GLOBAL government FORUM | DIGITAL

FROM LAGGING TO LEADING:

The Opportunity for a Breakthrough in U.S. Government Digital Service Delivery

KEVIN CUNNINGTON | ANDREW BESFORD

A STUDY OF U.S. FEDERAL CIO COUNCIL MEMBERS | NOVEMBER 2024

Contents

Thank you to the members of the US Chief Information Officers Council who took part in this study:

Clare Martorana
Federal CIO
Office of Management and Budget

David Shive
CIO
General Services Administration
(and vice-chair CIO Council)

Tony Arcadi
CIO
Department of the Treasury

Eric Hysen
CIO
Department of Homeland Security

Darren Ash
CIO
Department of the Interior

Cordell Schachter
CIO
Department of Transportation

Guy Cavallo
CIO
Office of Personnel Management

Jeff Seaton
CIO
National Aeronautics & Space Administration (NASA)

Ann Dunkin
CIO
Department of Energy

Gary Washington
CIO
Department of Agriculture

Brian Epley
CIO
Department of Commerce

Jennifer Wendel
Acting CIO
Department of Health and Human Services

Marcela Escobar-Alava
CIO
Social Security Administration

Introduction

The new administration has an opportunity to champion a bold vision that positions the U.S. as the global leader in modern government service delivery. The United Nations E-Government Survey 2024, a key measure of countries' digital government performance, currently ranks the U.S. in 19th position globally. Both the American public and global observers expect the U.S. to lead the world in digital government innovation—this is the moment to realize that vision.

To meet these expectations, the U.S. government must deliver a seamless, simple, and secure experience that meets the needs of the American people whenever they interact with public services, reflecting the world-class digital experience championed by the U.S. private sector as a global technology leader. There is consensus around the aim: this bold vision for digital government would center around citizen experience and improved use of data, enabling personalized services that cross agency boundaries, and bringing in new technologies like AI. It will require secure and resilient infrastructure, and the workforce to deliver it must have up-to-date technical skills and be empowered to deliver in an agile way.

However, during our program of interviews with members of the CIO Council, representing the largest U.S. Federal Departments, we identified the common themes which are preventing agencies from making enough progress toward this vision. Through this report we aim to prompt a meaningful discussion on how to unlock some of these challenges so that the U.S. Federal Government can establish itself as the global leader. Drawing on our international expertise, we have compared insights from the U.S. leadership with global best practices. Overall, we observe that initiatives like the Technology Modernization Fund (TMF) and Federal Information Technology Acquisition Reform Act (FITARA) have advanced the modernization of U.S. government digital services. However, during this time, other leading G7 countries have gone much further to modernize and create organizational capabilities and funding models, to push the boundaries of delivering a government that meets today's expectations of modern government service delivery. As a consequence the U.S. needs to be much more ambitious to get into the top 10 of the United Nations ranking during the four-year term of this next administration—and set an ambition onwards to the top position.

In developing our observations and recommendations, Global Government Forum (GGF) has compared the insights from the interviews with findings from other international reports produced by GGF, which include input from over one-third of the world's governments.

While no two countries are the same, the scale and complexity of the U.S. government is globally unique. The technology workforce within individual U.S. federal agencies is often larger than the entire technology workforce of many countries' governments. To offer a simplistic comparison: while the U.S. population is roughly five times that of the UK, the U.S. federal technology workforce seems to be at least 10 times larger than its UK equivalent, though exact figures are unavailable.

While a direct comparison between the U.S. and other leading digital governments presents challenges, several noteworthy distinctions are apparent:

- **There is a lack of a clearly stated ambition, political sponsorship, and representation for technology at the highest levels of government. CIOs told us that their Secretaries and Deputy Secretaries don't have a bold, impactful vision for the role of technology in support of their agency's mission, and technology leaders don't have sufficient influence at the most senior level.**

  Notably absent from our interviews was any mention of strong political sponsorship or support for their technology agenda. In other countries, modernization has been driven by senior political leaders with the objective of improving the citizen experience as well as providing greater effectiveness within the federal workforce. Typically, this sponsorship comes from a high-ranking Secretary within the Cabinet who is responsible for finance or efficiency. This senior Secretary is often regarded as a 'first among equals' within the Cabinet and has the influence and authority to drive this agenda.

  We note that the Director of the Office of Management and Budget and Director of the Office of Science and Technology do not carry the same level of seniority as their international counterparts in their equivalents of the Executive Office of the President.

  Additionally there is a need for clarity around the organization of federal technology. The executive digital leadership is dispersed across multiple entities, including the Office of the Federal CIO in the Office of Management and Budget (OMB), the General Services Administration (GSA), including Technology Transformation Services and 18F, and the United States Digital Service (USDS) within the Executive Office of the President of the United States. Federal employees who are technology professionals also fit into human resources policy as provided by the Office of Personnel Management (OPM). While we heard this does come together in a partial way in the CIO Council, there are additional councils of Chief Data Officers (CDOs), Chief AI Officers (CAIOs), and Chief Information Security Officers (CISOs). The current fragmented ecosystem, which depends heavily on collaboration, leads to a lack of a unifying vision for departments to align around. Formalizing the organizational structures and accountabilities to drive progress toward the vision, with an aligned funding plan, will be essential to accelerate digital modernization.

- **Investment in the federal technology workforce is insufficient, and their efforts are hampered by an environment weighed down by extensive, often outdated legislation and processes.**

  Current U.S. IT staffing frameworks—such as the GS-2210 Information Technology Management Series within the General Schedule—are based on experience and grade, where pay is tied to these criteria. By contrast, other advanced digital governments have

moved away from this model, instead adopting models that are more in line with the private sector, with compensation based on specific roles and competencies rather than tenure or grade.

- **Significant duplication exists across the federal government, as a result of a lack of central coordination, leading to extended times to market.**

  Across and within agencies, there is a very significant level of duplication of functions, technology, processes and data. This redundancy not only leads to inefficiencies but also complicates efforts to streamline operations, modernize systems, and improve service delivery. Agencies acknowledge that they frequently develop independent solutions to similar challenges, resulting in fragmented systems that are costly to maintain and difficult to integrate. In contrast, other countries have accelerated digital transformation by addressing duplication—leveraging common services, architectures, and training, under strong central mandates, to make their taxpayer dollars go further.

  A central theme of our recommendations is to address this duplication through intentional reuse and sharing across multiple federal entities. When done right, this approach can accelerate progress, reduce costs, and foster greater interagency collaboration, improving both operational effectiveness and the citizen experience. However, it will require thoughtful centralized control, funding, and governance to be effective, led by the formalized organizational structure noted above.

Our recommendations build upon the progress that has been made but also set the U.S. on a path to becoming the unrivaled global leader in modern government service delivery. In summary our five key recommendations are to:

1. **Build upon the success of the Technology Modernization Fund and modernize service delivery at scale**
2. **Increase the Federal CIO's authority to drive digital modernization**
3. **Modernize the technology workforce to get the Federal Government working differently**
4. **Support new CIOs and create a CIO talent pipeline**
5. **Pare down the accumulated legislation that holds back transformation**

The new administration should swiftly engage in detailed work to develop these recommendations to seize the opportunity to make meaningful progress during its tenure.

This is GGF's first report on the U.S. Federal Government. It is anticipated that we will revisit this subject on a regular basis to support the curation of the agenda and content for discussion at the annual Government Service Delivery conference in Washington DC. This event will be a unique opportunity to track progress on U.S. digital delivery under the new administration.

Challenges and progress in digital transformation across the U.S. Federal Government

This report set out to identify opportunities to accelerate modernization of public service delivery across the U.S. Federal Government. We interviewed the Federal CIO and 12 members of the CIO Council, following the structure of the 7 Lenses of Transformation methodology that was developed by the UK government. Further details are provided in Appendix I.

Our discussions with CIOs leading digital transformation in federal agencies revealed a clear and shared focus on five priority areas: cybersecurity, legacy modernization, skills development, user-centered design (UCD), and artificial intelligence (AI).

Central prioritization and support have driven clear progress

The clearest progress has been achieved on priorities where there has been centrally coordinated support from the Office of the Federal CIO and the CIO Council, bolstered by legislative or Executive Order direction. This progress highlights the value of a unified agenda, with consistent leadership messages and, ideally, aligned funding.

The CIO community, particularly through the CIO Council, has found value in working together and is optimistic about building on its success. Other linked communities, such as the CDO, CAIO, and CISO councils, were also cited as beneficial examples of collective leadership.

A number of positive actions were highlighted by interviewees:

- **Success of the TMF:** Every CIO told us about the scale of the challenges their agency faces remediating and modernizing its legacy IT systems and technology. Every CIO mentioned the Technology Modernization Fund (TMF), authorized by the Modernizing Government Technology (MGT) Act. The TMF has made 67 investments across 34 federal agencies.

  The success of the TMF has been attributed to its ability to evolve over the seven years it has been running. During this time the agencies, and the perspective from the White House, have evolved. At its inception, the TMF was created through a different process with budget colleagues, and pressure to turn it into a budget repair fund has been successfully resisted. CIOs, however, gave us a range of views on accessing funds. In particular there was inconsistent appreciation of the 'exploratory' direction of the fund, and the way of working where a larger (say, $100m) problem could be broken up into tranches (of say, $15m). This approach to the TMF could enable agencies to demonstrate the initial value, and having proven the concepts help support more effective conversations with appropriators for longer-term investments.

  While CIOs generally told us that the TMF had helped them make progress, they flagged

that much remains to be done on their legacy systems and technology, and that the TMF could evolve further to better meet their needs.

- **Urgent cybersecurity actions:** CIOs were particularly positive about the progress made in addressing urgent cybersecurity needs, largely driven by Executive Order 14028. They appreciated the OPM's Government-Wide Direct Hire Authority for Cyber Positions under the GS-2210 series, which has helped bring in specialists with the necessary skills. There was a strong sense of collaboration, with many CIOs expressing that they were "all in it together" on cybersecurity. Several CIOs also attributed successful turnarounds to effective monitoring and measurement efforts.

  Partly in response to cybersecurity incidents such as Log4j and then SolarWinds, the TMF allowed agencies to respond rapidly, accessing $1bn of funding quickly and outside of the normal appropriation cycle. As a result, the federal IT ecosystem is now secured at a much improved level. However, maintaining the security of legacy systems still remains a significant challenge, and new developments led by programs face delivery pressures that make it hard for them to prioritize cybersecurity capabilities.

Agencies agree on other priorities, but are implementing independently

In other high priority areas, which are as important as those above, there was greater variation in the response to the challenge. The response has been left to individual agencies, with less central coordination, leading to differing approaches, and only some areas where best practice has been established amongst CIO peers.

- **Funding**: All CIOs told us that they faced challenges with funding and saw addressing this as a priority.

- **Approach to prioritizing legacy modernization**: The scale of legacy systems and technology means CIOs have to prioritize which parts to address first. There is no shared view on how quickly they can go or what “done” on a practical level might look like. CIOs face tradeoffs, like whether to work on those with the most sensitive data vs. work on those that are preventing service modernization.

- **Skills**: CIOs are utilizing a broad spectrum of strategies, both within and across agencies, to acquire and retain the critical skills needed at various levels of seniority. At the same time they are trying to introduce modern work practices and emphasize user-centered design (UCD). We observed a variety of approaches on key topics such as hiring, contractor engagement, talent identification, and more.

Some common challenges do not have clear prioritization or ownership

Discussions with CIOs also highlighted areas that were generally acknowledged to be problems, but that do not have clear ownership to drive toward a way forward:

- **Legislation and compliance**: CIOs commented that they spend more time on compliance than assessing risks. Resolutions to these perceived issues can not be driven by agencies.

- **Vision and plan:** CIOs described a situation of siloed funding to siloed programs, making it challenging to align teams to a singular vision for technology modernization. Some agencies do have widely understood long-term plans for technology modernization, but most do not. CIOs told us they find it challenging to make multi-year technology investments that span administrations.

- **Opportunity to reduce duplication:** In our discussions with CIOs, many acknowledged the significant duplication of efforts across agencies, which not only risks inefficiencies in the use of taxpayer dollars but also limits the speed at which digital modernization can be achieved. Several participants cited the renewal of major vendor contracts as a clear example of where duplication could be reduced. Additionally, while AI is still in its early stages, agencies are mostly working independently to explore its potential impact and to address challenges related to managing federal data for training AI models.

Recommendations

Our recommendations focus on pragmatic, consensus-based steps that can realistically be implemented by any administration. We have prioritized actionable, achievable initiatives that will help to drive progress within the next administration's timeframe.

1. Build upon the success of the TMF and modernize service delivery at scale

The TMF has been a success. CIOs were quick to point out that there is a huge amount still to do. We recommend that the Federal Government should continue to fund the TMF in a robust way, and continue to evolve the way the fund works.

Tackle legacy now to be ready for the future

The TMF has been successful in addressing critical needs, yet several challenges remain. One issue is the misunderstanding around its purpose. While some CIOs view the TMF as a budget supplement, it is intended to be an exploratory fund—best used to explore the approach to tackling large modernization challenges and pave the way for formal appropriations. There also appears to be confusion about whether the TMF is applicable to all legacy services, with some believing it is limited to projects with a user experience focus.

At this point, the TMF has effectively run its course, with funds exhausted and no clear path to secure additional appropriations from Congress. Long-term, multi-year planning is essential to ensure that the TMF is more strategically targeted, not just for certain projects but for broader modernization efforts, including those beyond citizen-facing services. Technology investment is a lifecycle, not a one-time effort, and agencies should align their TMF proposals to reflect a five-year plan for their agency.

Additionally, while the TMF has made some provision for common platforms, we believe this could go much further. The fund could more effectively incentivize shared endeavors, as current structures have mostly led to duplications rather than consolidated solutions.

CIOs highlighted that while progress has been made, there is still much more to do, particularly in terms of agency-specific modernization efforts, potentially supported by the TMF. Modernization presents an opportunity to address other expectations, such as improving accessibility in line with Section508.gov.

CIOs suggested continuing to prioritize the top six federal agencies, which account for 80% of all public transactions each year on websites including IRS.gov, Medicare.gov, SocialSecurity.gov, StudentAid.gov, Travel.State.gov, and VA.gov. In addition to these high-volume systems, the appropriate prioritization may include others with a potentially debilitating impact, those on the Government Accountability Office’s High Risk List, or High Impact Service Providers (HISPs).

On the topic of branding, internationally, a number of countries have consolidated their digital efforts under a single online brand, and we discussed this during our interviews. While there are potential benefits to unifying the branding of federal websites beyond USAGov, we concluded

that the level of disruption and investment required would be difficult to justify at this time. Therefore, we are not recommending a full rebranding exercise.

Recommendation 1.1

Renew the Technology Modernization Fund (TMF): Ensure its purpose is clearly understood and continue successful remediation efforts.

Increase CIO discretion

In addition to the TMF, there remains a critical need for smaller, localized initiatives that agency CIOs can implement without the burden of lengthy application processes. In many cases, the cost of applying for funds can exceed the cost of the work itself.

This could be used, for example, to implement shared security features within agencies, such as a security operations center, or cybersecurity tools that could otherwise go unfunded due to ring-fencing.

CIOs expressed the necessity for more authority to allocate resources where they are most needed. One potential solution could be to provide each CIO with a dedicated fund—suggested by some as a flat percentage of the total IT budget—allowing them to utilize these resources to drive critical work within their agency.

Recommendation 1.2

Explore options for CIO discretion: Investigate methods to empower CIOs with greater discretion in spending decisions.

Expand the scope of shared initiatives

Some mechanisms already exist for sharing capabilities across agencies, such as SAM.gov and FedRAMP. However, the conditions required to establish large initiatives—such as leadership alignment, agency collaboration, and sufficient time remaining in an administration—make them relatively rare. Current structures do not systematize or incentivize cross-government sharing. None of our interviewees mentioned the Federal Infrastructure and Common Application Collaboration Center which was established under FITARA.

Despite the lack of mechanisms to share, CIOs identified numerous opportunities for collaboration, including shared contracts, joint development efforts, and exchanging best practices. Many believe that greater sharing would lead to faster, more efficient outcomes with less waste. As one CIO noted, “there’s a core set of imperatives that can move any agency forward”.

During our interviews, we identified a spectrum of sharing opportunities, including both existing and emerging areas. These opportunities could range from relatively light-touch collaboration to more deeply integrated approaches to implement solutions once for use across multiple agencies. Sharing could include creating templates and patterns, establishing framework

contracts, and developing centers of excellence, as well as building and hosting systems that serve multiple agencies. Emerging areas such as AI, digital twins, cybersecurity, and zero trust architecture (ZTA) present many opportunities for a more collaborative approach to develop better solutions, faster, and at lower cost. With strong central support, we believe that agencies can avoid the need to independently navigate complex challenges in these domains.

Opportunities for sharing between departments

- **Shared contracting**: Move toward framework agreements for common software services. Include security requirements and other common standards (such as ensuring the product operates within .gov domains) in these contracts, so agencies don't have to figure this out individually. Mandating this may not be necessary; agencies will adopt it if it proves useful.
- **Automation/cloud:** Identify shared approaches to encourage more automation and cloud adoption across agencies.
- **Shared services**: For example, one participant noted the consolidation of payroll providers in their agency. This move toward shared services could be expanded.
- **Shared infrastructure for smaller agencies**: While the 24 CFO Act agencies are able to manage their own infrastructure, smaller agencies may benefit from a shared model. GSA could be the agency to provide these services to support smaller agencies.
- **UX:** Develop web design systems and reusable design patterns to improve trust, efficiency, and speed in building user interfaces. Focus particularly on the top opportunities previously identified. Also, assess whether the "Life Experiences" approach has had the desired impact and could be taken further.
- **Login.gov:** Explore opportunities to ensure widespread adoption of Login.gov. Examine how data is reconciled with login.gov to prevent duplication across agencies.
- **App and mobile strategy:** Develop clear guidance for when and how to use apps, alongside mobile strategy (including responsive design), and accessibility.
- **App modernization:** Identify areas where new line-of-business applications could be shared between agencies to reduce duplication.
- **AI:** Develop a standard methodology for assessing confidence in AI systems, provide recommended models for specific tasks, and create a framework outlining where different types of AI can be best utilized.
- **Data:** Leverage the potential of data labs to help clean and sift through legacy data across systems, creating high-quality datasets for data-driven decision-making and AI training. Consider digital twins for key systems (e.g., social security systems).
- **Leveraging secure government R&D:** Extract valuable research and development efforts from secure government agencies, which are not currently being utilized in the federal civilian executive branch. Fund a central office to harness and apply this knowledge across federal agencies.

Evolve the TMF to fund modernization without duplication

The TMF can play a vital role in continuing remediation efforts, but there are additional initiatives that should be developed to go further to avoid duplication and promote modern digital development. The TMF could evolve to emphasize innovative working methods and select programs designed to reduce duplication and expedite time to market. To curate and manage shared endeavors, we suggest expanding the central organization responsible for administering these funds.

The TMF in future should be established not as a loan but as a mechanism to promote shared endeavors, potentially sharing costs in partnership with agencies. Going forward the TMF will need to evolve and be better understood as an exploratory fund that fosters new ways of working, which can then be integrated into the normal appropriation cycle. Key considerations should include supporting agencies in shifting toward technology operational expenditure from capital expenditure, and shifting over time to funding products rather than projects.

Requests for TMF support should align with a comprehensive plan. Some of our respondents suggested there should be an emphasis on longer-term planning. With oversight of this, it could be beneficial to appoint individuals to an advisory board or council for fixed terms that span multiple administrations. This could support CIOs and agency leaders in the exploration of long-term themes and opportunities.

Achieving these shifts will require a change in the way the center operates, as described in the section that follows. Without the appropriate central control, it will not be possible to address the complexity of activities across agencies, and take the opportunity to do things differently. Done well, there is considerable potential to expedite delivery, and also an opportunity to achieve cost savings.

Recommendation 1.3

Evolve the TMF to incentivize collaboration: In conjunction with a five-year plan across agencies, identify priority investments that promote sharing, reduce duplication, and decrease time to market.

2. Increase the Federal CIO's authority to drive digital modernization

Establish political sponsorship

There is a lack of a clearly stated ambition, political sponsorship, and representation for technology at the highest levels of government. CIOs told us that their Secretaries and Deputy Secretaries don't have a bold, impactful vision for the role of technology in support of their agency's mission, and technology leaders don't have sufficient influence at the most senior level.

Recommendation 2.1

The new administration should consider establishing a dedicated political role within the Executive Office of the President—a high-ranking individual tasked with setting a bold vision for digital modernization across the Federal Government. This leader would provide clear, authoritative direction to drive cohesive modernization efforts across all departments.

Elevate the visibility and authority of the Federal CIO

We heard that having a visible technology leader with the authority to work closely with lawmakers—and who is accountable for modernizing service delivery—would be highly beneficial. This role would bring a strong sense of purpose and direction, identify promising opportunities for shared initiatives, and drive their successful implementation.

The role would extend beyond the current scope of the Federal CIO, which, while demonstrating the position's potential, has been limited in visibility and impact due to its positioning within the Office of Management and Budget.

Recommendation 2.2

Elevate the Office of the Federal CIO: We recommend that this position be situated within the Executive Office of the President, remaining closely aligned with OMB, rather than under the Office of Science and Technology Policy. For instance, there could be a new OMB-level technology position, such as a Deputy Director for Technology, requiring Senate confirmation. This role could either elevate the Federal CIO or have the Federal CIO report directly to the Deputy Director. The post-holder, with the necessary gravitas, would be able to engage with Congress and drive budgetary priorities. This position would coordinate efforts across key agencies, including the GSA and OPM (for workforce matters), which would report to a Cabinet-level role within the OMB structure.

Formalize the Office of the Federal CIO as the center of digital government

The executive digital leadership is dispersed across multiple entities. The Federal CIO in the OMB holds the statutory authority to lead Administration priorities provided by Congress. Multiple service delivery partners exist, in particular the GSA, including Technology Transformation Services and 18F, and the USDS within the Executive Office of the President of the United States. Federal employees who are technology professionals also fit into human resources policy as provided by the OPM. While we heard this does come together in a partial way in the CIO Council, there are additional councils of CISOs, CDOs, and CAIOs. The current fragmented ecosystem, which depends heavily on collaboration, leads to a lack of a unifying vision for departments to align around.

Recommendation 2.3

Formalize the organizational structures and accountabilities at the center of government to drive progress toward the vision, with an aligned funding plan.

3. Modernize the technology workforce to get the Federal Government working differently

Establish the right balance between federal employees and contractors

Contractors play a vital role in bringing new skills and augmenting the expertise within the federal workforce. However, there should be a stronger focus on investing in federal technology employees, which would give agencies more flexibility to maintain the right balance of responsibilities between federal employees and contractors.

Address the challenge of the 'internal market'

A number of the CIOs noted the challenge that many of the existing federal IT staff had outdated skills on technologies and ways of working, and (re)training and hiring new staff remained a challenge. Pay is generally consistent, but there are exceptions that have been made for roles relating to the financial sector, such as at the Federal Deposit Insurance Corporation (FDIC), and the Department of Veterans Affairs (VA). Many CIOs noted that this had created internal competition for federal IT staff, resulting in a high attrition rate, and leaving their organizations starved of talent.

Transition away from pay grades to roles and competencies

The current U.S. framework for IT staff is based upon experience and grade, where pay is linked to this experience and grade as specified in the General Schedule. Other countries that also experienced the 'internal market' challenge, like the UK, have moved away from frameworks based on experience and grade to a framework in which technology roles reflect those in the private sector market. Each of these roles have several levels of competency and pay is linked to this combination of role and competency and aligned to the private market pay. The individual pay scales for each role and competency are aligned to the median of the private payscale and flexibility is provided by creating a range for pay which can also be used to accommodate exceptions like those noted in the paragraph above.

As a reference, since the introduction of the UK framework for technology, digital, data, and cybersecurity roles, it has been easier to hire from the external market, the 'internal market' has disappeared, and IT staff now have clear career paths that they can pursue.

Recommendation 3.1

Develop a new framework for careers and pay: The U.S. Federal Government should create a new single framework for careers and pay, across all agencies for IT, technology, digital, data, and cyber roles as described above.

This new framework should be built out from a cross-agency collaborative effort that includes mapping competencies by job family, creating pay bands, and ultimately addressing the issues in the pay structure. Ideally this would be done so as to be consistent with the General Schedule pay scale.

Focus on career paths and training

There is a lack of consistent training for U.S. federal IT staff. Other countries have addressed this centrally by establishing 'digital academies', which provide consistent training to all departments. These academies raise awareness among non-technical staff and support the specialized roles and career development of IT professionals.

A notable example of large-scale training is the UK's Digital Academy initiative. Between 2013 and 2018, the UK retrained 10,000 civil servants through these academies. In 2017, when the UK was ranked as the world's top e-government by both the UN and the OECD, the Digital Academies were widely credited as a significant contributor to that success.

Recommendation 3.2

Invest in academies at scale: A significant investment should be made in (re)training the federal IT workforce. The development of the curriculums should be centralized whilst the provision of the training can be both localized and virtualized. The purpose of this training should be both to familiarize all federal technology staff with new agile ways of working as well as provide training that is focused on the specific role and career of technology staff as described in the new framework above.

Become an 'intelligent buyer' of services

Other countries have used their newly (re)trained workforce to become a more intelligent buyer of services from the private sector. These newly acquired skills would enable the federal workforce to take more accountability for the development of new services, and this can enable a shift in accountability which can be further supported by the development of a deliberate disaggregation of services (moving away from the apparent reassurance of a single accountable vendor for large programs—sometimes referred to as "one throat to choke"), more flexibility in procuring services, and a stronger compliance process that limits the length and size of contracts that can be awarded.

4. Support new CIOs and create a CIO talent pipeline

All of the recommendations in this section should be relatively straightforward to implement and could be made the responsibility of the Office of the Federal CIO. These changes would give the Office of the Federal CIO more influence over the leadership cadre of CIOs across the Federal Government. We believe there would be a strong case for the value of this investment, as a relatively small investment in the center can support an improvement in performance across departments.

It is recognized that a number of the recommendations below have been addressed before, but for varied reasons, have not necessarily endured. Our recommendation to centralize these responsibilities in the Office of the Federal CIO is intended to provide continuity of responsibility to ensure that these recommendations do, in future, endure.

Additionally, it is worth noting that many of the recommendations in this section are widely employed by other international governments.

Foster the CIO community

All of the participants talked very positively about the CIO Council and how well the members worked together. Most felt that this community could be taken forward by holding their regular meetings in person rather than, as they currently are, by video conference.

Others noted that this CIO community could build on its success by working 'more in the open' by publishing some of their workings and also creating a playbook of best practice and practical examples for other members of the community to benefit from.

Ensure consistent induction for CIOs

CIOs generally agreed that all new potential CIO appointees, including political appointees, should be provided with an induction process that covers the necessary legislative and regulatory knowledge required by CIOs to be effective quickly in their roles.

CIOs commented that potential appointees need to be provided with a comprehensive knowledge of the organization and working of the agency. Several suggested that mentors both from within the agency and the wider CIO community could be assigned to support new appointees. This would include having deputies to the CIO who especially support understanding the context of their agency.

The induction program should include desired ways of working which are common across agencies. For example, some of our interviewees had formed CIO Councils within their agency, which were seen as a positive way to ensure activities are aligned to a shared vision.

As well as inducting new CIOs, we suggest that it would be valuable to create a digital induction for incoming agency senior leadership, including Secretaries and Deputy Secretaries. A main aim of this would be to help them appreciate the contribution of technology to their agency's mission. It should also include an inventory of systems and people to provide clarity on the high value assets within the agency and those systems that are more fragile, and represent a hidden

risk for the department. This would help CIOs and CISOs when they need to explain dependencies, and the case for remediation investments.

Create a CIO talent pipeline

A small number of participants mentioned that there had been prior attempts to create a pipeline of CIO talent within the Senior Executive Service. We recommend making the creation of this pipeline a core responsibility of the Office of the Federal CIO.

The Federal CIO should run a transparent talent pipeline, with its associated metrics, where progression of individuals on their journey to CIO can be independently reviewed on a regular basis. This could include identifying development opportunities, such as placements in other agencies.

In other countries, the equivalent of the Federal CIO is an active participant in the interview process and has authority over the appointment of departmental CIOs. They are also typically responsible for the management of the talent pipeline of senior technologists who are on the path to become future CIOs.

A number of participants commented on the positive progress made in increasing the tenure of new CIOs, which now stands in line with industry norms at around 20-24 months. It is still desirable to further extend this tenure.

Recommendation 4.1

Empower the Office of the Federal CIO to be responsible for the following:

- Support the President to establish the best balance of political and career appointments across the CIO council and for each department
- Define the qualifications and experience required for each CIO role. This would include technical knowledge as well as executive competencies
- Appoint CIOs in accordance with the qualifications and experience outlined above
- Develop and implement an induction program
- Develop the talent pipeline and its associated metrics and organize independent reviews
- Continue efforts to increase the tenure of newly appointed CIOs beyond the current 20-24 months average

5. Pare down the accumulated legislation that holds back transformation

Over the years, a substantial amount of legislation has been enacted, requiring CIOs and their teams to devote significant time and effort to compliance. This requires a comprehensive review.

CIOs need clear guidelines, boundaries, and direction to focus their efforts and respond effectively. Some legislation, dating back nearly 30 years, may be outdated or inconsistent, and should be identified for potential revision.

CIOs highlighted the importance of the Federal Information Technology Acquisition Reform Act (FITARA) in defining their roles but noted variability in how its priorities, along with those in other legislation and Executive Orders, are interpreted and applied. These directives can mean different things to different agencies. Some CIOs have found the guidance clear, while others have had to consult with legal teams for further clarification.

Executive Orders, when used selectively, have provided much-needed clarity and have been effective in driving specific actions. However, all CIOs indicated that they could implement these directives more efficiently if funding were attached.

There is a need for further examination into how Executive Orders might drive broader organizational change. While the cybersecurity EO has improved compliance, few CIOs reported leveraging EOs to initiate more transformative shifts within their agencies.

Recommendation 5.1

Review all relevant legislation and Executive Orders, to clarify their applicability and set clear expectations for agencies in a concise and practical manner.

The review should encompass the main legislation referred to by CIOs in our interviews: Evidence-Based Policymaking Act of 2018, Modernizing Government Technology Act of 2017 (MGT), Federal Information Security Modernization Act of 2014 (FISMA), Digital Accountability and Transparency Act of 2014 (DATA), Federal Information Technology Acquisition Reform Act of 2014 (FITARA), E-Government Act of 2002, and the Clinger Cohen Act of 1996 (CCA) which first established the role of the CIO in government agencies.

In particular, we recommend that FITARA, now over 10 years old, be reassessed to determine if it has met its original objectives and been consistently implemented across agencies. An updated and clear statement on its intended function may be necessary, along with greater clarity on the rating methodology.

Recommendation 5.2

Explore possible additional measures beyond FITARA to further empower CIOs in addressing long-term challenges. Key areas of focus should include:

- Preventing program offices from purchasing systems outside of the CIO's oversight
- Enabling CIOs to control and, where necessary, eliminate shadow IT (systems implemented outside the control of the CIO organization by programs, which may not be visible from a cybersecurity perspective)
- Ensuring continuity to complete ongoing (multi-year) initiatives

Recommendation 5.3

For future **Executive Orders**, we recommend greater consultation with agency experts who possess the detailed knowledge needed for implementation, along with a review of how these orders will be funded. While CIOs recognize the sensitivities around pre-signing discussions, involving those responsible for executing the changes is essential to ensuring success.

About the authors and Global Government Forum

This report was authored by Kevin Cunnington and Andrew Besford. Both Kevin and Andrew have extensive private and public sector technology backgrounds, and have lived and worked in the U.S.

Kevin and Andrew both joined the UK civil service in 2013.

Kevin was appointed as the director general of business transformation in the Department for Work and Pensions (one of the largest UK departments). In 2016, Kevin was promoted to be the head of all UK public sector technology and the director general of the UK Government Digital Service (GDS). Subsequently, Kevin served for two years as the UK's digital envoy before retiring in 2021. Kevin is an executive advisor on technology to Global Government Forum.

Andrew was a member of Kevin's executive management team at GDS. He led the creation of the 2017 UK Government Transformation Strategy and the 7 Lenses of Transformation. Since 2019 Andrew has been a non-executive director on the board of one of the UK's best-performing National Health Service (NHS) trusts, where he oversees a major digital, data, technology and cybersecurity investment program.

Global Government Forum is a publishing, events and research business that helps senior civil servants around the world to meet global challenges by building their expertise, knowledge and connections.

Appendix I - Methodology

The report, produced by Global Government Forum (GGF) comprised interviews with the Federal CIO and 12 members of the CIO Council from CFO Act[1] agencies. The interviews were conducted under the Chatham House Rule, and followed the structure of the 7 Lenses of Transformation that was developed by the UK Government.

We compared the findings from the interviews with insights from other international reports produced by GGF, which have involved participation from over one-third of the world's governments. This report offers an external perspective on U.S. digital delivery, and we hope that this perspective provides fresh insights and ideas.

We extend our sincere thanks to all the interviewees for their candor and participation in this study:

- **Clare Martorana**, Federal CIO, Office of Management and Budget
- **David Shive**, CIO, General Services Administration (and vice-chair, CIO Council)
- **Tony Arcadi**, CIO, Department of the Treasury
- **Darren Ash**, CIO, Department of the Interior
- **Guy Cavallo**, CIO, Office of Personnel Management
- **Ann Dunkin**, CIO, Department of Energy
- **Brian Epley**, CIO, Department of Commerce
- **Marcela Escobar-Alava**, CIO, Social Security Administration
- **Eric Hysen**, CIO, Department of Homeland Security
- **Cordell Schachter**, CIO, Department of Transportation
- **Jeff Seaton**, CIO, National Aeronautics & Space Administration (NASA)
- **Gary Washington**, CIO, Department of Agriculture
- **Jennifer Wendel**, Acting CIO, Department of Health and Human Services

[1] Chief Financial Officers Act (1990), which gave OMB new authority and responsibility for directing federal financial management, modernizing the government's financial management systems, and strengthening financial reporting.

Appendix II - Summary of recommendations

Recommendation 1: Build upon the success of the Technology Modernization Fund (TMF): and modernize service delivery at scale

Recommendation 1.1: Renew the TMF: Ensure its purpose is clearly understood and continue successful remediation efforts.

Recommendation 1.2: Explore options for CIO discretion: Investigate methods to empower CIOs with greater discretion in spending decisions.

Recommendation 1.3: Evolve the TMF to incentivize collaboration: In conjunction with a five-year plan across agencies, identify priority investments that promote sharing, reduce duplication, and decrease time to market.

Recommendation 2: Increase the Federal CIO's authority to drive digital modernization

Recommendation 2.1: The new administration should consider establishing a dedicated political role within the Executive Office of the President—a high-ranking individual tasked with setting a bold vision for digital modernization across the Federal Government.

Recommendation 2.2: Elevate the Office of the Federal CIO.

Recommendation 2.3: Formalize the organizational structures and accountabilities at the center of government to drive progress toward the vision, with an aligned funding plan.

Recommendation 3: Modernize the technology workforce to get the Federal Government working differently

Recommendation 3.1: Develop a new framework for careers and pay

Recommendation 3.2: Invest in academies at scale

Recommendation 4: Support new CIOs and create a CIO talent pipeline

Recommendation 4.1: Empower the Office of the Federal CIO

Recommendation 5: Pare down the accumulated legislation that holds back transformation

Recommendation 5.1: Review all relevant legislation and Executive Orders, to clarify their applicability and set clear expectations for agencies in a concise and practical manner.

Recommendation 5.2: Explore possible additional measures beyond FITARA to further empower CIOs in addressing long-term challenges.

Recommendation 5.3: For future Executive Orders, we recommend greater consultation with agency experts who possess the detailed knowledge needed for implementation, along with a review of how these orders will be funded.

Appendix III - What we heard

This appendix provides more detail on the CIOs' feedback. It is organized to follow the same order as the recommendations.

Current delivery priorities and funding

The challenges posed by **legacy systems**, including their security implications, are generally well-known and well-documented. The scale of the issue is vast, and while steps have been taken to address it, full remediation remains elusive. Sensible mitigation strategies have been implemented, but as we will highlight in our discussion on funding below, more extensive actions will be required to adequately tackle the problem.

While the Executive Orders have successfully driven action on priority areas, they **lack the necessary funding** to fully implement the specified initiatives. Many agencies will find it difficult, if not impossible, to achieve these ambitious goals within the constraints of a two-year budget cycle. Significant financial resources will be essential for a more comprehensive and effective modernization effort.

CIOs welcomed the **Technology Modernization Fund (TMF)**, which has been instrumental in addressing what they often described as "primarily citizen-facing services", helping to mitigate some legacy technology challenges. However, despite its considerable scale, the fund lacks the scope and resources required for a comprehensive overhaul of the broader IT infrastructure needed to support a truly modern digital experience. CIOs shared similar views on the TMF's limitations, for example around repayment requirements, and a perceived focus on citizen-facing projects.

The CIO community consistently faces funding challenges, with some viewing tight budgets as both a **constraint and an opportunity** for innovation. A primary frustration is the lack of budget flexibility, with most funding tied to specific programs rather than CIO priorities, limiting their ability to address broader agency needs.

Collaboration between agencies has also been difficult to establish, hindered in part by repetitive procurement processes and a lack of central support or formalized structures to facilitate sharing.

CIOs expressed a **strong need for more flexible, multi-year funding models** to support modernization efforts, while also reducing bureaucratic overhead.

One CIO put it that "the externalities move out of sync with the budget cycles", referring to the challenge of **finding funding for urgent cybersecurity remediations**, such as those required for the CrowdStrike outage in July 2024. They contrasted this with the routine cycle of conversations with appropriators around "predictable" levels of funding.

Legacy systems and technology

A primary challenge for all agencies is the extent of the **legacy systems and technology** on which they depend. As one CIO remarked, their IT "grew up organically around the need—and the deficiencies are now apparent". There is a strong desire for a workable approach to decreasing the technical debt, and CIOs highlighted the opportunity to reduce the cost of the federal IT portfolio through modernization.

CIOs are acutely aware that they still rely on **paper-based processes**, which significantly hampers their agency's ability to manage its workload. Those looking toward AI implementation emphasized the urgent need to "liberate the data that is on paper".

Most CIOs have come to the conclusion, as we have seen in other countries, that securing legacy systems is so difficult and costly that it **makes more sense to build new modern systems** rather than attempt to secure the legacy. It was also mentioned that CIOs "can't turn the old systems off until the new systems are ready".

However, we observed that CIOs face a considerable barrier in determining **where to begin**. Strategic decisions about which areas of legacy technology to address first are "not just a technology decision". Consequently, many lack a clear plan—some noted that their agency's mandated plan had not been updated, while others were reluctant to create a theoretical strategy that would merely "sit on the shelf".

This raises the issue of the **distinction between digitizing existing processes and completely reimagining them** for a digital age. We heard of instances where CIOs opted for different approaches based on their unique contexts.

We also included questions about **cost savings and efficiency**. CIOs are aware of the difficult balance between investing in running the enterprise—highlighting key activities like multi-factor authentication (MFA) and network remediation—and the desire to build new online citizen-facing services.

Several CIOs linked this to "**modernizing how we work**", both within the technology organization and across the agency. One CIO pointed out the difficulty of adopting new technology agency-wide, connecting it to cultural norms and processes. For instance, although Microsoft Teams was available in their agency before the pandemic, many employees did not use it effectively.

More technically inclined CIOs noted the **lack of a defined target architecture** for their agencies, with one attributing this to "too much liberty in the organization in the past".

CIOs recognized the importance of modernizing their agency's data practices, indicating that a **more effective data strategy** could not only reduce duplicate spending but also unlock valuable insights, as well as enable them to enhance the citizen experience of their agency's services. While the opportunities and challenges were clear, specific strategies for how agencies would tackle this work remained less defined.

We heard that the transition to cloud services had been successful in some areas, although many CIOs referenced the **multiple physical data centers** they still operate. For workloads that have migrated to the cloud, CIOs expressed concerns about vendor lock-in, worrying that

suppliers might alter pricing structures after agencies have invested in their services and become dependent on them.

Funding

The CIO community has a consistent expectation of a tight funding environment. Some members highlighted that this situation could be treated as an **opportunity to think differently** - particularly in identifying areas for rationalization.

Every CIO told us in one way or another that they **struggle with the funding model.** This presents a clear opportunity to accelerate progress as an enabler for the digital journey that agencies are on.

The most common issue we discussed was around **funding earmarked for specific programs**. CIOs are frustrated that this lack of budget ownership, or even visibility, prevents them from investing in priority areas, and limits their ability to meet the full needs of the agency outside the funded programs. Those with experience working in an environment where products (rather than projects) are funded recognized the restrictive nature of this approach and its consequences. We heard numerous comments such as, “We need a concerted effort to fund CIOs rather than the programs I have to provide a service to” and, “We need to move the dollars to where they can be used.”

When we enquired about collaboration, it was evident that the CIO community is aware they are **all solving similar problems**, risking re-invention of the wheel multiple times. Apart from certain very specific areas, there is no ‘department of doing it once’. While some agencies have unique needs stemming from their missions, all acknowledge there are opportunities to share resources. Sharing could potentially enable agencies to accomplish tasks more quickly, at lower costs, and with higher quality. For example, they cited the inefficiency of each agency writing security clauses into contracts for frequently used software, or asking vendors for their positions on various issues separately.

The most-used phrase from all of our interviews for this study was that the **“budget cycle is broken”**. We consistently heard that budgets are “too restrictive”, “unable to support multi-year investments”, “make things complicated” and make it “hard to get anything done”. Several participants noted that the “budget cycle doesn’t incentivize modern software delivery”, especially those who had led software development outside of government. Many raised concerns about being unable to request additional funding beyond the two-year budget. It was suggested that a new approach is needed to support multi-year investments—potentially involving a new class of financial experts who understand digital needs and can navigate these complexities.

As highlighted above, CIOs appreciated that the **Technology Modernization Fund (TMF) has been a good start** for investing in the most urgent cybersecurity, legacy upgrades, and digital experience projects. Several mentioned the legacy of under-investment prior to the TMF. However, the requirement for full repayment has been a barrier, and repayment flexibility has been welcomed by those CIOs who have managed to take advantage of it. Some told us they had made significant efforts to support agency colleagues to submit project proposals to the TMF.

While the focus on citizen-facing projects is seen as "**understandable but does limit the scope of project proposals**", others noted that the TMF funding approach is not compatible with modern subscription models they wish to adopt, which require a shift from capital expenditure to operational expenditure. It was recognized that the TMF "hasn't mapped to the needs in some agencies" and others remarked that it was "not sustainable". Some respondents who were newer to the Federal Government reflected that "the long-standing career civil servants are the ones who know how best to leverage these funding opportunities". Others highlighted that as a CIO you "need to be smart about what you request".

CIOs still faced a challenge finding the right people to deliver once they received funding, because **"TMF doesn't increase my resources"**.

In discussions beyond the TMF, several highlighted the **excessive paperwork required to spend allocated funds**. One CIO complained that the system is so focused on preventing fraud, waste, and abuse that it inadvertently causes significant waste itself. Processes were described as "inefficient", and "making government expensive".

CIOs were well aware that, when executed effectively, new digital services can provide a visible sign of progress for citizens and businesses. However, several mentioned that for every dollar spent, the CIO community must **demonstrate to taxpayers and Capitol Hill how the funding has enhanced the constituent experience**. They emphasized the need to make the case for investing the right money in the right areas to modernize the technology infrastructure while ensuring funds are accessible to all agencies, without imposing excessive bureaucratic overhead. CIOs also noted a challenge feeding back to Congress on their successes and needs, possibly linked to the political environment.

Cybersecurity

CIOs share a clear understanding of **cybersecurity as a top priority**, and significant progress has been made thanks to Executive Order 14028. Several respondents stated this EO was clear, and appreciated that its measures aligned to FISMA reporting, and as a consequence had high visibility and priority with both the CIOs and the Deputy Secretaries.

However, while the urgency of this mandate is well recognized, CIOs consistently highlighted the **challenges of securing funding and delivery capability** for its implementation. For instance, while investments and disruptions were necessary for multi-factor authentication (MFA), CIOs expressed satisfaction with the successful rollout.

Looking ahead, CIOs are focused on developing plans for implementing **Zero Trust Architecture, a task that presents a significantly greater level of complexity**, especially within environments that feature multiple networks and legacy systems. This challenge is exacerbated by the lack of associated funding.

CIOs also shared ongoing efforts to enhance their security posture, identifying high-risk areas that require attention, some of which entail costly remediation. In one notable case, addressing security event logging for outsourced systems in a shadow IT environment proved **particularly challenging within a project funding framework**, underscoring the need for dedicated budget allocations to achieve essential uplifts in cybersecurity capabilities.

Additionally, CIOs noted the success of the **CISO Council as a valuable companion community** alongside their own.

Building the future

The Executive Orders are widely understood, and there has been substantial progress on their initial priorities. Similarly, the priorities established from the Federal CIO and CIO Council are well-acknowledged and have **strong buy-in from CIOs**.

However, as agencies pursue future initiatives, the absence of a cohesive **federal IT strategy** stands out as a significant gap. While the shared priorities are well-defined, their application across each agency's unique context often leads to broad interpretation, creating ambiguity around how to translate these priorities into actionable plans. Developing a strategy across 430 agencies requires both local insights and a central consolidation effort. This coordination is essential; without it, fully understanding the landscape and identifying the best opportunities for interagency collaboration will remain out of reach.

Across the board, CIOs unanimously affirmed that "**data is a priority**". Several expanded on specific challenges they wish to address, such as reducing duplicate datasets for the same individuals. Others highlighted how more integrated data could significantly improve the citizen experience. Despite the emphasis on data, few CIOs mentioned the role of the Federal Chief Data Officer (CDO) or the CDO Council.

Respondents told us that around **60% of digital interactions with the government occur via mobile** devices. However, in the absence of a cohesive mobile strategy, agencies have responded inconsistently. CIOs shared examples of effective mobile apps, such as *CBP One*, which has a narrowly tailored specific purpose and an ongoing relationship. They also highlighted *AirNow*, one of the most popular air quality apps in the U.S. At the same time, many CIOs are focused on "preventing the proliferation of unnecessary apps" where their use may not be appropriate.

We discussed the varied **branding of federal websites**, noting that some other countries have consolidated their digital efforts under a single brand. CIOs generally agreed that a single brand could serve as a "potential unifying principle", though several questioned whether this was more about "optics than impact". Some success has already been achieved in promoting the use of .gov domains to enhance public trust, involving necessary changes related to shadow IT and third-party vendors. We concluded that we did not favor recommending a full rebranding of agencies at this time.

CIOs were enthusiastic about adopting **user-centered design (UCD)** approaches to improve citizen experience, and suggested that standardizing UI elements could enhance consistency without requiring a comprehensive federal rebranding initiative.

Progress is being made toward creating a **unified login** through Login.gov, with about 12 agencies currently using it. However, CIOs from agencies that have less direct interaction with the public were understandably less focused on its implementation within their own organizations.

When asked about **AI and other emerging technologies**, CIOs discussed potential use cases, such as AI tools for modernizing operations by prioritizing workloads. Other technologies, like Robotic Process Automation (RPA) and electronic signatures, were also raised in this context as opportunities to streamline processes and improve efficiency. IoT sensors and drones were also mentioned.

We invited CIOs to talk about **collaboration beyond their agencies**, and participants typically described collaborating with one or two agencies where their missions overlap, citing some examples of successful partnerships. Where collaboration has been effective, it is often built on a "shared mission" and "strong relationships". They stressed that collaboration must be "nurtured and supported", with "success dependent on how well we work together". CIOs were keen to emphasize that "this is not a command-and-control organization", noting that the focus should be on "creating the environment that fosters the necessary collaboration". Several CIOs also noted that collaboration has been most effective "in a crisis", a theme echoed in other countries.

CIOs observed there was "**a lot of room for consolidation**" by sharing between agencies. One had started in their role with "21 contracts with a major software vendor and 13 implementations". Many said consolidation around contracts and common capabilities "is the right thing to do", "but you have to be thoughtful about how far you go". "Standardization has huge wins" but CIOs do not want to be stuck with the "lowest common denominator" or a "lack of nimbleness". One CIO expressed it would be "really hard for [the existing system owners] to give up control", but thought it made sense for agencies to "only do the last mile" to customize shared capabilities for use in their context.

When discussing collaboration, we raised the topic of the **Life Experiences** organizing framework—a cross-agency effort to join up services based on key citizen milestones. Some CIOs were aware of these initiatives, though one respondent remarked that Life Experiences remain "a blind spot, unless your agency is closely tied to those journeys".

Federal technology workforce

CIOs universally recognize that **developing a skilled federal workforce** in technology and cybersecurity is crucial, yet many express frustration over the slow pace of training and skill acquisition. Inconsistent training opportunities and a shortage of staff hinder their ability to meet changing demands, leading to a reliance on contractors for specialized skills.

Recruitment and retention remain significant challenges due to competition among federal agencies. Agencies with special pay structures, such as the Department of Veterans Affairs, can offer more attractive salaries, making it difficult for others to retain talent. While CIOs successfully attract early-career professionals, keeping mid-career employees and filling senior positions requires substantial effort, exacerbated by lengthy hiring processes.

The **use of contractors is viewed as necessary to bridge skill gaps**, and CIOs have developed a range of different approaches to balance the development of internal talent with reliance on external resources.

Workforce development

The development of the federal employee workforce of technology and cybersecurity specialists was identified as a **key enabler** by all of the CIOs we spoke to. However, we received a mixed range of responses regarding how they were addressing this need.

There was a general consensus that CIOs feel they **"can't develop people fast enough"** to meet the demands, especially concerning the emerging skills needed in data and cybersecurity. Most commented that the training offerings could be inconsistent, and that it was challenging to allocate time for training when there was already a sense of being short-staffed. Funding also had to be found. CIOs also highlighted that in addition to skills acquisition, they needed to train the workforce to work in the "different environment" of digital. Several linked these issues to a heavy reliance on contractors, which we discuss in a separate section below.

Recruitment and retention

Another theme with strong consensus was the challenge of meeting the demand for skills when multiple federal agencies are **competing for the same people**. This 'internal market' was seen as particularly problematic, with delivery teams losing colleagues to agencies that have special arrangements granted by Congress to pay above the base General Schedule, such as those at the Federal Deposit Insurance Corporation, and the Special Salary Rates (SSR) for the Department of Veterans Affairs (VA). At the VA, the SSR has resulted in an average 17% pay rise for tech and cyber workers, leading to significantly higher retention rates.

Some participants added that disparities in the **remote working offer** made their recruitment and retention difficult when competing against agencies that would permit 100% remote work.

We consistently heard that the direct hire **exception process had worked well for urgently needed cybersecurity roles**. Some respondents recognized the potential benefits of adjusting individual components of the pay offer, such as the Department of Homeland Security Cybersecurity Talent Management System, but felt these could be overcomplicated. They also noted that the number of personnel required to operate the system has been underestimated. One participant mentioned that it took seven years to hire a single person through one such approach.

Participants generally expressed confidence in their offers to tech and cyber workers in the earlier stages of their careers, believing they could persuade them to "stay for mission" and **"work on something that matters"**. One respondent even suggested it was "easy to get junior developers". However, it was highlighted that **considerable effort is required to retain people**, especially those at mid-career levels. We will address issues related to the most senior members of the workforce in the following section.

For hiring more senior specialists, some participants found that the **hiring process takes too long** for key IT roles that they need to fill. Some expressed frustration with the requirements around competing applications for roles, and flagged that it was possible to "go down the wrong

path and have to start over" to meet certain standards, for example for GS-2210[2] roles. Even experienced CIOs reflected that "it is so complicated that nobody can keep all this in their head at once".

We heard various challenges around salaries, primarily that the **pay scales** are based on grade rather than competencies, and that there is a lack of defined job families. Some CIOs had to repeatedly remind agency colleagues that IT skills are distinct from program skills. We also learned of activity with the OPM regarding workforce policy to address these, but respondents questioned whether the current proposal has "consistent buy-in and support", expressing concern that it "wasn't going to come with any funding".

If pay scales are revised, the need for an approach which considers non-IT roles was flagged, to **avoid unfairness toward other federal employees who are working on the same scale**. However, it was also pointed out that this can be done, and has been done, for other professions like scientists and doctors.

Culture

Alongside the theme of maintaining skills, we had several conversations around the **culture of the technology workforce**. Some aspects were viewed positively, such as the understanding of an agency's mission, culture, and values. However, there were also concerns, with one respondent having the perception that some IT personnel were not accustomed to engaging with real users (citizens) or front-line federal workers.

Skills on legacy systems

A common concern was the dependence on a small number of individuals for technical knowledge on certain systems, especially **legacy systems**. There was no consensus on how to maintain specific technical skills, with some preferring a "build" approach (developing federal employees) and others opting to "rent" (contractors), arriving at different conclusions based on the criteria that applied in their respective contexts.

Use of contractors

CIOs consistently reported **significant reliance on contractors** to meet their needs. However, we identified variability in attitudes toward the supplier ecosystem, and differing views on how contractors should be utilized.

One aspect that everyone agreed on was that contractors are a critical resource, and that they **see their suppliers as partners**.

Beyond this there were **clear differences between and within agencies** on the best constructs. Some CIOs acknowledged this variability and provided examples of when they

[2] U.S. Office of Personnel Management - General Schedule Qualification Standards - GS-2210: Information Technology Management Series

preferred long-term embedded supplier teams and when they did not. Others emphasized the importance of clearly defining the roles of contractors from the outset, whether they are acting as consultants, experts, or providing resources.

Using contractors helps agencies bring in the required skills for a short period, but we found that there are no established criteria for deciding whether to procure these skills or **develop core competencies in the permanent workforce**. This decision is currently left to individual agencies' and CIOs' discretion. A recurring analogy was the 'Buy vs. Rent' model, which contrasts proactively hiring federal employees for essential roles with 'renting' niche skills from suppliers for short-term needs.

Our respondents expressed concern about agencies' overconfidence in appointing a single large supplier for major projects. Many articulated their understanding that it is **not possible to outsource the risk of a large digital program to a supplier**. However, they acknowledged that some agencies might find it easier or harder to transition to different models. One proposed model was a shift toward "government as integrator", where federal project managers lead contractors in 'rainbow teams' from different companies.

Many respondents indicated that contractors could meet their agency's needs for **up-to-date technology skills** in a shorter timeframe than growing the permanent workforce. Although not mentioned by our participants, we note that some other countries have observed a 'smokescreen' from the supplier community, where legacy-skilled staff are sent on short training courses and then returned to the customer re-badged as agile-certified, but without actual practitioner experience.

Finally, our respondents frequently noted the **cost of using suppliers**. In a constrained spending environment, several saw reducing the contractor workforce as a potential way to rebalance costs. Although some had cost comparisons in mind (for example, an indication that three federal employees might cost the same as two contractors), we suggest this needs further investigation. In this context, productivity and the costs of training and skill development are clearly relevant to the comparison. Other considerations include flexibility, salary vs. fees, recruitment costs, benefits (health, retirement, leave), overheads (office space, equipment, administrative support), and security clearances.

Some respondents felt the supplier landscape requires a more urgent shake-up. They expressed a **desire for better value**, felt there was insufficient competition, and feared that contracts were "bigger than required" and had "rolling extensions". One respondent was especially frustrated that the procurement regime often results in "contracts that are exactly what we want to avoid".

CIOs

It was clear from our discussions that the CIO Council has become a **strong and valued community** of CIOs, reflecting the diverse make-up of the CIO community, including Senior Executive Service career employees and politically appointed leaders.

As we anticipated, all of the CIOs were very clear on their **opportunity to serve the American people** through digital modernization, as well as their stewardship of taxpayer dollars, and the need to protect citizens' data. However, they also described their roles as "thankless" and "hard".

Political appointments

Some of our participants shared their views on **whether the CIO role should be a political appointment**, and we heard varying perspectives on this issue. Regardless of the respondents' positions, they did share consistent perspectives about the distinct nature of these two types of appointments.

Political appointees acknowledged their short-term tenure, aligning with the four-year political cycle. Their goal is typically to deliver visible results quickly, which can foster rapid innovation, but may reduce the incentive to create long-term sustainable solutions. Political appointees **are attuned to the President's policy priorities and focus on advancing them**. They told us that as a result they feel well-placed to push modernization projects, greater adoption of digital services or cloud, and demonstrate policy-related tech initiatives using innovative approaches. Many appointees come from the private sector or state governments, bringing valuable experience, along with fresh ideas and outside perspectives. However, this background means they have not built up a deep understanding of federal processes and bureaucracy.

Career appointees emphasized their responsibility to provide stability and continuity across transitions between administrations. They spoke about working toward long-term organizational goals, particularly as technology leaders focused on **building and maintaining durable systems and teams**, even as the political leadership changes. Most highlighted that major projects generally take longer than one administration to complete.

Many career officials possess deep institutional knowledge of their agency and its mission, making them more likely to understand its legacy technology and the history of funding requests to address it. They are more likely to have a detailed understanding of federal processes, rules, and budgets, which can include **navigating complex procurement rules and successfully applying for funding**. Most mentioned the necessity of compliance with the full range of federal regulations.

We concluded that any incoming administration should recognize the clear strengths of both groups, and that **successful digital delivery in federal agencies requires close collaboration between them**. In our conversations, the CIOs from both groups expressed their commitment to ensuring the smooth continuation of technology programs initiated by political appointees after their departure. Some did say, though, that "realistically you need to do the job for longer than two years".

Setting CIOs up for success

Members of **the CIO community agreed that they all face similar challenges** in their roles, regardless of the agency they work for. During our discussions, we explored the support currently available to them.

This conversation revealed that there is currently **no systematic way to set up CIOs for success**. While there is some level of peer support from colleagues within the CIO Council, the shift to online meetings has diminished the number of valuable 'side conversations' that used to take place. These informal exchanges were opportunities to share best practices and foster collaboration between agencies. Additionally, although a handful of CIOs had memories of a "CIO Handbook" there is no up-to-date consistent approach or framework, such as an induction

program, to help new CIOs get oriented. Around the community it was clear that some CIOs ask for help, and some do not. However, they did clearly all want their fellow CIOs in the community to be successful.

The challenge of getting all CIOs up to speed in their roles is significant, but it is **particularly acute for political appointees**, who are often less familiar with Federal Government operations. Without a formal induction process, these appointees risk spending their first two years merely learning the landscape—understanding the situation, priorities, and regulations. This delayed acclimation limits the time they have to be truly effective in their roles and to drive key initiatives forward.

Pipeline of senior talent

We inquired about **bringing senior talent into CIO roles** and discussed succession planning. Several respondents noted that transitioning from the private sector, particularly from high-paying areas like Silicon Valley, into Federal Government often involves a salary reduction. However, the opportunity to serve the American people is a powerful draw. CIOs who have made this transition shared that the chance to impact millions and contribute to the greater good can outweigh financial concerns. They emphasized the strong sense of purpose derived from mission-driven work and meaningful, large-scale projects.

Although one interviewee mentioned activity in the CIO Council Workforce Committee about strategic career roadmaps, CIOs were unaware of a **talent pipeline** for bringing in highly capable senior professionals, or to develop high-potential aspiring CIOs.

Several participants proactively raised the idea of bringing individuals into government who have experience working in the private sector, particularly those with a background in **leading modern software development**. One respondent noted, “We need people who have genuinely shipped products and understand that way of working.”

However, there is no proven **model for bringing senior hires from industry into government** roles, and some participants tempered their enthusiasm with the view that “Silicon Valley people struggle at the executive level”. In our global work with hires from industry, we have observed that success often hinges on their ability to recognize the challenging journeys the staff working for the agency have already undertaken. We heard in some discussions that new CIOs are most successful when they acknowledge the prior contributions of their technical teams over the years, and listen to staff at all levels to understand the “areas where you haven’t gotten much traction, but are important”.

Legislation and governance

There is a growing desire to streamline the significant regulatory overhead which CIOs must navigate. The community would welcome an opportunity to lead the shift from a compliance mindset to a risk management approach. With the extensive legacy systems and technology CIOs must deal with, better funding and governance support for legacy modernization will be essential to enabling more effective digital transformation across government agencies.

Regulation

We heard from all CIOs about the significant quantity of regulations they are required to navigate. Several described extensive discussions with legal teams about how certain legislation related to their agency. The **quantity and complexity of the regulations makes it "hard to keep everything in your head"** and understand what applies in any given situation, and when. Although public servants have developed a level of expertise in navigating the legislation, it remains time-consuming and cumbersome to manage. For CIOs, the implication was that this regulatory burden can detract from their ability to focus on strategic priorities.

Some CIOs did say that the **legislation is useful**, and has evolved with disruptive technology, doing a good job of providing guidance across government.

However, we heard that, in total, CIOs must comply with over 130 statutory requirements, which span across various areas of IT governance, security, and operations. Some of these date back to the 1990s, and there is a question about how much they remain relevant to today's IT and digital environment. CIOs strongly expressed the need for a **"burden reduction effort"** to streamline or update these requirements, making them more relevant and manageable, and mutually consistent. This would not only reduce the administrative load but also free up resources for more critical, forward-looking initiatives.

An important theme that emerged during our discussions was the **opportunity to shift from a "compliance mindset" to a risk management approach**. Many CIOs felt that their agency would benefit if they could move away from excessive time spent on regulatory compliance, toward proactive risk identification and mitigation.

CIOs further raised the tendency for legislative efforts to **focus too much on cutting-edge themes such as AI, at the expense of resolving some of the long-standing issues with the existing legislation**. While welcoming the development of a common approach to new high-potential areas like AI, CIOs emphasized the importance of balancing these efforts with easing the day-to-day realities of developing and securing their existing IT infrastructure.

Executive Orders

The CIOs shared a consistent perspective on effectiveness of Executive Orders (EOs), that where they have been used, they have been **effective and well adopted**. However, some mention that the quality of the EOs has been varied. EO 14028 on Improving the Nation's Cybersecurity was frequently cited as particularly impactful. Many welcomed its focus, stating that "cybersecurity focuses everyone's attention and is the common priority we all need to address". Several respondents also praised the EO on AI.

A key concern raised by CIOs was the **challenge of unfunded mandates**. While they acknowledged that the required actions may be completed, this often comes at the expense of other essential activities. At least one participant attributed this to "a misunderstanding in the White House that money comes from mission work for IT". Several were explicit that extra funding would be "the only way to get away from legacy systems".

CIOs cautioned that **"not everything can be the #1 priority"** and emphasized the significant effort required to prioritize resources in order to meet the wide array of expectations placed upon them, with some CIOs commenting that "new EOs come out before you have even had the chance to implement the last one on that theme".

CIOs also voiced frustration about the **lack of consultation** with those responsible for implementing the Executive Orders, noting that when there was greater engagement it improved both the quality of the directives and fostered stronger buy-in and understanding among the execution teams. However, some CIOs tempered this view, acknowledging that "not everyone will always have the chance to weigh in", and suggested they are familiar with the feedback channels that exist, and know where to go for clarification if needed.

Despite these issues, **success stories** emerged, with CIOs attributing positive turnarounds to effective monitoring and measurement. Many noted that "a little competition has been helpful" and "we are all in it together".

Leadership beyond the IT organization

As part of our methodology, we expanded the discussion beyond IT to assess the transformational leadership capability of agencies. Our CIOs welcomed this aspect of the interviews, emphasizing that the **modernization agenda involves more than just technology**.

In discussing organizational change, several conversations referenced their agency's Transformation Office. We observed that some CIOs were **unclear who had the accountability for business change enabled by digital transformation** in their organization.

A common issue frequently mentioned was that **technology is "perceived as an overhead"**. Some felt their Secretary and Deputy Secretary "aren't interested in technology", while others were more positive, but still noted that "it's crucial for the Deputy Secretary to take a very active role". Others struggled to make a compelling case for efficiency and the opportunities presented by digital transformation, even suggesting that there could be a clearer "head of efficiency" within each agency. One respondent proposed that every agency should have a Deputy Secretary for Management, which should include IT. Others only went as far as to say they are "not having good IT conversations". This sentiment varied by agency, as others reported having strong relationships and mutual understanding with their leadership.

Many respondents felt that the **Federal Information Technology Acquisition Reform Act (FITARA) introduced valuable concepts, particularly in granting CIOs authority over IT matters** at the executive level. They felt that this provided the CIO more of the influence they need (or as one respondent put it, "a small stick"). Some CIOs expressed appreciation that their agency's leadership was highly "in tune" with their FITARA scores and actively engaged in efforts to improve them. However, several questioned how consistently FITARA has been implemented across different agencies.

Several CIOs mentioned **significant levels of shadow IT** used by their agencies. Some attributed this to a historical approach in which CIOs were kept 'hands-off' regarding systems built by individual projects. They were acutely aware that this issue becomes particularly pressing during security incidents, when the CIO is held responsible—even if they did not oversee the system's implementation. Some CIOs highlighted the challenges of bringing shadow systems under the

monitoring of their security operations center. Others discovered that certain services were hosting websites not on a .gov domain.

We previously considered the question of political appointments to CIO roles. Regardless of their appointment process, **most participants felt that the federal CIO structure was generally appropriate**. We discussed the presence of multiple levels of CIOs in large agencies, where sub-agencies have their own IT directors or CIOs reporting to the agency CIO. This arrangement did not appear to create specific issues, and none of the respondents were eager to change it, although it adds complexity to the already wide span of control.

There was a strong desire for a change in **how the CIO interacts with the 'top table' at their agency**. Most respondents commented that the CIO needs to be a respected leader with a seat at the table. Some felt there was more to be done to facilitate closer collaboration between CIOs and their C-suites. Others observed that "some Secretaries and Deputy Secretaries don't understand that technology has changed".

CIOs expressed a strong desire to "help leaders understand what we do to enable their mission". In return, their primary request was for leaders to "**support our efforts**", "ask the tough questions", and "be informed consumers".

Although not applicable to every agency, some respondents urged caution around making separate appointments for **advisors to agency executives on technology**. The main concern was that this could become a "second CIO, without operational responsibility", and ultimately cause confusion and mixed messages.

Additionally, some respondents suggested that this senior-level influence should be mirrored at the federal level, giving **more influence to the Federal CIO in the Executive Office of the President**. This would elevate the role, ensuring that Secretaries view the Federal CIO as a peer, similar to leaders in national security, for example.

The need for **governance of multi-year programs** was emphasized. The general theme was that while new administrations may set different directions, the technology, digital and data services must continue to operate, requiring security, maintenance, and development. Although everyone acknowledged that stewardship rests with the agency, most expressed a desire for some assurance that they would be able to "finish what we have started".

Acknowledgements

Report authors: Kevin Cunnington & Andrew Besford

Editors: Richard Johnstone & Sarah Wray

Research Executive: Maria Fetta

Research Director: Chris Punch

For more information please contact the team at: editor@globalgovernmentforum.com

This report is part of the Digital Leaders Study program, published by:

GLOBAL government FORUM

Organizers of

GOVERNMENT SERVICE DELIVERY

Global Government Forum is part of Pendragon International Media Ltd

Registered address: The Old Vicarage, 10 Church Street, Rickmansworth, WD3 1BS, United Kingdom

www.globalgovernmentforum.com

www.pendragonim.com