TECH TALENT FOR 21ST CENTURY GOVERNMENT

APRIL 2020

PARTNERSHIP FOR **PUBLIC SERVICE**

🛜 **TECH TALENT PROJECT**

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.

The Tech Talent Project is a nonprofit, nonpartisan initiative focused on increasing the federal government's ability to recruit modern technical leaders to achieve critical human, economic, and policy outcomes. Having these leaders in the right roles means government can effectively leverage modern technology to develop policy, support and regulate emerging technologies, and ultimately improve education, reduce poverty, protect the environment, expand access to healthcare, and provide critical benefits to the poor, the unemployed, people with disabilities, and senior citizens.

To do this, the Tech Talent Project is:

- Identifying critical leadership roles in the government that require qualified modern technologists.
- Building awareness among elected, appointed, and hired government leaders of the need for modern technologists in a 21st century government.
- Sharing learnings about how to effectively hire and retain tech talent into all levels of government.
- Building a leadership bench of qualified modern technologists, innovation experts, and others who could bring the required expertise to such leadership roles.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The past decade has seen an incredible technological revolution. Ten years ago, smartphones and tablets hit the market for the first time. The wave of big data was still in its infancy. Ride-sharing companies did not yet exist. Working in the cloud was still an experiment. Digital streaming was not realistic. The idea of cheap genomic screening was still far over the horizon. And given the additional advancements we expect to see from artificial intelligence, data science, quantum computing and more, the world as we know it is likely to be radically different in the next decade too.

Even with new life-changing innovations on the way, antiquated technical systems and approaches in the federal government frustrate employees and the American public alike. There has never been a more important time to enhance policy design and implementation, and bring digital, technological and innovation expertise into federal agencies.

- **Policy:** Nearly every national priority depends on an accurate, thorough and contemporary understanding of how to use and leverage modern technology. Federal policies and programs that Americans depend on, including Medicare and our nation's defense, rely on digital services and information technology platforms. Looking ahead, any administration's cornerstone policy will inevitably rely on or be constrained by existing and new technologies such as artificial intelligence and machine learning. Building that policy without technologists at the table would be a mistake.

- **Digital delivery:** The federal government must increase its capacity to deliver services digitally to the public. Veterans should be able to access their benefits online and on mobile devices, the next-generation air traffic system must be delivered on time and within budget, and agency systems and data need to be secure from cyber threats. Unfortunately, time after time we have seen major federal information technology projects either fail or under-deliver with massive costs.

- **Innovation:** Some of the most important innovations in America have been led by federal institutions, including space exploration and the creation of the patent system. For government to provide first-class services, it must test and adopt new practices, methodologies and technologies, especially those proven to be effective in other sectors. The innovations of the next decades will dwarf those of the past decade through automation, artificial intelligence, bioengineering, quantum computing, the development of new materials and much more. It will be critical to ensure that the federal government continues to drive policy that encourages the best aspects of innovation, manages the risks and strengthens the nation's leadership in technology.

MAJOR TECHNOLOGICAL INNOVATIONS SINCE APPLE'S IPHONE

2007	**2008**	**2009**	**2010**	**2011**	**2012**
iPhone, Kindle and Airbnb launch.	Tesla Roadster launches.	Turn-by-turn directions on phone; WhatsApp and Uber launch.	Videos on mobile phones are adopted; Pinterest, Instagram and iPad launch.	Snapchat launches.	Lyft launches.

This is not impossible. For decades, agencies such as the Defense Advanced Research Projects Agency, NASA and the Department of Energy's national laboratories have attracted strong technical leaders responsible for major advancements in science, space exploration and technology.

More recently, the U.S. Digital Service, 18F and the Presidential Innovation Fellows program have brought modern engineering, design and technical product management to the front lines of government work. Combined with the skills and experiences of other dedicated public servants who have worked in government for years, these efforts helped accelerate the government's ability to create positive impact for the American public and deliver on policies while ensuring agencies have the infrastructure to meet their missions.

There are hundreds of federal leadership positions that involve technology, require innovative approaches and are necessary for a well-functioning government. The Tech Talent Project and the Partnership for Public Service gathered recommendations through interviews with dozens of current and former federal leaders across the political spectrum to identify a subset of critical leadership positions across government and their responsibilities and skills.

This report identifies and describes a wide range of presidentially appointed and other senior-level positions that are critical to the government's ability to deliver strong policies and services, and to advance our country's ability to innovate. It outlines the technology-related competencies and skills needed by leaders and their teams, and surveys the technological landscape at five Cabinet-level departments, outlining their challenges, opportunities and key technology positions.

This report is designed to help a second-term administration or a new president's team better identify key technology-related leadership positions. We hope that this information will be of value to presidential transition teams, the White House Office of Presidential Personnel, Cabinet secretaries and human resources staff.

Together, they can build effective policies and digital delivery systems as well as technology-literate leadership teams at key federal organizations to help set policy and provide support government-wide. Ultimately, having modern technical expertise is as vital to leaders as having economic, legal and financial expertise if we are to create a well-functioning government and policies that work.

REVOLUTIONIZED PEOPLE'S RELATIONSHIP WITH TECHNOLOGY

2015
23andMe receives the first Food and Drug Administration authorization for direct-to-consumer genetics testing; SpaceX successfully lands the first orbital rocket booster.

2016
First Amazon package delivered by drone.

2018
Self-driving cars hit the road; Waymo launches a self-driving taxi service in Phoenix.

2019
Lab-grown meatless meat takes off with companies such as Impossible Burger.

INTRODUCTION

Most federal policies and programs, from Social Security and health care to our nation's defense, rely on digital services and information technology platforms that are outdated and run ineffective software rife with security vulnerabilities. A lack of technological understanding by senior leaders in agencies—from Cabinet secretaries and deputy secretaries to explicitly technical executives—prevents much of the more than $90 billion spent annually on technology by federal agencies from delivering results for the American people.[1] There are numerous examples:

- **The 2013 rollout of Healthcare.gov shows how technical expertise can drive or derail policy outcomes.** Healthcare.gov initially faltered in large part due to technical systems, processes and regulations that did not focus on delivering outcomes. Unfortunately, it is only one of many such examples. It is a canary in the coal mine for presidential candidates who expect to make sweeping policy changes and are not preparing to engage the technical, digital and innovation leadership with the matching expertise to make those policies happen.

- **Social Security, which in fiscal 2019 paid almost $1.1 trillion to more than 71 million Americans,[2] relies on antiquated and brittle systems, processes and regulations.** Protecting Social Security is often mentioned on the campaign trail. However, disability and retirement claims processing—the bread and butter of Social Security's mission—relies on 60 million lines of code written in a computer language that was created in 1959.[3]

- **The 2014–2015 security breach at the Office of Personnel Management impacted 22.1 million federal employee records.** Not only did this breach make our country less safe, the time and focus required to recover impacted the federal government's ability to deliver on other priorities.

Technology and innovation go well beyond just having better federal IT systems. Rapidly evolving technologies are now deeply integrated in our businesses, homes, schools and cities as well as in our daily routines and relationships. In many ways, our lives are made easier by the new services we use to summon rides and meals to our doorsteps. At the same time, our activities are recorded and analyzed by the cameras and sensors installed in our streets, buildings and devices. Ever more sophisticated automation is expected to start replacing a labor force that is not fully prepared to transition. The American public needs leaders who meaningfully understand how these technologies work and their public policy implications.

The White House conducted a study in 2014 on how big data might transform the relationship between government, the American public and businesses, and how the public and private sectors could maximize big data's economic benefits. The study, for example, found that big-data techniques have the potential to enhance our ability to detect and prevent discriminatory practices. But if these technologies are not implemented with care, the study found, they can also perpetuate or mask harmful discrimination.[4]

---

1   Office of Management and Budget, "Analytical Perspectives: Budget of the U.S. Government Fiscal Year 2018," 2017. Retrieved from https://bit.ly/3aamc3U

2   Social Security Administration, "FY 2021 Budget Request: The Justification of Estimates for Appropriations Committees," 2020, 3. Retrieved from https://bit.ly/2VscZ21

3   Ibid.

4   The White House, "Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights," May 2016. Retrieved from https://bit.ly/2s0F8Ag

According to the 2018 President's Management Agenda, "modern IT must function as the backbone of how government serves the public in the digital age." For our government to be effective and move beyond the status quo, it must not only invest in modern digital service tools and systems, but also hire and empower skilled leaders who understand and know how to get the most from modern technology.

The federal government made sustained progress on the technology front during the Obama administration. Many of those efforts have been carried over and expanded by the Trump administration. For example, the U.S. Digital Service, begun in 2014, has continued to thrive, and improving information technology has been a pivotal part of the Trump administration's management agenda. The administration created the Technology Modernization Fund in 2017 to help agencies finance innovative technology projects. Additionally, President Trump issued an executive order in 2018 to guide U.S. efforts in artificial intelligence research, development and application, the first ever executive order on AI. And later the same year, the administration released the first national cybersecurity strategy since 2003 to outline steps to protect information networks in federal government and beyond.

To support these efforts, the Partnership for Public Service and the Tech Talent Project identified critical technology-related leadership positions across government, which, if filled with highly capable individuals, can further advance the federal government's technical infrastructure. The report identifies 10 critical competencies that technology leadership teams must have for success. While not every executive needs to have all 10 skills, leaders must ensure that team members have a wide range of technical expertise. The report also profiles five Cabinet departments to highlight the array of technology challenges and opportunities that leadership teams face as they work to serve the American public.

The pages that follow are based on interviews from December 2018 to February 2020 with more than 100 current and former federal employees across the political spectrum, including agency leaders, deputy secretaries and administrators, technology executives and subject matter experts. Agency reports and external assessments were reviewed along with a range of ideas on government technology to find prevailing patterns, common problems, hidden assumptions, dormant but still valid suggestions and overlooked assets. Finally, the systems used by agencies and the latest technology coming out of universities and corporations were reviewed.

Technology and Tech Talent Matter in Times of Crisis

The sudden and widespread outbreak of COVID-19 in 2020, a new infectious disease, has highlighted the importance of modern technology as well as the need for tech-savvy leaders and technologists in government. For example, governments at the federal, state and local level are relying on technology, such as easy-to-use websites and reliable mobile networks, to communicate relevant information to the public. Unfortunately, some state websites where people tried to sign up for unemployment benefits were not built to handle the extra web traffic, exacerbating already challenging problems.[5] Emerging technologies, such as artificial intelligence and telehealth, are helping governments track the spread of the disease, mine scientific information from medical articles and help treat patients with mild to moderate symptoms outside of hospital settings. And stable and secure information networks have been critical to ensuring federal employees from across the nation are able to continue serving the public while away from their offices and in the safety of their homes. To make sure technology systems can handle current and future tasks, strong technical leaders are more valuable than ever.

5   Sarah Chaney and Amara Omeokwe, "State Unemployment Sites See Surge in Jobless Claims," The Wall Street Journal, March 17, 2020. Retrieved from https://on.wsj.com/2Uge3Ud

GREAT POLICY DOES NOT BECOME REAL WITHOUT TOP MODERN TECHNOLOGY TEAMS

Our country needs leaders who understand the link between technology and organizational effectiveness, and who can launch delivery-driven policies and digital initiatives, prevent systemic failures, fix broken services, improve cybersecurity and protect privacy rights. We also need government leaders who can leverage rapidly developing technology such as artificial intelligence, machine learning, data science and nanotechnology.

More importantly, good policy requires good technology. As Americans increasingly access services using technology, the promise of a policy goal will be realized only if the technology and services are designed and executed well. Failing to do so will prevent beneficiaries from receiving needed services, impede policy goals and ultimately undermine public confidence.

Until 2019, for example, the Department of the Air Force division overseeing the nation's nuclear forces used an IT system from the 1970s, repeatedly included on Government Accountability Office lists of IT systems in desperate need of modernization and even featured in a 2014 "60 Minutes" episode. In 2019, the Air Force modernized the nuclear command computer system, upgrading it from a system that used floppy disks to a 21st-century digital system.[6]

Members of Congress and federal officials from current and past administrations have recognized the need to transition from outdated technical systems to modern technology that embodies innovation, manages risk effectively and deliver services to the public on par with private companies.

---

6   Valerie Insinna, "The US nuclear forces' Dr. Strangelove-era messaging system finally got rid of its floppy disks," C4ISRNET, Oct. 17, 2019. Retrieved from https://bit.ly/34JxxEN

"Modernizing government services includes delivering user experiences in the public sector at least as good as citizens enjoy in the private sector," said Chris Liddell, assistant to the president and deputy chief of staff for policy coordination at the White House.

Congress has recognized that the government needs skilled technical leaders with authority to manage this technology transition, as evidenced by passage of several laws, such as the Federal Information Technology Acquisition Reform Act in 2014. Among its many provisions, this law gives agency chief information officers a "significant role" in IT planning, budgeting, management and oversight decisions. Process and authorities are needed, but they cannot replace the value of experience and modern technical expertise.

EIGHT CRITICAL POSITIONS FOR AGENCY LEADERSHIP TEAMS

There are dozens of federal leadership positions that, if held by individuals with the right knowledge and skills, can play an outsized role in bringing modern technology to government. Eight of these positions play important technology-related roles in the federal departments and agencies.

The first four positions below have responsibilities beyond their agency's technology systems, and require an understanding of modern technology and the ability to hire, retain and effectively use technologists for policy, digital service and innovation.

Deputy secretaries or their agency equivalents

By law, departmental deputy secretaries or their agency equivalents are chief operating officers with responsibility for managing performance and ensuring resources and capacity are focused on accomplishing administration priorities.[7]

At a time when major policies and programs require large investments in technology, deputy secretaries should understand the importance and role of modern technology. Deputy secretaries who work closely with technologists to achieve their agencies' missions are more likely to be effective. Those with a deep understanding of technical priorities and tradeoffs are particularly critical at agencies that account for significant portions of government-wide IT spending, such as the departments of Defense, Veterans Affairs, Homeland Security and Health and Human Services.[8]

Deputy secretaries also have to be willing to invest time and personal capital to support and advocate for innovation and technology leadership in their organizations. Looking to the future, technology's primacy at many agencies might even call for rethinking the traditional candidate profile of a deputy secretary, particularly when an agency's priorities rely heavily on technology.

General counsels

The general counsel is the chief legal officer of a department or agency, providing legal services to the secretary and all operating units. Departmental general counsels oversee hundreds of attorneys who provide legal guidance to agency employees, and are often called on to navigate and resolve inevitable tensions when new technologies encounter legacy laws and regulations.

General counsels who understand modern technology and product and service delivery can be game-changers for federal agencies. A general counsel must be able to partner with technology leaders on infrastructure modernization, service delivery and new technology development. They should have a track record of working with operational and product leaders to deliver a product or service that is both legal and works for those using the technology. Strong candidates should have deep knowledge of relevant federal rules and regulations, and the legal and policy issues associated with technology, hiring, procurement and data. And they should be able to understand the value of speedy, strategic decision-making. General counsels can provide creativity in hiring, procurement and budgeting while complying with existing statutory authorities and therefore enable better adoption and use of technology.

Conversely, a general counsel candidate or team with a large gap or blind spot with regard to technology may not adequately and comprehensively assess legal and policy risks. Since there are few opportunities for general counsels or their teams in government to gain experience on strong technology product teams, administrations should consider candidates with this experience outside of government and invest in building this experience for current staff.

Chief human capital officers

Chief human capital officers are responsible for managing and leading talent recruitment and development efforts within an agency, and are essential to building strong technical teams.

As the chief talent officer for an agency, CHCOs need to understand key technology-related skills and competencies, and how to acquire, retain, train, develop and

7   "Government Performance and Results Act Modernization Act of 2010," Pub.L. 111–352

8   The White House, "Analytical Perspectives, Budget of the United States Government, Fiscal Year 2021," Feb. 2020, 220. Retrieved from https://bit.ly/2wDXHg9

engage technical talent. Specifically, they could improve approaches to hiring within existing laws and regulations. Ultimately, CHCOs need to focus on hiring highly qualified technologists into key capacity-building roles more than simply hiring additional technologists.

The Department of Health and Human Services and the National Park Service have piloted programs where they engaged subject matter experts early in the hiring process to partner with HR to assess applicants' competencies before they were considered qualified. These types of pilot programs exemplify the importance of CHCOs, HR and subject matter experts working in partnership to attract and assess top talent for the government.

Key program administrators

Leaders in charge of major government programs, such as the administrator for the Centers for Medicare and Medicaid Services, can be much more effective if they understand the technical opportunities and constraints of their current technology platforms and of potential advanced systems.

Because technology has become essential to deliver services and enact policy, program administrators who are tech savvy can be markedly more effective. For example, Medicare in fiscal 2019 processed transactions representing approximately 3.0% of the U.S. gross domestic product,[9] but it relies on a technological platform that is decades old. Moving from a legacy platform to a modern system is complex and fraught with potential problems, as is keeping the status quo. In such cases, those in charge of major programs must have enough technical knowledge to make informed tradeoffs and to hire individuals who are deeply steeped in current technology and processes.

Chief privacy officers

Chief privacy officers or senior agency officials for privacy are becoming increasingly important to agency leadership as government analyzes and collects growing amounts of data. These individuals generally serve as deputy assistant secretaries or an equivalent level. They should have a central role at their agency to oversee relevant operations and have regular access to agency leaders, including the agency head, according to an Office of Management and Budget memo on agency privacy officials.[10]

A privacy official has three principal responsibilities: ensuring privacy is considered in developing relevant legislative, regulatory and other policy proposals; ensuring the agency complies with privacy laws and rules; and ensuring the agency appropriately manages risks relating to the privacy and confidentiality of data and information, according to the same OMB memo.[11]

These individuals should ensure responsible and lawful use of agency data, and should work closely and at the earliest stages with those developing information systems or programs handling personal data. The privacy official's role should include designing privacy protections, including information security, at the inception of any project or product. Privacy officials focused on using significant data assets to further the agency mission within the law and with privacy concerns in mind are likely to have a valuable impact.

---

9   The White House, "Budget of the United States Government, Fiscal Year 2021," Feb. 2020, 113. Retrieved from https://bit.ly/2ukosFu

10 Office of Management and Budget, "Role and Designation of Senior Agency Officials for Privacy," M-16-24, Sept. 15, 2016. Retrieved from https://bit.ly/35SC1Jq

11 Ibid.

The individuals holding the following three positions across government are directly responsible for federal IT and should be highly trained and experienced technologists.

Chief information officers

The Federal Information Technology Acquisition Reform Act requires chief information officers to review the entire portfolio of technical investments in their agencies, look for ways to improve them and have a significant role in "the decision processes for all annual and multi-year planning, programming, budgeting, and execution decisions, related reporting requirements, and reports related to information technology and management, governance and oversight processes related to information technology."[12] FITARA also requires the CIO to report to or work directly with the agency head or their deputy.[13] But according to the Government Accountability Office, "executive-level governance and oversight across the government has often been ineffective, specifically from chief information officers."[14]

CIOs should be modern technical leaders capable of making significant decisions to radically improve the protection and use of information for digital service delivery. The decisions a CIO might make include moving from legacy systems to cloud computing; building teams that are skilled in technology, information security and cybersecurity; or retraining employees. Effective CIOs should engage with strategy and policy, and should be engaged by a leadership team as peers.

Chief data officers

Clean, relevant and useful data in secure technical environments requires the focus and expertise of a chief data officer. Signed into law in January 2019, the Foundations for Evidence-Based Policymaking Act mandates that agencies appoint a "trained, experienced and nonpolitical Chief Data Officer."

Effective CDOs are core members of the agency leadership team and are responsible for several functions. These include managing information through the data life cycle, from collection to analysis to deletion; coordinating data-related efforts across the agency; managing the agency's data assets; and contributing data to help achieve the agency's mission. Other functions involve ensuring the agency uses data in its day-to-day work; working with stakeholders to improve the agency's use of data; and working with the agency chief information officer to ensure proper data access.[15] At their best, CDOs have a portfolio that they drive and are responsible for, including weighing in on prioritized policy issues.

Chief technology officers

Chief technology officers can be highly effective when they serve as senior technology policy advisers within agencies. While chief information officers manage the internal technology infrastructure that keeps an agency running, ideally, federal CTOs focus on developing technologies, services and products that serve the external customer—the American public.

---

12 "Federal Information Technology Acquisition Reform Act," Pub.L. 113–291

13 Office of Management and Budget, "Management and Oversight of Federal Information Technology," M-15-14, June 2015. Retrieved from https://bit.ly/398stfh

14 Government Accountability Office, "Information Technology: Implementation of IT Reform Law and Related Initiatives Can Help Improve Acquisitions," GAO-17-494T, March 28, 2017, 4. Retrieved from https://bit.ly/37Qn7nE

15 "Foundations of Evidence-Based Policymaking Act of 2018," Pub.L. 115–435

The most effective CTOs should be key members of the agency leadership team and work directly with the secretary or deputy secretary. They also should partner with the agency chief information officer, have access to the secretary or deputy secretary, work with peers across government, and be highly skilled at understanding how agencies can fulfill their missions through technology. The clearer CTOs are on the power and constraints of technology, the better they will understand how technology can be used as a lever to advance public policy.

Other critical roles

There are many other political and nonpolitical roles within agencies that require individuals with deep technical expertise. A clear example is the senior agency information security officer, often called the chief information security officer. CISOs oversee agency cybersecurity, including training others in information security and ensuring that the agency has an effective information security program, according to the Federal Information Security Management Act of 2014. As leaders in charge of cybersecurity, each CISO should have modern technical expertise and experience.

Another critical role is the inspector general. Agency inspector general offices audit agency decisions and thus have a role in identifying technical challenges at their agencies. IGs with modern technical expertise could hold agencies to account on technology matters. Additionally, chief evaluation officers—created through the Foundations for Evidence-Based Policymaking Act, the same legislation that created the chief data officer role—can influence and guide the use of technology.

Some agencies have recognized the value of having a senior adviser for innovation, although the name and responsibilities will vary from agency to agency. These advisers can play a variety of roles. First, they can create a culture of innovation and experimentation within the agency. For example, the Department of Health and Human Services has encouraged civil servants to propose new approaches to solving a given problem, such as improving the logistics for transporting organs for transplants. HHS employees with the most promising ideas are given time, funding and training in innovation methodologies like lean startup and human-centered design. Second, they champion new approaches to problem-solving, such as open innovation, incentive prizes, public–private partnerships and procurement mechanisms that allow agencies to interact with startups and commercial firms.

Ultimately, new roles will have to be created in agencies that can identify emerging trends in science and technology that have strategic implications for a given agency, and identify concrete steps that agencies can take to harness and promote science and technology that is relevant to their mission. However, building the core group of the eight positions above should be a priority.

KEY
CROSS-AGENCY POSITIONS
REQUIRE TECHNOLOGY EXPERTISE TO DRIVE PROGRESS

Many issues, from national security to data privacy, are so complex that no single agency can solve them alone. To become more effective, agencies must increasingly work together and with center-of-government organizations, such as the White House Office of Presidential Personnel, Office of American Innovation, Office of Management and Budget, Office of Science and Technology Policy, Office of Personnel Management and General Services Administration.

Center-of-government organizations have the ability to drive policy and create standards across government. Ultimately, they have the power to help facilitate effective and efficient hiring, improve budgeting and acquisition processes, and equip agency leaders to create relevant policy, improve operations, build teams and purchase modern technology. Therefore, it is imperative that leaders at the center-of-government understand the opportunities and limitations of modern technology and how to use technology to help enable better government. Conversely, these leaders could inadvertently block improvements at agencies if they do not understand the opportunities technology affords.

As a result, the alphabetically ordered cross-agency positions below, most of which sit in center-of-government organizations, are important parts of the technology leadership in government and should be filled with highly trained and experienced technologists.

Executive Office of the President

Administrator, Office of Information and Regulatory Affairs

The administrator of the Office of Information and Regulatory Affairs, which is part of the Office of Management and Budget, oversees a key federal organization that collects information from customers, applicants and beneficiaries, including via websites and digital services. The 1980 Paperwork Reduction Act placed OIRA in charge of government-wide policies regarding the collection of information and minimizing the burden on people interacting with government. At the time, it principally meant streamlining tax and other paper forms and surveys. It also gave OIRA a powerful role managing information, privacy and statistical policies—even more crucial in today's digital age. OIRA approves new information collection requests from agencies, which includes reviewing every new form.

The OIRA administrator should work with the federal chief information officer, digital service offices such as U.S. Digital Service and customer-focused agencies such as the Department of Veterans Affairs to modernize government's information collection rules and processes—including those in the Paperwork Reduction Act—to ensure agencies can deliver smooth and satisfying digital experiences for the public.

Administrator, U.S. Digital Service

The U.S. Digital Service administrator is responsible for building and deploying a rotating team of 150 to 200 digital experts to address citizen-facing challenges at federal agencies across government. The administrator's role includes developing USDS's ability to attract, select and hire short-term technical talent from around the country, and bring that talent to project teams in USDS and at other agencies. The USDS also has helped further the CTO's mission to expand the number of technical experts advising, discussing, debating and aiding policymaking.

The administrator should have deep experience building and leading highly effective modern technical teams. In the past, the administrator has been charged with solving high-visibility, high-leverage crises as well as working with the White House and agencies to prevent such crises in the first place.

Deputy director for management, Office of Management and Budget

The OMB deputy director for management has many roles. This individual serves as the federal government's chief performance officer and develops and executes the administration's management agenda, including its information technology, financial management, acquisition, organizational performance and human capital policies.

In overseeing OMB's management arm, the deputy director should work effectively with several technical leaders and provide thoughtful guidance on key issues. For example, the deputy director oversees the Office of the Federal Chief Information Officer and chairs the Chief Information Officers Council, along with other government management councils. As the government's chief performance officer, the deputy director for management also helps set and measure agency performance goals, many of which are technical in nature, according to a Partnership analysis.[16]

Deputy national security adviser

While the national security adviser does not need to have deep knowledge about technology, it is important for the National Security Council to have a senior leader at the

---

16 Partnership for Public Service, "Federal Position Descriptions," 2016. Available at https://bit.ly/2lpxX1I

table who understands how modern technology intertwines with national security. Every National Security Council is organized differently, usually with several deputies overseeing different portfolios. At least one of these deputy national security advisers should have an understanding of modern technology and the ability to effectively oversee these issues.

During the past decade, America has faced many national security threats that were technical in nature, including issues around information encryption, cyberwarfare and foreign hacks of technical platforms. Addressing these threats requires a deep understanding of both national security and technology. Further, technology and digital services play a significant role in many other national security priorities, such as countering violent extremism, traveler vetting and aviation security.

With so much at stake, having someone with technical expertise at the national security table with the capacity to engage the appropriate experts when it comes to decision-making is vital. There is currently no such specific role.

Director, Office of American Innovation

Created by presidential memorandum in March 2017, the White House Office of American Innovation's mission is to bring together innovative public- and private-sector ideas to solve pervasive problems in government management, improve Americans' quality of life and create jobs. The director works with the Office of Science and Technology Policy to carry out its initiatives, according to the order creating the innovation office.[17]

The office works closely with USDS and other digital services throughout government to understand how to solve management problems with modern technological and design approaches.

Director, Office of Science and Technology Policy

The director of the Office of Science and Technology Policy, also known as the president's science adviser, has two main responsibilities: science for policy and policy for science. Science for policy means ensuring that decisions made by the president are informed by the best available scientific and technical information. For example, before agreeing to pursue and finalize an arms control agreement with a foreign government, the president should know whether the United States has the technical capacity to verify compliance with that agreement. Policy for science refers to steps that the government can take to foster America's science and technology enterprise.

For example, the OSTP director works closely with the director of OMB on the level of investment that is proposed by the president's budget, and the identification of research and development topics that agencies should prioritize in their budget submissions. OSTP is home to the U.S. chief technology officer.

Director, White House Office of Presidential Personnel

The presidential personnel director oversees the selection of political appointees and verifies that candidates are qualified. As a result, the PPO director can ensure that political appointees for technology-related positions have relevant technical expertise and experience. A number of technology leaders who were courted for government positions in current and previous administrations reported that, during the interview process, they were not asked any questions that tested their technical acumen.

The personnel director should improve the quality of technology appointments by using qualified subject matter experts in modern technology to source, recruit and review candidates, and help expedite the hiring process.

---

17   The White House, "Presidential Memorandum on The White House Office of American Innovation," Presidential Memorandum, March 27, 2017. Retrieved from https://bit.ly/2og4Crr

Federal chief information officer

The federal chief information officer, located in OMB, oversees the government's internal information technology and leads the Office of E-Government and Information Technology.

The federal CIO focuses on reviewing the government's use of technology and leverages OMB's budgetary, political and priority-setting strengths to define the best possible technology infrastructure and innovative solutions. The federal CIO largely uses influence and convening power to support agency CIOs throughout the government. The CIO leads the interagency Chief Information Officers Council—comprising the major federal departments and agencies' CIOs—on behalf of OMB's deputy director for management.

The federal CIO should help set high expectations for government CIOs to increase the ability of their agencies to serve users and effectively accomplish their organizational mission, as well as deeply understand the current state of CIO effectiveness. They can then focus on providing the support, policies and resources to bridge that gap.

U.S. chief data scientist

After being created during the Obama administration, the chief data scientist was located within the office of the U.S. CTO with the mission to responsibly unleash the power of data to benefit all Americans. The first chief data scientist was the initial convener of the Data Cabinet, consisting of chief data officers from all federal agencies both in unclassified and classified settings.

The chief data scientist should advocate for sourcing, processing and leveraging data in a timely fashion to enable transparency, provide security and foster innovation to maximize the return on investment in data. The chief data scientist should have the ability to weigh in on government-wide policy priorities.

U.S. chief technology officer

The U.S. chief technology officer, housed within the Office of Science and Technology Policy, advises the president on using technology, data and innovation to create effective public policy and build the capacity of government. The role was created in 2009 to help modernize a federal government that has relied heavily on aging technology.

The CTO should set the technology policy agenda and identify and support the most significant opportunities across government. For example, in the past, the CTO's office helped strengthen the ability of the USDS to serve as a hub of technology experts to support agencies.

General Services Administration

Administrator, General Services Administration

The administrator of general services has executive authority over a variety of technology-related offices and staff. These include the Technology Transformation Services, which houses government-wide online technical platforms, such as Login.gov and Cloud.gov; the Federal Acquisition Service; 18F; Centers of Excellence for IT modernization; and the Presidential Innovation Fellows program. The administrator also controls the Acquisition Services Fund, a key source of funding for integrated technology services and other procurement operations.

The administrator of GSA should promote modern, user-focused practices that improve the public's experience with government, develop shared services and platforms

that can be used across government, and set procurement policies and standards that require vendors to effectively collaborate with digital service teams.

Commissioner, Federal Acquisition Service

The Federal Acquisition Service, part of GSA, buys goods and services on behalf of government, making it a resource for agencies seeking to efficiently purchase computers, IT hardware, technical consulting services and software to accomplish the mission. The commissioner oversees the annual delivery of more than $50 billion in products, services and solutions.[18] FAS also provides guidance to the thousands of contracting and procurement professionals throughout the federal government.

The commissioner should work to ensure that procurement policies require technology vendors to demonstrate how they use modern, user-focused and agile practices in their approaches, and that internal GSA stakeholders are aligned in their approaches to agency partner work.

Deputy commissioner, Federal Acquisition Services, and director, Technology Transformation Services

The deputy commissioner oversees the Technology Transformation Services, the GSA's internal service organization that helps manage government's information technology portfolio and is responsible for improving the federal customer experience through modern technology. TTS helps agencies more effectively and efficiently build, buy and share technology. This unit houses 18F, the Presidential Innovation Fellows and Data.gov, three programs working to enhance data and innovation and to improve technology in agencies, according to the Partnership's analysis.

The assistant commissioner should advocate for effective approaches to building and buying digital services across government, and engage frequently with external agency partners and internal GSA stakeholders to ensure that TTS offices have the runway to expand their reach within regulatory frameworks.

Executive director, 18F

The executive director leads 18F, an internal digital services consultancy of about 120 people within GSA. The organization is staffed by nonpolitical, term-limited designers, software engineers, product managers, operations specialists and leaders versed in modern digital services development and procurement. Unlike USDS, 18F is a fee-for-service consultancy—agencies pay for services, which uniquely positions 18F to meet specific agency demands. 18F offers different services from USDS in that it rarely takes on rapid-cycle turnaround, validation or improvement work, and instead focuses on long-term, sustainable changes in government, according to the Partnership's analysis.

The executive director of 18F should ensure that there is a pipeline of projects that further the mission and a pipeline of talent that can effectively execute the work. This person will work closely with the FAS deputy commissioner, internal GSA stakeholders and external partners to advocate for effective digital services approaches.[19]

18 General Services Administration, "Commissioner, Federal Acquisition Service," Oct. 18, 2019. Retrieved from https://bit.ly/2qmdPzw

19 Partnership for Public Service, "Federal Position Descriptions," 2016. Available at https://bit.ly/2lpxX1I

Office of Personnel Management

Director, Office of Personnel Management

As government's workforce policy leader, the OPM director oversees federal policy on recruitment and hiring, training, performance management and human resources management. As a result, the director is in a unique position to build a strong and capable modern technical workforce and must be able to coordinate with and support best private-sector practices in recruiting and hiring strong technical talent.

The director should develop a portfolio of hiring modernization activities that enable the building of a strong, capable technical workforce. For example, a prior OPM director developed a Hiring Excellence Mythbusters campaign that debunked myths, including a mistaken belief that hiring managers are not allowed to actively recruit for qualified candidates and that subject matter experts are not allowed to help determine the candidate's subject matter expertise until after an HR specialist has reviewed and potentially cut candidates. The campaign also showed how experts may "work with the HR specialist during the minimum qualifications review, so long as the HR specialist has the final authority and responsibility for signing off on the minimum qualifications determination. This is especially helpful when the position is highly technical," according to OPM.[20]

---

20 Office of Personnel Management, "Mythbusters – Hiring," 12. Retrieved from https://bit.ly/2v6NGrz

CORE TECHNICAL COMPETENCIES
OF A 21ST CENTURY WORKFORCE

Government leaders must ensure that their agencies have the technical competencies needed to deliver on their missions. Agency technology leaders should have a team of employees who possess a range of technical skills and understand how technology can be deployed to meet policy goals. These experts should be part of the policymaking process, with the goal of continually monitoring outcomes and giving feedback as initiatives are deployed.

Ensuring agencies have these competencies organization-wide could result in more effective delivery of services, more efficient internal operations, improved technology reliability, greater security compliance and cost savings.

While some leaders holding top operational and technical jobs, such as chief information officers or chief technology officers, should have specific technical experience, not all leaders—nor everyone on their staff—must have expertise in all 10 areas. For example, not every leader needs to know how to program in JavaScript or Python, two commonly used programming languages. Rather, they need a thorough understanding of these core competencies and how best to build and deploy them to achieve agency missions. They need a deep appreciation of technology's role in creating effective policies, improving government services and performance, and communicating this information to agency leaders, Congress and employees.

THE COMPETENCIES

1. Tech-informed decision-making
2. Security
3. Data governance and use
4. Human-centered design
5. Product management
6. DevOps and site reliability engineering
7. Modern stack software development
8. Technology procurement
9. Institutional innovation and change management
10. Emerging technologies

TECH-INFORMED DECISION-MAKING

Bring technologists to the policy table. Infuse technology expertise into policy—and vice versa.

Tech-informed decision-making means that agency leaders understand the role technology plays in implementing policy, and they engage technologists to provide advice, guidance and feedback for policy decisions.

Major companies and organizations rely on technology to serve people and to continuously improve services and products. Effective leaders in these organizations prioritize understanding the opportunities, constraints and tradeoffs of the technologies they plan to rely on. They then build feedback loops that provide insights into the outcomes of the policies and opportunities for improving delivery.

Secretaries and deputy secretaries should have a deep appreciation and understanding of modern digital technology, given how central technology has become for agencies to meet their missions. In addition, chief information and technology officers should be part of strategic decisions so they can provide guidance and feedback on the convergence of policy and technology. One senior federal leader noted in an interview that it is concerning to be in a room when decisions are being made with deep impact on many lives and not have someone at the table who understands the technology that underpins those decisions.

What it means for government

When policies are designed without input from technology and digital leaders, it can result in significant unintended consequences and costs. For instance, U.S. Citizenship and Immigration Services invested more than $2 billion over a decade to place paper forms online.[21] A review of the effort showed that while it was meant to be part of a big push to overhaul immigration policies, the agency did not put in place the right technical decision-making processes and specifications. As a result, just three online forms were created after almost 10 years, and they were less efficient for both the public and agency staff than old paper forms (with eight online forms available as of early fiscal 2020[22]). In 2015, technologists became more deeply involved in the decision-making process. They dropped the previous approach, adopted modern cloud computing technology and revamped the system in less than a year to make the benefit request process more efficient.

In a best-case scenario, an agency head would choose the top three to five policies that need to be implemented and have the technical teams work with policy and operational leaders to help create the product, measurements and dashboards to manage success. Those metrics would be a regular, ongoing source for how the agency is doing, the same way that today's tech CEOs obsess over how their product is performing in the market.

As federal government agencies wrestle with issues such as encryption and algorithms in all programs, decision-makers need to actively bring technologists to the table. Failure to do so could lead to missed opportunities, missteps that derail governmental initiatives and painful problems for everyday Americans.

---

21 Jerry Markon, "A decade into a project to digitize U.S. immigration forms, just 1 is online," The Washington Post, Nov. 8, 2015. Retrieved from https://wapo.st/2PHcbU1

22 U.S. Citizenship and Immigration Services, "USCIS Makes Another Form Available for Online Filing," Oct. 30, 2019. Retrieved from https://bit.ly/2qtJUWQ

SECURITY

Improve all types of security—from information to cyber—by building both technical capabilities and security-minded organizational cultures.

Security is ultimately everyone's job, though different types of security require different expertise. Information security, for example, is the "state of being protected against the unauthorized use of information, especially electronic data, or measures taken to achieve this."[23] Cybersecurity is a subset of information security, specifically the "protection from criminal or unauthorized use of electronic data."[24]

In today's world, the interdependence of actors in the digital ecosystem, the entrance of 8.4 billion devices connected to the internet, and understaffed, underbudgeted IT departments in all sectors have created an environment that leaves organizations vulnerable. It should be no surprise that a recent survey from The Conference Board found that cybersecurity threats ranked as the number one business concern for CEOs.[25]

What it means for government

The federal government is entrusted with some of the most sensitive information in America, including personal details about individuals contained in medical records, tax returns, social security numbers and student loans. Protecting this information from domestic and foreign threats is a paramount challenge for federal agencies.

In interviews with the Trump administration and former high-ranking federal officials, cybersecurity was one of the topics mentioned most frequently and with the greatest sense of urgency. For government, attacks on data sources and infrastructure increase by the day as foreign and domestic agents try to undermine the stability and strength of the country. Protocols to counteract these threats are outdated and too complicated, focused on completing existing paperwork and checking boxes rather than creating accurate threat assessments, and agencies are slow to adopt best practices.

In 2017, more than 35,277 cybersecurity incidents were reported to the Department of Homeland Security's U.S. Computer Emergency Readiness Team. In 2014 and 2015, two targeted hacks and a cybersecurity lapse led to an Office of Personnel Management breach of the personnel records of 22.1 million government employees, one of the largest government data thefts in American history. While DHS is responsible for leading federal cybersecurity efforts, much of the work is still left to the agencies, and a majority remain vulnerable.[26] Indeed, the Government Accountability Office issues multiple reports each year detailing security concerns with agencies and various technology systems.

For years, the Pentagon struggled with unknown vulnerabilities in their computer systems. In 2016, with support from the Defense Digital Service, DOD launched its first Hack the Pentagon bug bounty program—programs that provide compensation for identifying security vulnerabilities—that identified nearly 140 vulnerabilities for $150,000. Achieving the same goal—identifying vulnerabilities—might have cost millions more but been far less effective using more traditional efforts. By 2018, DOD increased its investment in the Hack the Pentagon program to $34 million.

Organizing programs that actively encourage people to find and help fix security vulnerabilities, invest in more secure technology products and services, and enable technology security staff to stay up-to-date on the latest threats and protections will help improve the overall security capability of an agency.

"We have a pressing need to recast what cybersecurity means. Our adversaries are thinking about multidimensional vectors of attack and we are still hunkered down in our antiquated ways, leaving whole spaces vulnerable."

—Laura Rosenberger, former senior official, National Security Council and Department of State

23 Dictionary.com and Oxford University Press, "Information security," Lexico. Retrieved from https://bit.ly/2nxFLiR

24 Dictionary.com and Oxford University Press, "Cybersecurity," Lexico. Retrieved from https://bit.ly/2ll48PX

25 "U.S. CEOs rank cybersecurity as their #1 external concern for 2019," The Conference Board. Retrieved from https://bit.ly/36TJ19G

26 House Committee on Oversight and Reform, "FITARA Scorecard June 2019," 2019. Retrieved from https://bit.ly/33hryX0

DATA GOVERNANCE AND USE

Manage the complexities of data—the lifeblood of service delivery and many emerging technologies.

Data is essential to modern information technology solutions. Effective data governance—the responsible management and strategic use of data—is an essential part of every organization, including federal agencies. Data governance in government should include agreement among stakeholders and agencies on how to manage data and use it to modernize and innovate government services. Data governance also should allow agencies to build a data ecosystem that ensures data privacy and security. With this effective governance as a cornerstone, agencies also would default to making data open to the public, and use data to continuously learn and improve how to deliver digital services, programs and policies. In addition, agencies need to find ways to share data across government.

What it means for government

The federal government constantly collects data from the public on everything from health care to finances to demographics. Americans expect that governmental agencies will use this data to provide the kinds of effective and timely services they typically receive from the private sector in the digital age.

At the same time, the public has an expectation that government will value its privacy and use data in an unbiased way. As a first step, the Trump administration in June 2019 released the Federal Data Strategy and, in December 2019, a one-year plan to implement it.

Proper data governance and use requires extensive work, including crafting clear definitions for collecting, using and storing data; the minimization and security methods necessary to assure appropriate access and protection of the data; the privacy rights of individuals, as weighed against the purpose for which it was collected; and the fairness in the quality, collection and use of the data. The effort also must consider the legal obligations to provide access, delete, disclose or prevent disclosure, and provide oversight and auditing of data practices. Leaders who understand technology and data need to be at the table and part of agency policy discussions.

Individual agencies must have the ability to execute against these priorities in an effective way. They already have internal operations specialists and attorneys who can assist with the execution. However, hiring digital or technical experts, such as engineers who specialize in data, has not been easy. Agencies and the Executive Office of the President often need to rely on experts who have come in through U.S. Digital Service or 18F.

To build strong teams that can store, manage and secure data, agencies will need to develop in-house leadership. That starts with each agency having a clear sense of what data governance and use currently looks like and can look like and showing examples of how data can be valuable to programs and agency policy decisions. It continues with understanding the skills of current staff and then investing in the right people, systems and infrastructure. With that in place, an agency can develop robust data governance and use strategies, run internal analyses and share insights with leaders and program staff.

> **"In a perfect world, executing against [a data governance] framework would be done by a technical expert, but it almost always requires close collaboration between a technical expert, an operations specialist and an attorney."**
>
> *—Nicole Wong, former deputy U.S. chief technology officer*

HUMAN-CENTERED DESIGN

Create processes and technology that focus on the needs, desires and expectations of end users—citizens, beneficiaries, employees and military personnel.

Human-centered design starts with asking a few basic questions: Who is receiving the experience you are creating, what do they need, and how are current solutions working? At their best, software developers and technical teams design systems with end users and understand their needs before writing the first line of code. They use this understanding to set priorities and guide decisions about features, functions, process steps and interactions throughout the development cycle. Teams approach their work iteratively, launching and improving technical systems based on constant feedback from users. As a result, applications and programs are easy and even enjoyable for people to use. Systems provide timely and correct information on demand, so people are less confused. Services get better over time as teams learn more about how people use them.

What it means for government

Users of government services bear the cost of administering government programs if services are not designed to minimize burdens of time, money and complexity. This can mean that veterans must try 12 times to sign up for health care, repeating the same steps on the same website over and over again before ultimately being told that the Department of Veterans Affairs can't help them.

"At one point, if a veteran wanted to change her address, she had to call 15 to 20 places to have it changed, but changing it in one place didn't change it in the other databases," said Marina Nitze, a former chief technology officer at the VA. "The Holy Grail was to have the veterans' personal data [personal information, service data, medical records] at a central point, where a change would fill out all the databases at once. That was implemented in early 2019, and now all records are filled in and changed automatically."

Fortunately, human-centered design has gained traction in government during the past 10 years. Agencies such as the General Services Administration and the VA have dedicated offices focused on understanding how people use their programs and services. While they go by names such as innovation centers, customer offices or design labs, they tend to specialize in applying human-centered design techniques to improve program delivery and digital services. The VA Innovation Center, for example, has undertaken large-scale efforts to study and document the lives of veterans, and use those observations and insights to redesign digital services and technical systems. The U.S. Citizenship and Immigration Services developed an "immigration front door" that provides users with personalized applications, information about immigration benefits, tools for applicants and lawyers, and a dashboard for the immigration service officers who must track it all.

Yet many other agencies are not using human-centered design. They create online applications that involve many complicated steps and confusing language, and sometimes do not work. Websites may not work across every mobile platform or in every browser—and sometimes only run on one out-of-date browser. Data upload sites provide little feedback. And many programs still require downloading and printing out forms, filling them out in pen, taking a day off work to go stand in line at a federal office and then having to make a phone call to check the status every 30 days.

As a result, farmers might not get financial assistance to improve their operations because they cannot understand the requirements. Veterans might have to wait years to get access to the doctors and medications they deserve and desperately need. People become frustrated and believe that government is out of touch with what everyday people require.

"The fundamental principles of design—placing users at the center and building empathy to understand their needs—are proving to be uniquely suited for identifying and tackling some of the most complex problems in government and building trust and confidence in our institutions," said Kyla Fullenwider, Census Bureau's first chief innovation officer.

Setting up a dedicated office or center in an agency has proven an effective way to get human-centered design techniques more widely adopted, particularly in the design of technology products and services. By using the techniques and tools of human-centered design, agencies can create digital systems that serve people more efficiently, effectively and easily.

> **"The customer experience officer exists to represent the interests of the customer in a way that goes across the organizational divide and across federal agencies. When the public interacts with the government, they aren't interacting one agency at a time, they are engaging with government as a whole."**
>
> *— Anahita Reilly, former chief customer officer, General Services Administration*

PRODUCT MANAGEMENT

Deliver a robust product, service or system on schedule with the right functions and features.

Top technical teams rely on product management to help scope, plan, deliver and improve digital services and technology systems. Product managers knit together technical, customer-facing and operational efforts to focus on improving outcomes. The work is continuous because the manager is always assessing how well the product being delivered addresses user needs and recommending improvements. Product management is different from project management, which is far more common in government, and focuses on a predefined set of deliverables and tasks rather than outcomes.

What it means for government

Modern product management in government is not a standard practice. Complex products and services can have dozens of contractors on the job with no one leader who has the accountability and resources to ensure the goals are met and the product is delivered on time and in a way that meets user needs. The majority of federal technical teams lack properly skilled and trained product managers. "Very few projects in government even designate a product manager," according to one former federal executive. At the federal level, few individuals have a global view of the system and fewer still have the authority to make decisions about what teams should and should not be working on.

Without good product management, teams end up wasting time arguing about what they should do and less time actually getting the work done. Development times and costs balloon, and products become bloated and unstable. Vendors rack up expenses for change orders waiting for program and technical staff to resolve their differences. Systems go online but are plagued with bugs and poor functionality, and budgets get tightened to pay for rework.

At the very least, government agencies need to hire more product managers to work on technology products and services, and make them mandatory, equally empowered members of technical teams. Product managers in government should focus on three key areas: solving the right problem, creating a shared vision and prioritizing the right work.

Product managers also should help surface and resolve conflicts, and keep teams focused by gathering and sharing user feedback and performance data. Resolving conflicts is critical in government, where there are requirements from Congress, the White House, agency heads, users and many others. To be successful, a product manager must meet the requirements while balancing the needs of actual users and the technical complexity and cost to taxpayers to implement features and solutions. With a shared sense of priorities, team members can create new applications, products or services faster and more efficiently.[27]

Seeing the need to improve agencies' product management capabilities, alumni from USDS have worked closely with Georgetown University to develop a new technical product management training and certification program that launched in 2019. That joins other early efforts by agencies such as OPM and the Federal Reserve to build stronger technical product management competencies.[28, 29]

27 Natalie Kates and Kelly Taylor, "Where Policy Meets Product," Nov. 30, 2017, U.S. Digital Service. Retrieved from https://bit.ly/39NqH3A

28 Karen Trebon, "Government Product Managers Play a Key Role in UX," Nov. 27, 2015, General Services Administration. Retrieved from https://bit.ly/2FAXonu

29 Dan Zirkelbach, "Product Management at the Federal Reserve Bank," April 3, 2019, Product School. Retrieved from https://bit.ly/30babGU

DEVOPS AND SITE RELIABILITY ENGINEERING

Break down organizational barriers among technical disciplines to deliver better software faster.

DevOps—a combination of the words "development" and "operations"—is focused on reducing friction between software development and operations teams.[30] Site reliability engineering is focused on explicitly reaching quantifiable measures of success in software development and operations by moving beyond organizational silos. The SRE discipline was developed at Google after internal teams found it hard to productively discuss software development without a clear, mutual understanding of website uptime and availability, two key measures of website reliability.

What it means for government

Technical systems tend to fail under high loads or peak demand, such as surges in use. Site reliability engineers plan for these failures and fix them when they happen. The Social Security system that prints checks every month is under maximum load and fails in various ways every month—and may eventually fail in spectacular fashion, leaving thousands of seniors without their checks. SREs identify the weaknesses and prepare for those failures so they can get the system back up as quickly as possible.

The silos and challenges that led to the creation of SRE and DevOps exist throughout government. Most federal agencies, each with multiple programs running hundreds of websites and apps, are accessed by thousands of people at the same time, which means the federal digital infrastructure needs the capacity to handle massive demand at any time. Not surprisingly, SREs were indispensable players in the revitalization of the Healthcare.gov website in 2013 because they focused explicitly on measuring the system's availability or uptime targets. They were able to improve the website substantially, creating a system that responds more quickly and costs less.[31] SREs also work to quantify acceptable risk to make failure something that is manageable, normalized and planned for rather than something that surprises everyone.

A few agencies have piloted DevOps and SRE teams, including the IRS, Air Force and General Services Administration. According to the IRS, their use of DevOps significantly helped reduce testing and deployment times of releases and upgrades of technology systems from months to minutes, and automated testing time from minutes to milliseconds.[32] GSA used an SRE approach to develop, deploy and improve Login.gov, a single sign-on solution for government websites. Despite pockets of progress, many agencies still lack proper DevOps and SRE functions.

Allocating budgets and opening up positions for hiring trained DevOps and SRE staff can go a long way to building competency. At the same time, because of the unique scale, reach and security needs of federal agencies, it would be valuable for experienced agencies to document and share the challenges and emerging best practices of federal government–specific DevOps and SRE to help other agencies build their individual competencies.

Without SRE and DevOps, changes start to look risky and operations teams force multiple redundant reviews before allowing new code to be put online. Problems often are not resolved fast enough because there are not proper feedback loops or action plans. Projects also can stall or go over budget and teams get frustrated by the lack of progress. Once sites and digital services are up, they are fragile and full of glitches. Teams often do not have quick, reliable data or analytics about why problems occur and cannot do proper preventative planning or react quickly enough.

> **"I often find myself going back to the site reliability engineer skill set. There are many times when I needed to trace a request through a technical stack, ask questions and understand what is happening, even if I cannot go deep enough myself to fix it, to go all the way down to the source code and logs. Having some people in leadership who can do that sets the tone for the whole organization and makes sure there is accountability."**
>
> *—Charles Worthington, chief technology officer, Department of Veterans Affairs*

30 Seth Vargo and Liz Fong-Jones, "SRE vs. DevOps: competing standards or close friends?" May 8, 2018, Google. Retrieved from https://bit.ly/3cTa9cG

31 Robinson Meyer, "The Secret Startup That Saved the Worst Website in America," July 9, 2015, The Atlantic. Retrieved from https://bit.ly/32EkTHb

32 "Pandya Highlights DevOps Benefits for IRS at ATARC Summit," MeriTalk, March 12, 2019. Retrieved from https://bit.ly/36y16uo

MODERN STACK SOFTWARE DEVELOPMENT

Use the right systems, tools and programming languages on the back end and front end.

A stack is the set of technologies, techniques and tools such as computer codes that developers use to develop websites and mobile applications. Developers use the technology stack in one of three areas: front-end development, which is building the parts of a website or application visible to users; back-end development, which includes the "under the hood" infrastructure or databases; or full-stack development, which is a hybrid of both.

What it means for government

Technology stacks change over time as innovation creates new programming languages. Information systems and software now considered to be legacy technology were once new and prevalent. For example, when electronic medical records were developed for the Department of Veterans Affairs using MUMPS, a programming language created in 1966, the language and application were cutting edge. When Medicare's payment platform was developed partly using COBOL, a programming language created in 1959, COBOL and the accompanying code were cutting edge. While these government digital services still run on 50-year-old MUMPS and COBOL, modern stacks have been created for which developers can be hired without massive onboarding periods, code can be created more quickly and with fewer bugs, and engineers have the ability to make changes to existing systems far more easily.

Many agency software systems were written decades ago in these old computer programming languages and formats. Re-creating those systems using a modern stack threatens to introduce bugs, compromise

data integrity, slow processes down rather than speed them up, and even jeopardize long-standing contracts and employees' jobs. Keeping those old systems may keep old security holes open and leave brittle systems in place. In many cases, even seemingly insignificant changes such as adding a value to a drop-down menu to align with new legislation could take months of coding and testing in these old systems, and each change risks being the cause of a system-wide failure. New systems change slowly, and old legacy systems remain because retiring them would cost too much time, people and money.

According to the Government Accountability Office, the "10 most critical federal legacy systems in need of modernization are becoming increasingly obsolete," including one at the Department of Health and Human Services that is 50 years old, for which the last hardware upgrade is unknown.[33] In addition to using outdated languages, "several of these legacy systems are also operating with unsupported hardware and software and known security vulnerabilities."[34]

A 2019 Defense Innovation Board study on software acquisition practices within the Department of Defense is illustrative and could have been written about almost any agency. As software became central to executing DOD's mission, multiple studies identified deficiencies in software acquisition, yet little has changed. To improve practices, the

innovation board's report recommended focusing on speed and cycle time—the time between starting and finishing a process, such as correcting a problem or adding a new function—as the key metrics of software, building software differently than hardware, and attracting and building digital talent.[35]

Leaders in agencies need to invest in people and infrastructure to build their competency in modern stack software development. They need to hire experienced engineers and train staff on newer programming languages and techniques. At the same time, identifying systems that are running on dated platforms and creating initiatives for upgrades will increase the demand for modern software engineering at agencies.

> **"The current approach to software development is broken and is a leading source of risk to DOD: It takes too long, is too expensive and exposes warfighters to unacceptable risk by delaying their access to tools they need to ensure mission success."**
>
> *—Defense Innovation Board "Software Acquisition and Practices" study[35]*

33 Government Accountability Office, "Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems," GAO-19-471, June 2019, 23. Retrieved from https://bit.ly/31y2Xgk

34 Ibid.

35 Defense Innovation Board, "Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage," May 3, 2019, viii. Retrieved from https://bit.ly/2WGWdKU

36 Ibid. i.

TECHNOLOGY PROCUREMENT

Apply the most effective and efficient approach to acquiring technological tools and talent.

Procurement is the means by which an organization buys services or goods, including information technology and digital services. Technology procurement in the federal government spans the gamut from buying new laptops and software licenses to cloud services and consultants. Beyond just clicking to add items to a cart on a website, complex procurement rules, procedures and policies govern everything from communication methods to pricing. These rules are designed to safeguard government buyers and vendors, as well as the public interest.

What it means for government

Procurement in government is complex, slow and unwieldy. It often takes too much time to scope requirements, identify the right vendors and find the right provider while keeping in compliance with the Federal Acquisition Regulations, the federal government's primary set of rules for agency purchasing.

The effectiveness of the federal government is undermined by the inability of agencies to efficiently contract or purchase reliable digital and technical solutions and services. This begins with a bias toward building or buying custom technology, even when off the shelf systems may work, and continues into how the government designs projects, creates requests for proposals, evaluates and selects vendors, negotiates terms, writes requirements and structures contracts.

Currently, most government procurement systems support software creation the same way the federal government supports battleship construction: incentivizing large investments over long time periods,

often with rigid requirements and written by people focused on policy, not technology. This is called "waterfall" development. For many software and more evolving technical products, investing small sums early on, getting feedback from users quickly and continuously iterating based on feedback—often called an "agile" approach—is much more effective.

Waterfall development in government software has often led to failure and budget and cost overruns. The Department of Agriculture's Modernize and Innovate the Delivery of Agricultural Systems program and OPM's Retirement Systems Modernization program are two of many examples where waterfall development resulted in hundreds of millions of dollars in overruns and little to show in the way of actual functioning products.[37] The Department of Homeland Security's Secure Border Initiative Network program was abandoned in January 2011 after the department obligated more than $1 billion and put in five years of work. And at the Department of Defense, software is the primary risk in 60% of defense system acquisitions.[38]

Yet there has been some innovation over the past several years, such as the Digital IT Acquisition Professional program, which identifies procurement specialists, trains them on how to buy software and is

developing a network of alumni.[39] The DHS Procurement Innovation Lab creates an environment where acquisition professionals have the leadership support to take managed risks and find innovative ways to improve procurement.[40] And the TechFAR, a guide for buying digital services, helps agencies navigate the federal acquisition process for software purchasing.[41] These innovations could and should be tried across government.

37 Government Accountability Office, "Information Technology Reform: Agencies Need to Improve Certification of Incremental Development," GAO-18-148, Nov. 2017. Retrieved from https://bit.ly/2Nee4p6

38 Defense Science Board, "Design and Acquisition of Software for Defense Systems," Feb. 14, 2018, 4–5. Retrieved from https://bit.ly/2TbyqRS

39 U.S. Digital Service, "The Newest Breed of Federal Acquisition Professional: The Digital Specialist," May 23, 2018, Medium. Retrieved from https://bit.ly/2HUOSRz

40 Partnership for Public Service and Slalom, "Risk and Reward: A Framework for Federal Innovation," Oct. 2019, 12–13. Available at https://bit.ly/38GMxVt

41 U.S. Digital Service, "TechFAR: Handbook for Procuring Digital Services Using Agile Processes," Aug. 2014. Retrieved from https://bit.ly/2v9NHek

INSTITUTIONAL INNOVATION AND CHANGE MANAGEMENT

Re-engineer business processes to create better user outcomes and meet agency missions.

Innovation in government is a new or improved process, program, product or service that delivers significant positive outcomes to further the public good, according to the Partnership's research.[42] It applies to technology and business practices and processes. Underlying business rules, requirements and metrics can make digital solutions succeed or fail, despite everyone's best training and intentions.

What it means for government

Government employees are often tethered to policies, requirements and checklists that prevent them from trying new processes or approaches to using technology. They are also hindered by "water cooler rules," practices that have been in existence for so long that everyone treats them as rules even though technically they are not. Asking experienced employees to do their work in an unfamiliar way might put them at risk of violating their job requirements as well as challenging their hard-earned seniority. Changing these practices to focus on outcomes, not only processes, could be one of the main differences between the successful launch of a key presidential initiative and its failure.

More often than not, quantitative and qualitative outcomes dependent on technology are set by groups that have never been involved in technology implementation. Dedicated employees with limited resources and serious constraints do what they can, but it is demoralizing when it is impossible to achieve a stated goal within current resource constraints.

Strong technical and innovation leadership could effectively manage this change and bridge these gaps, providing practical solutions to efficiently deliver services. These solutions include updating performance reviews and required paperwork to reflect changed needs, updating agency policy or even federal law when outdated language puts up barriers to modern solutions, and working with employees to understand and remove barriers. Leaders are most effective when they have the flexibility and resilience to find ways to bring new technology into existing regulatory frameworks and approval processes or to change them. One example of such leadership was the Innovators Network launched within the VA Healthcare System by a Presidential Innovation Fellow. This program rewards medical centers and employees for developing new ideas that effectively support veterans.

Further, agency employees often do not have the incentives or opportunities to see the entirety of a customer's online experience, and might spend time and money recreating common website elements such as buttons, forms and search bars that already exist for agencies to use.[43] Experienced technical leadership can look across departments or agencies to identify common themes and patterns of need, such as case management or electronic forms, and leverage the unique scale of government to deploy even greater, more cost-effective and more user-friendly solutions that span silos.

As one former senior agency leader, originally from the private sector, said, "I often come back to the need for organizations to operate like an integrated enterprise, whether that is within a department, across a department, or across the entire federal government. I learned the hard way that you have to have common IT platforms, or at least interoperable platforms, to accomplish that goal."

Seeing this need, in 2017, the General Services Administration created centers of excellence to accelerate IT modernization with a focus on artificial intelligence and cloud computing, among other technologies. And in 2018, the Army launched the Business Process Reengineering Center of Excellence to help make better technical and organizational decisions. Unlike the narrow cost-savings focus of many earlier efforts, these new centers focus much more on helping staff define problems, processes and accountabilities to make better decisions.[44]

It's a need that the VA also recently highlighted when it rolled out its Light Electronic Action Framework focused on improving internal systems. Several different internal staff teams have used a new technology platform to identify, scope and solve key business process and management issues that are standing in the way of delivering better services and information. Already in use in over 100 VA medical centers, the program is being adopted rapidly by VA staff.[45]

> **"At the VA, it was easy for any technologist to spot the potential for hundreds of millions of dollars in annual cost savings—not to mention a significant improvement in uptime performance—moving key applications into a cloud computing environment. But getting approval to use the cloud required technical leaders to work with the inspector general to train them on how they could conduct their investigations more easily using online tools."**
>
> *—Marina Nitze, former chief technology officer, Department of Veterans Affairs*

42 Partnership for Public Service and Slalom, "Risk and Reward: A Framework for Federal Innovation," Oct. 2019, 2. Available at https://bit.ly/38GMxVt

43 U.S. Digital Service, "Report to Congress – December 2016." Retrieved from https://bit.ly/2kaP2Ky

44 Emad Elias and Bob Etris, "How business process reengineering can support performance improvement," Aug. 30. 2018, FCW. Retrieved from https://bit.ly/35MzFvr

45 Chase Gunter, "VA employees tap open source to solve workflow problems," April 26, 2019, FCW. Retrieved from https://bit.ly/35Fv5ij

EMERGING TECHNOLOGIES

Create the next generation of breakthroughs and advancements.

Advances in technology and science in the past few decades have yielded new possibilities for how people interact with one another and the digital world. The internet, GPS technology and smartphones are all changes a previous generation could not imagine. The pace of innovation is accelerating further and, coupled with the creative mindset of researchers and engineers, is leading to a class of emerging and breakthrough technologies that have the potential to alter entrenched practices and disrupt industries.

Emerging technologies are enabled by a computer science principle that says computer processing power doubles every two years. These technologies include artificial intelligence and machine learning, synthetic biology, personalized medicine, virtual reality, genome editing, lab-grown animal proteins and quantum computing.

What it means for government

Talent is a significant factor in successfully building and deploying emerging technologies. Federal leaders will need to direct their teams to play the right roles as funders, regulators, catalysts and standard creators to encourage emerging technologies while keeping the public's best interests in mind. This will involve filling existing roles and may require creating new ones.

For example, AI applications in government require strong talent. "Talent remains the most important driver of progress in all facets of AI. ... Within government, recruiting, training, and retaining AI talent will be essential to maximize AI's

potential," according to the National Security Commission on Artificial Intelligence.[46] Yet government continues to fall behind in hiring AI talent, along with technical talent in general, which hampers agencies' ability to implement and use AI tools to achieve the mission, according to the Partnership's analysis.[47]

Leaders with AI knowledge are as essential as having an AI-savvy technical workforce building and using the tools, according to the AI commission. "Developing AI-ready leaders is especially critical. Without more well-informed leaders who can go beyond talking points and reshape their organizations, [government agencies] will fail to compete in the AI era," the commission said.[48] Accordingly, responsible use of AI and other emerging technologies will depend on leaders who know the technology, are equipped to ask the right questions and understand the tradeoffs. They also must have team members who understand the theoretical underpinnings of emerging technologies, how they work and what impact they could have on the public and government employees.

Additionally, many emerging technologies rely on massive amounts of data. As a result, agencies will need in-house talent for

data analysis. In the future, this might involve evaluating data to determine data quality, if bias exists, and whether predictions or recommendations based on that data could be trusted.

"There is not a person at the Department of Energy who doesn't need to understand artificial intelligence. Sounds crazy, but if you do a deep dive into anything DOE funds, there is a significant application for new technologies like AI."

—Jetta Wong, former director of the Office of Technology Transitions, Department of Energy

---

46 National Security Commission on Artificial Intelligence, "Interim Report," Nov. 2019, 16. Retrieved from https://bit.ly/33QG5bC

47 Partnership for Public Service and IBM Center for the Business of Government, "More Than Meets AI Part II: Building Trust, Managing Risk," July 2019, 6. Available at https://bit.ly/2uxE6O1

48 National Security Commission on Artificial Intelligence, "Interim Report," Nov. 2019, 36. Retrieved from https://bit.ly/33QG5bC

LEADERS NEED EXPERIENCE IN SPECIFIC TECHNICAL COMPETENCIES

The technical competencies described in the previous pages are agency-wide competencies. Competencies show up in the skills of many different individuals and teams, enabled by hardware and software and promoted with cultural and organizational messages and incentives. As stated earlier, every leader does not need to have deep skills in every competency. However, it is beneficial for leaders to have hands-on experience in certain competencies and knowledge of others. The following charts summarize which technical competencies are most critical for each agency and cross-agency leader to have experience in.

AGENCY LEADERSHIP POSITIONS

	Tech-Informed Decision-Making	Security	Data Governance and Use	Human-Centered Design	Product Management	DevOps and Site Reliability Engineering	Modern Stack Software Development	Technology Procurement	Institutional Innovation and Change Management	Emerging Technologies
Deputy secretaries or their agency equivalents Manage performance and ensure resources and capacity are focused on accomplishing administration priorities.	★	★		★					★	
General counsels Oversee attorneys who provide legal services to the secretary and operating units in an agency, help navigate and resolve tensions when new technologies encounter legacy laws and regulations and understand the risk landscape and tradeoffs associated with technology decisions.	★	★	★					★	★	
Chief human capital officers Manage and lead talent recruitment and development efforts within an agency and improve approaches to hiring within existing laws and regulations.	★			★					★	
Key program administrators Understand the technical opportunities and constraints of their current technology platforms and of potential advanced systems, see how technology is essential to deliver services and enact policy, make informed tradeoffs and hire individuals who are deeply steeped in current technology and processes.	★			★					★	
Chief privacy officers Ensure privacy is considered in developing relevant legislative, regulatory and other policy proposals, ensure the agency complies with privacy laws and rules, ensure the agency appropriately manages risks relating to the privacy and confidentiality of data and information, and ensure responsible and lawful use of agency data.	★	★	★	★					★	
Chief information officers Review the portfolio of technical investments in their agencies, look for ways to improve systems and play a significant role in planning, programming, budgeting, and execution decisions and reporting related to information technology and management, governance and oversight processes related to information technology.	★				★	★	★	★	★	
Chief data officers Manage the data life cycle from collection to analysis to deletion, coordinate data-related efforts across the agency, manage each agency's data assets, contribute data to help achieve the agency's mission, help the agency use data in its day-to-day work and work with stakeholders to improve the agency's use of data.	★	★	★				★		★	
Chief technology officers Serve as senior technology policy advisers within agencies, manage the internal technology infrastructure that keeps agencies running and focus on developing technologies, services and products that serve the outside customer.	★	★	★	★			★		★	★

CROSS-AGENCY LEADERSHIP POSITIONS

	Tech-Informed Decision-Making	Security	Data Governance and Use	Human-Centered Design	Product Management	DevOps and Site Reliability Engineering	Modern Stack Software Development	Technology Procurement	Institutional Innovation and Change Management	Emerging Technologies
Administrator, Office of Information and Regulatory Affairs Oversees a key federal organization that collects information from customers, applicants and beneficiaries, including via websites and digital services.	★			★	★				★	
Administrator, U.S. Digital Service Builds and deploys a rotating team of 150 to 200 digital experts to address citizen-facing challenges at federal agencies across government.	★	★		★		★	★		★	

	Tech-Informed Decision-Making	Security	Data Governance and Use	Human-Centered Design	Product Management	DevOps and Site Reliability Engineering	Modern Stack Software Development	Technology Procurement	Institutional Innovation and Change Management	Emerging Technologies
Deputy director for management, Office of Management and Budget Serves as the federal government's chief performance officer and develops and executes the administration's management agenda, including its information technology, financial management, acquisition, organizational performance and human capital policies.	★							★	★	
Deputy national security adviser Understands how modern technology intertwines with national security, including issues around information encryption, cyberwarfare, foreign hacks of technical platforms, countering violent extremism, traveler vetting and aviation security.	★	★					★		★	★
Director, Office of American Innovation Leads a team that brings together innovative public- and private-sector ideas to solve pervasive problems in government management, improve Americans' quality of life and create jobs with modern technological and design approaches.	★			★					★	
Director, Office of Science and Technology Policy Ensures that decisions made by the president are informed by the best available scientific and technical information and promotes steps that the government can take to foster America's science and technology enterprise.	★								★	★
Director, White House Office of Presidential Personnel Oversees the selection of political appointees and verifies that candidates are qualified.	★			★	★				★	
Federal chief information officer Oversees the government's internal information technology, leads the Office of E-Government and Information Technology, focuses on reviewing the government's use of technology and defines the best possible technology infrastructure and innovative solutions.	★	★	★			★	★		★	
U.S. chief data scientist Responsibly unleashes the power of data to benefit all Americans, convenes the Data Cabinet, advocates for sourcing, processing and leveraging data in a timely fashion.	★	★	★				★		★	★
U.S. chief technology officer Advises the president on using technology, data and innovation to create effective public policy and build the capacity of government.	★	★		★			★		★	★
Administrator, General Services Administration Has executive authority over the Federal Acquisition Service and the Technology Transformation Services, which houses government-wide online technical platforms, such as login.gov and cloud.gov, 18F, Centers of Excellence for IT modernization and the Presidential Innovation Fellows program.	★							★	★	
Commissioner, Federal Acquisition Service Oversees the annual procurement of more than $50 billion in products, services and solutions and provides guidance to the thousands of contracting and procurement professionals throughout the federal government.	★							★	★	
Deputy commissioner, Federal Acquisition Service, and director, Technology Transformation Services Oversees the GSA's internal service organization that helps manage government's information technology portfolio and is responsible for improving the federal customer experience through modern technology.	★				★			★	★	
Executive Director, 18F Leads an internal digital services consultancy that focuses on long-term, sustainable changes in government.	★	★		★	★	★	★		★	
Director, Office of Personnel Management Oversees federal policy on recruitment and hiring, training, performance management and human resources management.	★	★							★	

DEPARTMENTAL OPPORTUNITIES AND CHALLENGES
REQUIRING TECHNOLOGY LEADERSHIP

Technology underlies much of the work of government, but many departments and agencies struggle to make full use of technology, hampering their ability to improve services to the public and modernize internal operations.

The five departments profiled in this section provide insights into the variety of technology challenges and opportunities facing our government. The key leaders with technology roles identified earlier in this report must work together with departmental technical leaders, some of whom are identified below, to face a wide array of critical challenges.

The five departments profiled were chosen to represent a variety of missions and technology challenges. The Department of Veterans Affairs, for example, is one of the largest government agencies and provides direct services to the public. The Department of Energy, in contrast, is smaller in size.

These profiles are based on conversations with current and former officials in these departments as well a review of departmental strategic plans, Government Accountability Office and inspectors general reports.

Overview

The Department of Health and Human Services impacts every family across the United States. HHS oversees healthcare providers, insurance, pharmaceutical companies, medical device manufacturers and health and life sciences research.

The 11 operating divisions within HHS include the Administration for Children and Families, Centers for Disease Control and Prevention, Centers for Medicare and Medicaid Services, Food and Drug Administration and National Institutes of Health.

By far the largest component of HHS is CMS, which had a budget of $794.2 billion dollars in fiscal 2019,[49] impacting 44 million Americans who are enrolled in Medicare and almost 74 million Americans who are enrolled in Medicaid.[50] CMS also is the component with the largest information technology budget. In fiscal 2019, it spent almost $2.85 billion on IT.[51]

Significant technical opportunities

- **Building technology to facilitate a move from traditional fee-for-service health care.** HHS's technology needs to accommodate the shift to value-based health care, such as rewarding providers based on quality and outcomes, not simply services provided, and includes improving components such as payment processing systems, data sharing and analytics tools.

- **Developing strategies for using data across the department.** HHS should ensure that insights and data can be shared across its divisions to improve both operational efficiency and the agency's strategies for improving the health of the country. This requires understanding the trade-offs between sharing data and protecting the privacy of patients and providers.

- **Using new and emerging technologies.** Innovative technologies, such as digital health records, telemedicine, artificial intelligence–powered medical tools and wearable devices, are reshaping the health care industry, with implications for HHS's mission. The department's IT strategic plan for fiscal years 2017–2020 builds on the recognition of the changing technology landscape and recommends HHS focus on building a technology workforce adept at using and deploying current and future technology.[52]

- **Ensure the privacy of information.** HHS collects and stores highly sensitive information about the Americans it interacts with, and its strategic plan calls on the department to ensure private data is protected.[53] Data privacy will become even more important for the department with the proliferation of health care technology that collects and uses unprecedented amounts of data about its users.

- **Overhauling Medicare and Medicaid's technical infrastructure.** The underlying 50-year-old technology used by Medicare and Medicaid should be modernized to accommodate potential surges in the number of people who rely on their services while ensuring sensitive information remains secure.[54]

Current state

Nearly all priority areas outlined in a recent report from the Office of the Inspector General, "2018 Top Management and Performance Issues Facing HHS," require improved technological solutions. In addition, the 2018–2022 HHS strategic plan highlights effective management and stewardship, including technology investments, as a primary goal. These priorities are based on the recognition that outdated payment processing, insufficient data sharing, legacy systems and inefficient technical processes are holding back many of HHS's core operating agencies from serving the public better and ensuring a new future for health care in America.

The legacy Medicare payment processing infrastructure, for example, is antiquated, hard-coded and monolithic—it uses ancient programming languages on cumbersome computer systems and relies on costly data centers. "About 40 percent of the systems of record at HHS are 'legacy' information technology, meaning they are no longer supported by their manufacturers," according to the department's strategic plan.[55] But it is expensive and time-consuming to undertake small upgrades or adopt new functionality, making it often impossible to keep pace with the changing nature of health care. As a result, payment innovation is often

---

ly/2rOrdNC

53 Ibid.

54 Department of Health and Human Services Office of Inspector General, "2018 Top Management and Performance Challenges Facing HHS," 2018. Retrieved from https://bit.ly/2nhmPop

55 Department of Health and Human Services, "Strategic Objective 5.3: Optimize information technology investments to improve process efficiency and enable innovation to advance program mission goals," Feb. 25, 2019. Retrieved from https://bit.ly/2WLdL8W

52 Department of Health and Human Services, "HHS Information Technology Strategic Plan FY 2017-2020." Retrieved from https://bit.

slow to be incorporated. A future where doctors are paid for value, not volume, is hamstrung by systems that cannot adapt. The department is taking significant steps to modernize these payment processing systems. An incremental, modular move to modern programming languages and the cloud are allowing CMS to shift underlying technology and engage the entire agency in discussions about how data is used across components. This will support better policy making and program integrity, and ensure that providers, beneficiaries and caregivers have access to the information they need.

Future state

Consider a future of health care oversight across HHS that is enabled by advanced digital technology—a future that rewards doctors for providing high-value care to patients rather than simply individual services. This requires systems that can sift through massive amounts of patient data, recognize patterns, support precision medicine and ensure reliability and accuracy. It also requires seamless data sharing, system interoperability and rigorous privacy protections balanced with accessibility, so that patients know their records are safe but available to doctors and caregivers.

New technology could power the delivery of the highest quality, lowest cost care while also helping HHS reduce waste, reimbursement fraud and abuse. Leaders will be able to focus on sustainability and continual improvement of cost, quality and outcomes for current and future generations.

Key technical positions

Without a leadership team who understands new technologies, how to implement them in a legacy environment, how to shore up the system gaps and how to accelerate the pace of innovation for improved effectiveness, the health care system that could be possible will not come to fruition.

National coordinator for health information technology: The national coordinator is responsible for national health IT initiatives, efforts to implement and use the most advanced health IT and electronic exchange of health information, and providing assistance on health IT projects across the entire federal government.

Digital Services executive director: The executive director heads a team of more than 10 employees who design digital tools to focus on two main challenges: measuring the quality of medical care and organizing Medicare recipient claims to improve the payment process.[56]

Administrator, Centers for Medicare and Medicaid Services: The administrator "oversees 6,000 staff members who run a $1 trillion budget, representing 26% of the federal budget, and administers health coverage programs reaching more than 130 million Americans" across all programs.[57] The CMS administrator should be able to work well with technology leaders on complex technical transitions.

Director, Center for Medicare and Medicaid Innovation: The Center for Medicare and Medicaid Innovation was established by law in 2010 to promote reforms that can "improve the quality and value of care in Medicare, Medicaid and the Children's Health Insurance Program, while helping achieve health reform's goals of more efficient, coordinated and effective care."[58] The center director must work across agency silos to build strong health care outcomes that are powered by effective, coordinated technologies.

Director, Center for Medicare: The director reports to the administrator of Medicare and "leads the staff that develops policies for and manages the operations of the fee-for-service portion of the Medicare program, and has responsibility for Medicare Advantage and Medicare Prescription Drug Programs."[59] Significant improvements in policy or operations will require ongoing transformation work in databases and analytics technology, and this requires a director who understands how these technical and policy facets intersect.

> **"Everything we do is dependent on technology. When defining the future of health care, it cannot be an afterthought. Technical strategy has to coexist with policy and agencies must recognize that the technical choices made across HHS and especially at CMS reverberate across the health care industry. If technical leadership does not come from CMS, health care technology will continue to be decades behind other industries."**
>
> —Shannon Sartin, former executive director, CMS Digital Service

56 Charles S. Clark, "Meet the Executive Bringing Digital Savvy to Health and Human Services," Government Executive, Sept. 11, 2018. Retrieved from https://bit.ly/2C7RJnh

57 Centers for Medicare and Medicaid Services, "CMS Leadership - Administrator." Retrieved from https://go.cms.gov/2JPIpIN

58 Stuart Guterman, Karen Davis, Kristof Stremikis and Heather Drake, "Innovation in Medicare and Medicaid Will Be Central to Health Reform's Success," Health Affairs 29(6), June 2010. DOI: 10.1377/hlthaff.2010.0442. Retrieved from https://bit.ly/36He9tE

59 Centers for Medicare and Medicaid Services, "CMS Leadership - Office of the Administrator." Retrieved from https://go.cms.gov/2WFuytK

Overview

The Department of Veterans Affairs cares for our nation's approximately 20 million veterans and their families with a budget of more than $200 billion and almost 360,000 full-time employees.

The VA provides many essential services—including health care, disability payments, housing support, education and access to national cemeteries—through three divisions: Veterans Health Administration, Veterans Benefits Administration and National Cemetery Administration.

Despite the importance of its mission, VA programs run on software that lags far behind private-sector equivalents. Some VA systems are almost five decades old, according to the Government Accountability Office.[60] Resistance to change, an unwillingness to make tough decisions at times, overwhelming technical debt and the sheer difficulty of its scale on the technology front have made it even more difficult to keep up with the growth in demand for benefits and health care.

Significant technical challenges

- **Overcoming the lack of interoperability so that different VA systems can share data.** The VA runs nine lines of business, including the largest health care organization in America, using hundreds of systems, very few of which are interoperable. For example, the system that provides education benefits through the GI Bill does not share information with the system tracking housing benefits. The VA needs an architecture to get all the systems to talk to one another.

- **Establishing electronic health records systems that meet the needs of veterans.** There are multibillion-dollar projects in the works to replace the VHA's electronic health records and to make them fully interoperable with the Department of Defense. The challenge is complex and requires both modern technical and political acumen.

- **Improving the user experience for veterans and VA staff.** While great strides have been made to consolidate a veteran's interactions with VA into one place through VA.gov—formerly Vets.gov— applying for many VA services remains a byzantine process. Processing claims continues to be an uphill battle for staff members who are forced to use antiquated systems.

- **Reducing backlogs leading to substantial delays in services.** The disability claims backlog has improved significantly, yet "is worse than leaders there have acknowledged," according to the department's Office of Inspector General."[61] Currently, the disability claim processing system does not interface with the medical records systems of DOD or the VA.

- **Migrating from legacy systems written in computer languages no one learns anymore.** It is vital for the VA to move from legacy systems that place basic day-to-day operations at risk. Many VA systems currently run on outdated computer language. For example, the electronic health record system powering every VA hospital is based in MUMPS. And VA is a top employer for Pascal programmers, a computer language created in 1968 that only 2% of businesses said they still looked for in 2017.[62]

- **Information security.** Maintaining the integrity of VA's information systems is a key component of the VA's IT strategic plan, underpinning its IT-related goals.[63] Yet several Government Accountability Office reports point to shortfalls in VA's information security, with one report saying its programs to ensure security are "deficient" and "ineffective."[64] The security weaknesses include not addressing known security risks in a timely manner, managing risks in its security supply chain and effectively evaluating security-related staffing needs, among others, according to the same GAO report.

Current state

Five years ago, veterans calling the VA suicide hotline were sometimes routed to voicemail and did not receive immediate support.[65] Veterans often found accessing information and services online confusing and time consuming. Since then, there has been an increased focus on the customer experience, including the creation of a unified online portal called Vets.gov, now called VA.gov, and focused efforts to ensure that crisis lines are staffed and available. In 2015,

61 Leo Shane III, "Watchdog report: The VA benefits backlog is higher than officials say," Military Times, Sept. 10, 2018. Retrieved from https://bit.ly/33fyZOH

62 Sarah K. White, "9 legacy programming skills still in demand," CIO.com, Dec. 20, 2017. Retrieved from https://bit.ly/34sDUf3

63 Department of Veterans Affairs, "Enterprise Technology Strategic Plan, Fiscal Year 2017-2021," March 8, 2016. Retrieved from https://bit.ly/368o4HF

64 Government Accountability Office, "Information Security: VA and Other Federal Agencies Need to Address Significant Challenges," GAO-20-256T, Nov. 2019. Retrieved from https://bit.ly/2r8ACzL

65 Department of Veterans Affairs Office of Inspector General, "Healthcare Inspection: Veterans Crisis Line Caller Response and Quality Assurance Concerns Canandaigua, New York," Feb. 11, 2016. Retrieved from https://bit.ly/32b6kJf

the Veterans Experience Office conducted in-depth interviews of veterans and their support networks to make sure that the products, services and offerings veterans earned through their service were meeting their needs, according to Sarah Brooks, former VA chief design officer. This, along with leadership, training, accountability, funding and support, has led to improvements that have brought veterans' trust in VA from below 50% to 72%.[66]

Yet in certain areas, VA services still fall short. For example, it takes so long to appeal a disability ruling that one in 14 veterans die while waiting for an appeal decision, according to the department's inspector general.[67] These wait times are due, in part, to over 40 databases holding different pieces of information about veterans for different purposes, which often cannot be reconciled.

Additionally, the VHA had a long operating tradition of focusing on physical VA medical centers as fundamental building blocks for its health care delivery. This created a perception that every medical center was inherently different and led to a culture of customization of electronic health records at each local hospital.

While the theory behind these custom-built data systems was that veterans would receive better local service, in practice it created a complex web of isolated systems. And while VA had a reputation for being a pioneer in electronic medical records, as a result there were 123 different instances of electronic medical records software operating in 150 different medical centers—making simple tasks such as getting a prescription filled, or visiting a different VA facility for care while away from home, potentially extremely difficult.

VA leaders recognize the need to modernize. "Business transformation is essential if we are to move past compartmentalization of the past and empower our employees serving veterans in the field to provide world-class customer service," VA Secretary Robert Wilkie said in congressional testimony. "This means reforming the systems responsible for claims appeals, GI Bill benefits, human resources, financial and acquisition management, supply chain management and construction."[68]

Future state

With modern technology and leadership support, veterans could receive the benefits they have been promised in a quicker, more accurate and customer-focused way. In this future state, routine veteran surveys will show that veterans have come to expect great service from the VA, represented by ease of creating doctor appointments and a streamlined process that provides benefits as effectively as the private sector. The service products VA provides will be processed quickly using organized and comprehensive databases that share information with one another. Medical records will be shared effectively and in real time between the Defense Department and VA. Disability claims and appeals will be reviewed fairly and quickly with responses being received within a week.
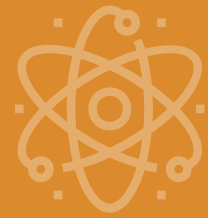
Key technical positions

The most important initial roles at the VA are the eight positions cited earlier in this report that are critical to every agency. At the VA, the CIO and CTO both serve distinct functions that are nonetheless intertwined.

Executive director, Digital Service at VA: The director recruits a world class team of designers, technologists and product managers to use design and technology to make services for veterans "simple, fast and easy to use." [69]

> **"When I first joined the VA, the fragmentation of systems leading to a truly painful customer experience was the biggest a-ha moment for me. Technology isn't just one organization; technology must be in everything. Using technology to scale services needs to be a more strategic partnership, working with the business side to create a plan together, not just reacting to the plan from the business side."**
>
> *—Sloan Gibson, former deputy secretary, VA*

66 Department of Veterans Affairs, "Agency Priority Goal Action Plan: Veteran Customer Experience," June 2019. Retrieved from https://bit.ly/2JObW5w

67 Ben Kesling, "Hundreds of Thousands of Veterans' Appeals Dragged Out by Huge Backlog," Wall Street Journal, Aug. 22, 2018. Retrieved from https://on.wsj.com/2MslCq1

68 "Statement of the Honorable Robert Wilkie Before the Senate Veterans' Affairs Committee." Hearing on "The State of the Department of Veterans Affairs," Senate Veterans' Affairs Committee, 2018. Retrieved from https://bit.ly/2vaKV8F

69 Digital Service at VA, "Transforming technology within VA." Retrieved from https://bit.ly/2JPojOX

DEPARTMENT OF ENERGY

Overview

The Department of Energy is a science and technology agency with a mission to ensure America's safety through energy, environmental and nuclear policy.[70] It oversees the nation's nuclear weapons stockpile and nuclear energy policy.

In fiscal 2019, the agency's total budget was $35.5 billion and its information technology budget was $2.4 billion.[71, 72] Its workforce consists of around 14,000 federal employees and more than 95,000 contractors, according to department estimates.[73]

The department also manages 17 national laboratories, which conduct innovative scientific and technology-related research to achieve DOE's mission. For close to eight decades, national laboratories have contributed to the development of a range of innovations from nuclear weapons to LED lighting, and participated in activities ranging from sequencing the human genome to exploring the planet Mars. The latest strategic plan said a key department goal is to "optimize information processes, services and technology to deliver high-quality solutions, reduce costs, improve security and enhance collaboration across the Department by 2017."[74]

In addition, DOE plays an important role in the research, development and deployment of energy technologies needed to accelerate the transition to a low-carbon economy. These include solar and wind energy, energy-efficient buildings, electric vehicles, advanced nuclear power, carbon capture and sequestration, and new, energy-efficient processes in the manufacturing sector. The department funds research and development, providing loans and loan guarantees to clean-energy projects and identifying policies that will increase private sector investment in low-carbon technologies.

DOE also recognizes that its mission is "enabled, advanced and reliant on [internal] information and information systems that must be effectively managed to ensure mission success."[75]

Significant technical challenges

- **Combating cyberattacks.** DOE houses the technical systems that control nuclear energy and missiles, in addition to cutting-edge research facilities and protection of the country's power grid, requiring that the agency have a culture and the technical capacity to protect against cyberattacks. "One of the biggest challenges DOE faces due to the complexity of the enterprise and the diversity of its missions is gaining and maintaining comprehensive situational awareness" of "today's rapidly shifting cyber threat landscape," according to the department's IT strategic plan for fiscal 2018–2022.[76]

- **Upgrading major technology infrastructure.** Reports from the Government Accountability Office have cited modernization of legacy systems among DOE's IT-related challenges. According to GAO, DOE operates legacy systems in high-impact, high-risk areas that include managing nuclear waste.[77]

- **Working across silos.** In its most recent IT strategic plan, DOE committed "to seek opportunities to remove silos and fully interconnect the enterprise to strengthen the workforce's ability to collaborate seamlessly, resulting in maximized productivity and cost efficiency."[78]

- **Incorporating emerging technologies into energy-related goals.** One of the department's stated goals is incorporating new technologies into its information systems. The department identified cybersecurity as a fundamental area where new technologies could help DOE achieve its mission, according to its IT strategy.[79]

- **Building foundational data systems.** DOE must ensure that its data collection and dissemination system, the basis for reliable decision-making, is clean, accurate and up-to-date.

Current state

While among the most technology-forward federal agencies, DOE still operates burdensome legacy systems that do not serve employees or the public well. The process

---

75 Department of Energy, "U.S. Department of Energy Order 200.1A: Information Technology Management," Dec. 23, 2008, 1. Retrieved from https://bit.ly/2lIKuO4

76 Department of Energy, "Information Resources Management Strategy FY 2018-2022," 13. Retrieved from https://bit.ly/2rX6ozC

77 Government Accountability Office, "Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems," GAO-19-471, June 2019, 7. Retrieved from https://bit.ly/31y2Xgk

78 Ibid.

79 Ibid.

to apply for entrepreneurial funding programs for advanced technologies is so opaque and onerous that many are turned off.

Also, the department funds and commercializes technologies that have significant impact, but that operate on multiple systems that require the offices of the secretary, CTO and CIO to input data with little quality control. This results in data cleanup issues that lead to a range of problems.

Despite these challenges, the department has an advantage attracting young mission-critical talent compared to other agencies, even private-sector companies. University students place DOE among their top employers-of-choice. In 2019, for instance, the department ranked as the 23rd most attractive employer for engineering students and 19th for natural sciences students, ahead of companies that included IBM, Facebook, Samsung and Lego, according to a Universum survey of more than 53,000 students.[80]

The department houses some of the most valuable intellectual and scientific innovation infrastructure in the country, including national laboratories, nuclear facilities and the Advanced Research Projects Agency–Energy, a sponsor of high-risk, high-return energy research. The department also has created the Artificial Intelligence and Technology Office to coordinate AI research across DOE.

According to the department, DOE-funded AI is already being used to strengthen our national security and cybersecurity, improve grid resilience, increase environmental sustainability, enable smarter cities and improve water resource management.[81] It is also being used to speed the discovery of new materials and compounds, and further the understanding, prediction and treatment of disease. DOE's national laboratories are home to four of the top 10 fastest supercomputers in the world, and they have plans for three more next-generation machines which will be even faster and more AI-capable.

Future state

Future innovations in manufacturing, transportation, space exploration and health care will increasingly rely on energy and well-operating technologies. The department and its national laboratories have always played a crucial role in many of these areas and must continue to do so through a new focus on emerging technologies. For example, national laboratories house some of

the most powerful technical and computing systems in the world, which could offer more opportunities for scientists and researchers with access to solve seemingly unbreakable scientific mysteries. The department also could lead and fund more demonstration projects of emerging technologies to spur greater private investments and ultimately drive private-sector job creation.

The department's mission includes working on cutting-edge science and technology. Perhaps even more so than at other agencies, technical acumen must be infused at every level of the department. Divisions within DOE such as the Office of Management or the Office of the Chief Financial Officer should be equipped to make smart decisions while moving fast to greenlight necessary funding, move projects forward, reduce delays and improve transparency.

Key technical positions

There are many critical leadership positions requiring technical expertise throughout DOE. In addition to more clearly defined technical roles, leaders in financial and operational positions need to speak the same language as their scientifically driven counterparts and assess priorities and trade-offs to make quick, informed decisions. Experts in the positions below must partner with technology experts from the center-of-government agencies to drive mission outcomes.

Director, Advanced Research Projects Agency-Energy: The director of the Advanced Research Projects Agency-Energy reports to and advises the secretary on energy technologies and barriers to their development, while managing research programs that address these matters. The director leads a team of technical experts that assesses and selects transformative technology projects for federal funding. According to the law that created the position, the director should be "qualified to advise the secretary on, and manage research programs addressing, matters pertaining to long-term and high-risk technological barriers to the development of energy technologies."[82] The director also should have expertise managing a diversified portfolio of multiyear, multimillion dollar technology projects and a deep understanding of technology research funding processes, including public, private and combined public–private streams.[83]

Director, Office of Management: The director is the central management and administrative leader at DOE,

80 Universum, "US's Most Attractive Employers 2019," June 4, 2019. Retrieved from https://bit.ly/2Wesw22

81 Department of Energy, "Secretary Perry Stands Up Office for Artificial Intelligence and Technology," Sept. 6, 2019. Retrieved from https://bit.ly/2oLitXD

82 "America COMPETES Act of 2007."

83 Partnership for Public Service, "Federal Position Descriptions," 2016. Available at https://bit.ly/2lpxX1I

overseeing core roles in the $2.3 billion dollar IT organization, such as project management and acquisition.[84, 85]

Administrator, Energy Information Administration: The administrator leads a comprehensive program collecting, analyzing and disseminating data and information relevant to energy resource reserves energy production, demand and technology, as well as energy-related economic and statistical information, according to the Department of Energy Organization Act of 1977, which created the administration. The administrator has to be "specially qualified to manage an energy information system," according to that 1977 law. The data collected by EIA is used for decisions in and out of the department; as a result, ensuring the data is accurate, relevant and secure is paramount.

"There need to be organizations within DOE that develop data analytics and machine-learning tools, use the data and turn it into something of value for energy-related applications. This could be embedded broadly across many offices in DOE."

—*Arun Majumdar, former director, Advanced Research Projects Agency–Energy*

---

84 Department of Energy, "Department of Energy FY 2020 Budget Request Fact Sheet," March 11, 2019. Retrieved from https://bit.ly/2JOQXQp

85 Department of Energy, "About Us." Retrieved from https://bit.ly/2qhaQbU

DEPARTMENT OF TRANSPORTATION

Overview

The Department of Transportation plans and coordinates federal transportation projects. In fiscal 2019, it had a budget of $87.4 billion[86] and more than 52,000 employees as of March 2019. DOT sets safety regulations for all major modes of transportation, including emerging new technologies such as hyperloop, autonomous driving vehicles and drones. The agency serves as something akin to a holding company, with the Office of the Secretary establishing policy and overseeing 10 administrations, including the National Highway Traffic Safety Administration, Federal Aviation Administration, Federal Highway Administration, Federal Railroad Administration, Federal Transit Administration and Maritime Administration.

The Office of the Chief Information Officer within the department was created in 2016 and oversees the entire department's information technology portfolio. This budget totaled $3.4 billion in fiscal 2019, the sixth largest in the federal government.[87]

The 2018–2022 DOT Strategic Plan identifies technical priorities that include improved data collection, cybersecurity, and use of modern technical systems and practices when it comes to safety, infrastructure, innovation and accountability.[88]

Significant technical challenges

- **Cybersecurity:** The department continues to struggle with cybersecurity preparedness. DOT's inspector general highlighted cybersecurity as a top management challenge for the department, including standardizing security processes across all subcomponents and continuing to identify and address existing security weaknesses in departmental networks.[89] Indeed, according to a fiscal 2019–2021 DOT technology strategy, there were 11.9 billion cybersecurity events, ranging from security policy violations to hacks, in a single year. Additionally, as of 2019, 36% of DOT websites were not secured with standard HTTPS internet security protocol, and as of 2018, 24% of employees of one division were susceptible to phishing.[90] The unpredictability associated with breaches and forensic difficulty of tracking down perpetrators leaves DOT's systems vulnerable.

- **Improving information technology workforce planning.** DOT's IT workforce planning activities have several shortfalls, according to a Government Accountability Office report that assessed planning at all major agencies.[91] GAO said that while the department developed competencies and staffing targets for its IT staff, it has not regularly assessed competency and staffing needs and has not developed plans to address skill gaps.

- **Building a technical and governance infrastructure that effectively manages data.** Data management and governance will be imperative to emerging technologies, such as autonomous or driverless vehicles and intelligent transportation systems, as the department must help develop and set safety standards for driverless vehicles to ensure public safety. Data is also the backbone for some of DOT's most crucial services.

Current state

The FAA, the department's largest subcomponent, has struggled to implement modern technology in the Next Generation Air Transportation System, or NextGen, a multi-year, multi billion-dollar program to modernize America's aging air traffic control system. Between 2004 and 2016, NextGen received several billion dollars—and will probably require several billion dollars more to manage the exponential increase in national airspace needed for 1.3 million drones, commercial spaceflight and even private air taxis, according to Ty McCoy, the former acting secretary of the Air Force.[92, 93] Moreover, a member of the DOT management advisory council's board noted that the government is operating "50-year-old radar installations and antiquated equipment. There's no resiliency and redundancy in the system so if something went wrong, there wouldn't be back up."[94]

However, the department has made strides in improving its internal information technology operations. For example, in 2018 the chief information officer began a technology transformation project called

90 Department of Transportation, "DOT IT Strategy fiscal 2019-2021." Retrieved from https://bit.ly/2PRGE1P

91 Government Accountability Office, "Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities," GAO-20-129, Oct. 2019. Retrieved from https://bit.ly/2Pfwiqj

92 Connor Collins, "At FAA, Data and Modernization Mean Safer Skies," Government CIO, April 30, 2019. Retrieved from https://bit.ly/33gSEOb

93 Tidal W. McCoy, "The Dangers of Delaying FAA Modernization," Wired, Sept. 27, 2019. Retrieved from https://bit.ly/32fh5dB

94 Kim Riley, "Long-term FAA funding stability needed, says Capitol Hill insider," Transportation Today, March 13, 2018. Retrieved from https://bit.ly/2qmgf14

DestinationsDIGITAL, which funds mission-related technical programs out of savings from consolidating duplicative support services. Internet technology support service consolidation is a priority outlined in the department's 2018–2022 strategic plan.

Additionally, the department is taking steps to better use data to ensure the safety of self-driving or autonomous vehicles. DOT's Intelligent Transportation Systems Joint Program Office, for example, is working with state and local governments, academia, nonprofits and private-sector companies to share data with one another. Through data sharing, the office hopes that stakeholders involved in rolling out self-driving cars—from manufacturers to state departments of transportation—could learn from one another, as "access to data is a critical enabler for the safe, efficient and accessible integration of AVs into the transportation system, according to the department."[95] In 2018, DOT created the Non-Traditional and Emerging Transportation Technology Council chaired by the deputy secretary. The council serves as an internal deliberative body at the department responsible for identifying and resolving jurisdictional and regulatory gaps that may impede the deployment of new technologies, such as tunneling, hyperloop and autonomous vehicles. The NETT also serves a coordinating function to help innovators and investors obtain necessary safety authorizations, permits and funding across the various authorities.

Future state

In 10 years, transportation in the United States will look far different than it does now. Underpinning the emerging technologies on the roads will be a technical infrastructure and agency culture that houses, manages and uses data effectively, and that engages technical and user feedback to proactively address user concerns and cybersecurity issues. Already, vehicle-sharing and electrification are widespread, and autonomous vehicles and the Internet of Things are poised to make even bigger waves. The FAA will turn to next-generation technologies for air traffic control and testing emerging technologies such as low-boom supersonic aircraft. Drones and artificial intelligence software will be used to deliver a plethora of transportation and infrastructure solutions. None of this works effectively without streamlined technical infrastructure and strong data governance.

Key technical positions

Leadership positions will need to be filled in sub-agencies within the department to achieve a future state en-

abled by tech. Three positions at the department level that will be particularly important are listed below.

Undersecretary for policy: The undersecretary serves as the focal point for developing and coordinating the department's automated vehicle policies, which requires knowledge of artificial intelligence and data analytics, two fields important to the safe and efficient deployment of self-driving cars.

Assistant secretary for research and technology: The assistant secretary provides, among other functions, support for the advancement of innovation, technology development and breakthrough knowledge, and fosters technology transfer through partnerships within the department and with others, such as academia and private entities.

Director, Office of Intelligence, Security and Emergency Response: The Office of Intelligence, Security and Emergency Response develops, coordinates and executes plans for transportation security, and oversees programs that collect and analyze intelligence and prepare for and respond to emergencies. The director serves as a federal senior intelligence coordinator and represents DOT within the intelligence community.[96] Given the threats facing transportation systems, the director's role increasingly includes assessing and mitigating the risk of various cyber threats, according to an interviewee.

95 Department of Transportation, "Data for Automated Vehicle Integration (DAVI)," Dec. 4, 2019. Retrieved from https://bit.ly/2RmoK7Z

96 Department of Transportation, "Office of Intelligence, Security and Emergency Response - Organizational Functions," Oct. 2, 2018. Retrieved from https://bit.ly/34YOTOk

DEPARTMENT OF HOMELAND SECURITY
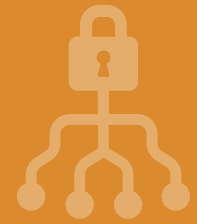
Overview

The Department of Homeland Security was created in 2003 in the aftermath of the September 11, 2001 terrorist attacks, consolidating functions such as emergency management, counterterrorism, cybersecurity and immigration from across the federal government. DHS is the third largest federal department after the departments of Defense and Veterans Affairs, employing more than 170,000 people as of March 2019 with a budget of about $81 billion in fiscal 2019.[97] It has one of the most wide-ranging sets of missions and functions among all agencies.

The DHS operating and support agencies include U.S. Citizenship and Immigration Services, Immigration and Customs Enforcement, Customs and Border Protection, Coast Guard, Transportation Security Administration, Federal Emergency Management Agency, Secret Service, Cybersecurity and Infrastructure Security Agency, Science and Technology Directorate and Office of Intelligence and Analysis.

The promise of consolidating 22 agencies was designed to improve communication between agencies and increase their ability to deliver on DHS's five central missions: preventing terrorism and enhancing security; securing and managing our borders; enforcing and administering immigration laws; safeguarding and securing cyberspace; and ensuring resilience to disasters. In addition to its own work, DHS is responsible for the information security of the entire civilian federal government, including providing mandated security services to other agencies and handling incident response. However, DHS has publicly suffered from the merger of such diffuse responsibilities, and particularly the conflict between law enforcement and service functions. The 2018–2024 DHS strategic plan outlines six major goals, all of which require a world-class ability to manage and govern data and modern, effective technical processes and systems.[98]

Significant technical challenges

- **Moving to a 21st-century model for information security.** DHS currently mandates that government follow a 20th-century model for information security—heavily reliant on perimeter security, protecting systems as a whole rather than individual devices within a system. Outdated approaches to cybersecurity contributed to the major 2014–2015 Office of Personnel Management breach and other government breaches.

- **Effectively sharing data.** DHS should improve its data strategy across the dozens of agencies and hundreds of systems involved in vetting every person who enters the United States, including travelers and immigrants, while respecting privacy.

- **Improving outcomes of humanitarian missions.** The department should use modern technology to support acute and ongoing humanitarian missions, including FEMA disaster response operations, while ensuring the security of sensitive data about these populations.

- **Digitizing immigration application process.** Efficiently processing millions of legal immigration applications each year, many of which are still on paper, and building capacity to handle any potential immigration reform legislation.

Current state

There are several technical systems and areas that lack the right technical expertise at DHS. According to the Government Accountability Office, in 2016, a $6 billion "intrusion detection system" called Einstein failed to catch 94% of common cybersecurity vulnerabilities.[99, 100] A more recent report said DHS has been making efforts to improve the system, but did not provide another tested outcome to show if Einstein caught more security vulnerabilities. The report also highlighted that the vast majority of agencies had not fully implemented Einstein despite improvements.[101] For example, only two of 23 agencies had implemented all email requirements.[102] A September 2019 report suggests that DHS does not have the cybersecurity talent it needs to reach related goals.[103]

In addition to security systems that need improvement, agencies such as USCIS are struggling with basic data intake and management systems. USCIS had only eight forms for immigration services functioning online as of 2019. The

97 Department of Homeland Security, "FY 2021 Budget in Brief," Feb. 2020, 1. Retrieved from https://bit.ly/2TiA2cB

98 Department of Homeland Security, "The DHS Strategic Plan Fiscal Years 2020-2024," 2019. Retrieved from https://bit.ly/34lVul4

99 Government Accountability Office, "Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System," GAO-16-294, January 2016, 22. Retrieved from https://bit.ly/2NgnSiK

100 "DHS EINSTEIN firewall fails to detect 94% of threats, doesn't monitor web traffic," CSO Online, Feb. 4, 2016. Retrieved from https://bit.ly/2PIwZKC

101 Government Accountability Office, "Information Security: Agencies Need to Improve Implementation of Federal Approach to Securing Systems and Protecting against Intrusions," GAO-19-105, December 2018, 46. Retrieved from https://bit.ly/36BhudM

102 Ibid.

103 Department of Homeland Security Office of Inspector General, "DHS Needs to Improve Cybersecurity Workforce Planning," Sept. 23, 2019. Retrieved from https://bit.ly/2NFjJnC

rest of the forms must be completed on paper.[104] Prior efforts had been attempted through contracts with outside companies and resulted in processes that were more difficult than paper for those adjudicating the forms.[105]

In interviews with former and current technology leaders at DHS, one theme came through clearly. "One of the biggest barriers in modernizing the federal government at the pace that's expected is the pace of the end to end acquisition process. While there have been some promising approaches to modernizing this, these efforts are not wide spread. More needs to be done to adopt these advanced methods in order to meet the increasing demands of the agencies" according to former DHS CIO Luke McCormack.

While there are initial efforts such as the Silicon Valley Innovation Program, a $10 million initiative to harness commercial technologies for government applications, many ongoing issues—such as program delays, wasted funds, data inconsistency, cyber challenges and unnecessary redundancies—will continue to weigh down departmental operations.

Future state

A DHS that has improved technology systems, data governance and procurement procedures can become a model for how data and information enables more effective policy and programs. USCIS, for example, could more effectively and accurately process refugees, reduce the immigration case backlogs and application wait times, and provide asylum seekers more clarity and transparency. FEMA could track damage claims and recipient progress and implement heightened fraud detection. The department could adopt a more modern approach to information security that makes future breaches across government less likely and accelerates the pace of all government software development by replacing burdensome security requirements with modern guidelines and solutions.

Key technical positions

DHS needs a blend of technical expertise, strategic leadership and vision to motivate people and shape process and culture to achieve the mission. In addition to key agency roles laid out above, such as the chief information officer and chief technology officer, the following roles are critical.

DHS Digital Service executive director: The DHS branch of the U.S. Digital Service has roughly 35 engineers, product managers, designers and policy and operations experts working on core service delivery programs across the department. The director reports to the DHS CIO but has staff embedded within major programs in different components. The team generally acts as highly empowered consultants accountable to senior DHS and White House leadership, occasionally taking on temporary management roles in projects but rarely building products or services in-house. Projects have included immigration benefits processing, refugee admissions, import and export processing, Trusted Traveler Program applications and FEMA disaster grants management.

Director, U.S. Citizenship and Immigration Services: The director of USCIS oversees more than 18,000 employees processing immigration applications around the country. This is not actually a policy-focused role—many of USCIS's challenges are around innovating and optimizing largely paper-driven operations. It requires a true operational leader with an understanding of how technology can be harnessed to substantially transform the organization.

Director, Cybersecurity and Infrastructure Security Agency: CISA is the new name for an agency that oversees and coordinates federal government civilian cybersecurity efforts, including operating a 24/7 cybersecurity incident command center, issuing directives around potential threats, conducting vulnerability assessments of infrastructure and building relationships with public, private and international security partners.

Assistant director for Cybersecurity Division, CISA: This individual is directly responsible for cybersecurity of the civilian federal government. The assistant director oversees cybersecurity monitoring and operations as well as the development and adoption of major cybersecurity policies, products and services.

Deputy administrator, Federal Emergency Management Agency: The deputy administrator assists the administrator in leading FEMA in its mission to support the American public and first responders, and to sustain and improve the government's capability to prepare for, protect against, respond to, recover from and mitigate all hazards, according to the Partnership's analysis.[106] The deputy administrator should work with technical and product experts to improve the security of FEMA's technology, as well as its use of technology in federal emergencies.

> **"Strong technical leadership and operational innovation at DHS can help transform the lives of millions of people, from rebuilding after a natural disaster to refugees fleeing persecution, and make our country safer from threats of all kinds. DHS has started to make progress, but needs experienced technical and operational leaders who bring modern approaches to get things done."**
>
> *— Eric Hysen, former executive director, DHS Digital Service*

104 U.S. Citizenship and Immigration Services, "USCIS Makes Another Form Available for Online Filing," Oct. 30, 2019. Retrieved from https://bit.ly/2qtJUWQ

105 Department of Homeland Security Office of Inspector General, "U.S. Citizenship and Immigration Services Information Technology Management Progress and Challenges," July 2014, 17. Retrieved from https://bit.ly/36qg8lM

106 Partnership for Public Service, "Federal Position Descriptions," 2016. Available at https://bit.ly/2lpxX1I

CONCLUSION

The federal government has attracted dedicated professionals to lead missions to fly to the moon, protect our country and serve America's veterans. As we look to the next decade, leaders who understand modern technology, innovation and digital service delivery will be valuable players in implementing federal policy, and experts in emerging technologies will play a major role in evaluating and regulating their use.

New innovations in data science and biotechnology will require both federal support and appropriate regulation. Calls to use artificial intelligence to make government work better and cost less need to involve knowledgeable technology leaders who understand how to use AI without reinforcing existing biases in the data it relies on.

Handling the increase in the number of people on Medicare, providing services and benefits to an aging veteran population, managing the nation's transportation system and strengthening our national defense and intelligence capabilities will also require sophisticated technical platforms work today and can be expanded and upgraded to meet evolving needs.

Bringing in leaders to our government who understand technology, increasing the skills of the existing workforce and hiring to build the competencies of a 21st-century agency would be major steps forward.

The federal government has the opportunity and responsibility to use new technology to the greatest extent possible in the delivery of services and in pursuit of our national priorities. That goal will require a second-term Trump administration or a new president to have a laser-like focus on bringing knowledgeable, skilled technical leaders into the government.

Appendix A: Roles on a Technical Team

Natalie Kates and David Koh, two U.S. Digital Service experts in product and engineering, developed an outline and key questions to understand key roles on technical teams in government seeking to build a service or a product. Each role is responsible for a specific set of goals.

- **Product owner**
  - **Key question to ask:** What's the right product?
  - **Responsibilities:**
    - Define the product that will be built.
    - Prioritize what gets built as the person ultimately responsible for the outcome of the product.
    - Articulate product vision to the team and externally, usually working with a communications lead.

- **Project manager**
  - **Key question to ask:** How can I make this release smooth and easy?
  - **Responsibilities:**
    - Responsible for the success of all software releases.
    - Manage release schedules and dependencies.
    - Create rollout plan and manage rollout activities and schedules.

- **Design**
  - **Key question to ask:** What is a usable and productive solution for the user's need?

- **Engineering**
  - **Key question to ask:** How do I build this product correctly?
  - **Responsibilities:**
    - Oversee the technical development of the product.
    - Communicate technical constraints and level of effort for feature prioritization and design.
    - Advise on the practical efficacy of automation and other technologies.
    - Estimate return on investment for prioritizing non-user-facing technical and architectural work.

- **Testing**
  - **Responsibilities:**
    - Ensures that new features don't break the existing software.
    - Collaborate actively and continuously with design at all stages of the design process, rather than interpreting written requirements.
    - Mitigate post-deployment errors or bugs.
    - Write test cases based on the outcome of design.
    - Write test cases early in the process to allow regular iteration.
    - Write and maintain automated testing suites.

- **Stakeholders outside the technical team, such as agency leads**
  - **Key question to ask:** How does this product fit in with the organization's goals and how can I help make sure it is successful?
  - **Responsibilities:**
    - Create the initial vision for the product and provide ongoing leadership support within an agency.
    - Remove any barriers identified by the product delivery team.
    - Provide 'air cover,' so the team can take on necessary risks.
    - Hold the product owner accountable for achieving the outcomes described in the overall vision.

Appendix B: Opportunities for Further Study

There are many important topics and associated positions related to science, technology and innovation that this report does not cover and that provide opportunities for further study. These areas include:

- Policy toward the broad range of technologies beyond information and communications systems, such as clean energy, biotechnology and the bio economy, advanced manufacturing, advanced materials and space.

- Key science agency leadership, such as at the National Institutes of Health, National Science Foundation, Defense Advanced Research Projects Agency, the Department of Energy's Office of Science and NASA.

- Identification and pursuit of grand challenges or moonshots—ambitious but achievable goals that have the potential to capture the public's imagination.

- Detailed exploration of new ways agencies could solve important national problems, including incentive prizes, "lean startup" methodologies and public–private partnerships.

- Strategies that involve government paying for outcomes rather than inputs, including successful contracts, performance-based milestone payments and advance market commitments.

- Policies that strengthen America's innovation ecosystem, such as inspiring more students to excel in STEMM education, fostering the commercialization of federally funded research, and ensuring that tax and regulatory policies encourage private investment in R&D and startups.

- Social innovation, such as experimenting with new approaches to education, workforce development and alleviating poverty; rigorously evaluating promising interventions; and providing funding to scale effective programs.

Appendix C: Acknowledgements

The individuals listed below generously offered their input on technology talent in government. We greatly appreciate their time and counsel. The contents of this report do not necessarily reflect the views of those with whom we engaged, and the views of participating federal officials do not necessarily reflect positions or policies of the federal government or its agencies.

Marc Aidinoff
Doctoral Candidate, Massachusetts Institute of Technology
Former Assistant Director of Policy, Office of the Vice President of the United States

Tom Allin
Visiting Professor of the Practice, Sanford School of Public Policy, Duke University
Former Chief Veterans Experience Officer, Department of Veterans Affairs

John Bailey
Visiting Fellow, American Enterprise Institute
Former Special Assistant to the President for Domestic Policy, The White House
Former Deputy Policy Director, U.S. Department of Commerce

Scott Blackburn
Partner, McKinsey and Company
Former Chief Information Officer and Interim Deputy Secretary, Department of Veterans Affairs

Sarah Brooks
Distinguished Designer and Design Executive, Digital Growth and Commerce, IBM
Former Chief Design Officer, Department of Veterans Affairs

Phaedra Chrousos
Chief Strategy Officer, Libra Group
Founding Commissioner, U.S. Technology Transformation Service

Beth Cobert
CEO, Skillful (A Markle Initiative)
Former Acting Director, Office of Personnel Management

Betsy Cooper
Founding Director, Aspen Tech Policy Hub
Former Attorney Advisor to the Deputy General Counsel and Policy Counselor, Office of Policy, Department of Homeland Security

Daniel Correa
Director, Day One Project
Former Assistant Director for Innovation Policy, Office of Science and Technology Policy

Joe Crobak
Engineering, Confluent
Former Software Engineer, U.S. Digital Service

Matthew Cutts
Administrator, U.S. Digital Service

Jennifer Daskal
Professor and Faculty Director, Tech, Law and Security Program, American University Washington College of Law
Former Counsel to the Assistant Attorney General for National Security, Department of Justice

Alan Davidson
Vice President of Global Policy, Trust, and Security, Mozilla
Former Director of Digital Economy, Department of Commerce

Ted Dean
Head, Public Policy, Dropbox
Former Deputy Assistant Secretary and Acting Assistant Secretary, International Trade Administration, Department of Commerce

Mikey Dickerson
Executive Director and President of the Board, The New Data Project
Former Administrator, U.S. Digital Service

Michèle Flournoy
Co-Founder and Managing Partner, WestExec Advisors
Former Undersecretary of Defense for Policy, Department of Defense

Mark Forman
Vice President, Digital Government, Unisys Federal
Former Administrator, Office of E-Government and Information Technology, Office of Management and Budget

Kyla Fullenwider
Fellow, Beeck Center for Social Impact and Innovation, Georgetown University
Former Presidential Innovation Fellow and First Chief Innovation Officer, U.S. Census Bureau, Department of Commerce

Victor Garcia
Co-Founder, &Partners
Former Director of Engineering, U.S. Digital Service

Alex Gaynor
Chief Information Security Officer, Alloy
Former Engineer, U.S. Digital Service

Lisa Gelobter
CEO, tEQuitable
Former Chief Digital Service Officer, Department of Education

Sloan Gibson
Former Deputy Secretary, Department of Veterans Affairs
Former President and CEO, United Service Organizations (USO)

John Gilligan
President and CEO, Center for Internet Security
Former Chief Information Officer, Department of the Air Force, Department of Defense
Former Chief Information Officer, Department of Energy

Lindsay Gorman
Fellow for Emerging Technologies, Alliance for Securing Democracy
Former, Office of U.S. Senator Mark Warner and Office of Science and Technology Policy

Zach Graves
Head of Policy, Lincoln Network
Visiting Fellow, National Security Institute, Antonin Scalia Law School, George Mason University

Natalie Evans Harris
Co-Founder and Head of Strategic Initiatives, BrightHive
Former Senior Policy Advisor, Office of Science and Technology Policy, Obama Administration

Josh Hochman
Associate, WestExec Advisors

E.J. Holland, Jr.
Former Assistant Secretary for Administration, Department of Health and Human Services

Mina Hsiang
Head, New Market Development, Devoted Health
Founder and Former Executive Director, Digital Service, Department of Health and Human Services

Eric Hysen
Director, Justice and Opportunity Initiative, Chan Zuckerberg Initiative
Former Executive Director, Digital Service, Department of Homeland Security

Marcy Jacobs
McKinsey and Company
Former Executive Director, Digital Service,
Department of Veterans Affairs

Garrett Johnson
Co-Founder, Lincoln Network
Former Professional Staff to the Ranking
Member, U.S. Senate Foreign Relations
Committee

Thomas Kalil
Chief Innovation Officer, Schmidt Futures
Former Deputy Director for Technology and
Innovation, Office of Science and Technology
Policy

Natalie Kates
Director, New Product Development, Alloy
Former Head of Product, U.S. Digital Service,
Department of Health and Human Services

Patrick Kelley
Executive Vice President, Live Oak Bank
Former Deputy Associate Administrator,
Office of Capital Access, and Former Deputy
Chief of Staff, Small Business Administration

Ann Kim
Former Chief Design Officer for the Office of
the Surgeon General of the United States, U.S.
Department of Health and Human Services
Former Innovator-in-Residence, Department
of Health and Human Services

Chase Kimball
Product Manager, Rebellion Defense
Former Product Manager, U.S. Digital Service

Christopher Kirchhoff
Senior Fellow, Schmidt Futures

David Koh
Co-Founder, Slipstitch LLC
Former Digital Service Expert, U.S. Digital
Service

Eli Lehrer
President, R Street

Mathew Lira
Special Assistant to the President for
Innovation Policy and Initiatives, Office of
American Innovation, The White House

Chris Lynch
Co-Founder, Rebellion Defense
Former Director, Defense Digital Service,
Department of Defense

Alexander MacGillivray
Co-Founder, Alloy
Former Deputy U.S. Chief Technology Officer,
Office of Science and Technology Policy

Arun Majumdar
Jay Precourt Provostial Chair Professor at
Stanford University
Former Director, Advanced Research Projects
Agency-Energy, Department of Energy

Hala Maktabi
Former Director, Enterprise Measurement and
Performance Improvement, Department of
Veterans Affairs

Joshua Marcuse
Former Executive Director, Defense Innovation
Board
Former Innovation Advisor, DOD Chief
Technology Officer, U.S. Department of Defense

Clare Martorana
Chief Information Officer, Office of Personnel
Management
Former Digital Service Expert, U.S. Digital
Service

Jason Matheny
Founding Director, Center for Security and
Emerging Technology (CSET)
Former Director, Intelligence Advanced
Research Projects Activity

Andrew Mayock
Director of U.S. Public Sector Operations,
McKinsey and Company
Former Deputy Director for Management,
Office of Management and Budget

Alejandro Mayorkas
Partner, WilmerHale
Former Deputy Secretary, Department of
Homeland Security

Dave McClure
Principal Director, CIO Advisory Services,
Accenture Federal Services
Former Associate Administrator, Citizen
Services and Innovative Technologies, General
Services Administration

Luke McCormack
Former Chief Information Officer, Department
of Homeland Security
Former Chief Information Officer, Department
of Justice

Denis McDonough
Senior Advisor, Markle Foundation
Former White House Chief of Staff

Andrew McMahon
Partner, Ridgeline
Former Senior Advisor, General Services
Administration

Terrell McSweeny
Partner, Covington & Burling LLP
Former Commissioner, Federal Trade
Commission

Bruce Mehlman
Founder, Mehlman Castagnetti Rosen & Thomas
Former Assistant Secretary, Technology Policy,
Department of Commerce

Victor Mendez
Principal, VM Consulting Group, LLC
Former Deputy Secretary, U.S. Department of
Transportation

Carlos Monje, Jr
Director of Policy and Philanthropy for the
U.S. and Canada, Twitter
Former Acting Undersecretary and Assistant
Secretary for Transportation Policy,
Department of Transportation
Former Chief of Staff, White House Domestic
Policy Council

Andrew Nacin
Director, Infrastructure and Security, Chan
Zuckerberg Initiative
Lead Developer, WordPress
Former Engineer and Senior Advisor, U.S.
Digital Service

Stephanie Neill
Senior Director, Product Management, Amazon
Former Executive Director, U.S. Digital Service

Marina Nitze
Head, Public Interest Technology Child
Welfare Vertical, New America Foundation
Former Chief Technology Officer, Department
of Veterans Affairs

Kerry O'Connor
Chief Innovation Officer, City of Austin
Former Innovation Catalyst, U.S. Department
of State

Jennifer Pahlka
Founder, Code for America
Former Deputy U.S. Chief Technology Officer,
Office of Science and Technology Policy

Ryan Panchadsaram
Former Deputy U.S. Chief Technology Officer,
Office of Science and Technology Policy

Todd Park
Co-Founder and Executive Chairman, Devoted
Health
Former U.S. Chief Technology Officer, Office of
Science and Technology Policy

DJ Patil
Head of Technology, Devoted Health
Former Chief Data Scientist, Office of Science
and Technology Policy

Udaya Patnaik
Co-Founder, Jump Associates

Kathy Pham
Founding Member, Product and Engineering,
U.S. Digital Service

Arthur Plews
User Strategy and Operations, Stripe
Former Chief Innovation Officer, Small
Business Administration

Daniel Portillo
Managing Partner, Sweat Equity Ventures

Dave Powner
Director, Strategic Engagement and
Partnerships, The MITRE Corporation
Former Director, Information Technology
Management Issues, Government
Accountability Office

Jennifer Purdy
Executive Director for Patient Experience,
Veterans Experience Office, Department of
Veterans Affairs

Doug Rand
Senior Fellow and Director, Technology and
Innovation Initiative, Federation of American
Scientists
Former Assistant Director, Entrepreneurship,
Office of Science and Technology Policy

Jeff Ratner
Head, Global Cyber Policy, Apple
Former Director for Legislative Affairs and
Cybersecurity Policy, National Security Council
Former Deputy Chief of Staff, National
Protection and Programs Directorate,
Department of Homeland Security

Anahita Reilly
Former Chief Customer Officer, General
Services Administration

Leon Rodriguez
Partner, Seyfarth Shaw, LLP
Former Director, U.S. Citizenship and
Immigration Services, Department of
Homeland Security

Laura Rosenberger
Director, Alliance for Securing Democracy
Former Chief of Staff, Office of the Deputy
Secretary, Department of State

Shannon Sartin
Former Executive Director, Digital Service,
Centers for Medicare and Medicaid Services,
Department of Health and Human Services

Nick Sinai
Adjunct Faculty, Harvard Kennedy School
Former Deputy U.S. Chief Technology Officer,
Office of Science and Technology Policy

Amber Schleuning
Former Executive Director, VA Center for
Innovation, Department of Veterans Affairs

Ari Schwartz
Managing Director of Cybersecurity Services,
Venable
Former Special Assistant to the President and
Senior Director for Cybersecurity, National
Security Council

Mark Schwartz
Enterprise Strategist, Amazon Web Services
Former Chief Information Officer, U.S.
Citizenship and Immigration Services,
Department of Homeland Security

Tony Scott
CEO, The TonyScottGroup
Former Federal Chief Information Officer,
Office of Management and Budget

Bryan Sivak
Managing Director, KP Ventures and Vice
President, Medicaid Transformation, Kaiser
Permanente
Former Chief Technology Officer, Department
of Health and Human Services

Anne-Marie Slaughter
CEO, New America
Former Director of Policy Planning,
Department of State

Jennifer Smith
Head of Data Acquisition, Alloy
Former Acting Head of People Operations, U.S.
Digital Service

Teresa Takai
Venture Partner, RIDGE-LANE Limited
Partners
Former Chief Information Officer, Department
of Defense

Emily Tavoulareas
Fellow, Digital Service Collaborative, Beeck
Center for Social Impact and Innovation,
Georgetown University

Jennifer Tress
People Operations Leader, State of California
Former Chief of Staff, Technology
Transformation Service, General Services
Administration
Former Director of Talent, 18F

Cyrus Wadia
Head of Sustainable Product, Amazon
Former Assistant Director, Clean Energy and
Materials Research and Development, Office
of Science and Technology Policy

Traci Walker
Director, Digital Service Procurement, U.S.
Digital Service

Sabrina Williams
Former Director of Engineering, U.S. Digital
Service

Jetta Wong
President, JLW Advising
Founding Director, Office of Technology
Transitions, Department of Energy

Nicole Wong
Senior Advisor, Albright Stonebridge Group
Former Deputy U.S. Chief Technology Officer,
Office of Science and Technology Policy

Charles Worthington
Chief Technology Officer, Department of
Veterans Affairs

Cori Zarek
Director, Digital Service Collaborative, Beeck
Center for Social Impact and Innovation,
Georgetown University
Former Deputy U.S. Chief Technology
Officer, White House Office of Science and
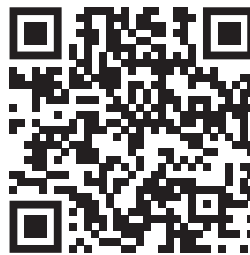Technology Policy

PARTNERSHIP
FOR **PUBLIC SERVICE**

partnershipforpublicservice

@RPublicService

rpublicservice

To learn more about this project, visit:
ourpublicservice.org/publications/tech-talent/