Developer Platforms: Shared Services for Common Developer-Focused APIs and Services

About the Federal CIO Council

The CIO Council is the principal interagency forum on Federal agency practices for IT management. Originally established by Executive Order 13011 (Federal Information Technology) and later codified by the E-Government Act of 2002, the CIO Council's mission is to improve practices related to the design, acquisition, development, modernization, use, sharing, and performance of Federal Government information resources.

Distribution

Contents

Executive Summary

The availability and power of cloud services has changed software development. Cloud and hosted application programming interfaces (APIs) that provide functionality such as payments, analytics, and data storage or simplify and accelerate testing, hosting, deployment, monitoring, and other aspects of the software development process have become ubiquitous components of web and mobile applications built today. Rather than writing functionality from scratch, a team can *compose* cloud APIs and services together to build and deliver much of an application's functionality. This has resulted in significant efficiency and effectiveness improvements over the past few years for software development teams leveraging these modern approaches.

Common Platforms

Internal *platform teams* that make common APIs and services available are a key part of modern "digitized" organizations. Platform teams expose services to developers and teams within the organization that improve time to market, enhance security, increase performance, and reduce costs.

Other governments have recognized the opportunity provided by common developer platforms and services. Inspired by work in Estonia, the Government Digital Service (GDS) in the United Kingdom adopted a Government-as-a-Platform approach to IT service delivery. This approach divides primitive components of application delivery such as payments, user authentication, analytics, and workflow management into distinct components that can be built once, offered as developer-focused services, and shared between missions.

Federal Developer Platforms and Services

The ability to share resources and functions within and across Federal departments and agencies using developer APIs and services offers a new way to improve efficiency and effectiveness. This includes services that directly impact mission delivery such as citizen-facing applications or optimization of internal operations through consolidation or de-duplication of IT functions. There are already examples of this model working in the Federal Government for application development and deployment, analytics, user authentication, payment processing, and data discovery.

Opportunities and Priorities

Given this background, a key question is how to support the maturation and growth of existing developer platforms and services and the development of new developer platforms and services. One way to approach this question is to look at existing public and private-sector platforms. Comparing services offered by major commercial public cloud providers, those offered by the UK Government Digital Service, and by U.S. Federal departments and agencies provides several insights. First, the utility of a given developer platform or service across different departments, agencies, and mission spaces is a helpful way to assess potential value for the broader Federal Enterprise. Second, when significant investment would be required to duplicate or copy the functionality provided by a given developer platform or service, there is more value for platform adopters.

As the Federal Government considers where and how to invest, it is helpful to keep in mind that the vast majority of developer platforms and services used by Federal departments and agencies will likely be procured directly from private-sector providers. This means that efforts to streamline the ability of Federal departments and agencies to agilely procure solutions will be critical in increasing uptake within the Federal Enterprise. As articulated in the 2012 Federal Information Technology Shared Services Strategy and in alignment with guidance from the Office of Management and Budget (OMB), the default approach for departments and agencies should be to procure external commercial solutions. However, there may be situations where public-sector developer platforms and services deployed in partnership with industry are needed. Ideally, these should be rare situations, but it does not make such instances less important or critical for supporting mission and service delivery.

Marketplace Development

This report looks at more than 25 different developer platforms and services and leverages existing work in shared services ecosystem development to assess potential delivery models. This includes direct delivery through commercial entities, a marketplace of Federal providers, and delivery through a Federal provider. Given the broad range of solutions and complexity of the Federal IT landscape, a one-size-fits-all approach is often not the most effective and multiple approaches are often necessary.

Accelerating Adoption

Finally, it is also helpful to keep in mind a broader set of considerations that can affect the creation, development, and adoption of developer platforms and services. These considerations include challenges related to agile software development and policy challenges related to the ATO process, clarifying responsibilities in shared environments, the interaction of Trusted Internet Connections (TICs) with modern technology, the Privacy Act's application to digital services, and funding mechanisms.

Key Findings

This report provides background and support for three central findings:

1. Developer platforms and services are key mission enablers in the public and private sectors. The shared service model already deployed in the Federal Government provides an approach to governance, deployment, and funding for developer platforms and services.
2. There are a wide range of immediate opportunities for the Federal Government to support a growing ecosystem and marketplace of developer platforms and services (e.g. identity, notifications, data sharing) based on an analysis of needs and on experiences from the private and public sectors.
3. There are policy reform opportunities that can accelerate developer platforms and services, as well as certain administrative shared services, including streamlining the ATO process, clarifying responsibilities in shared environments, modernizing TIC policy, exploring how the Privacy Act applies in these contexts, and further supporting new funding models.

These findings support an aggressive approach to building a robust ecosystem of developer-focused shared services designed to support Federal departments and agencies. This will require close collaboration between industry and government, disseminating lessons learned from early adopters, leveraging existing services and contracts, and sharing information.

Introduction

We are in a new era of technology and innovation in the U.S. Government. While there are many examples of modern technology making government more efficient and producing better outcomes for citizens, we are still at the beginning of this transformation. There are massive opportunities throughout the Federal Government to upgrade the large installed base of legacy IT applications and deliver new, more customer-centric, high-quality and secure services and products. In 2012, the Federal Chief Information Officer issued the Digital Government Strategy, which outlines a vision to "to seize the digital opportunity and fundamentally change how the Federal Government serves both its internal and external customers."[1] One of the strategy's four key principles is a *shared platform* approach and a call to "share capacities to build the systems and processes that support our efforts, and be smart about creating new tools, applications, systems, websites and domains. Ultimately, a shared platform approach to developing and delivering digital services and managing data not only help accelerate the adoption of new technologies, but also lowers costs and reduces duplication."

While the Federal Government's vast scale, distributed structure, and complex legal environment impose many unique requirements, the opportunity to use a shared approach to broadly improve usability, security, and the efficiency of operations and service delivery has never been higher. Indeed, as sophisticated software enables solutions to complex problems and situations, *cloud services* provide fundamental economies of scale realized through sharing infrastructure, software, and services across multiple customers and tenants.

While not necessarily apparent to many end users, most web and mobile applications built today leverage cloud providers or services. Cloud-powered APIs enable core application functionality such as payments, analytics, and data storage, while other cloud services simplify and accelerate testing, hosting, deployment, monitoring, deployment, operations and other aspects of development. The availability and power of cloud services has changed software development. Rather than writing functionality from scratch, a team can *compose* APIs and services together to build and deliver much of an application's functionality.

A software development team today can leverage open source frameworks and libraries for basic functions and integrate cloud API services to implement backend features. This significantly reduces the amount of source code needed—a team of two can implement what formerly took a team of twenty. The whole process is further accelerated by the use of robust testing frameworks and services, continuous integration and deployment, and other tools that empower developers to own features from ideation to production. This has resulted in a huge improvement in productivity over the past few years for teams leveraging these modern approaches.

Within the private sector, internal *platform teams* are an essential part of modern "digitized" organizations. These platform teams expose services to developers and teams within an organization that improve time to market, enhance security, increase performance, and reduce costs. Platform teams can transform the ability of organizations to deliver products and services and can provide new ways to better serve customers. The cloud offerings of several large commercial cloud providers started as internal platform products before becoming commercial products offered to external customers.

There has been advocacy for cloud services within the Federal Government, but efforts to migrate to common platforms that serve Federal software developers and contractors within the Federal Enterprise are still nascent. The lack of internal developer-focused platforms and services results in software projects within and across departments and agencies rebuilding much of the same functionality. This can significantly raise the cost, complexity, and development time of projects, while hurting their usability

[1] https://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html

and chance of a successful outcome. When software projects must write or integrate hundreds of thousands of lines of software code to implement account management and authentication infrastructure, collect payments, or validate the citizenship and income of an individual, complexity and cost will increase.

Given trends in the private sector, this problem will only grow more acute over time. As the integration of developer-focused platforms and services continues to grow in importance for delivering web and mobile applications, the lack of shared infrastructure and services within the Federal Enterprise may lead to poorer usability, less security, reduced performance, and higher costs. Furthermore, as migration to developer platforms and services continues, Federal departments and agencies will fall further behind the private sector and other public-sector entities.

The need for common developer platforms and services has been recognized by other governments. Inspired by work in Estonia, the Government Digital Service (GDS) in the United Kingdom adopted a Government-as-a-Platform approach to IT service delivery. This approach divided primitive components of mission application delivery such as payments, user authentication, analytics, and workflow management into distinct components that can be built once, offered as developer-focused services, and shared between organizations across the government.

Fortunately, a model for sharing services already exists within the U.S. Federal Government, used for common administrative functions such as financial management, human resources, payroll, and acquisitions. On May 4, 2016, the Office of Management and Budget (OMB) issued M-16-11, *Improving Administrative Functions Through Shared Services*. Building on the work that had previously been done in individual administrative functions, M-16-11 put forth an enterprise-wide shared service strategy for the Federal Government. Many of the same principles and challenges for administrative shared services are applicable to developer platforms and services and are explored in this report. The goal of this report is to leverage ongoing international and U.S. Government efforts to identify opportunities for accelerating the development and adoption of developer-focused platforms and services.

Federal Shared Services

The sharing of services and functions across departments and agencies has a rich history in the Federal Government crossing administrations and political parties. The notion of *shared services* was first substantively addressed by the Federal Government in the early 1980s with the creation of the National Finance Center within the Department of Agriculture to reduce redundancy in hiring administrative staff. The objective was to leverage economies of scale in hiring functions, enabling small agencies to control the fixed cost of full-time staff when part-time, on-demand work was sufficient. The value of sharing was self-evident, and in the 1990s, a series of projects to share back-office services were established and made permanent. The consolidation of 26 payroll systems to 4 government-wide providers, championed by the second Bush administration, realized over $1.1 billion in cost savings over ten years and is often held up as one of the prime examples of reducing duplication in administrative services.[2]

Recognizing the powerful impact that the government's internal operations have on service to its citizens, the Obama Administration made transformation of management practices within the Federal Government a key priority and included shared services as a Cross-Agency Priority (CAP) Goal. The CAP goal focused on strategically expanding high-quality shared services to improve performance and efficiency throughout government and built on existing policies as well as others that came out as a part of its execution[3]:

- Federal Cloud Computing "Cloud First," February 2011
- Shared Services Strategy "Shared First," May 2012

[2] GAO, Streamlining Government, May 2012.
[3] http://www.performance.gov

- OMB Memorandum 13-02 *Improving Acquisition through Strategic Sourcing*
- OMB Memorandum 13-08 *Improving Financial Systems Through Shared Services*
- OMB Guidance - *Transforming the Marketplace: Simplifying Federal Procurement to Improve Performance, Drive Innovation, and Increase Savings*, December 4, 2014
- OMB Memorandum 16-11 *Improving Administrative Functions Through Shared Services*
- OMB Memorandum 16-12 *Improving the Acquisition and Management of Common Information Technology: Software Licensing*

In October 2015, OMB and General Services Administration (GSA) established the Unified Shared Services Management (USSM) office to oversee the current shared service ecosystem and provide a consistent long-term strategy for the expansion of administrative shared services.[4] As described by USSM, "shared services are about delivering mission support functions – acquisition, human resources, financial management – better, faster and more efficiently. If agencies cannot do these things well, it will impede the administration's ability to deliver on public priorities – building the nation's infrastructure, protecting public health and ensuring our security."[5] USSM further outlines the key benefits of shared services along five vectors:

- **Enable agency mission** by redirecting the workforce to mission functions and reducing administrative burden.
- **Improve data based decision-making** through access to reliable, standardized, and just-in-time data for better management.
- **Increase cybersecurity** with fewer systems that are easier and more cost efficient to protect and modernize.
- **Attain economies of scale** through consolidating and modernizing technologies across the government.
- **Recognize cost efficiencies** in mission support operations by leveraging common practices, maintaining fewer systems, and distributing personnel in lower-cost areas.

This approach has been recognized by good government groups and industry associations. Organizations such as the Partnership for Public Service, the American Council for Technology and Industry Advisory Council (ACT-IAC), and the National Academy of Public Administration (NAPA)—often led by bi-partisan groups of former government executives and industry experts—have supported the continued investment of political capital and resources in advancing the use of shared services across the Federal Enterprise.

The notion of shared services as a foundation upon which the Federal Enterprise can improve the performance, cost, security, and usability of tools and services it provides applies to more than just administrative functions. Indeed, shared services that provide common developer-focused platform and API services available to Federal departments and agencies have the potential to improve efficiency, effectiveness, promote innovation, and increase the ability of the Federal Government to deliver on mission objectives.

Developer APIs

Modern application development relies on the composition of discrete, well-tested software components. Ideally, these components are lightweight with low demands on resources, are robust and can quickly recover from failure, and use industry standards for data representation and transmission (e.g. JSON, XML, HTTPS). Each component typically provides a specific feature that can be combined with the services offered by other components to satisfy application requirements. This loose coupling of services

[4] Office of Management and Budget Memorandum 16-11, "Improving Administrative Functions Through Shared Services"
[5] "CAP Goal Quarterly Progress Update, Shared Services, FY2016 Quarter 4" on http://www.performance.gov/

allows developers to combine and recombine services as needs change over time without rebuilding or rewriting large functions.

Web services are "software system[s] designed to support interoperable machine-to-machine interaction over a network."[6] Web services often present themselves as an API accessible via the World Wide Web. An API is a "set of routines, protocols, and tools for building software applications."[7] APIs are a popular way for developers to integrate data and computation services that leverage cross-cutting software components into a broad range of applications and systems. For example, a user authentication service is needed for many applications. Rather than each development effort crafting their own design, implementation, and operation of a user authentication function, a common authentication service provided through an API can be leveraged by developers who can instead focus effort on other aspects of application design, development, and operation.

API designs will vary depending on their purpose. Both the *18F API Standards* and *White House API Standards* provide guidance for Federal API developers.[8] At the time this report was written, the *18F API Standards* recommend use of JSON as the default format for APIs, and UTF-8 for encoding. The *White House API Standards* further encourage RESTful interfaces and provide examples and guidelines for designing good APIs.[9] APIs also present opportunities for continuous improvement based on observing customer behavior. It is possible to continuously collect data on how customers use a web service API, allowing the API provider to detect and remediate errors, fix performance problems, and identify new product development opportunities using that data.

Because APIs are interfaces for developers, the same user-centered design principles that have helped to transform other government user interfaces and services can also be applied to developer-focused APIs and services.[10] Leveraging user-centered design approaches helps ensure each new API meets a key unmet need of a target audience and provides a process to gather input from users and continuously improve the API service.

Federal Developer Platforms and Services

The ability to share resources provided by the shared services model and the mechanism of sharing provided by developer APIs offers a new way to improve the efficiency and effectiveness of the Federal Government. In fact, there are already a few examples of this model working successfully. A survey of existing Federal developer platforms and services was conducted as part of developing this report.[11] Appendix A provides the result of that survey and a list of offerings for developers by Federal departments or agencies. The services in Appendix A are mostly provided through .gov top-level domains and cover a range of API use cases that include application development and deployment, analytics, user authentication, payment processing, and data discovery.

---

[6] W3C Web Services Working Group, "Web Services Glossary," https://www.w3.org/TR/2004/NOTE-ws-gloss-20040211/.

[7] USGEO Data Management Working Group, "Common Framework for Earth Observations"

[8] 18F, "18F API Standards," https://github.com/18F/api-standards.

[9] "The REST Web is the subset of the WWW (based on HTTP) in which agents provide uniform interface semantics – essentially create, retrieve, update and delete – rather than arbitrary or application-specific interfaces, and manipulate resources only by the exchange of representations. Furthermore, the REST interactions are "stateless" in the sense that the meaning of a message does not depend on the state of the conversation." (W3C Web Services Architecture, https://www.w3.org/TR/2004/NOTE-ws-arch-20040211/#relwwwrest)

[10] The Digital Services Playbook https://playbook.cio.gov/

[11] Throughout this report the terms 'developer platforms' and 'developer services' are used synonymously to denote functionality that is provided by means of an API that is operated as a service to implement part of a software application.

Appendix B provides case studies on three of those developer services, including Login.gov, a shared authentication and identity proofing platform under development that offers a login experience for citizens to securely access personal information and Federal Government services; Cloud.gov, a Platform as a Service (PaaS) that allows government development teams to quickly launch and scale applications through a streamlined ATO process; and Pay.gov, a secure platform for handling payments to the Federal Government.

International Examples and Lessons

As their citizenries move online, governments around the world are confronting similar challenges as the U.S. Federal Government—legacy systems, redundant proprietary software and digital systems that are not interoperable. Estonia and the United Kingdom (UK) have demonstrated leadership in the movement toward common platforms, cloud infrastructure, and shared services in government. The following is set of opportunities and lessons from digital teams in the UK and Estonia.

United Kingdom

The UK's Government Digital Service (GDS) launched its "Government as a Platform" strategy in 2013, setting out to create common core infrastructure and practices that would make it easier to build high-quality, user-centered government services. This effort came out of successes with GDS' 2011 GOV.UK Verify initiative, which allows any UK citizen to prove who they are online to gain access to a variety of government services like tax filing and benefits applications. Since then, GDS has created standards and guidelines to make the experience of government more consistent across sites and services and pursued projects to take common user actions like payments, and create one system that works government-wide.

The move toward common platforms started with publishing—the government wanted all of its messaging to conform to content and design standards defined by GDS. This prompted an effort to move all government departments and agencies to GOV.UK within two years to enforce a level of consistency. In the process, they saw exactly how many different tools were being used for the same actions. GDS spearheaded a broader transformation movement to break down silos and create tools that could be used across government. To start, they identified the top 50 most common government transactions and decided to make the top 25 digital by default, modular, and shareable across departments and agencies.

The GDS team has completed many of these migrations. Payments, appointment booking, automated notifications and secure hosting are examples of single tools that can now be used across government. For instance, today there are different services hosted at separate agencies that use the same payment tool. This saved the time and money it would take those agencies to create their own payment systems, which had often been the case in the past. The idea is to build these types of tools once and well so they can be used—and more importantly, reused—sustainably for years in an interoperable manner and in a variety of use cases.

Notably, GDS doesn't build all of these tools centrally. They provide support for agencies that want to take on the challenge of building a tool or system that can then be shared, as long as they are built openly, have the best talent for the project, meet GDS standards, and keep their eventual, broader audience in mind. Prior to the "Government as a Platform" initiative, single departments would be given money to build tools for the entire government and face challenges in delivering a result that was widely adopted by other departments. GDS' common set of standards and mandate to open all source code turned this situation around. Funding for projects may not be granted if these conditions are not met. At the same time, the government is able to invest more in the best team of developers with the highest likelihood of building something good. Controlling funding has made a significant difference in the quality and interoperability of products created and offered by agencies. Now code for GOV.UK's Pay and Notify tools is flexible and open enough to be borrowed and used by organizations internationally.

Ultimately, a vision set out by GDS is to provide a canonical "one stop shop" for citizens accessing government services no matter what they're trying to do. To deliver this truly user-centered experience, they believe that it should matter less how services and responsibilities are distributed behind the scenes. Departments and agencies should be empowered to facilitate information sharing necessary to make it feel like everything is centralized and easy to use. This process is now underway with shared data

registries today. There is an opportunity to make the government start thinking of itself and behaving as a single entity, because that is the way citizens perceive it.

Progress toward this vision has been gradual as departments become familiar with common components and find ways to adapt custom requirements for use cases like payments to general platform offerings. To break down barriers, it has been critical to demonstrate how much money has been saved by sharing tools. 1.7 billion pounds were reported to be saved in 2015 through all technology transformation efforts.[12] Controlling funding for projects has made a major difference, as well as rallying disparate agencies around a shared, often reiterated goal of raising standards for services delivered to UK citizens.

The UK's strategy toward common platforms, data repositories, and cloud infrastructure has been significantly informed by Estonia's experience with digital government. The two countries established ways of facilitating regular knowledge transfer and allowing reuse of successful approaches.

Estonia

Following its independence, Estonia launched a technology strategy defined by the need for exceptional security on a very lean budget. This led to the adoption of very simple, backbone infrastructure that would make it simple and inexpensive to launch government services. This backbone is known as the X-Road interoperability platform and launched in 2001 to create one secure and shared environment for the exchange of data between systems and organizations within government.

The X-Road model has created a number benefits for users within government and citizens accessing services. For example, a citizen portal makes all government services effectively available in one spot, ranging from information queries to form submissions. This means that end users can apply for municipal day care and access their electronic health care records through the same system. All identity data is encrypted and only provided if mandatory for the agency providing a particular service. The Estonian E-File system uses X-Road to connect courts to police, public prosecutors, prisons, and lawyers. The E-Police system gives police officers access to vehicle and document registries so that citizens do not even need to carry their driver's license or registration. Data is stored, verified, and available to call up on the spot. All of these databases are decentralized, so there is no single owner or controller. The one thing they have in common is that they are connected through X-Road.

The X-Road architecture includes databases run by private-sector companies, particularly banks and telecommunications companies. To access data, citizens provide their eID, a nationally-standardized system that verifies their identity online. The chip on the eID card carries embedded, encrypted files that serve as an electronic credential. Citizens can use their eID cards as their national health insurance cards, to prove identity when logging into their bank accounts, for signing digital documents, electronic voting, picking up prescriptions ordered online, and more.

Several rules and regulations make this degree of interconnectivity possible in Estonia. For instance, no entity, including government agencies and companies, can ask citizens for personally identifying information that is already available in another database through X-Road. Systems that touch citizen data are built on open source platforms, allowing software to be continuously updated and giving developers the tools they need to easily build on top of the backbone X-Road provides. The vast majority of government transactions are now handled machine-to-machine, but the government retains ownership of intellectual property and citizen data.

Encryption between organizations is enforced by law such that agencies and companies can only access information needed to provide services. This technology is built by the private sector. Many external developers are encouraged by the government to actively contribute. For example, there was recently a

[12] https://gds.blog.gov.uk/2015/10/23/how-digital-and-technology-transformation-saved-1-7bn-last-year/

hackathon for developers to create new services relevant to Estonians. One solution coming out of that event enabled people to transfer money using their digital identity. There is also a digital identity app store offering a range of software allowing people to use their eID cards for new purposes.

There are still significant challenges to overcome. Because the government has a responsibility for personal data for Estonia's citizenry, there are important privacy considerations. This requires continual work to build trust by being open, communicative, and transparent. And, more pressingly, while there has been significantly success in achieving data interoperability, there are opportunities to improve design and content standards. Because services are decentralized on the front-end, they may not adhere to user-centered design and other principles that have made a positive impact for other public-sector services.

Opportunities and Priorities

Experiences with shared developer platforms and services from the private sector, other governments, and pilots within the U.S. Federal Government demonstrate the opportunity to use a shared environment to improve efficiency, security, usability and support the Federal Government's modernization of legacy IT systems. A key question in supporting the growth of developer platforms and services is where and how to encourage the adoption of shared offerings.

Evaluating Opportunities

One approach for evaluating investment opportunities to grow and support an ecosystem of developer platforms and services is to look at where existing public and private-sector entities have invested. Below is a table showing a comparison of developer platforms and services offered by two major commercial public cloud providers, offered by the UK Government Digital Service, and offered by U.S. Federal departments and agencies. The groupings defined by the rows in this table were developed by the UK GDS as a way of segmenting common platforms and services.[13]

	Commercial Provider A	Commercial Provider B	UK Government Digital Service	U.S. Federal Departments and Agencies
Messaging *Incorporate and track secure, reliable messaging to users or within an application.*	**22** messaging and queueing services, including services to integrate with IoT devices, comment handling, and push notification services.	Third-party messaging services for applications built within the same environment.	**GOV.UK Notify** is a product to keep users updated by helping government service teams to send text messages, emails or letters.	No current Federal providers.
Identity and Security *Manage user authentication, single sign-on, and services to keep data safe.*	**6** services to establish identity (e.g. OAuth) and connections to other online identities (e.g. password-less login). **6** services for security, including SSL encryption for https URLs and website security scanning.	Cloud interconnect technology and managed VPN; tools for ensured compliance with common security standards.	**GOV.UK Verify** is a platform for identity assurance, so that individual users can access digital government services securely by stating who they are.	**Login.gov** is under development to provide a shared authentication and identity proofing platform supporting a streamlined login experience for end users accessing public Federal Government services.
Payments *Accept, process, store or transmit payment information in a secure environment.*	**1** unified add-on service to handle payments, mainly to supplement existing solutions (e.g. APIs for third-party applications) with automated billing.	No payment APIs, but platform validated for PCI data security standards.	**GOV.UK Pay** is a product that allows users to make payments to government in the same way, regardless of what service (e.g., passport or license renewal) is used.	**Pay.gov** provides a secure platform for handling payments to the Federal Government.
Deployment *Deploy, test, and share applications within a broader ecosystem to serve end users.*	**3** separate continuous integration and deployment add-on services. **3** additional testing services, including continuous, performance, and load	Open-source infrastructure to configure, continuously monitor, and manage deployment of containers. Hosted	**Platform as a Service for government (PaaS)** is cloud hosting that makes it easier and cheaper for teams across government to host	**Cloud.gov** is a new service that seeks to provide a Platform as a Service (PaaS) allowing government development teams to

[13] UK.GOV November 7, 2016 https://www.gov.uk/service-manual/technology/using-common-components

	testing. **1** private deployment environment.	application development for local testing. Additional GUIs for deployment and management.	applications, services and components. PaaS provides all the infrastructure you need for hosting services. This means individual teams do not need to build and manage their own infrastructure.	quickly launch and scale applications supported by a streamlined ATO process.
Shared Data Repository *Securely share continuously updating data with and between organizations.*	Provides hosted data storage APIs and services that could be used to implement this functionality.	Provides hosted data storage APIs and services that could be used to implement this functionality.	**Registers** are lists of information, and each register is the most reliable list of its kind. Each register is managed by a single person, known as a 'custodian,' who is responsible for keeping it up to date and accurate.	**Federal Data Service Hub** is a new service that seeks to provide privacy-protected verification services for certain program eligibility and enrollment decisions.

This table provides a few key insights. First, the services highlighted above are relatively flexible and are capable of being incorporated into many different end-use applications. A payment service, for example, could be used by agencies with widely different missions because the actual workflow and transactions are very similar. As potential developer platforms and services are considered, the applicability and use of those APIs across different departments, agencies, and mission spaces may be a helpful way to consider prioritization.

Second, when significant investment to build, maintain, and operate would be required to duplicate or copy the functionality provided by a service, there is more value for platform adopters. For example, significant costs are associated with securely storing and maintaining user accounts and providing strong authentication credentials that appropriately protects privacy. Services such as GOV.UK Verify that amortize high investment and operating costs across multiple consumers are good candidates for shared developer platforms and services.

Finally, many of the services highlighted in the table have both public and private-sector implementations. As the Federal Government considers where and how to invest, it is helpful to remember that the vast majority of developer platforms and services used by Federal departments and agencies will likely be procured directly from private-sector cloud and service providers. This means efforts to streamline the ability of Federal departments and agencies to procure commercial developer platforms and services will be critical to increasing uptake within the Federal Enterprise. As articulated in the 2012 Federal Information Technology Shared Services Strategy and in alignment with OMB guidance, the default approach for departments and agencies should be to procure external commercial solutions.

However, there are some requirements that may demonstrate the need for government-provided platforms and services created in partnership with industry. These include:

1. **Legal requirements** – there may be legal restrictions that limit the ability of Federal departments and agencies to procure or deploy certain external solutions;
2. **Unique mission requirements** – private-sector APIs and tools that meet certain unique needs of Federal departments and agencies may not exist;
3. **Data sensitivity** – data may have privacy requirements or other unique characteristics that prevent it from being hosted by or transmitted through external infrastructure;
4. **National security considerations** – there may be national security considerations for data or functionality that limit how private-sector solutions can be used.

Situations where one or more of the above criteria apply are generally rare when considering the whole Federal Enterprise but are nonetheless important to consider as part of a Federal ecosystem of developer platforms and service providers. It is also important to note that just because a service is provided by one department or agency to another does not mean that it will be wholly built or operated by Federal employees. Significant parts of a Federal developer platform or service may be built on existing commercial software and/or operated by private-sector entities or contractors. Thus, as the Federal Government considers where to invest in developer platforms and services, it is important to separate the mechanism of construction and operation from the model of delivering a service from one agency to another. As an example, the Intelligence Community (IC) implemented a high-security cloud shared between 17 different IC entities called IC ITE, based in government-owned facilitates but operated by a private-sector cloud vendor.[14]

Opportunities for Developer Platforms and Services

Appendix C provides a matrix of potential opportunities to support Federal departments and agencies considering investments in shared developer platforms and services. The matrix is derived from existing public and private cloud offerings and organized as a list of potential service areas evaluated across the following criteria:

- **Category** – A categorization of shared services based on common groupings in both the private and public sectors (e.g. infrastructure, messaging).
- **Benefit of Shared Service to Adopter** – A qualitative assessment of the benefits the service could provide to Federal departments and agencies if it were offered as a service bucketed into three categories: low, medium, and high.
- **Cost to Build, Deliver, and Maintain Service** – A qualitative assessment of the costs required if a Federal department or agency were to build, deliver, and operate a service bucketed into three categories: low, medium, and high.
- **Maturity** – A short description of service offerings within the Federal government and private sector.

The platforms and services listed in Appendix C are not intended to be comprehensive but should help provide the dimensions of possible investments as well as means for quickly comparing opportunities. For example, a shared service that generates PDFs from web pages may provide less overall value to Federal departments and agencies than a service that could perform multi-modal notifications or a service that provides website analytics. Even though a platform or service provides significant value, it may not be a good candidate for a Federal shared service. For example, if departments and agencies have effective procurement vehicles and the authority to use developer platforms or services offered directly from commercial vendors, the value of Federal shared service offerings goes down. Similarly, if there are no specific legal requirements, unique mission requirements, data sensitivities, or national security constraints associated with a candidate developer platform or service, it may be better for Federal departments and agencies to procure directly from the private sector rather than another agency.

Another important dimension to consider is the number of competing implementations of certain type of developer platform or service offering. The USSM model typically involves a single managing partner and multiple competing providers of a shared service to promote a competitive marketplace that reduces costs and increases value for customers. However, in certain very narrow situation, it may be appropriate to have a single Federal provider rather than a marketplace of providers. For example, there may be laws or regulations that limit the number of providers or there may be usability reasons to limit the ecosystem to a single Federal shared service provider. These complexities mean that care should be taken to consider the marketplace model when determining where to invest in developer platforms and services.

[14] IC ITE Fact Sheet https://www.dni.gov/files/documents/IC%20ITE%20Fact%20Sheet.pdf

Opportunities for Developer Data Services

Another approach to delivering a developer platform or service is the sharing of data rather than functionality. Federal departments and agencies procure, collect, and maintain data that may have value when shared with other Federal departments and agencies. Developer-focused APIs and services that host and provide secure access to data in a variety of useful formats from one Federal department or agency to another can be an important tool for increasing reuse and improving efficiency, effectiveness, and security across the Federal Government. This could include sharing data that already exists or sharing the collection or acquisition of new data to reduce costs.

Today, many Federal departments and agencies default to not sharing or limiting sharing of data. Part of the challenge is that there is inconsistency in statutory, privacy, security, and policy guidance on how data can be shared. Another challenge is that there is no database or registry of the available data across the Federal Enterprise. This makes it difficult to identify what data is available or which department or agency has or could share a particular data resource.

The interagency data science community of practice, the Data Cabinet, works with data leaders across the Federal Government to identify considerations and opportunities for encouraging appropriate and secure data sharing between agencies.[15] Experiences of the Data Cabinet have highlighted opportunities in data sharing, several of which are described below.

Consolidating Data Sharing Governance

The Data Cabinet found that the Federal departments and agencies most active and effective in sharing data typically had a single conduit (both within their agency and external to their agency) for responding to requests for data sets, analyzing data disclosure considerations, and generating data sharing agreements. This reduces duplication of work, increases data discoverability, ensures consistency of privacy, legal, and security analysis, allows for standardized templates to be used, and enables lifecycle tracking of data sharing agreements. Such agency centralization also encourages cross-agency collaboration in establishing and implementing data governance best practices. An example is the Office of Data Exchange under the Office of Data Exchange and Policy Publications (ODEPP) at the Social Security Administration.[16] ODEPP provides a central office to govern data exchange and facilitates coordination, oversight, strategic decision-making, policy, and procedures related to data sharing.

Streamlining Data Sharing

Another opportunity highlighted by the Data Cabinet is the development of common templates and agreements to streamline the data sharing process. Once appropriate authorizations are in place between two Federal departments or agencies, a data sharing agreement is typically needed. Similar to tools and guidance developed to support the Federal procurement process, there is an opportunity to establish models and create standard templates for data sharing agreements between agencies. For example, there are new efforts underway to break these “trust frameworks” down into fundamental assertions through a unified solution.[17] These assertions can be joined together to create new agreements out of already agreed-upon components simplifying and streamlining the process of generating agreements for new data sets. This work is being piloted in the national security and emergency response arena.

The approach of establishing clear, common patterns for government-wide use can have a significant impact. For example, the GSA Office of Government-wide Policy[18] has had success in standardizing a

[15] http://www.ntis.gov/thedatacabinet/index.html

[16] https://www.ssa.gov/dataexchange/

[17] https://trustmark.gtri.gatech.edu/

[18] http://www.gsa.gov/portal/content/104550

variety of operations data through the Data 2 Decisions initiative.[19] This is an important case study as it highlights how a policy directive can be used to effectively implement a common approach that simplifies the sharing of data. There is an opportunity to take this concept further and to streamline data sharing that meets statutory, privacy, security, and other legal requirements through common templates and patterns.

[19] https://d2d.gsa.gov/report/benchmarking-initiative

Barriers to Creation, Development and Adoption

Long-standing government-wide policies that were not written at a time when shared services were possible or available are opportunities for policy modernization. This section summarizes a set of those policy challenges including the ATO process, responsibilities of shared service providers and consumers under the Federal Information Security Modernization Act (FISMA), the interaction of Trusted Internet Connection policy with modern deployment and delivery models, the application of the Privacy Act, and funding models that support the growth and adoption of existing shared services and encourage the creation and development of new shared services.

Increasing Efficiency and Reuse of the Authority to Operate

FISMA and the Federal Information Technology Acquisition Reform Acts (FITARA) strengthened rules around ATOs and the internal security assessments and approvals required for an agency to utilize information technology in a production capacity. FISMA ensures that the head of each agency is responsible for "providing information security" of "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." FITARA in turn requires that each agency Chief Information Officer (CIO) have "a significant role in … the management, governance, and oversight processes related to information technology" and that an agency "may not enter into a contract or other agreement for information technology or information technology services, unless the contract or other agreement has been reviewed and approved by the Chief Information Officer of the agency." These are among other CIO authorities, some of which may be delegated in certain circumstances. In addition, the National Institute of Standards and Technology (NIST) Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," details requirements generally used to assess an information technology system for an ATO.

Some Federal agencies have interpreted existing authorities and guidance to require them to run independent evaluations without reliance on prior work done by other agencies. The Federal Risk and Authorization Management Program (FedRAMP) was established as "a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services."[20] As part of FedRAMP, the Department of Defense, the Department of Homeland Security (DHS), and the General Services Administration (GSA) established a Joint Authorization Board (JAB). In accordance with a 2011 memo from the Federal Chief Information Officer, the JAB grants "provisional authorizations for cloud services that can be used as an initial approval that Executive departments and agencies leverage in granting security authorizations and an accompanying Authority to Operate (ATO) for use."[21] Unfortunately, practice appears to indicate that many agencies continue to rely minimally, if at all, on these provisional authorizations in granting individual agency ATOs.

Compounding this issue, agencies often do not have the information necessary to leverage existing ATOs completed by other agencies. While GSA has established a cloud-ATO database, many agencies do not use it. While each agency must assess the details of a particular implementation, such as interaction with existing systems and specific data input into a system, there is a significant opportunity for agencies to share or build on other agencies' ATOs, especially in the context of shared services where agency implementation may be substantially similar. There are also opportunities for agencies to study the

[20] https://www.fedramp.gov/about-us/about/

[21] https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fedrampmemo.pdf

feasibility of relying more on provisional authorizations without performing complete re-assessments. Even if there is a need for supplementary levels of validation that exceed prior ATO efforts, NIST standards address the vast majority of controls and are therefore largely addressed by programs like FedRAMP.

Shared Responsibilities

As identified above, FISMA places primary responsibility for each agency's information technology systems with the agency head but does not detail the relative roles and responsibilities of provider and customer agencies. This lack of clear delineation between the roles and responsibilities of provider and customer agencies in the context of shared developer platforms and shared services may slow adoption. This current lack of detail provides an opportunity for further policy clarification.

Modernization of Trusted Internet Connections (TICs)

The TIC initiative facilitates perimeter control through a "reduction of our external connections, including our Internet points of presence."[22] The TIC program was important to increase government-wide network situational awareness at the time of its establishment, but some requirements have not kept up with technological innovations. In particular, increased use of cloud services and mobile devices by agencies can be incompatible with the current TIC reference architecture because of its network-focused perimeter control methodology. The focus on network-level security also misses important modern security data inputs such as end-host and application-level logs. As demonstrated by the TIC Overlay pilot program implemented by DHS in coordination with OMB in 2016, there are other methods of implementing security controls that can improve security without significant additional costs.

Applying the Privacy Act

The Privacy Act requires that each agency "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President." In addition, to the extent that an agency establishes a new system of records to maintain such information, it must publish a System of Records Notice (SORN) in the Federal Register and comply with other requirements under the Privacy Act, such as potentially executing a computer matching agreement (CMA) with any other agencies who may exchange records with the new system of records.

Shared services can give rise to new, complex questions under the Privacy Act. For example, to the extent that a shared service is merely technical infrastructure that does not incorporate a client agency's data into its systems, the provider agency may not need to publish a SORN. Instead, depending on the facts and circumstances, the SORN may be maintained by the agency responsible for the data flowing through the infrastructure. Wide-scale adoption of these types of arrangements could have a big impact on promoting the use and realizing the benefits of shared services.

Funding Mechanisms

Another challenge faced by shared service providers is the lack of access to capital necessary to modernize existing legacy applications, replacing of obsolete infrastructure, expanding services, and keeping up with rapidly changing technology. This limits the effective and efficient delivery of services. In addition, prospective customers can sometimes face large upfront capital requirements to support migration to a shared service.

[22] Established in OMB M-08-05

Many shared services are financed through a fee-for-service approach via intragovernmental revolving funds, which include working capital funds, supply funds, and franchise funds. While there are similarities in their authorities and operations, lack of consistency in their authorizing language and agency interpretations have created an uneven playing field across the environment. A well-functioning marketplace will require normalized interpretations of rules surrounding revolving funds and financial transparency around the use of customer payments. Additionally, a centrally-managed fund for government-wide use that supports the need for more capacity at shared service providers, provides seed money to improve shared services systems, and assists customers with modernizing and migrating to shared service providers, would help address some of the current state challenges. Overall, these efforts would allow providers to operate more like a business by having the pricing flexibility to more strategically align investments to future demand and providing the opportunity for technical innovations while also providing consistency and increased transparency to the marketplace.

Conclusion and Key Findings

This report has sought to explore the potential of developer-focused shared services as a core strategy in transitioning to a more efficient, effective, and modern Federal Government. The central hypothesis explored in this report is that a system made of small, modular, reusable, shareable components can be more agile and flexible than a tightly-coupled monolithic system. Loosely coupled modular building blocks can be readily rearranged, whereas it can be hard and expensive to make significant changes to a large monolithic structure in a complex environment like the Federal Enterprise.

The trend toward modularity is also common in the private sector where a platform group provides common infrastructure and services that are available to teams across the organization. The Federal Government is behind in adopting this modular approach. Indeed, the lack of developer platforms and services available to departments and agencies is a problem that will only become more acute with each passing year as the need for APIs supporting the delivery of web and mobile applications continues to grow in importance.

There is good news. This report has shown that the shared services model previously applied to administrative and other back-office functions can provide a foundational approach for sharing developer platforms and services. Other countries like the United Kingdom and Estonia have implemented platform strategies based on similar models. This report explored a wide range of possible Federal developer platforms and services, including data sharing services and investigated different approaches and prioritization models for deploying them as shared offerings. This report has provided background support for three central findings:

1. Developer platforms and services are key mission enablers in the public and private sectors. The shared service model already deployed in the Federal Government provides an approach to governance, deployment, and funding for developer platforms and services.
2. There are a wide range of immediate opportunities for the Federal Government to support a growing ecosystem and marketplace of developer platforms and services (e.g. identity, notification, data sharing) based on an analysis of needs and on experiences from the private and public sectors.
3. There are policy reform opportunities that can accelerate developer platforms and services, as well as certain administrative shared services, including streamlining the ATO process, clarifying responsibilities in shared environments, modernizing TIC policy, exploring how the Privacy Act applies in these contexts, and further supporting new funding models.

These findings support an aggressive approach to building a robust ecosystem of developer-focused shared services designed to support Federal departments and agencies. This will require close collaboration between industry and government, disseminating lessons learned from early adopters, leveraging existing services and contracts, and sharing information.

Appendixes

Appendix A: Examples of current Federal developer platforms

Service	Brief Description
login.gov	Shared authentication and identity proofing.
fedramp.gov	Standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
cloud.gov	Cloud-hosting product line for Federal teams, addressing security and scalability.
analytics.usa.gov	Analytics and user tracking for government websites.
pay.gov	A secure platform for handling payments to the Federal Government.
federalist.gov	A unified interface for publishing static government web pages.
api.data.gov	A free API management service for federal agencies aimed at making it easier for agencies to release and manage APIs.
ipp.gov	Invoice Processing Platform is a secure, web-based service that more efficiently manages government invoicing from purchase order (PO) through payment notification.
esc.gov	Department of Transportation's Enterprise Services Center provides a wide array of platforms to manage information. IT Services offers support in numerous areas: Applications Services, Customer Services Center (help desk), Data Center Services, Information System Security, Media Solutions, Office Automation Support, Project Management Office, National Wireless Program, and Telecommunications Services.

Appendix B: Case studies of existing Federal developer platforms and services

Case Study: Login.gov

Login.gov is a shared authentication platform under development by 18F, part of the General Services Administration (GSA) Technology Transformation Service (TTS). The primary objective of the platform is to support a streamlined login experience for end users accessing Federal Government services.

In addition to making logging in to government sites easier, the public will also benefit from a more streamlined and efficient interaction with the Federal Government in general. This system is designed to provide a single account for government, giving control over interactions with agencies, and breaking down critical barriers between participating agencies. It will enable government to:

- Create a simple, elegant way for the public to verify their identity, log in to Federal Government websites, and, if necessary, recover their account.
- Build experiences, processes, and infrastructure that will use the latest available technology to safeguard all user data.
- Deliver software that allows government developers to integrate in hours instead of weeks.
- Leverage private-sector innovation and capabilities wherever possible.
- Preserve privacy by mitigating privacy risks while also adhering to all Federal privacy guidelines.

How it works

When a citizen attempts to access an agency service or record they will be directed to login.gov. Login.gov will then allow the user to sign-in and/or create an account based on whether the user has created an account previously. In addition, the user will register their phone to allow her or him to sign in securely using multifactor authentication (MFA) moving forward. In addition to account maintenance, the service also allows full account recovery functionality.

Login.gov will also provide identity proofing for users logging into the platform. Identity proofing enables agencies to share more sensitive data and functionality with their users because they will have already verified their identity through login.gov. The platform will do this through third-party identity service providers, government APIs and other data sources integrated into the experience. By doing this work on a single shared platform, user interactions are streamlined with the public while also reducing costs.

The largest cost in software is frequently integration. Agencies and login.gov reduce this cost considerably by leveraging industry standard protocols and APIs. By doing this once as a shared platform, the software, documentation, and processes are reusable across agencies, providing value for the entire government ecosystem.

Next steps and further development

At the time this document was written, the login.gov platform was in the process of being productionized. The platform is expected to roll out early in 2017, allowing adoption across Federal departments and agencies in FY2017 and FY2018.

Future development within login.gov will focus on improving identity proofing. The initial implementation will leverage third-party financial proofing, but will quickly expand to include state identifications, government data verifications, and potentially other methods to identity proof individuals.

Case Study: Cloud.gov

Cloud.gov allows a government development team to focus on what matters: their applications. As a Platform as a Service (PaaS), cloud.gov eliminates the need to manage infrastructure such as virtual machines and servers. This enables the development team to rapidly iterate, quickly launch, and scale applications to ensure mission success. Because cloud.gov is based on open source technologies, it provides portability to other cloud providers or an existing on-premise solution. 18F, housed within the General Services Administration (GSA) Technology Transformation Service (TTS), develops and operates cloud.gov.

There is a long list of requirements and best practices for digital services provided by Federal agencies, some of which are legally binding. Deploying an application in this regulatory environment is difficult and costly. It is costly to both manage the ATO process and design a robust service infrastructure. Cloud.gov manages the shared technical and legal requirements common to Federal Government systems.

How it works

Cloud.gov is based on Cloud Foundry, an open source cloud computing platform distribution. It is deployed on Amazon Web Services in the dedicated GovCloud environment. Third-party developers can host their own deployment of the cloud.gov platform on their own servers since 18F makes available all modifications and enhancements as open source code. Tools to generate security documentation, continuing assurance, and other features to comply with FISMA regulations and agency specific ATO requirements are also provided through the cloud.gov Compliance Toolkit.

Cloud.gov offers a free sandbox account to all government staff to evaluate the platform. After an Inter-Agency Agreement to procure cloud.gov services is executed, 18F provisions a new project setup for the development team which can house a number of environments for a given system (e.g. QA, staging, production). This setup also provides additional team management capabilities. Through the cloud.gov marketplace, developers can view and utilize offered technology services such as databases or cloud storage. Developers can deploy applications into their cloud.gov environment and immediately access and scale them. Additional management and maintenance capabilities such as metrics and logs are available.

Next steps and further development

Cloud.gov was built as a multi-tenant service. Roughly 300 applications from various agencies were operating on cloud.gov as of January 2016, with the ability to scale based on demand. The operating applications include Every Kid in a Park, College Scorecard, and Federalist. The outstanding issues around cloud.gov have not been compiled, however the 16 Github repositories that comprise the developer platform have dozens of feature requests and bug fixes from both government and third-party developers. GSA is currently funding cloud.gov, but revenue is full cost-recovery through GSA Acquisition Services Revolving Fund via Inter-Agency Agreements (IAA).

Case Study: Pay.gov

Pay.gov is a secure platform for handling payments to the Federal Government. It was established in October 2000 by the Bureau of the Fiscal Service to satisfy the U.S. Department of the Treasury Financial Management Service's commitment to electronic collections processing using Internet technologies.

How it works

Pay.gov provides four modular services to agencies:

1. **Collections**. Pay.gov processes ACH (Automated Clearing House) debits and plastic card collections, and allows payments using alternative payment services such as PayPal and Dwolla. After payments are processed, the resulting deposits are forwarded to the Collections Information

Repository (CIR). Deferred and recurring payment options are available for some payment methods.

2. **Reporting**. Aggregated reports of transactions are also generated through platform use.
3. **eBilling**. This service allows agencies to send electronic billing notifications for payments due. The notifications are sent to the user by email and includes instructions on how to view the bill and make a payment.
4. **Forms**. Pay.gov can host agency forms online. Over 1,000 electronic forms are hosted.

Security is a core dimension of pay.gov, specifically ensuring that transaction pipelines meet FIMSA and FIPS 140-2 guidance, use SSL, and are hosted in the Treasury Web Application Infrastructure (TWAI) located in Federal Reserve Banks.

Next steps

As of 2016, Pay.gov collects over 119 million transactions worth over $106 billion per year and has broad acceptance across agencies. More features, new operating systems, and devices are in planning stages for the service. Knowledgeable clients can spin up a pilot in days and a small program in two weeks. Reducing the transaction or development costs as business development accelerates is required for widespread adoption.

Appendix C: Federal developer platforms and services opportunity matrix

Category	Service	Benefit of Shared Service to Adopter	Cost to Build, Deliver, and Maintain Shared Service	Current Maturity *(As of publication date)*
Analytics	Basic website analytics	**[Medium]** Provides agencies and leadership visibility into online service and information engagement	**[Low]** A simple service can be provided as wrapper on top of existing website analytics services	*GSA provides analytics.usa.gov as a free service to Federal departments and agencies*
Analytics	Exception reporting	**[Medium]** Provides alerts, warning, and track of errors, warnings, or other unexpected behavior of online services	**[Medium]** Requires a secure high-availability service that can manage large volumes of data and accept input from a wide range online applications and services	*No Federal providers, some mature private-sector providers*
Business Processes	Eligibility determination	**[High]** Ability to determine benefits eligibility provided as a service is complex and centralization can enhance efficiency, security, fraud detection and prevention	**[Medium]** Services could be built and delivered on top of key Federal data sources but require data protection	*Federal Data Service Hub provides privacy-protected verification services for certain program eligibility and enrollment decisions*
Business Processes	Workflow management tools	**[High]** Workflows involving documents, notifications, eligibility determinations, and other verifiable steps are ubiquitous across government; better tools to securely manage those workflows could improve the ability of agencies to deliver on mission activities	**[High]** Workflow management tools are complex, involve many integrations, and must continually evolve as new inputs, outputs, and processes evolve with technology	*No Federal providers, many mature private-sector providers*
Business Processes	Sentiment analysis	**[Low]** Ability to automate detection of shifts in the tone of conversations	**[High]** Natural language processing is an emerging field and, at scale, requires significant computing resources and sophistication with NLP algorithms	*No civilian Federal providers; a range of open source software is available*
Business Processes	Generate PDFs from web pages	**[Low]** Crude webpage-to-PDF tools exist at the end-user operating system level, but don't provide a consistent user experience	**[Medium]** A PDF generator that is fully compliant with Federal data standards can be complex to build, deliver, and maintain	*Range of existing commercial products and some open source solutions*
Business Processes	Optical character recognition of documents	**[Low]** Can provide some possible efficiency gains to certain workflows	**[Medium]** A service could be built on top of existing OCR products and software	*No Federal providers, many private-sector products, providers, and open source solutions*
Business Processes	Generate QR codes	**[Low]** QR codes are 2-dimensional bar codes that allow linkages between non-digital and digital content; some QR scanner apps are installed on smartphones	**[Low]** QR code generation is relatively simple and could be wrapped in a package to ensure compliance with Federal open data standards	*Open source tools exist*
Collaboration Tools	Project management	**[High]** Efficiency, security, end-user experience, better organization of projects, better visibility for leadership	**[Medium]** Building and maintaining secure and available project management systems with notifications, mobile support, and other modern features can be complex	*No mature Federal providers, many mature private-sector providers*
Collaboration Tools	Source code hosting	**[High]** Efficiency, security, end-user experience, faster delivery of projects; a set of repositories for Federal workers could help facilitate interagency sharing and collaboration	**[Medium]** Operating a secure and available source code repository with bug tracking and other modern features is complex	*No Federal providers, many mature private-sector providers*

Collaboration Tools	Bug reporting and tracking	**[Medium]** Modern bug tracking systems are often integrated into project management and/or source code hosting functions; this is an important and useful function but it is unclear if it should be separated	**[Medium]** Operating a secure and available bug tracking management system with notifications, mobile support, and other modern features is complex	*No Federal providers, many mature private-sector providers; also, there are open source bug tracking systems that could be leveraged*
Identity	Authentication of Federal workers and affiliates	**[High]** Significant efficiency and security advantages to centralizing validation of HSPD-12/PIV credentials and to aggregating certificate information from across Federal Enterprise	**[High]** Authentication infrastructure is complex, requires strong security, and needs high-availability	*No mature government-wide federal provider today but Treasury maintains PKI infrastructure that could be scaled*
Identity	Secure and reliable authentication for citizen-facing services	**[High]** Significant efficiency, security, end-user experience benefits in centralizing authentication to Federal resources and supporting a variety of strong credentials as innovation continues	**[High]** Authentication infrastructure is complex, requires strong security, and high-availability	*Login.gov is a Federal provider of developer APIs for citizen-facing authentication under development by GSA; There are private-sector identity providers*
Infrastructure	Fraud detection	**[Medium]** Improved efficiency, security, reduced losses due to fraud; there are benefits to sharing signatures of fraudulent behavior across Federal departments and agencies	**[High]** Fraud detection takes on many forms and requires an understanding of the complex interaction of user needs, Federal services, and regulations	*No Federal providers, some emerging private-sector API providers*
Infrastructure	DDoS detection and prevention	**[High]** DDoS detection and prevention have become increasingly important as more critical services that citizens rely upon are moved online	**[High]** DDoS detection and prevention require a sophisticated understanding of network architecture and often access to significant resources	*Many mature private-sector providers*
Infrastructure	Load testing	**[Medium]** Helps ensure that services and sites perform under expected normal and peak load using testing tools and server capacity to simulate high demand	**[Medium]** The infrastructure (network resources, bandwidth, etc.) required for proper load testing can be significant	*Many mature private-sector providers*
Infrastructure	Archiving data (long-term storage)	**[High]** Long-term storage to support backup, disaster resilience, and retention use cases for large amounts of data cheaply	**[High]** Archival of Federal data with high reliability and low cost typically requires significant investment to achieve meaningful economies of scale	*Many mature private-sector providers*
Infrastructure	File/data storage	**[High]** Simple, secure, reliable storage of data is a critical component in building most digital services	**[High]** Building and maintaining a secure and highly-available data storage environment is complex and requires significant operational resources	*Many mature private-sector providers*
Infrastructure	Website hosting	**[High]** Secure, reliable website hosting is an essential part of delivering digital services	**[High]** Building and maintaining a secure and highly-available hosting environment is complex and can require significant operational resources	*Cloud.gov is a shared service web hosting environment provided by GSA; There are also many mature private-sector offerings*
Infrastructure	Container repository	**[Medium]** Containers offer developers a way to package applications and all their dependencies to enable rapid deployment with consistent configurations	**[Low]** container repositories are simple to host and maintain	*No Federal providers; private-sector services are emerging with competing container standards*

Infrastructure	DNS management	**[Medium]** Domain name management is an essential part of building and delivering reliable digital services	**[High]** Delivering reliable and secure DNS is complex and requires careful monitoring and upkeep at all times	*Many mature private-sector providers and dotgov.gzov (GSA) for .gov domain registrations*
Infrastructure	Continuous integration testing	**[Medium]** Ensures that mobile and online services perform as expected when deployed; requires testing tools and processes to ensure changes don't introduce bugs or feature regressions	**[Medium]** Continuous integration services often require a supporting many programming languages and frameworks, making it challenging to generalize across agencies' needs	*A range of emerging, hosted private-sector providers exist and there are many open source solutions*
Messaging	Notification service	**[High]** Notifications are a key part of many government workflows; a service that provides a range of notification modalities such as postal mail, email, push notifications, text, and calls in a secure and reliable manner can accelerate the delivery of many online services	**[Medium]** There can be significant complexity in integrating a range of communication modalities that perform in a reliable and secure manner; there are some advantages to Federally-provided service that can validate addresses against internal data sources and save preferences once for each citizen	*No Federal providers, some private-sector providers*
Payments	Payments in	**[High]** Accepting payments is a key aspect of many government workflows; the utility is higher if multiple currencies, languages, and payment providers are also supported	**[High]** Payment infrastructure is complex, requiring strong security, and high-availability	*Pay.gov is a mature provider established in 2000 by the Bureau of the Fiscal Service; there are also a range of private-sector providers*
Payments	Payments out	**[Medium]** Sending payments is a key aspect of some government workflows; the utility is higher if multiple currencies, languages, and payment providers are also supported; fraud detection is also critical	**[High]** Payment infrastructure is complex, requiring strong security and high-availability; there are also significant anti-fraud mechanisms required for sending payments	*No Federal providers, some private-sector providers*
User Management	Status tracking	**[Medium**] Maintaining the state of a transaction or object in government workflows is a common task; a secure, reliable, hosted service for status tracking could be a helpful tool for implementing online services	**[Medium]** A secure and reliable service for maintaining status across many types of transactions, objects, and supported by many programming languages, is challenging to build and operate	*No Federal providers, some private-sector providers*
User Management	Simple appointment booking	**[Low]** Could help provide a unified end-user experience for certain workflows	**[Medium]** A secure and reliable service for providing appointment booking across many use cases can be challenging to build and operate	*Some mature private-sector providers*