Preliminary Concept Paper

Provisioning Digital Tools and Systems for Government Use

REDESIGNING THE GOVERNANCE STACK
GEORGETOWN LAW

Preliminary Concept Paper

Provisioning Digital Tools and Systems for Government Use

SEPTEMBER 2024

Julie E. Cohen

Brenda Dvoskin

Nina-Simone Edwards

Meg Leta Jones

Paul Ohm

Smitha Krishna Prasad

Co-signers*:

Kenneth Bamberger

Elana Zeide

---

*The ideas in this concept paper were developed in part through workshops held with academics and regulators. Some of the attendees have decided, as well, to co-sign the paper. Although not every one of the co-signers agrees with every idea set forth below, each supports the proposals overall. In addition to the co-signers, we would like to thank Aaron Snow, Alicia Elizabeth Boyd, Alicia Solow-Niederman, Cynthia Khoo, danah boyd, David Zvenyach, Dominic Campbell, Elana Judith Zeide, Emily Tavoulareas, Hannah Bloch-Wehba, Harlan Yu, Hilary Allen, Kenneth Bamberger, Laura Moy, Mason A. Kortz, Michael Veale, Michelle Gilman, and Solon Barocas for their participation in the academic workshop, and their constructive and generous feedback. This work was developed with the support of the Tech & Public Policy program at the McCourt School of Public Policy at Georgetown University, the Fritz Family Fellowship at Georgetown University, the Ford Foundation, the Reset Foundation, and the Economic Security Project.

Executive Summary

This document is part of a larger project aimed at reinventing the administrative state for effective governance of the digital, information-driven economy. It explores how the administrative state can more effectively equip itself with digital tools and systems that align with and improve government's ability to serve public values.

Established approaches to digital provisioning fail in many important respects. Among others, they introduce thorny coordination problems while doing little to ensure design for broader public values; they cause obsolete and/or poorly conceived requirements to cascade through the development process for new tools and systems; they magnify the potential for technology-driven lock-in and vendor capture at scale; and they are unacceptably opaque to policymakers and the public. We trace some of these dysfunctions to the private-sector preference that underpins federal govtech provisioning and others to a top-down mode of development in which "solutions" are decreed at the outset rather than after consultation and conversation.

The paper recommends a series of changes to the current policy landscape for govtech provisioning to correct these dysfunctions. One important recommendation involves rethinking the traditional "make vs. buy" dichotomy in public procurement and the underlying presumptions that have animated the dichotomy. Recentering public values and outcomes in govtech development also requires measures for ensuring the interoperability and transparency of govtech tools and systems. Another important recommendation involves reenvisioning processes for govtech development and implementation. Generally speaking, the best way to ensure that govtech tools and systems serve desired outcomes while minimizing harmful effects is to engage in a robust design phase that involves consultation with multiple stakeholder groups, to consider the full lifecycle of the envisaged system, and to engage in ongoing monitoring and assessment throughout the lifecycle. A good process, however, will also avoid development "waterfalls," incorporating flexibility to revisit and revise plans and technical specifications as design and implementation progress.

To support these policy changes, the paper recommends improved support and coordination for five important govtech-related functions and proposes corresponding changes to institutional structure and organization. Additionally, it emphasizes the need to bolster technical capacity within government by developing a pipeline of specialized, govtech-related training programs, curricula, and fellowships.

Introduction

Increasingly, agencies are turning to digital methods to improve efficiency and facilitate provision of services at scale. Within the federal government, however, those efforts have been hobbled by coordination problems, by the statutorily encoded preference for procurement from the private sector, and by a variety of downstream effects that flow from those two problems. As a result, challenges in addressing, upholding, and even identifying (often competing) public values arise across the lifecycle of such tools and systems.

Meanwhile, governments around the world are no longer simply using existing or available technology but instead are focused on commissioning and/or developing govtech: technologies and systems designed for and around government priorities and needs. This paper adopts that focus and terminology and considers what effective processes for provisioning govtech— processes that put public needs and values first—should look like.

The ideas in this concept paper were developed in part through workshops held with academics and current or former government officials. As with other modules in this project, we first workshopped our ideas in a draft that received significant edits from subject matter experts. We then presented the revised draft to people with experience in government for another round of feedback. Following those in-person meetings, revised drafts were circulated and re-circulated to members of those groups for their additional comments. While the ideas we propose in this concept paper are ours, they are grounded in the input received from the two groups of experts.

Part 1 provides an overview of the existing institutional landscape for govtech provisioning within the federal government. Part 2 identifies some important ways in which existing arrangements do not work well for govtech. Part 3 describes changes to the policies underlying current govtech provisioning arrangements that are necessary to address the dysfunctions described in Part 2. Part 4 proposes corresponding shifts in institutional structure and organization. Our primary goal is to elucidate what the administrative state needs to do its job. At this stage, we are less concerned with how that might affect operational costs or how these proposals might be challenged under current law.

Part 1: Existing institutional arrangements for govtech provisioning

Multiple offices both within specific agencies and elsewhere play roles relating to govtech provisioning. These arrangements are not the results of comprehensive planning, but rather have emerged piecemeal over the course of decades. In this section we review existing institutional arrangements and highlight some of their gaps and overlaps.

Agency-driven provisioning

Individual agencies drive the vast majority of provisioning activity for digital tools and systems. For decades, most digital tools and systems used by federal government agencies have been developed and maintained by vendors and consultants pursuant to long-term contracts negotiated with agency procurement teams. More recently, agencies are beginning to develop increasing numbers of digital tools and systems in-house.[1] In recent years federal hiring policies have been amended to allow for more flexibility in pay and focus on skill-based hiring qualifications.[2] However, in-house development capabilities are uneven across agencies. Experts note that larger agencies are increasingly building their own teams of technologists, but smaller agencies do not necessarily have such capacity, even if the work they undertake is critical.

Leadership arrangements for technology-related activities within agencies vary. Currently, some agencies have Chief Technology Officers (CTOs) who are generally responsible for selecting or developing digital tools and systems that can be harnessed to improve the agency's performance. In agencies that do not have CTOs, the Chief Information Officer (CIO) oversees provisioning of technology ranging from desktop and laptop computers to software licenses to tools and systems developed specifically for the agency's use. By default, the CIOs in those agencies also make decisions about maintenance, upgrades and, as needed, termination of particular digital tools and systems. In agencies that have both CTO and CIO roles, the CTO typically reports to the CIO; in a few cases, the roles are merged. Agencies are also in the process of appointing Chief AI Officers, as prescribed by the Biden Administration's Executive Order on AI. While there is no structure prescribed as yet for this office, agencies must ensure that the Chief AI Officer is "positioned highly enough" to engage with other leadership at the agency.[3] Agencies have flexibility to appoint existing officials, such as CTOs, as their Chief AI Officers.

1 For one useful recent review of agency activities involving artificial intelligence and machine learning technologies, see Admin. Conf. of the U.S., Appendix, Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies (2020) (coding for whether projects were procured from a commercial contractor, developed via a non-commercial collaboration, or developed in-house).

2 Executive Order 13932 of June 26, 2020, Modernizing and Reforming the Assessment and Hiring of Federal Job Candidates; Jory Heckman, *VA CIO: 'Historic' pay raise coming for IT workforce, as Special Salary Rate goes into effect in July*, Federal News Network (July 10, 2023), **https://federalnewsnetwork.com/pay/2023/07/va-cio-historic-pay-raise-coming-for-it-workforce-as-special-salary-rate-goes-into-effect-in-july/**; Jason Miller, *OMB tells agencies to target the use of special salary rate*, Federal News Network (December 15, 2023), **https://federalnewsnetwork.com/pay/2023/12/omb-tells-agencies-to-target-the-use-of-special-salary-rate/**.

3 Off. Of Mgmt. & Budget, Exec. Off. Of the President, OMB M-24-10, Memorandum on Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence 8 (2024).

People with experience in government note that in practice, CIOs often come from a sales or business background in private industry, resulting in both lack of technical expertise and a significant revolving door problem. Hiring practices for CTOs do prioritize technical expertise, but CTO positions generally are not statutorily required positions. As a result, CTOs may have the power that comes with political backing while lacking statutory authority within the agency. There is also considerable turnover in CTO appointments with changes in political leadership.

Specialized (government consultancy-based) provisioning

Two specialized entities created during the Obama Administration focus on govtech provisioning: the US Digital Service (USDS), which is housed within the Office of Management and Budget (OMB) in the Executive Office of the President, and 18F, which is part of the office of Technology Transformation Services (TTS) in the General Services Administration (GSA). Both offer govtech-related services to other agencies on an ad hoc basis. The USDS works on the basis of priorities set by the administration in the White House, while 18F offers its services directly to agencies on a cost-recovery basis. Both entities work primarily to develop public facing tools and systems, although they have also assisted with procurement of public facing tools and systems from external vendors and consultants. Both also publish guidance documents on IT acquisition and development.

Experts note that, originally, both USDS and 18F were envisioned as temporary measures that could be dissolved as agencies developed the capacity to fulfill their own govtech development needs. Instead, both entities have grown considerably in size and scope.

There is considerable overlap in the work that USDS and 18F undertake, potentially leading to duplication of work and provision of conflicting guidance to agencies. Additionally, particularly in their early years, cultural differences between the technical teams at USDS and 18F and practices at existing federal agencies created friction. More recently, both entities have worked more carefully with agency CIOs and staff to ensure that the agencies' needs are met. In response to recommendations from the Government Accountability Office (GAO), USDS and 18F also have established more formal mechanisms for coordination.[4]

Loose coordination via OMB, GSA, and NIST

The Office of Management and Budget (OMB), General Services Administration (GSA) and the National Institute of Standards and Technology (NIST) play different roles in planning, coordination, and oversight of agency activities relating to digital tools and systems. Each has a different mandate that both informs and constrains the task of govtech provisioning.

The OMB establishes overarching federal policies on IT procurement and government IT modernization. The point person for those efforts is the Federal Chief Information Officer (FCIO), who leads the Office of E-Government and Information Technology. Together with other OMB officials and the GSA's CIO, the FCIO also leads the Council of Chief Information Officers (CIO Council), an interagency forum comprised of agency CIOs that works to develop and coordinate best IT practices among federal agencies. Through the CIO Council, agency CIOs address practices including design, development, acquisition, use, and sharing of technologies and information.[5] Among other things, the CIO Council's functions include developing rec-

4 U.S. Gov't Accountability Off., Gao-24-106693, Information Technology: Federal Agencies Are Making Progress in Implementing GAO Recommendations 10 (2023) [hereinafter GAO Information Technology Recommendations].

5 Fed. Chief Info. Officers Council Charter 2 (2010).

ommendations for OMB on federal government IT management practices; assisting the FCIO in identifying, coordinating and developing multi-agency projects; and promoting interagency information sharing.

The GSA provides centralized procurement services for the federal government, covering everything from office buildings to desk chairs and staplers. It has implemented a "category management infrastructure" to provide agencies with some information vendor management, covering such matters as common contracting options and contracting with small businesses.[6] In the context of digital technology, it helps agencies comply with the OMB's policy directives and, more generally, assists agencies with developing digital strategies. The GSA has multiple offices that deal with different aspects of govtech development and implementation. These include: the Office of Technology Policy (OTP), which facilitates agency implementation of government-wide information technology policies; the IT Modernization division, which provides agencies with support and guidance for cloud strategy and datacenter optimization; and the Technology Transformation Services (TTS), which provides a range of services to help agencies use modern applications and platforms; and, most recently, the GSA Centers of Excellence, which are tasked to "leverage[] commercially available solutions and expertise from industry to deliver enterprise transformation initiatives" involving particular kinds of digital technologies and services.[7]

Agency work involving technical standards requires additional coordination with NIST. NIST operates pursuant to a statutory mandate to promote development of voluntary consensus standards through engagement with the private sector.[8] Federal agencies are expected to participate in standards development activities and to ensure that appropriate standards are incorporated in their programmatic activities and their procurement and development of digital tools and systems. Unless the use of such standards would be inconsistent with applicable law or otherwise impractical, agencies are required to use voluntary consensus standards identified by NIST.[9] Government unique standards can be developed and used in limited circumstances when no other appropriate standards exist. In such cases, the agency must submit a report to the OMB through NIST describing the reasons for the use of government unique standards.[10]

Oversight by the GAO and agency inspectors general

Federal agencies are subject to oversight by the Government Accountability Office (GAO) and by agency-specific Inspector General (IG) offices. The GAO investigates agency expenditures and provides recommendations on economy and efficiency in government spending. With regard to govtech more specifically, it investigates whether those managing procurement initiatives or developing technologies in-house have followed prescribed processes and standards. It also resolves bid protests that are filed against agency procurement actions. Agency IGs typically are charged with detecting and preventing fraud, abuse and waste within agencies and promoting efficiency, economy and effectiveness of agency operations. They conduct internal audits and investigations, make recommendations, and report to Congress and the head of the agency about any problems.

---

6 *See Category Management*, U.S. Gen. Services Admin., **https://www.gsa.gov/buy-through-us/category-management** (last visited Aug. 27, 2024).

7 *See The Centers of Excellence*, U.S. Gen. Services Admin., **https://www.gsa.gov/about-us/organization/federal-acquisition-service/technology-transformation-services/the-centers-of-excellence** (last visited July 23, 2024).

8 15 U.S.C. § 272.

9 Off. Of Mgmt. & Budget, Exec. Off. Of the President, OMB Circular No. A-119, Memorandum on Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities 7 (1998) [hereinafter OMB Consensus Standards].

10 *Id.* at 7-8. NIST also oversees reporting on agencies' self-assessment of conformity with various requirements contained in standards, prescribed by law, or established by agencies themselves via procurement actions or as programmatic policy.

Part 2: Why existing provisioning arrangements fail for govtech

Digitalization of government functions promises significant benefits but also poses significant risks. The institutional arrangements for govtech provisioning are enormously important to determining the extent to which both benefits and risks will materialize. Here, we focus on six dysfunctions that loom especially large in the current landscape: coordination problems resulting from institutional overlaps, private-sector preferencing and its downstream effects, technology-driven lock-in and capture, opacity to policymakers and the public, disparate impacts and other unintended consequences, and accountability overload. To be clear, current institutional arrangements do not create all of these problems. Some would exist in any institutional configuration—official activities undertaken at scale inevitably create path dependencies of one sort or another and produce some unintended effects. Current arrangements, however, magnify these risks and create other, enormously significant obstacles to effective govtech provisioning that serves public values.

Coordination problems

The institutional arrangements described in Part 1 involve significant overlaps in responsibility for govtech-related policymaking and policy implementation. This, in turn, has necessitated increasingly elaborate coordination structures. People with experience in government note that, in practice, the current arrangements have produced blurred lines, confusion, and diffusion of responsibility. The GAO concurs with this assessment.[11]

Ideally, institutional overlaps should make the federal government more resilient, ambitious, and effective for the public. Political units can encourage technical areas of government to set more ambitious goals. Properly designed oversight processes can function as feedback loops to improve outcomes recursively and minimize the impacts of failure. The challenge is to create an institutional structure that (mostly) encourages these types of positive interactions while (mostly) avoiding the negative ones.

Current institutional arrangements for govtech provisioning fall far short of this vision. Dysfunctional coordination processes produce predictable results. Some problems are horizontal. To take one small example, meetings involving staff from multiple agencies are hard to schedule because the federal agencies do not share a common calendaring system and the systems in use are not interoperable. As another example, there are multiple different "official" systems in use for filing public records requests under the Freedom of Information Act. Other problems are vertical, causing obsolete and/or poorly conceived requirements to cascade through the development process for new tools and systems.[12] We discuss some examples in the sections below.

11 The GAO observed that without coordination, the similar activities of USDS and 18F "risked overlapping or duplicating their efforts or presenting conflicting information . . . ." GAO Information Technology Recommendations, *supra* note 3, at 9.

12 *See* Security Design Collective, Inc., Security & the Federal Risk Management Framework (2023), available at **https://www.servicedesigncollective.com/wp-content/uploads/2023/09/Security-the-Federal-Risk-Management-Framework.pdf.**

The private-sector preference and its downstream effects

Few would dispute that government should use its resources efficiently. Efficiency, however, can have many meanings. Govtech provisioning unfolds within constraints created by a particular vision of government efficiency that revolves around procurement from the private sector.

Since 1979, GSA has operated pursuant to statutory mandates to procure needed resources from private sector suppliers.[13] Guidance issued by OMB and administered by OMB's Office of Federal Procurement Policy instructs that agencies may develop their own products or services only where they perform an "inherently governmental function" (IGF).[14] Similar reasoning underlies NIST's mandate to work with industry to identify voluntary consensus standards, which dates to 1998, and the consequent requirement that development and use of government unique standards be justified and documented.[15]

In many contexts, including some digital technology contexts, the private-sector preference is sensible. There is no reason, for example, for the government to manufacture office furniture or personal computers. The private-sector preference, however, runs more deeply than such common-sense observations and is culturally and ideologically ingrained. It is grounded in two propositions: first, that government cannot innovate (and should not be trusted to try) and, second, that "government should not compete with its citizens." [16] As a historical matter, the former proposition is incorrect and the latter considerably oversimplified. Foundational contemporary technologies owe their origins to government research and development programs, and such programs can fuel markets and competition rather than crowding them out.[17] More specifically, govtech tools and systems implicate a broad range of public values, including both particular, substantive policy goals and more general goals of fairness and inclusiveness in access to government services. For govtech, at least, supply decisions should not be so heavily predetermined.

The most glaring downstream effect of the private-sector preference is the "make or buy" binary that structures govtech provisioning. The buy side is preeminent and elaborately proceduralized in ways that position vendors and consultants, rather than the public, as the most important customers.[18] Typically, metrics in place to assess the efficacy of procurement processes have focused narrowly on procedural accountability in the context of bidding or contracting processes.[19] The make side, meanwhile, has been systematically starved of resources. More recent efforts to create capacity for government consultancy-based technology provisioning via 18F and USDS

---

13 *See, e.g.*, The Office of Federal Procurement Policy Act Amendments of 1979, Pub. L. No. 96-83, §6(c), 93 Stat. 648, 649 (1979); The Clinger-Cohen Act of 1996, Pub. L. No. 104-106, tit. xxviii, §2836, tit. xxxiv, § 3412, tit. li, §5101,, tit. liv, §5401, tit. lvii, §5702 (1996).

14 Off. Of Mgmt. & Budget, Exec. Off. Of the President, OMB Circular No. A-76, Memorandum on Performance of Commercial Activities 2 (1983) [hereinafter OMB Commercial Activities].

15 OMB Consensus Standards, *supra* note 7, at 7, 14.

16 OMB Commercial Activities, *supra* note 11, at 1; *see also* Jennifer Pahlka, Recoding America: Why Government is Failing in the Digital Age and How We Can Do Better 101-07 (2023). *See generally Jodi Short, Regulatory Managerialism as Gaslighting Government*, 86 L. & Contemp. Probs. 1, 9-12 (2023) (discussing the import of business management techniques into regulatory domains, including nuanced theories of competition and outsourcing, that form an anti-administrative ideology).

17 *See* Janet Abbate, Inventing the Internet 2 (1999); Mariana Mazzucato, The Entrepreneurial State: Debunking Public vs. Private Sector Myths 69-85 (2013).

18 *See, e.g.*, The Office of Federal Procurement Policy Act Amendments of 1979, Pub. L. No. 96-83, 93 Stat. 648, 649 (1979); The Competition in Contracting Act of 1984, 41 U.S.C. § 253 (1984); 10 U.S.C. § 3451 et seq. (1994); 48 C.F.R. § 1.102 (1995); 60 Fed. Reg. 34733 (1995); Clinger-Cohen Act of 1996, 40 U.S.C. § 11101 et seq. (1996); 40 U.S.C. § 501 (2002).

19 *See id.*

have achieved high visibility but have not meaningfully altered a decades-long imbalance.

A subtler downstream effect of the private-sector preference relates to the processes of govtech design and implementation. Without sufficient guidance both at the outset and throughout the design and implementation processes, systems designers may tend to prioritize formal compliance with written requirements and short-term cost reductions over more general concerns such as efficacy or fairness.

Technology-driven vendor lock-in and capture at scale

Procuring govtech tools and systems from private-sector vendors and consultants can engender a modern form of capture that flows from privileged access to the technical specifications of important tools and systems. Unlike more traditional forms of capture—such as successful rent-seeking by influential lobbyists or the intellectual capture produced by the revolving door between government and industry—technology-driven capture is less visible and more insidious.

Govtech procurement contracts can layer proprietary systems directly into the public machinery of government. In particular, the push toward interoperable systems, the shift toward cloud-based configuration of computing resources, and the preference for vendors with relevant experience all drive toward awarding contracts to repeat players with significant industry power. This may make government dependent both on particular, proprietary technologies and on the resources and expertise of particular companies.[20] All of these services come with high price tags, including some set by dominant market actors without much competition. Millions of taxpayer dollars are being directed to particular vendors, and due to technology-driven lock-in, these fees will be paid for years or decades to come. The chosen vendor or consultant, selected in part because of already-existing government dependence on that vendor's systems or other specialized technical expertise, will have privileged access to government data. Meanwhile, government employees will organize workflows and other programmatic activities around the company's standards, technical approaches, and tool suites. Vendors or consultants that provide suites of products and services across multiple agencies can engage in capture at scale. The resulting configurations can be expensive or impossible to uproot, creating lock-in on an infrastructural level.

Opacity to policymakers and the public

Govtech tools and systems can incorporate multiple layers of opacity. The private-sector preference and technology-driven lock-in exacerbate these effects and introduce new ones.

One kind of opacity is inherent to all digital tools and systems that rely on machine learning to produce recommendations and results. The operations of such processes—and particularly the reasons for the recommendations and results they produce—can be difficult or even impossible to explain in cause-and-effect terms.[21] Although some vendors publish performance metrics for their systems, experts note that such metrics tend not to convey useful information.

---

20 *See, e.g.*, Mariana Mazzucato & Rosie Collington, The Big Con: How the Consulting Industry Weakens Our Businesses, Infantilizes Our Governments And Warps Our Economies (2023) (describing the perils of an overreliance on consultants which include an increasing lack of knowledge); Eric Geller, *The US Government Has a Microsoft Problem*, Wired (April 14, 2024), **https://www.wired.com/story/the-us-government-has-a-microsoft-problem/**; April Glaser, *Thousands of Contracts Highlight Quiet Ties Between Big Tech and U.S. Military*, NBC NEWS (July 8, 2020), **https://www.nbcnews.com/tech/tech-news/thousands-contracts-highlight-quiet-ties-between-big-tech-u-s-n1233171**.

21 *See generally* Andrew D. Selbst & Solon Barocas, *The Intuitive Appeal of Explainable Machines*, 87 Fordham L. Rev. 1085 (2018); Jenna Burrell, *How the machine 'thinks': Understanding opacity in machine learning algorithms*, 3 Big Data & Soc'y 1 (2016).

A different kind of opacity involves the absence—or, sometimes, the deliberate withholding—of essential technical documentation. When such tools and systems are procured from vendors, staff within government agencies and departments too often find themselves unable to fully understand how they work or even access necessary documentation. This compromises their ability to use, maintain, update, and, as appropriate, request changes to such technologies and/or to policies surrounding their operation.[22] Even when digital tools and systems are developed in house, agency staff and members of the public that must use them may have similar difficulties.

A third kind of opacity relates to procurement processes. Information about vendors and their systems typically is not widely available to the public or even to agencies themselves.[23] As noted in Part 1, the GSA's category management infrastructure provides agencies with some information about vendors and contracting options. In practice, however, the relationships between agencies, on one hand, and vendors and consultants, on the other, tend to involve pronounced information asymmetries. Experts note that agencies often lack detailed information regarding past work undertaken by the vendors or consultants placing bids. Too often, the only source of information is what has been provided by the bidders themselves, and their disclosures are too limited and vague to provide the information the agencies need. So, for example, one agency may not even be aware that another agency has procured a similar system from vendor XYZ and has faced problems in implementation or operation, and, if it is aware, it may not have good information about the problems, the vendor's behavior generally, or the terms of the arrangement.

The multiple, overlapping varieties of opacity surrounding govtech tools and systems makes it more difficult to understand and, as necessary, change the government processes that the tools or systems are intended to implement. They can delay or prevent entirely detection of mistakes, disparate impacts, and other unintended consequences. They can thwart efforts to develop opportunities for participation in policymaking, permitting, and enforcement proceedings by affected publics. And they can provide cover for waste, abuse, and fraud, fueling distrust.

Disparate impacts and other unintended consequences

Govtech systems can engender a range of unintended consequences, some of which may undermine government's ability to serve public needs effectively.

One important category of unintended consequences involves disparate impacts on citizens and communities who are differently situated. As adoption of govtech systems becomes increasingly pervasive, such systems determine who in a society can access vital services and to what extent. Features and capabilities that make some things easier for some people to do may make the same things harder or less intuitive for others. Systems built to serve underserved populations may have unintended effects on those populations. Other systems built for general use may affect different citizens and communities differently for reasons relating to their design, their implementation, or both. Such outcomes undermine the government's ability to set and pursue public-regarding policy goals in ways that serve all citizens and communities.[24]

Another important category of unintended consequences involves function creep. Modern technological systems are designed to be modular and extensible in ways that

22 *See, e.g.*, Deirdre Mulligan & Kenneth Bamberger, *Procurement As Policy: Administrative Process for Machine Learning*, 34 Berkeley Tech. L. J. 781, 795-96, 808-09, 821-22 (2019); Danielle Keats Citron, *Technological Due Process*, 85 Wash. U. L. Rev. 1249, 1279-81 (2008).

23 *See, e.g.*, Robert Brauneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City*, 20 Yale J. L. & Tech. 103, 109-10, 116-17 (2018); Hannah Bloch-Wehba, *Transparency's AI Problem*, Knight First Amend. Inst., (June 17, 2021), **https://knightcolumbia.org/content/transparencys-ai-problem.**

24 *See, e.g.*, Mulligan & Bamberger, *supra* note 20; Citron, *supra* note 20.

allow for expansions of scope and use. On the one hand, this seems to build beneficial flexibility and resilience into the system. On the other hand, when a tool or system is extended to a context or use other than the one for which it was originally deployed, the policies and processes that informed its creation may not translate well, and safeguards intended to constrain its use may be less effective.[25]

Self-defeating constraints and compliance doom loops

It is useful to frame the process of govtech provisioning in terms of competing tensions that must be navigated successfully if the project of digitalizing government consistent with public values is to succeed. Generally speaking, the best way to ensure that govtech tools and systems serve desired outcomes while minimizing harmful effects is to engage in a robust design phase that involves consultation with multiple stakeholder groups, to consider the full lifecycle of the envisaged system, and to engage in ongoing monitoring and assessment throughout the lifecycle. For this to work well, the process must be iterative and incorporate a degree of flexibility to revisit earlier stages and interrogate technical specifications and constraints.

Currently, however, it is far more usual to see govtech development processes reduced to rigid schematics involving sets of prescribed choices that are heavily constrained. One influential critique refers to this approach as the "waterfall" mode of development.[26] Experts are clear that this approach—in which "solutions" are decreed at the outset, rather than after consultation and conversation—is counterproductive.

To similar effect, it is a truism that government should be accountable to the public, but poorly designed accountability mechanisms can have pernicious effects. On one hand, oversight and accountability processes may be reduced to perfunctory checklists that do little to advance underlying policy goals. On the other, they can become bureaucratic nightmares, requiring devotion of substantial effort and time in ways seemingly untethered from underlying policy goals and, in the worst cases, becoming self-reinforcing doom loops that frustrate efforts to serve important public goals.

The Federal Enterprise Architecture Framework (FEAF) is a useful example of the dysfunctions that an overly rigid approach to the govtech development process can produce. Created by the CIO Council in 1999 and updated in 2012, the FEAF is intended to promote a common approach to developing and maintaining enterprise architectures.[27] It lays out progressively more specific sets of requirements to be met for systems performing different types of functions. The Department of Defense requires its vendors to adhere to an enterprise architecture framework derived from the FEAF. As a result, the developer team tasked by the Air Force with updating the data transmission system used by GPS satellites was required to use an outdated mechanism called an enterprise service bus (ESB), which would slow data transmission significantly. The vendors encountered delays as they attempted, unsuccessfully, to build a state-of-the-art system that could provide data transmission at the rates required by the system's control stations while still routing the data through the ESB. The satellites were eventually launched without the software updates.[28]

---

25 *See e.g.*, Paul W. Grimm, Maura R. Grossman & Gordon V. Cormack, *Artificial Intelligence As Evidence*, 19 Nw. J. Tech. & Intell. Prop. 9, 51–52 (2021) ("COMPAS was originally designed for assessing the treatment needs of offenders, but its use morphed . . . despite its lack of validation for the additional purposes."); *see also* Blagovesta Kostova, Seda Gurses & Carmela Troncoso, *Privacy Engineering Meets Software Engineering. On the Challenges of Engineering Privacy By Design*, arXiv:2007.08613, **https://arxiv.org/abs/2007.08613** (discussing current software development's heavy reliance on standardized service architectures and development methods and the necessity of understanding those architectures for future research).

26 Pahlka, *supra* note 14, at 58-60.

27 Off. Of Mgmt. & Budget, Exec. Off. Of the President, Federal Enterprise Architecture Framework Version 2 (2013).

28 Pahlka, *supra* note 14, at 78-82, 88-94.

A different example illustrates both the coordination problems that current institutional arrangements create and the powerful downstream effects of the private-sector preference. Login.gov is a GSA service that provides online identity verification services to participating government agencies. When login.gov was developed, the relevant NIST standard (SP 800-63-3) on secure identity verification required the use of biometric or physical comparison, with facial recognition technologies (FRT) as the mechanism for remote verification. OMB, for its part, had issued a memorandum requiring federal agencies to implement shared federally or commercially provided identity authentication services in a manner compliant with the NIST standard.[29] Due to equity and accuracy concerns about the use of FRT, the TTS-based developers of login.gov chose not to incorporate the biometric comparison method called for by the standard. The IG at the GSA then initiated an investigation, which culminated in a report stating that login.gov's services were not compliant with NIST standards.[30] Meanwhile, NIST was preparing to update the secure identity verification systems precisely because of the equity and accuracy concerns that critics had raised.

In this situation, it is clear that each of the actors prioritized different values. The login.gov development team prioritized the most up-to-date research regarding equity and accuracy concerns about FRT.[31] NIST eventually responded to the same research, but far more slowly and only after academic and civil society researchers had raised a persistent drumbeat of criticism. The IG at the GSA focused on procedural and contractual compliance, and GSA focused on responding to the IG's report. Following the investigation, GSA worked to make commercially provided, FRT-based identity verification available to customer agencies, and many agencies elected to license the technology and offer it to the public. Some agencies, however, may not have carefully considered the implications of using this controversial technology. And citizens presented with the choice between login.gov and FRT-based commercial identity verification may not have understood the implications of that choice.

---

29 Off. Of Mgmt. & Budget, Exec. Off. Of the President, Omb M-19-17, Memorandum on Enabling Mission Delivery Through Improved Identity, Credential, and Access Management (2019).

30 *See GSA Misled Customers on Login.gov's Compliance with Digital Identity Standards*, U.S. Gen. Services Admin (March 7, 2023), **https://www.gsaig.gov/content/gsa-misled-customers-logingovs-compliance-digital-identity-standards.**

31 *See generally* Joy Buolamwini & Timnit Gebru, G*ender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proc. Machine Learning Res. 77 (2018).

Part 3: Policy changes for effective govtech provisioning

This Part describes changes to the policies underlying current govtech provisioning arrangements that are necessary to address the failures described in Part 2. The proposals range from finely detailed fixes to less specific shifts in focus or approach.

Dethroning the private-sector preference and deemphasizing "make vs. buy"

Too often in govtech provisioning, the "make vs. buy" decision presents a consequential and early fork in the road. Each choice subjects a project to very different processes and documentation requirements, which in turn distract from and mask the issues the two pathways have in common.

As Part 2 explained, the root causes of this distortion are the statutorily mandated private-sector preference and the undue weight given to whether the particular product or service being provisioned performs an inherently governmental function. The private-sector preference and the IGF construct are ill-suited to the complexity and interconnectedness of govtech. We suggest that the statutory requirement to procure needed resources from the private sector be amended to specify a different approach for govtech. Even absent legislation, we suggest replacing the IGF construct with a broader test focusing on "inherent public values" or "inherent public interests" and specifying that, before deciding whether to make or to buy and before receiving input from vendors or consultants, public officials should engage in lifecycle planning focused on public values and needs. This would entail a broad evaluation of the impacts the product or service will have, the cross-service complexities it may engender, and the infrastructural dependencies it will entail.

Public values and needs also should carry greater weight in choices about technical standard-setting. Government involvement in standard-setting is a topic that lies mostly outside the scope of this module of our project. For govtech, however, the requirement to use voluntary consensus standards should be replaced with a less stringent requirement that voluntary consensus standards be considered and departures from them documented and explained.

Avoiding vendor lock-in and capture at scale through managed interoperability

Part 2 noted that vendor lock-in is a pressing concern in govtech provisioning. Experts note that winning bidders too often become privileged incumbents simply because of their prior experience with similar contracts. One way to prevent such lock-in is to evaluate incumbents using an enhanced set of criteria, including technical performance, achievement of desired outcomes, avoidance or mitigation of harmful impacts, and responsiveness to needs for monitoring and assessment. Another small step would be to do away with the sometimes explicit presumption that contracts will be renewed and to build explicit requirements for transition planning into agency RFPs. Forcing vendors and consultants to win each new contract on equal footing with competitors and to plan for the eventuality of handoff will enhance accountability and transparency.

As Part 2 explained, a significant and rising concern in the context of complex digital technologies is the emergence of large-scale, platform-based, "enterprise architecture" services that provide a full stack of interdependent components. Selecting one such component may reduce

an agency's future freedom to choose another vendor's products or services. Technology built by in-house teams will not necessarily avoid the problem of infrastructural dependency. Even if rules or policies prioritize building systems that are modular and interoperable with multiple platforms, it is hard to build a sophisticated technical system today without relying at least in part on a specific cloud computing provider's infrastructure.

At least in the near term, it is unrealistic to think the government can replicate the entire infrastructural stack, so a more realistic near-term goal is to build certain linchpin components of govtech infrastructure in-house and to mitigate the risk of lock-in through forced interoperability and modularity requirements. Agencies can build these requirements into their charges to in-house development teams and their RFPs. (The success of this approach also depends on access to technical specifications, which we discuss next.)

A longer term digital strategy for government, however, must include development of a wider array of digital public infrastructure. One first step might involve assessing common infrastructural needs that cut across different government agencies and govtech functions. Another might involve studying similar efforts now being undertaken around the world.[32]

Ensuring transparency to policymakers and the public

Other policy changes should address the transparency deficits that Part 2 identified.

A large and growing literature describes best practices for addressing the explainability and technical documentation issues described in Part 2, and policymakers can draw upon this literature to specify documentation and disclosure requirements and any related design requirements for govtech tools and systems.[33] During lifecycle planning, in-house teams should document the technical choices they make and the reasons for those choices. Where tools, systems, or components will be procured from vendors or consultants, transparency requirements should attach at the bidding stage and should be nonnegotiable requirements for a contract award. For example, bidders should be required to provide complete and sufficiently detailed answers to the following questions:

- How do automated, algorithmically-driven components of the product or service work? Vendors and consultants should be required to supply meaningful explanations of the processes and operations that shape outputs and outcomes.
- How were automated, algorithmically-driven components of the product or service trained?

32 See Jonathan Marskell, Georgina Marin and Minita Verghese, *Digital Public Infrastructure: Transforming Service Delivery Across Sectors*, in Digital Progress and Trends Report 2023, World Bank (2023), **https://www.worldbank.org/en/publication/digital-progress-and-trends-report**; Frank Nagle, *Digital infrastructure is more than just broadband: What the US can learn from Europe's open source technology policy study,* Brookings Institute (November 9, 2021), **https://www.brookings.edu/articles/digital-infrastructure-is-more-than-just-broadband-what-the-u-s-can-learn-from-europes-open-source-technology-policy-study/**; Steven Vaughan-Nichols, Switzerland now requires all government software to be open source, ZDNET (July 23, 2024), **https://www.zdnet.com/article/switzerland-now-requires-all-government-software-to-be-open-source/**

33 *See generally,* Selbst & Barocas, *supra* note 19; Burrell, *supra* note 19; Tal Zarsky, *The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making*, 41 Sci. Tech. & Hum. Values 118 (2016); Finale Doshi-Velez & Been Kim, *Towards a Rigorous Science of Interpretable Machine Learning*, arXiv:1702.08608 (Mar. 2, 2017), **https://arxiv.org/abs/1702.08608**.

- Is any part of the product or service an opaque "black box" to the bidder, and if so, why is the use of this part justified? There should be a strong presumption against incorporation of black box functionalities sourced from third parties.
- Does any part of the product or service depend on a different product or service to operate?
- What kind of maintenance and update requirements does the product or service have? Will agency staff or third parties have access to all the information and other resources needed to maintain or update the product or service? The vendor or consultant should explicitly guarantee such access.

Unless they are restricted by law, these disclosures should be shared with the public. To the greatest extent possible, agencies should require bidders to disclaim any right to invoke trade secrecy in the services or products delivered.[34]

Additionally, and importantly, the transparency deficits relating to the procurement process and to the procurement histories of specific vendors and consultants must be corrected. Currently, as described above, agencies tend not to share essential information regarding their experiences with private vendors and consultants and the digital tools and systems they have furnished, and this harms both other agencies and the public. Complete information about prior experiences with vendors and consultants should be available to agencies and to the public.[35]

Centering outcomes and impacts

The goal here is easy to describe abstractly: Govtech teams should work at every phase of the development lifecycle to advance desired outcomes and minimize negative impacts.

It is much harder to chart a durable, institutionally supported path toward achieving that result. Critics of the excessively bureaucratic requirements that have hobbled govtech development inside the administrative state view most internal accountability processes as inherently problematic and envision giving internal govtech development teams mostly free rein to engage in agile development.[36] Critics of technology in government see automation of government processes as inherently problematic and envision multiple, slowly accreting layers of accountability as a second-best solution.[37]

Neither approach is fully tenable. To put the matter bluntly, accountable government needs to be accountable, and effective government needs to govern effectively. But the two approaches also are not as fundamentally opposed as their partisans sometimes assume. To some extent, the two groups described in the previous paragraph are talking past each other, with the former focused on the process challenges confronting govtech development teams and the latter focused on the downstream effects of the private-sector preference.

To design systems that serve policy and operational goals effectively and that work for the people who need to use them, govtech development teams need flexibility to

---

34 For a detailed discussion of issues related to the effects of overbroad trade secrecy claims on government transparency, see Christopher J. Morten, *Publicizing Corporate Secrets*, 171 U. Penn. L. Rev 1319 (2023).

35 As an analogous example, the Financial Industry Regulatory Authority's BrokerCheck is a publicly searchable database that provides information about registered brokers and investment advisers. *See About BrokerCheck*, FINRA, **https://www.finra.org/investors/investing/working-with-investment-professional/about-brokercheck**.

36 *See, e.g.*, Pahlka, *supra* note 14.

37 *See, e.g.*, Citron, *supra* note 20, at 1295 (describing a due process regime because automated systems "impose accountability deficits"); Mulligan & Bamberger, *supra* note 20, at 809-811 (describing the use of administrative law as an avenue for accountability in light of an increase in automation in government).

revisit earlier decisions and leeway to probe the reasons for apparent technical and operational constraints. A good process should align with those needs throughout the govtech lifecycle. According to experts, important elements of the process include the following:

Identifying desired outcomes. At the start and iteratively throughout design and implementation, it is important to identify, revisit, and refine benchmarks for desired outcomes. In particular, it is important to ask and answer questions that link system outcomes to underlying policy goals: Why was the underlying program or initiative created? What problem is it trying to solve? What stakeholders does it serve? What are their needs?[38] This process works best when it involves substantive engagement with relevant stakeholders both within and outside the agency or department (including not only agency policy staff but also agency staff who will operate the systems, service recipients, and other affected citizens and communities). The design team should also consider the ways that system accessibility and usability may affect outcomes and the extent to which system alternatives or workarounds will be available.

Defining failure. Relatedly, it is useful to identify and periodically revisit markers for failure and/or redundancy. These might include, for example, failure to produce the desired outcomes, usability problems, other harmful impacts, and policy redundancy.

Mapping interoperability implications. The design and development processes must consider needs for interoperability and data portability. Govtech systems will often need to be interconnected to each other, not only within agencies but also across agencies. In some situations, it may be best to connect only relevant parts or modules. For example, there may be situations in which some resources and technological capacity need to be shared, but underlying personal data used by the systems should not or cannot legally be shared.

Understanding legacy systems constraints. Relatedly, the design and development processes must identify any legacy systems on which the new tools or systems will need to rely and the constraints such systems may or will impose. The team working on the new project and the team that supports the legacy system will need to work together to identify and avoid (or mitigate) negative impacts to the policy goals and the populations that the legacy system is or was serving.

Understanding capacity and resource requirements throughout the lifecycle. The design and development processes should identify capacity and resource requirements for development, implementation, maintenance, and updating of govtech systems and components. Relevant resources will include institutional and policy knowledge as well as technical and financial capacity.

Identifying relevant standards. The design team will need to identify any relevant standards and any resources required for ongoing compliance with them. As described above, voluntary consensus standards originating in the private sector may not be most appropriate for use in govtech systems. The design team should consider whether that is the case and, if so, should identify resources needed to modify existing standards or develop new ones.

Monitoring and iterative review of implementation. Even a robust design process cannot predict every problem that may arise during implementation and operation of govtech systems. The design and development processes should provide for adequate ongoing monitoring and oversight of system implementation and operation and for periodic assessment of maintenance and update needs. As with the initial design phase, processes for monitoring and oversight should include ongoing or periodic engagement with all relevant stakeholders (including not only agency policy staff but also agency staff who operate the systems, service recipients, and other affected citizens and communities)

38 *See, e.g.*, Service Design Collective Inc., Success and Failure in Federal Service Delivery (2023), **https://www.servicedesigncollective.com/wp-content/uploads/2023/07/Success-Failure-in-Federal-Service-Delivery-v1.2.pdf**

Assessing the full range of impacts. In the best of all possible worlds, digital tools and systems will still introduce new kinds of opacity that require translation and will produce unintended outcomes and unforeseen technical and/or policy-related path-dependencies. Govtech design and implementation teams need to be alert to these possibilities. It is important to document and evaluate all significant impacts, both intended and unintended, flowing from implementation and use of a govtech tool or system. In particular, staff should be trained to explore how users interact with public facing digital tools and systems and how the implementation of such tools and systems affects users and communities.

Transition planning. Monitoring and iterative review may reveal that a govtech system has either failed or has become redundant. Before suspending use, transition planning should account for transfer of needed functions and services to new systems and should consider what changes need to be made in any connected systems to avoid disrupting other agency functions and services. Transition planning also requires attention to protocols for proper storage, security, and deletion of data used by failed or redundant systems.

Avoiding compliance doom loops

In brief, we recommend that existing accountability ecosystems be pared back and reoriented toward iterative and flexible lifecycle development as described in section 3, above. In part because of the cascading effects of the private-sector preference and in part because oversight systems have become organized around entrenched habits of "waterfall" development, in-house govtech teams confront sometimes-ludicrous burdens. Private vendors confront some of the same burdens, but in other respects face relatively lenient accountability requirements. This polarity should be reversed.

Agency govtech design and implementation teams need the flexibility to question obsolete and/or poorly conceived requirements and to revise prior decisions as iterative processes reveal new information. Process requirements should be designed with such flexibility in mind and with the goal of facilitating rapid, iterative communication. Budgeting and related reporting requirements–currently implemented on an annualized basis without sufficient allowance for longer term govtech modernization and development projects–should also allow for such flexibility, to enable iterative design and development processes across the lifecycles of govtech systems.[39] Design and implementation choices should be documented and explained. Govtech teams also need good mechanisms for securing user input from non-industry stakeholders, including the citizens served by govtech systems, agency staff who operate the systems, and agency policy staff.[40]

Return to the examples of process failure described in Part 2, above: In the case of the failed satellite software updates, a better accountability process would have allowed the design team to override the requirement to use an obsolete data transfer architecture after documenting the evolution of industry best practices. Additionally, and crucially, that decision would have prompted the CIO Council to clarify and/or update the

39 Currently, federal agencies must follow "capital planning and investment control" (CPIC) processes for the acquisition, maintenance and disposal of technology systems. *See* Chief Information Officers Council, CIO Handbook, available at **https://www.cio.gov/assets/files/Handbook-CIO.pdf**. Although these processes could be designed to support more agile development practices, experts note that, in practice, they are implemented in a lockstep manner that tends to further entrench "waterfall" development.

40 For an example of the general sort of thing we have in mind, see Reeve T. Bull, *Making the Administrative State 'Safe for Democracy': A Theoretical and Practical Analysis of Citizen Participation in Agency Decisionmakin*g, 65 Admin L. Rev. 611 (2013).

now-obsolete guidance document. Communication between the design team and the CIO Council would have been rapid, dynamic, and iterative. In the case of login.gov, a better accountability process would have allowed the login.gov to depart from the NIST standard for remote biometric authentication after documenting the substantial efficacy and equity concerns that had been raised about FRT technology. Additionally, and crucially, it would have afforded customer agencies leeway to adopt the login.gov tool as designed, even though it did not satisfy the NIST standard.

When an agency decides to procure govtech tools, systems, or components from a vendor or consultant, it should build robust, lifecycle-based accountability requirements into the bidding process. Vendors should be required to explain how they will develop and implement the technology and to work with agency staff to identify and monitor all potential impacts, including impacts on the rights and interests of individual users and communities and impacts on connected government systems. Contracts with vendors and consultants should provide for periodic review during the term of the contract and for termination if designated performance criteria are not met.

Part 4: Changes to institutional structure and organization

The policy changes described in Part 3 point toward a need for corresponding changes to institutional structure and organization. Below, we identify five significant functions that we believe would benefit from improved support and coordination: lifecycle planning, interoperability management, vendor management, technical standard setting, and development of a set of core functionalities that function as common digital infrastructure. We then recommend institutional restructuring to support those functions more effectively. To state one of our core recommendations at the outset: we call for the creation of a central hub outside OMB to perform a well-defined and limited set of functions supporting agency-driven development of govtech. The new hub, which could be situated in GSA or in an independent agency, would absorb the coordinating functions currently housed at OMB and GSA and the government unique standards functions currently housed at NIST. Finally, we discuss means for developing the pipeline of federal employees with the necessary skill sets.

Major functions requiring improved support and/or coordination

In this section, we discuss five major functions that are necessary for effectively provisioning govtech in a way that centers public values and needs. Each of these functions requires improved institutional support and coordination.

Lifecycle planning. Agency teams tasked to conduct independent assessments that identify desired outcomes, impacts, and failures and redundancies at various stages of the govtech lifecycle, will work more effectively if provided with guidance on best practices, training programs, and other resources. To be clear, guidance on particular topics is not the same as top-down control. Agencies are in the best position to assess their own programmatic and operational needs. All agencies, however, would benefit from access to state-of-the art thinking about, for example, techniques for assessing interface usability or understanding the societal impacts of digital tools and systems. As a general matter, however, support for lifecycle planning should not function as a development bottleneck but rather should afford resources that empower agency govtech teams.

Interoperability management. As described above, common underlying infrastructure is often needed for technical functions and services (for example, cloud services) within and across agencies. One of the reasons private vendors and consultants become incumbent is because they can provide such cross cutting technologies. Agencies should be able to adopt govtech systems without subjecting themselves to vendor lock-in, and in at least some cases, they should be able to choose standardized govtech services designed to public specifications. All agencies would benefit from better-organized processes for collecting and sharing information about the capabilities, limitations, and interoperability requirements of different govtech tools and systems. They also would benefit from better coordination in identifying and recommending common technical systems and infrastructures for functions that are replicated across agencies.

Core common digital infrastructure elements. As described above, a longer term strategy for digital government involves in-house development of govtech tools and systems that function (or should function) as common infrastructure for all agencies. Examples of missed opportunities to advance that project include the login.gov system, which no longer functions as a single identity architecture for government following the events described in Part 2 above, and the common calendaring system that currently does not exist. All agencies would benefit from improved coordination to identify, develop, and implement basic elements of a core common digital infrastructure.

Vendor management. As described above, the same vendors and consultants often provide similar services across multiple agencies. Agencies need to be able to learn from each other to improve their ability to supervise design and development processes, to avoid capture and lock-in, and to provide more uniform and accessible services to citizens. Many aspects of this process can and should be supported centrally. All agencies would benefit from access to a dynamic repository of information about the expertise and govtech provisioning histories of vendors and consultants, covering especially behaviors relating to technical transparency, attempted lock-in, responsiveness to requests for design and/or implementation changes, and responsiveness to requests for ongoing monitoring and assessment. Such data should be systematically collected and shared not only with agencies but also with vendors and consultants themselves, with researchers, and with the public. In addition, all agencies would benefit from guidance on managing bidding processes and negotiating contracts that impose lifecycle-based requirements.

Technical standard setting and coordination. As detailed above, where technical standards are concerned, agencies generally are standard takers rather than standard setters. Although they are encouraged to participate in NIST's standards processes, many do not have the capacity or resources to engage more deeply with the potential impact of adopting a particular standard. Meanwhile, NIST's mandate to let the private sector lead in standards development creates potential conflicts of interest between agencies and NIST. These arrangements may have made more sense when digital tools and systems played less central roles in government operations; now, however, it is important for decisions about govtech standards to consider the full range of impacts that such standards may produce and the full range of public values that govtech tools and systems are meant to serve. All agencies would benefit from improved support for their participation in standards development processes and from better coordination in identifying needs for departure from voluntary consensus standards and, as needed, recommending government unique standards.

Proposals for institutional restructuring, large and small

In this section we recommend changes to existing institutional structures that could address the problems identified above.

Agency-specific improvements. In-house govtech development capability is essential in the digital era. Each agency's enabling statute should provide for a CTO with clearly delineated authority, perhaps deriving that authority from the CIO, to whom many CTOs report. Each agency's budget should include the resources to assemble an in-house govtech team. Those appointed as CTO should at a minimum have the technical expertise to manage the govtech design and development processes. They should also have an adequate understanding of the agency's mission, the services it provides, and the values it seeks to advance. Similar expertise and understanding should be required for the Chief AI Officer positions that are now being created. The office of the CIO should be structured in a manner that encourages collaboration among the three lead officers and their staffs.

Coordination improvements. In theory, some of the policy changes that we describe above could be accomplished via the office of the Federal Chief Information Officer and the CIO Council. If the existing institutional structure is retained, the CFIO and the CIO Council could be charged with implementing the policy shifts described in Part 4, with supporting the specific capabilities described in Part 5, and with approaching those tasks in ways that further coordination and collaboration across agency boundaries.

We note, however, that this approach would do little to cure the coordination problems that currently hinder effective govtech provisioning and might make them worse. Many of the proposals in Parts 4 and 5 would require new forms of significant cross-agency cooperation. Some would operate at cross purposes with the mandate of the newest GSA office, the Centers of Excellence, "deliver enterprise transformation initiatives" that "leverage commercially available solutions."[41]

We also think that the current coordination arrangements must be viewed within the context of the increasingly wide ranging role that OMB plays in relation to the administrative state. Observers note that OMB's powers (which have grown significantly over the years) allow it to exercise significant control over administrative agencies, thereby allowing the executive to attain policy aims without having to go through the legislative process.[42] An arrangement that requires agency CIOs to route policy and best practices recommendations through OMB furthers political control of govtech-related decision making. It also frames govtech as an instrumentality of "management" rather than a locus of policymaking in its own right.

Larger-scale reorganization. We think, therefore, that the priorities we have identified will be served more effectively by moving govtech-related policymaking and coordination functions out of OMB and by centralizing a well-defined and limited set of support functions elsewhere in the federal government. The entity that we envision would act as a resource hub and knowledge provider—a platform for agency-driven govtech provisioning that supports the five core sets of functions described in Part 4, above.

There is more than one way to achieve this result. One path might involve relocating govtech-related activities into a newly-created, independent Department of Technology that would serve as a hub supporting agencies in their govtech development activities. Another path would involve restructuring the GSA to enable a more well resourced and cohesive approach to the coordination, guidance, and development functions that smaller GSA offices such as the OTP, the IT Modernization Division, and TTS currently undertake on a more piecemeal basis and relocating OMB's govtech policymaking and coordination functions into GSA.

Either approach would represent a beneficial separation between the changing policy priorities that inform OMB's work and the continuing need of all agencies for fair and accountable digital tools, systems, and services. Under either approach, USDS would remain in OMB and continue project development work according to the priorities of each administration.

Under either approach, the specific NIST functions relating to public sector departure from voluntary consensus standards would be carved out and moved to the new support hub. The hub would coordinate agency participation in standards development processes relating to systems and tools that are used or could be used in govtech. It would work with agencies to identify needs for compliance with or departure from standards for particular govtech tools and systems, to determine whether development of government unique standards is warranted, and, if so, to lead that process on behalf of agencies, in dialogue with experts at NIST. (Through give and take with such an entity, NIST itself might be encouraged to address public values more comprehensively in the processes it superintends.)

---

41 *See The Centers of Excellence, supra* note 6.

42 *See, e.g.*, Cass R. Sunstein & Peter L. Strauss, *The Role of the President and OMB in Informal Rulemaking*, 38 Admin. L. Rev. 181, 187-188 (1986); Elena Kagan, *Presidential Administration*, 114 Harv. L. Rev. 2245, 2279 (2001) (discussing the use of OMB's oversight to drive regulation without Congressional delegation or authorization).

Oversight improvements. Existing agency oversight mechanisms should be updated to reflect the recommendations above. The GAO's processes for assessing expenditures and resolving bid protests should be revised substantially to comport with a changed landscape in which the private-sector preference no longer holds sway and agencies and the public rather than vendors and consultants are the customers for govtech systems. Similarly, agency IGs should be required to assess agencies' work on govtech systems in ways informed by the policy changes described in Part 3.

Building the pipeline

The most common issue that arises in discussions on govtech is that of technical capacity within agencies. Many agencies still lack such capacity and even some agencies that do have such capacity face difficulties hiring and retaining staff with the relevant skill sets. It is not the case that all technology used by government agencies must be designed, developed, implemented, and maintained in house. However, it is almost always the case that a decision has to be made on whether or not to do so. Ideally, such a decision will not be predetermined because of capacity constraints.

To address these needs, the federal government should promote the development of curricula and training programs that map to the lifecycle approach described in Part 3. It should offer grants to universities, community colleges, technical institutes, and other institutions interested in developing new programs or improving existing ones. Such programs should extend beyond computer science and information technology departments to include information schools, law schools, and public policy schools, all of which play important roles in training students to think through the social impacts of technology development and set substantive benchmarks for policy work. Over time, training programs for agency staff should be updated to include results from these programs. Additionally, the federal government should offer scholarships for prospective students and create fellowships and other research opportunities for more advanced study.

Other obstacles to hiring and retaining govtech staff are more bureaucratic in nature. The federal Office of Personnel Management currently supports the hiring of technologists for various agencies. While centralizing hiring can reduce costs, it might not be the most productive way of recruiting technically skilled staff. Domain-specific agencies tend to have a better understanding of their needs and can be more effective in finding the right people for their teams. Some domain-specific policies that affect hiring, however, would benefit from centralized attention. Agencies typically prohibit employees from holding financial interests in firms they regulate.[43] Such prohibitions are entirely appropriate, but a wide range of different policies to prevent financial conflicts of interest can make hiring cumbersome, especially when candidates would work on govtech tools or systems intended for adoption across multiple agencies. It may be more effective to create a single baseline policy for govtech employees that focuses more specifically on managing technology industry conflicts of interest, and that could be supplemented as necessary for more agency-specific assignments.

43 5 C.F.R. § 2635.403 (1992).

Bibliography

Background on Current Provisioning Processes and Practices

Brian J. Baldus & Lindle Hatton, *U.S. Chief Procurement Officers' Perspectives on Public Procurement*, 26 J. Purchasing & Supply Mgmt. 1 (2020).

Cong. Rsch. Serv., RS22536, Overview of the Federal Procurement Process and Resources (2023).

Kate M. Manuel, Brandom J. Murrill & Rodney M. Perry, Cong. Rsch. Serv., R43368, Contractors and Healthcare.gov: Answers to Frequently Asked Questions (2014).

Kate M. Manuel, Cong. Rsch. Serv., R42325, Definitions of "Inherently Governmental Function" in Federal Procurement Law and Guidance (2014).

Critiques of Current Provisioning Processes

Kenneth A. Bamberger, *Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State,* 56 Duke L. J. 377 (2006).

Aristotelis Mavidis & Dimitris Folinas, *From Public E-Procurement 3.0 to E-Procurement 4.0; A Critical Literature Review*, 14 Sustainability 1 (2022).

Bessma Momani, *Management Consultants and the United States' Public Sector*, 15 Bus. & Pol. 381 (2013).

Mariana Mazzucato & Rosie Collington, The Big Con: How the Consulting Industry Weakens Our Businesses, Infantilizes Our Governments And Warps Our Economies (2023).

Ines Mergel, *Digital Service Teams in Government*, 36 Gov't Info. Q. 1 (2019).

Jennifer Pahlka, Recoding America: Why Government Is Failing in the Digital Age and How We Can Do Better (2023).

Integration of Automation and Artificial Intelligence in Government

Admin. Conf. of the U.S., Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies (2020).

Kate Crawford & Jason Schultz, *AI Systems as State Actors*, 119 Colum. L. Rev. 1941 (2019).

Cary Coglianese, *Procurement and Artificial Intelligence*, *in* Handbook on Public Policy and Artificial Intelligence (2024).

Cary Coglianese & David Lehr, *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, 105 Geo. L.J. 1147 (2017).

Doaa Abu Elyounes, *"Computer Says No!": The Impact of Automation on the Discretionary Power of Public Officers*, 23 Vand. J. Ent. & Tech. L. 451 (2020).

Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (2018).

Michele Estrin Gilman, *Me, Myself, and My Digital Double: Extending Sara Greene's Stealing (Identity) From the Poor to the Challenges of Identity Verification*, 106 Minnesota L. Rev.: Headnotes 301 (2021).

Woodrow Hartzog et al., *Inefficiently Automated Law Enforcement*, 2015 Michigan State L. Rev. 1763 (2016).

Merve Hickok, *Public Procurement of Artificial Intelligence Systems: New Risks and Future Proofing,* 39 Artificial Intel. & Soc'y 1213 (2024).

Blagovesta Kostova, Seda Gurses & Carmela Troncoso, *Privacy Engineering Meets Software Engineering. On the Challenges of Engineering Privacy By Design*, arXiv:2007.08613, https://arxiv.org/abs/2007.08613.

David S. Rubenstein, *Acquiring Ethical AI*, 73 Fla. L. Rev. 748 (2021).

Proposals for Institutional Changes to the Procurement Process

Ryan Calo & Danielle K. Citron, *The Automated Administrative State: A Crisis of Legitimacy*, 70 Emory L. J. 797 (2021).

Danielle Kriz, Council on Foreign Rels., Improving Supply-Chain Policy for U.S. Government Procurement of Technology (2015).

Susan Landau, James X. Dempsey, Ece Kamar & Steven M. Bellovin, Challenging the Machine: Contestability in Government AI Systems (2024).

Jonathan Marskell, Georgina Marin & Minita Verghese, *Digital Public Infrastructure: Transforming Service Delivery Across Sectors, in Digital Progress and Trends Report* 2023, World Bank (2023), https://www.worldbank.org/en/publication/digital-progress-and-trends-report.

Deirdre K. Mulligan & Kenneth A. Bamberger, *Procurement as Policy: Administrative Process for Machine Learning*, 34 Berkeley Tech. L. J. 773 (2019).

Frank Nagle, *Digital infrastructure is more than just broadband: What the US can learn from Europe's open source technology policy study,* Brookings Inst. (November 9, 2021), https://www.brookings.edu/articles/digital-infrastructure-is-more-than-just-broadband-what-the-u-s-can-learn-from-europes-open-source-technology-policy-study/.

Rashida Richardson, Best Practices for Government Procurement of Data-Driven Technologies (2021).

ITT REDESIGNING THE GOVERNANCE STACK

GEORGETOWN LAW