

MORE THAN MEETS AI

PART II

BUILDING TRUST, MANAGING RISK




JULY 2019



PARTNERSHIP FOR PUBLIC SERVICE



IBM Center for
The Business of Government



This white paper follows “More Than Meets AI: Assessing the Impact of Artificial Intelligence on the Work of Government,” in which the Partnership for Public Service and the IBM Center for The Business of Government explored how the technology might affect federal employees. The experts we spoke with said automating administrative tasks will be one of AI’s initial benefits. Over time, federal employees will spend less time on repetitive work and more of their workday on tasks that are core to their agencies’ missions. If this prediction becomes reality, and given the increasing amount of information AI can collect and analyze, employees could focus more attention on tailoring services to customer needs. AI also is expected to change what skills are necessary to succeed in the federal workplace by bringing technical, digital and data literacy to the fore.

The Partnership for Public Service is a nonpartisan, nonprofit organization that works to revitalize the federal government by inspiring a new generation to serve and by transforming the way government works. The Partnership teams up with federal agencies and other stakeholders to make our government more effective and efficient. We pursue this goal by:

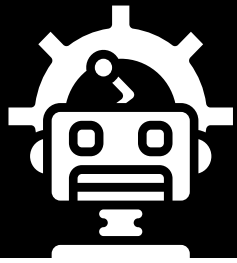
- Providing assistance to federal agencies to improve their management and operations, and to strengthen their leadership capacity.
- Conducting outreach to college campuses and job seekers to promote public service.
- Identifying and celebrating government’s successes so they can be replicated across government.
- Advocating for needed legislative and regulatory reforms to strengthen the civil service.
- Generating research on, and effective responses to, the workforce challenges facing our federal government.
- Enhancing public understanding of the valuable work civil servants perform.

About the IBM Center for The Business of Government

Through research stipends and events, the IBM Center for The Business of Government stimulates research and facilitates discussion of new approaches to improving the effectiveness of government at the federal, state, local and international levels. Since its creation in 1998, the Center has awarded research stipends to public management researchers in the academic and nonprofit communities that have resulted in nearly 350 reports—all of which are available on the Center’s website at businessofgovernment.org.

About IBM Global Business Services

With consultants and professional staff in more than 160 countries globally, IBM Global Business Services is the world’s largest consulting services organization. IBM Global Business Services provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build and run those solutions in a way that delivers bottom-line value. To learn more visit ibm.com.



Introduction

Artificial intelligence has great potential to improve how the federal government works. AI can increase operational efficiency and effectiveness, free employees of repetitive tasks, uncover new data insights, and enhance service delivery to customers. While they take advantage of these benefits, federal agencies must also manage real and perceived risks associated with AI to build trust in these technologies.

Federal, state and local governments are embracing AI. Federal agencies use it to identify insider threats, support military deployment planning and scheduling, and answer routine immigration questions. Agencies are considering additional uses that range from checking compliance with tax laws and regulations to assessing the accessibility of government products and websites.

This white paper draws on lessons from companies and countries around the world that use AI. These organizations have identified and are addressing AI issues that include bias, security, transparency and job impact, and their insights can be instructive for federal agencies.

Many Americans have questions about effects AI technologies may have on aspects of their lives. According to an October 2018 survey of more than 2,500 Americans, 59% of respondents are “very concerned” or “somewhat concerned,” with job loss and displacement worries ranking highest.¹ They also conveyed concerns about data privacy, security, hacking and the safety of AI systems.²

Although these risk factors also affected public perceptions when other technologies were introduced, leaders now need to also address these concerns to foster trust as agencies rely more on AI to carry out missions.

Through an executive order, an AI summit, and the creation of a website and a White House Select Committee on AI, the Office of Management and Budget and the Office of Science and Technology Policy are leading a government-wide effort to maximize AI’s benefits, while laying the groundwork for agencies to address risks responsibly. To increase the trust the public and federal employees have in government’s use of AI tools, the government’s strategy deals with transparency, security, technological know-how, procurement, budgeting and risk management. This white paper discusses further steps agencies can take to manage risks, and looks at pitfalls the AI research and development community has faced.

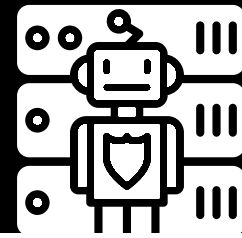
Even as agencies address concerns, they must move forward with implementation. If they do not incorporate AI tools into their work, they are likely to find it more difficult to address a growing number of complex challenges, according to Joshua Marcuse, executive director of the Defense Department’s Defense Innovation Board. “In most cases, the risks of going too slowly exceed the risks of some projects failing,” he said.

At AI roundtable discussions and interviews conducted by the Partnership for Public Service and the IBM Center for The Business of Government, participants were optimistic about their agency’s ability to implement the technology. Many of them described a path to success that would start by using AI in smaller, attainable projects, enabling their agencies to develop expertise and experience. With government-wide initiatives putting AI front and center, and progress being made in AI research and development, now is the time to act.

¹ Omnicom’s AI Impact Group, “AI Threat Survey,” October 2018.

² Ibid.

UNDERSTANDING AND ADDRESSING AI RISKS



As agencies integrate AI into their work, they will have to pay attention to issues ranging from the ethical to the practical. Top challenges include bias, security, transparency, employee knowledge about AI technology, and federal budget and procurement processes. Each of these challenges is discussed below, along with recommendations for how agencies could address potential concerns and develop strategies to mitigate them.

It is important for federal organizations to move forward with implementing AI technologies as they address AI's risks. Their approach to lessening AI risks also must evolve rapidly if they hope to use AI to address government's most pressing challenges.

Bias

Bias in AI outcomes can stem from a number of issues, including poor-quality data, limited amounts of data or data that doesn't fully represent all aspects of a matter. Knowing that biased data may lead to biased results, agencies need to pay special attention to what information is being used with these new technologies. AI technology is "trained" on data, yet not all the information that has been collected over the years is necessarily of the highest quality. "Because AI tools are data-driven, there is the issue of bias and latent bias—hidden, unknown and unwanted—in data," said Michael Garris, senior computer scientist at the National Institute of Standards and Technology.

A machine by itself could forge ahead churning out results that are biased or inconsistent with the organization's values. When humans trained in data analysis work with an AI tool, they could evaluate if the outputs generated are inconsistent with expected results or the values

of the organization. "A human in the loop could see if what the machine is producing resonates with what we as a society are comfortable with," said David Bray, executive director at the People-Centered Internet coalition and senior fellow with the Institute for Human-Machine Cognition.

For example, a Toronto-based startup developing an AI tool that analyzes speech patterns to diagnose neurological disorders, such as Alzheimer's, inadvertently trained the product on the speech of one group of individuals: native English speakers speaking the local Ontarian dialect. As a result, the speech-analysis tool was biased against speakers whose first language was not English, identifying variations in pronunciation or inflection as signs of Alzheimer's.³ These results, and others built on

them, could institutionalize such biases into the future.

To address AI bias, federal organizations need employees with technical acumen and data analysis and interpretation skills who can detect data bias and inaccuracies. Experts in government need to understand the theory behind AI, how the algorithms work and how conclusions are reached. Under the White House's February 2019 AI executive order, National Institute of Standards and Technology researchers are exploring ways to test and measure AI security and trustworthiness. As part of its task, the agency is working with international partners to explore the potential for global AI standards. These and similar efforts should include creating a framework for assessing bias.

³ Dave Gershgorn, "If AI is going to be the world's doctor, it needs better textbooks," Quartz, Sept. 6, 2018. Retrieved from <http://bit.ly/2MZPEC5>

Security

As with any IT product or service, AI needs strong cybersecurity to protect against vulnerabilities and threats from bad actors. However, AI's potentially widespread impact amplifies cybersecurity concerns. If AI systems "are driving cars, fighting wars, and the like," hackers who can compromise these systems "have greater capacity to do enormous damage more quickly," according to "Machine Learning for Policymakers," a 2017 Harvard University research paper.⁴

AI is vulnerable in several ways if designed without proper security measures. Attacks could alter AI training data or introduce corrupted or incorrect data that changes the conclusions of the AI tool. Hackers also could act to reveal personally identifiable information in the data on which an AI tool was trained.

With security paramount, the Defense Department is investigating how to safeguard AI technology from attacks. In a 2018 strategy, the department committed to fund research and development of reliable and secure AI systems, but more work is needed to evaluate the security of AI technologies.⁵ Right now, "the science of measuring AI security doesn't exist," said Jason Matheny, director of Georgetown University's Center for Security and Emerging Technology. Observers with technology backgrounds suggest methods for protecting the technology that include assigning human beings to monitor AI for integrity and attacks and enlisting employees to purposely attack systems

4 Ben Buchanan and Taylor Miller, "Machine Learning for Policymakers: What It Is and Why It Matters," Harvard Kennedy School, June 2017, 39. Retrieved from <http://bit.ly/2UrMWrB>

5 Department of Defense, "Summary of the 2018 Department of Defense Artificial Intelligence Strategy," Feb. 12, 2019, 8. Retrieved from <http://bit.ly/2P417h9>

to identify and fix vulnerabilities.

Our government and governments in other countries could share knowledge and lessons learned, as security concerns are global in nature. Tim Clement-Jones, a former chair of the Artificial Intelligence Committee in the United Kingdom's House of Lords, indicated that given these interconnected security implications, government has to ensure data safety and "spend some time reassuring people that our cybersecurity is very much up to scratch."

Transparency

With AI, agencies have the ability to accomplish activities more quickly and accurately; by making AI transparent, users can learn how and why the tool arrived at a conclusion and what data the AI technology used. Lack of transparency can pose issues when people want an explanation for why decisions were made. "Most of the AI decision-making process today is a 'black box' to non-AI experts, and even to some AI experts," according to the National Science Foundation.⁶ Some AI algorithms are proprietary; others are so complex that it is hard to explain, or for people to understand, how conclusions were reached.

Without clarity about how AI produces its recommendations and conclusions or understanding from employees as to how to explain results derived from AI technology, governments may risk losing the public's trust and could, for example, face challenges similar to the one a Texas school district confronted over

6 National Science Foundation, "Learning Mathematical Concepts and Computational Thinking through Explainable Artificial Intelligence in a Simulation-based Learning Environment," Sept. 11, 2018. Retrieved from <http://bit.ly/2JIA7Oz>

using AI for teacher evaluations (see text box below).

Between 2011 and 2015, the Houston Independent School District used a private company's AI algorithm to evaluate teacher performance and, in some cases, to determine which employment contracts to terminate or renew. Although the system used existing data on instructional practices, professional expectations and student performance, the teachers' union filed a lawsuit arguing the system was not transparent because teachers could not find out how the algorithm scored their performance or came up with recommendations for personnel actions.

Court filings alleged these evaluations led to dozens of teachers being terminated from the school district, yet the AI system developer would not share the proprietary formula used for weighing and scoring their performance. The school district agreed to discontinue using the AI tool.⁷

7 Shelby Webb and John Harden, "Houston ISD settles with union over controversial teacher evaluations," Houston Chronicle, Oct. 12, 2017. Retrieved from <http://bit.ly/2lq3Ccx>

The AI research and development community recognizes that transparency will promote trust in AI systems. Researchers are looking into explainable AI and making AI algorithms and results less of a black box. This will enable governments and others that incorporate AI into their processes to respond to questions about the decisions involving AI technology.

Some agencies, such as the Defense Advanced Research Projects Agency and National Science Foundation, have funded research into explainable AI. This could help users "understand, appropriately trust, and effectively

manage an emerging generation of artificially intelligent machine partners,” according to DARPA.⁸ Related research on explainability involves adding interpretability to AI technology to help address ways that AI algorithms can be seen as black boxes; such results can occur when users lack insight into a decision, or redress if they believe a decision was wrong, or when the complexity of AI is nearly impossible to explain. And the Centers for Medicare and Medicaid Services hopes to acquire AI tools that could “explain AI predictions to clinicians and patients to build trust and drive transparency,” seeking ways to predict hospitalizations and medical problems.⁹

Employee Knowledge

Maximizing AI benefits while managing AI risks hinges on hiring or training employees who understand and use the technology responsibly. Getting enough of the workforce up to speed is critical, but government often faces funding and other challenges—and often falls short on AI training and education, according to several participants in recent Partnership and IBM Center AI roundtables. Echoing comments by other participants, Lee Becker, chief of staff at the Department of Veterans Affairs’ Veterans Experience Office, said, “In the context of AI, our dedicated employees may feel like they do not have the necessary skills to address issues that may come up. By investing more in providing AI-related training to our existing employees, they could help agencies use the AI technology to achieve

8 Defense Advanced Research Projects Agency, “Explainable Artificial Intelligence (XAI),” August 2016. Retrieved from <http://bit.ly/2IsWagV>

9 Centers for Medicare and Medicaid Services, “AI Health Outcomes Challenge Launch Stage Judging Criteria,” 2019. Retrieved from <http://bit.ly/2Ktu6MZ>

Over the years, Congress has called for transparency in numerous areas before AI came on to the scene, leading to practices that have become institutionalized in our society. For example, the 1970s law that established fair lending practices set transparency requirements for financial service providers that issue credit. Providers are now required to explain certain adverse decisions to credit applicants, such as denying credit or changing the terms of an existing arrangement. For most adverse credit actions, the applicant must receive—in writing, within 30 days—the reasons for the denial. This improves applicants’ ability to get credit in the future by, for example, changing their spending habits.

Lawmakers recognized that “explainability”—a term of art in AI—was critical for maintaining Americans’ trust in financial institutions. If agencies use AI to make consequential decisions, transparency will be important to retain taxpayers’ trust.

greater impact for the American people.”

The federal government should emphasize expertise in technical, digital and data skills. It should provide extensive and ongoing training to employees so they can create, understand, manage and work with AI technology.

At the outset, even small changes, such as educating employees on key AI terms and definitions, could be beneficial for increasing transparency. “Employees need to learn to communicate about AI algorithms so that people can understand what the tool does,” said Dorothy Aronson, chief information officer at the National Science Foundation.

Federal Budget and Procurement Processes

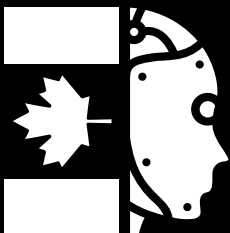
Outdated federal acquisition and budget processes prevent agencies from buying and deploying new technology quickly and efficiently. Since most agencies start budgeting two years in advance, they often do not have the flexibility or “clairvoyance” to buy the newest technologies, said Aronson, CIO at the National Science Foundation.

Additionally, the typical acquisition process involves purchasing a finished product or service, yet many AI applications are iterative, improving over time through experience with more and more data and evolving with

technological advances. The rapid pace of AI development and improvement can leave government lagging behind, as has been the case with the introduction of many emerging technologies in the past. “AI is transforming economic and social sectors deeper and faster than expected,” according to a conference paper by the Organization for Economic Co-operation and Development, an international economic organization with 36 member nations, including the U.S. “AI is moving fast, so should governments,” the paper stated.¹⁰

As with other technology innovations, agencies should obtain what they need for AI by taking full advantage of the tools and flexibilities available in the budget and procurement processes. For example, agencies could use “try before you buy” acquisitions that allow them to experiment with new tools on a small scale, or staged contracts to evaluate proposals and pilot tools before investing in full.

10 Organization for Economic Co-operation and Development, “AI: Intelligent Machines, Smart Policies Conference Summary,” 2018. Retrieved from <http://bit.ly/2G3hi1q>



CASE STUDY

LESSONS FROM CANADA ON MAXIMIZING AI BENEFITS AND MANAGING RISKS

As the U.S. government aims to assess and mitigate AI risks, agencies can look to international models. The AI research and development community considers Canada to be at the forefront among governments at managing AI risks. The Canadian government has taken steps to ensure its departments and agencies have tools, rules and people to use AI responsibly. As our government adopts AI, it should enable agencies to buy tested and trusted AI products and create effective ways to identify and manage potential risks. Additionally, government should equip enough of the workforce—especially those working with AI directly—with knowledge and skills to use the technology well.

Based on the Canadian government's experiences, U.S. government agencies will need to balance regulation and oversight with support for private sector research, development and innovation. Canada's example outlines potential tools, rules and people issues for consideration.

Tools: Simplify Buying Credible AI Products

To procure AI faster and more efficiently, the Canadian government in September 2018 released a list of more than 70 suppliers proficient in AI and AI ethics.¹¹ The government deemed these qualified vendors to have delivered a successful AI product or service. They also were required to describe “how they address ethical considerations when delivering AI” by, say, providing examples of “applying frameworks, methods, guidelines or assessment tools to test datasets and outcomes.”¹²

11 Government of Canada, “AI-IA Artificial Intelligence Source List,” Jan. 28, 2019. Retrieved from <http://bit.ly/2VCSzV1>

12 Government of Canada, “Invitation to qualify (ITQ) on a source list of suppliers to provide Canada with responsible and effective Artificial Intelligence (AI) services, solutions and products,” Oct. 29, 2018. Retrieved from <http://bit.ly/2vZdv9K>

Rules: Create a Framework to Assess the Risks of Using AI in Government

According to an April 2019 Canadian government directive, if a department or agency is using automated decision-making in support of service delivery, it is required to assess the associated risks. The government developed four levels of impact an AI tool might have on society and government, ranging from little to no impact that could be “reversible and brief” to very high impact, which might lead to “irreversible” and “perpetual” changes.¹³ Programs in defense, national security and law enforcement are exempt from the requirement.

For use of AI with little or no impact on service programs, the directive

13 Government of Canada Treasury Board of Canada Secretariat, “Directive on Automated Decision-Making,” Feb. 5, 2019. Retrieved from <http://bit.ly/2JEDfA1>

allows for the possibility of automated end-to-end decision-making—in other words, making decisions without human involvement. However, it states that program officials must be able to explain how conclusions were reached. For example, they could provide a frequently asked questions section on the program's or agency's website. At this level, input from AI usually is used for reversible decisions, such as whether to provide clearly needed medical services to veterans—for example, gunners who have bad hearing or paratroopers who suffer from knee issues because of their military service, said Chief Technology Officer Marc Brouillard of the Canadian government.

Requirements for AI used by high-impact programs, on the other hand, include a peer review by government

experts, academics, nongovernment organizations or other advisory boards; repeated training for employees using the AI tool; and documentation posted on relevant websites describing how the tool works. In addition, a person must make any final decisions based on an AI tool's recommendation.¹⁴

Depending on the impact level, programs also must disclose to the citizen whether a decision affecting them is made partly or wholly by an AI tool.¹⁵

The directive also addresses AI transparency and the Canadian government's right to access and test proprietary AI systems if "necessary for a specific audit, investigation, inspection, examination, enforcement action, or judicial proceeding."¹⁶ Brouillard said this ensures that "if something goes wrong, you can break the glass and see what happened."

14 Ibid.

15 Ibid.

16 Ibid.

People: Train Public Servants on How to Use AI Tools

To address a skills gap and ensure government programs use AI tools responsibly, the Canada School of Public Service, the Canadian government's primary educational institution, in January 2019 launched a pilot cohort of its public sector Digital Academy. It is seeking to improve the digital acumen of public servants at all levels and eventually expanding training to all public employees. The training "will aim to build key digital competencies in data analysis, design, development and automation, disruptive technology and artificial intelligence, and machine learning," according to a government press release.¹⁷

Elevating the digital literacy of employees can help them get more comfortable with new technologies. "It can cause stress and angst if

you don't understand artificial intelligence and you are working alongside it," Brouillard said. Aside from providing digital, data and AI skills, the government hopes the training eases concerns by raising awareness among public servants about the current state of AI and other digital technologies, and how they could affect their jobs and even private lives.

17 Government of Canada, "Government of Canada launches Digital Academy," Oct. 16, 2018. Retrieved from <http://bit.ly/2VoBVno>

Conclusion



Few technological innovations offer the many potential benefits of artificial intelligence. AI tools range from entertaining to productivity-improving to life-saving, from playing poker or creating paintings in Vincent van Gogh's style to transcribing audio to diagnosing diseases or predicting financial fraud.

AI tools also are expected to impact the federal government substantially, with implications for federal systems and structures. To capture the benefits of AI, federal agencies must be prepared to address related

risks. The Office of Management and Budget and Office of Science and Technology Policy should continue to lead efforts to manage those risks, given the technology's potential to transform work government-wide.

The Partnership for Public Service and the IBM Center for The Business of Government hope this white paper will spark conversations in government. Future issues we will consider include defining different approaches to using AI with human oversight in simplifying processes and saving time, relative

to approaches using AI to support complex human decision-making. Canada's experience provides one such model for this shift. Another question on using the technology may be how best to make AI part of agency mission planning and delivery, rather than a separate technology activity loosely linked to agency programs. We will continue our research and discussions into AI and its potential to make government more efficient and effective.

Appendix I Methodology

This white paper is part of a multiyear series. The Partnership for Public Service and the IBM Center for The Business of Government previously published two research publications on AI, “The Future Has Begun: Using Artificial Intelligence to Transform Government” in January 2018 and “More Than Meets AI: Assessing the Impact of Artificial Intelligence on the Work of Government” in February 2019.

The information presented here is based on four roundtable discussions

our organizations hosted between July 2018 and May 2019 and interviews we conducted in the spring of 2019. The 68 participants have AI expertise in a variety of sectors and fields. The four roundtable discussions focused on: the potential applications of AI and the types of challenges it best lends itself to solving; the technology’s workforce implications; its connectedness with other emerging technologies, including blockchain and cloud computing; and

managing AI risks, such as bias, security and transparency.

Our conversations to inform this white paper explored AI ethics, an expansive and hard-to-define topic, according to most interviewees and roundtable participants. Instead of broadly tackling ethics, this paper discusses related subtopics relevant to government agencies, such as bias, security and explainability.

On Artificial Intelligence

The term artificial intelligence refers to machines and software able to perform tasks we typically associate with humans, such as recognizing speech or images, predicting events based on past information, or making decisions. Machine learning, another commonly used term, is a subset of AI that uses large amounts of data and information to continually improve how a system performs a task.

The computing power behind AI enables machines to complete tasks faster than humans, and machines do not tire after hours or days of repetitive tasks. AI is continuing to improve at tasks such as transferring information from paper into computers, answering questions by quickly finding relevant information in large databases or long documents, detecting patterns in troves of data, making decisions about simple queries, and predicting someone’s behavior based on past conduct.

Appendix II Acknowledgements

The individuals listed below generously offered their input on the use and potential of artificial intelligence in government. We greatly appreciate their time and counsel. The contents of this white paper do not necessarily reflect the views of those with whom we spoke. Additionally, the views of participating federal officials do not necessarily reflect positions or policies of the federal government or its agencies.

Roundtable Participants

Jonathan Alboum, Public Sector Chief Technology Officer, Veritas Technologies LLC

Calvin Andrus, Data Scientist, Central Intelligence Agency

Natasha Amonkar, Intern, Office of the Chief Procurement Officer, Internal Revenue Service, Department of the Treasury

Angela Bailey, Chief Human Capital Officer, Department of Homeland Security

Sandy Barsky, Deputy, IT Software Category Manager, Emerging Technologies, General Services Administration

Lee Becker, Chief of Staff, Veterans Experience Office, Department of Veterans Affairs

Anita Blair, Fellow, National Academy of Public Administration

James-Christian Blockwood, Managing Director, Strategic Planning and External Liaison, Government Accountability Office

Marc Brouillard, Chief Technology Officer, Government of Canada

Alana Cober, Branch Chief, Office of the Chief Human Capital Officer, National Aeronautics and Space Administration

Michael Conlin, Chief Data Officer, Department of Defense

Stacey Dixon, Director, Intelligence Advanced Research Projects Activity, Office of the Director of National Intelligence

R. David Edelman, Director, Project on Technology, Economy and National Security, Massachusetts Institute of Technology

Simona Folescu, Manager, Emerging Trends Program, Center for the Study of Intelligence, Central Intelligence Agency

Mark Forman, Vice President and Global Head, Public Sector, Unisys

Michael Garris, Senior Computer Scientist, National Institute of Standards and Technology, Department of Commerce

Alexandra Givens, Executive Director, Georgetown University Institute for Technology Law and Policy

Karyn Gorman, Privacy Analyst, National Highway Traffic Safety Administration, Department of Transportation

Joseph M. Greenblott, Associate Director, Analysis Division, Office of Planning, Analysis and Accountability, Office of the Chief Financial Officer, Environmental Protection Agency

David Grier, Technology Principal and Chief Technology Officer, Djaghe LLC

Benjamin Isaacoff, The Optical Society and SPIE Arthur H. Guenther Congressional Science and Technology Fellow, Office of Sen. Gary Peters, U.S. Senate

John Kendall, Border and National Security Program Director, Unisys

Sunmin Kim, Technology Policy Advisor, Office of Sen. Brian Schatz, U.S. Senate

Frank Konieczny, Chief Technology Officer, Department of the Air Force, Department of Defense

Varun Krovi, Deputy Chief of Staff and Legislative Director, Office of Rep. Brenda Lawrence, U.S. House of Representatives

Dimitri Kusnezov, Deputy Under Secretary for Artificial Intelligence and Technology, Department of Energy

Ricky Le, Vice President, Information Technology Industry Council

Gregory Little, Team Lead, Business Integration Office, Department of Defense

Jennifer Main, Chief Operating Officer, Centers for Medicare and Medicaid Services, Department of Health and Human Services

Joshua Marcuse, Executive Director, Defense Innovation Board, Department of Defense

Lauren Marshall, Legislative Assistant, Office of Sen. Mark Warner, U.S. Senate

Katharina McFarland, Commissioner, National Security Commission on Artificial Intelligence

Barbara McIntyre, Office of the Director of National Intelligence

Alexander Measure, Economist, Bureau of Labor Statistics, Department of Labor

Oki Mek, Chief Technology Officer, Division of Acquisition, Department of Health and Human Services

Meagan Metzger, Founder and CEO, Dcode

Alan Monico, Procurement Analyst, Department of the Treasury

Daniel Morgan, Chief Data Officer, Department of Transportation

Keith Nakasone, Deputy Assistant Commissioner, Acquisition, Office of Information Technology Category, General Services Administration

Sandeep Neema, Program Manager, Defense Advanced Research Projects Agency, Department of Defense

Thomas Oscherwitz, Senior Advisor and Counsel, Markets Office, Consumer Financial Protection Bureau

Timothy Persons, Chief Scientist, Government Accountability Office

Robyn Rees, Senior IT Advisor, National Science Foundation

Todd Rosenblum, Senior Fellow, Atlantic Council

Todd Rubin, Attorney Advisor, Administrative Conference of the United States

Alan R. Shark, Executive Director, Public Technology Institute (a subsidiary of CompTIA)

Catherine Sharkey, Crystal Eastman Professor of Law, New York University School of Law

Robert Simpson, Deputy Executive Director, Planning, Program Analysis and Evaluation Directorate, Office of Human Resources, U.S. Customs and Border Protection, Department of Homeland Security

Elanchezhian Sivagnanam, Chief Architect, National Science Foundation

Teresa Smetzer, CEO, Smetzer Associates, LLC and Former Director of Digital Futures, Central Intelligence Agency

Jude Soundararajan, Executive Director of Health Information Technology, Social Security Administration

John Sprague, Acting Associate Chief Information Officer for Technology, Data, and Innovation, National Aeronautics and Space Administration

Elham Tabassi, Acting Chief of Staff, Information Technology Laboratory, National Institute of Standards and Technology, Department of Commerce

Peter Tseronis, Founder and CEO, Dots and Bridges LLC

Scott de la Vega, Designated Agency Ethics Official, Department of the Interior

Mitchell Winans, Special Assistant, Office of the Chief Procurement Officer, Internal Revenue Service, Department of the Treasury

Jeremy Wood, Director, Enterprise Architecture, Millennium Challenge Corporation

Interviewees

Jose Arrieta, Chief Information Officer, Department of Health and Human Services

Alan Arsenault, Chief, Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance Branch, Research and Development Center, U.S. Coast Guard, Department of Homeland Security

Dorothy Aronson, Chief Information Officer, National Science Foundation

David A. Bray, Executive Director, People-Centered Internet coalition and Senior Fellow, Institute for Human-Machine Cognition

Ben Buchanan, Assistant Teaching Professor, Georgetown University School of Foreign Service

Tim Clement-Jones, Member, House of Lords of the United Kingdom

Michael Curtis, Executive Director, GrantSolutions.gov, Department of Health and Human Services

Kevin Desouza, Professor of Business, Technology and Strategy, Queensland University of Technology

Chuck Howell, Chief Scientist for Dependable Artificial Intelligence, The MITRE Corporation

Jason Matheny, Director, Georgetown University Center for Security and Emerging Technology (CSET)

Michael Sulmeyer, Director, Cyber Security Project, Harvard Kennedy School Belfer Center for Science and International Affairs

Lawrence Tabak, Principal Deputy Director and the Deputy Ethics Counselor, National Institutes of Health, Department of Health and Human Services

Appendix III Project Team

Partnership for Public Service

Mallory Barg Bulman, Vice President,
Research and Evaluation

Allison Benjamin, Intern

Samantha Donaldson, Vice President, Communications

Peter Kamocsai, Associate Manager and Project Lead

Katie Malague, Vice President, Government Effectiveness

Tim Markatos, Associate Design Manager

Ellen Perlman, Writer and Editor

Jaimie Winters, Associate Manager

IBM Center for The Business of Government

Daniel Chenok, Executive Director,
IBM Center for The Business of Government

Alayna Kennedy, Cognitive Process Transformation
Consultant, IBM Global Business Services

Tatiana Sokolova, Senior Consultant, Cognitive Business
Decision Support, US Public Service, IBM Global Business
Services

Claude Yusti, Partner, Public Sector Watson AI and Data
Platform, IBM Global Business Services



PARTNERSHIP FOR PUBLIC SERVICE

1100 New York Avenue NW
Suite 200 East
Washington DC 20005

(202) 775-9111
ourpublicservice.org
CFC# 12110

 partnershipforpublicservice

 RPublicService

 rpublicservice



IBM Center for The Business of Government

600 14th Street NW
Second Floor
Washington DC 20005

(202) 551-9342
businessofgovernment.org