer Science, University of Maryland; Program Mgr/Chief Scientist (IPA), Information Systems, Def Advanced Research Projects Agency (DARPA); Open Data Advisor, New York State (unpaid), NYS Government; Internet Web Expert, Data.gov project, IPA to GSA, working w/OSTP; Member Advisory Committee, Homeland Security Science and Technology Adv. Comm, DHS; Board Member, Board on Research Data and Information, Nat'l Acad Science, Engineering and Medicine; Director's Advisory Committee Member, Nat'l Security Directorate, Pacific Northwest National Laboratories

Mark Reger
Former Deputy Controller, Office of Federal Financial Management, U. S. Office of Management and Budget, U.S. Executive Office of the President. Former Deputy Assistant Secretary for Accounting Policy, U.S. Department of the Treasury; Chief Financial Officer, US Office of Personnel Management; Chief Financial Officer, Federal Communications Commission. Former positions with State of Maryland: Chief Deputy Treasurer; Assistant State Treasurer. Former positions with Maryland Department of Agriculture: Chief Financial Officer; Deputy Director of Administration; Internal Auditor Agriculture.

Priscilla Regan
Chair, Department of Public & International Affairs, Professor of Government & Politics, George Mason University. Former Program Director, Science and Society Program, Social, Behavior & Economic Sciences, National Science Foundation (NSF). Former positions with the Office of Technology Assessment: Senior Analyst; Analyst.

Peter Winokur
President & Founder, Integrated Safety Solutions, LLC; Chairman Emeritus, Defense Nuclear Facilities Safety Board; Former Chairman, Defense Nuclear Facilities Safety Board; Senior Policy Analyst, National Nuclear Security Administration; Congressional Fellow, Office of Senator Harry Reid; Manager, Radiation Technology & Assurance, Sandia National Laboratories; President, IEEE Nuclear and Plasma Sciences Society; Member, IEEE-USA Board of Directors; 40 years of experience as a scientist and engineer in the field of radiation effects science, technology, and hardness assurance in support of military and space systems. Fellow, Institute of Electrical and Electronic Engineers and American Physical Society.

Staff

Joseph P. Mitchell, III
Director of Strategic Initiatives and International Programs, National Academy of Public Administration; Member, National Science Foundation Business and Operations Advisory Committee; Associate Director, Office of Shared Services and Performance Improvement, General Services Administration; Director of Academy Programs, National Academy of Public Administration; Project Director, Senior Analyst, and Research Associate, National Academy of Public Administration.

James Higgins
Research Associate for Grand Challenges in Public Administration, National Academy of Public Administration; Researcher, Cohen Group; Extern, U.S. Patent and Trademark Office.

This page is intentionally blank