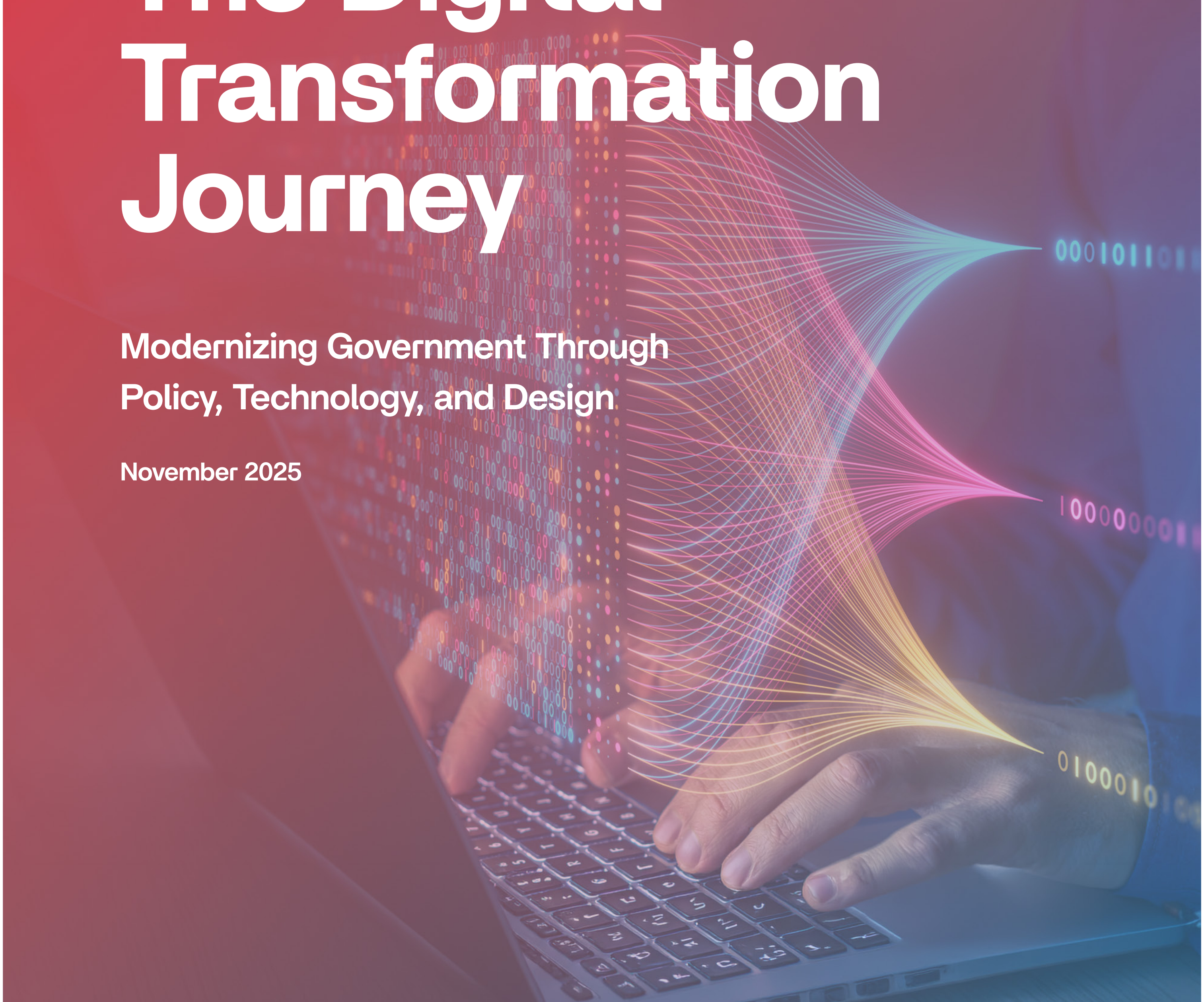
Evolver

The Digital Transformation Journey

Modernizing Government Through Policy, Technology, and Design

November 2025



Introduction

Across the United States federal government, digital transformation is no longer optional; it is a "must do" and a true mission enabler. Each year, the U.S. government spends well over $100 billion on Information Technology (IT) products and services and cyber-related investments, yet agencies historically allocate most of their budget, nearly 80% of those dollars, to operations and maintenance of legacy systems—systems that drive cost, risk, and inflexibility [1, 2].

At the same time, modernization funding is limited. The Technology Modernization Fund (TMF) has only been authorized up to $1B to work across 60+ large-scale IT modernization projects, accelerating cloud adoption and service digitization [3].

In this whitepaper, we outline a practical, outcomes-oriented approach to achieve successful digital transformation programs tailored to meet the needs of U.S. federal government critical missions.

We recommend the proactive integration of leading AI-based commercial IT products and integrated professional services. As part of this integration, we recommend that every digital transformation group focus from the start on both enterprise data governance and cybersecurity by design.

Furthermore, every digital transformation program should place special emphasis on human-centered design, Customer Experience (CX) & User Experience (UX), while fully leveraging modern software development models—including low-code/no-code (LC/NC) and AI-powered coding assistant software—to shorten time-to-value under strict ethical compliance guidelines.

Finally, we advocate for a cloud-first development plan while leveraging Financial Operations (FinOps) analysis to ensure a complete and accurate understanding of the Total Cost of Ownership (TCO) and the rate of return on investment (ROI) for each digital transformation program. The U.S. taxpayers deserve to have their money wisely spent to improve performance results.

What is Digital Transformation?

Digital transformation is the sustained re-design of services, operations, and decisions by aligning policy, process, people, data, cybersecurity, and technology to deliver measurable mission outcomes. In the federal context, transformation is codified through mandates and guidance:

- 21st Century The 21st Century Integrated Digital Experience Act (IDEA) requires accessible, mobile-friendly, secure, and user-centered federal digital services, as well as digitization of forms and e-signatures [4].
- Executive Order 14058 directs agencies to prioritize life-experience journeys and improve the federal customer experience (CX) [5].
- OMB M-22-09 requires agencies to adopt Zero Trust and meet specific cybersecurity objectives, making security architecture foundational to modernization [6].

PRO TIP

Anchor every transformation business case to a statutory or policy driver (IDEA, EO 14058, M-22-09). This tightens scope, clarifies acceptance criteria, and eases governance reviews.

Why Do So Many Digital Transformation Programs Fail?

Multiple studies show high failure rates for large-scale transformations; widely cited research estimates the figure at nearly 70% when initiatives lack clear value realization, sustained leadership engagement, and capability building [7, 8]. In government, failure is rarely about vision; it is about execution under constraints—legacy technical debt, fragmented data, regulatory compliance, budget structures, and workforce capacity.

Common Root Causes

- **Strategy–execution gap.** Ambition outpaces productized roadmaps, value metrics, and change capacity. [9]
- **Legacy drag.** O&M-heavy portfolios starve modernization lines of effort. [10, 11]
- **Security bolted on late.** Controls retrofit slows delivery and increases cost of rework; modern programs must start "secure-by-design." [12]
- **Fragmented CX.** Services are designed around org charts, not life experiences; IDEA and EO 14058 expect the opposite. [13, 14]
- **Talent and tooling misfit.** Teams lack product, UCD, and platform skills; procurement cycles misalign with iterative delivery.
- **Insufficient data governance.** Poor metadata, lineage, and access controls block analytics, automation, and AI.

PRO TIP

Treat transformation as a portfolio of measurable bets–each with a product owner, service-level objectives (SLOs), and quarterly value reviews that can pivot or sunset work.

Key Challenges Facing U.S. Federal Digital Transformation Programs

- **Legacy Systems and Technical Debt.** Agencies still direct ~80% of IT spending to O&M, limiting modernization headroom and keeping cyber risk high. [15, 16]
- **Security, Compliance, and Zero Trust Adoption.** OMB M-22-09 and CISA require concrete Zero Trust milestones; DoD's strategy adds mission-specific depth. [17, 18, 19]
- **Cloud and Authorization Velocity.** FedRAMP's modernization and TMF's growth indicate strong momentum, but authorizations and backlog management remain execution challenges that require automation and reusable controls. [20]
- **Human-Centered CX/UX.** IDEA and EO 14058 push agencies to redesign around user journeys with accessibility and equity; analytics show the public's demand is massive (billions of pageviews monthly). [21, 22]
- **Data Foundations for AI/Automation.** Without clear ownership, catalogs, and protection, agencies struggle to exploit AI safely; breach costs highlight the stakes. [23]
- **Workforce and Ways of Working.** Product management, DevSecOps, and platform engineering are not yet universal disciplines across government.

U.S. Federal Digital Transformation Program & Technology Best Practices

1 Anchor Transformation in Policy, Statute, and Integrated Commercial Solutions

Effective federal digital transformation begins by explicitly tying each initiative to statutory and policy drivers—such as the 21st Century IDEA, Executive Order 14058, and OMB M-22-09—and then translating those mandates into clear, measurable outcomes. These drivers provide both the urgency and the governance framework that help agencies sustain momentum across budget cycles and leadership changes.

Within that policy frame, agencies should default to leading commercial IT platforms and Software-as-a-Service (SaaS) offerings, combined with integrated professional services for architecture, implementation, cybersecurity, and change management. Rather than bespoke, one-off builds, program leaders can adopt productized commercial capabilities and surround them with mission-aligned services that accelerate time-to-value, simplify operations, and reduce technical debt.

Each major capability should have a clearly accountable product owner (e.g., a CIO/CTO/CISO delegate) responsible for aligning commercial platforms and services to mission needs, defining service-level objectives (SLOs), and coordinating performance-based contract incentives. This creates a direct line of sight from policy requirement to commercial capability to measurable mission outcome.

PRO TIP

For each major initiative, maintain a one-page "Policy-to-Product" map that links statutory/policy drivers to specific commercial platforms, integrated services, and performance measures. Use this map in governance boards to keep discussions grounded in outcomes rather than tools.

2 Modernize in Increments and Fund Legacy Retirement

Large, monolithic modernization programs are risky and slow. Agencies are more successful when they treat transformation as a portfolio of incremental bets that progressively retire legacy systems while delivering visible, user-facing improvements.

A modernization roadmap should include a proven effective methodology to implement a phased transition of IT capabilities off legacy information systems onto modern commercial cloud, data, and security services. Each release should decommission at least one legacy module, interface, or manual process. The savings in operations and maintenance (O&M) can then be transparently reinvested into development, modernization, and enhancement (DME), creating a self-reinforcing cycle of improvement. [24, 25]

Modernization increments should be sized to demonstrate tangible improvements within 3–9 months—such as a new digital service, a simplified user journey, or a retired legacy interface—while also advancing Zero Trust, data governance, and observability. Integrated professional services are critical here: they align sequencing across policy, architecture, cybersecurity, and change management, ensuring that each increment meaningfully reduces risk and operational complexity.

PRO TIP

Require every program increment to show three artifacts before funding the next: (1) the legacy capability reduced or retired, (2) the new commercial platform or service that replaced it, and (3) quantified O&M savings or risk reduction.

3 Start with Cybersecurity and Zero Trust Design

Cybersecurity must be treated as a design constraint from day one, not a late-stage compliance exercise. Agencies can map transformation epics and user journeys to Zero Trust pillars—identity, devices, network/environment, applications & workloads, and data—and plan objective evidence for each pillar per OMB M-22-09 and CISA's Zero Trust Maturity Model. [26, 27]

Leading commercial identity, endpoint, and cloud security platforms—integrated with professional services for architecture, configuration, and continuous operations—can provide the backbone for Zero Trust implementation. These platforms should be embedded directly into delivery pipelines so that new services inherit standardized policies, controls, and logging from the start.

Adopting secure-by-design practices further reduces risk and accelerates authorization. This includes threat modeling, software bills of materials (SBOMs), software composition analysis (SCA), infrastructure-as-code (IaC) scanning, and supply-chain risk management integrated into CI/CD. Agencies can operationalize "risk-as-code" by using automation to generate continuous, machine-readable evidence that feeds Authorizing Officials (AOs) and Information System Security Managers (ISSMs). AI-enabled continuous ATO (C-ATO) patterns will then reduce friction as portfolios scale.

PRO TIP

Treat the ATO as a living program artifact, not a one-time gate. Define a standard set of commercial security platforms, telemetry, and automated tests that every new workload must use. Feed their outputs directly into your C-ATO evidence pipeline to keep authorization current with minimal overhead.

4 Leverage Low-Code/No-Code and AI-Enabled Development Under Guardrails

Low-code/no-code (LC/NC) platforms and AI-enabled coding assistants can dramatically increase delivery speed for forms, workflows, case management, and integration services—especially where 21st Century IDEA and EO 14058 emphasize digitization, accessibility, and mobile-friendly design. Gartner forecasts that by 2025, 70% of new applications will use LC/NC, up from less than 25% in 2020, a trend that federal agencies can harness with appropriate guardrails. [28]

A sound LC/NC strategy for government involves:

- Platform baselines: Selecting FedRAMP-authorized LC/NC and integration platforms, with standardized identity, logging, and security configurations.
- Governed citizen-development: Providing role-based templates, component libraries, and data policies so that mission teams can build safely without creating shadow IT. [29]
- DevSecOps integration: Treating LC/NC outputs as first-class workloads, subject to scanning, testing, monitoring, and change control like any other application.
- Leading commercial LC/NC platforms, paired with structured implementation and enablement services, can shift routine automation work to mission teams while central IT focuses on platforms, security, and data. AI-enabled coding assistants can further accelerate complex development, provided they operate under clear guardrails for privacy, intellectual property, and security.

PRO TIP

Establish a "pattern catalog" of pre-approved LC/NC solutions (e.g., permit intake, grants triage, case intake) that combine a commercial platform, reference architecture, and reusable assets. This accelerates delivery while keeping security and compliance consistent.

5 Make Human-Centered CX/UX and Analytics Non-Negotiable Requirements

Executive Order 14058 and the 21st Century IDEA push agencies to design services around life experiences and user journeys, not internal organizational charts. [30, 31] Human-centered design should therefore be a first-order requirement in every transformation effort, on par with cost, schedule, and security.

Programs can start by mapping priority journeys—for example, applying for benefits, contesting a decision, or updating records—across channels and touchpoints. Inclusive research across languages, abilities, and demographics ensures that redesigned services are equitable and accessible. Modern commercial experience analytics and feedback platforms, integrated with professional services in CX, design, and content strategy, can help agencies continuously refine services based on real-world behavior and feedback.

Analytics must be treated as part of the experience, not as an afterthought. Participation in the Digital Analytics Program (DAP) and use of common analytics patterns allow agencies to benchmark traffic, task completion, accessibility, and latency across websites and applications. [32, 33] These data, combined with user research and qualitative feedback, create a closed feedback loop to guide further investment.

PRO TIP

Build "CX gates" into delivery pipelines: no release moves to production unless it meets accessibility (e.g., WCAG 2.2), plain-language, and analytics instrumentation criteria, with defined success metrics tied to user tasks.

6 Adopt a Cloud-First Model with FinOps to Understand TCO and ROI

A cloud-first deployment model, when combined with rigorous Financial Operations (FinOps), allows agencies to understand and manage the true Total-Cost-of-Ownership (TCO) and Return on Investment (ROI) of digital transformation programs. Rather than defaulting to on-premises or bespoke solutions, agencies should begin by evaluating leading commercial cloud, data, and security platforms—Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and SaaS—against mission, security, and financial criteria.

FinOps brings engineering, finance, and mission owners together to continuously monitor and optimize cloud consumption. Practices such as right-sizing, reservation management, elasticity, and chargeback/show back help ensure that cloud spending aligns with usage and value. When integrated with program management, FinOps provides agencies with transparent TCO and ROI projections over a 3–5-year horizon, supporting more informed investment decisions and stronger justification of budgets.

Commercial cloud providers and FinOps tooling, combined with advisory and operational services, can help agencies automate cost reporting, forecast demand, model trade-offs between architectures, and tie financial metrics directly to mission outcomes (e.g., cost per transaction completed, cost per citizen served). This transparency is critical to sustaining affordable digital transformation at scale.

PRO TIP

Require a standardized "Cloud Value & FinOps" assessment for every major initiative, including: a cloud-first architecture option, a 3-5-year TCO/ROI view, and specific optimization levers (e.g., auto-scaling, storage tiering) identified in advance. Use this assessment to inform governance decisions and to track realized value over time.

Conclusion

U.S. Federal government digital transformation is accelerating under clear policy, measurable public demand, and maturing delivery models. Yet, the failure patterns are well known, including strategy–execution gaps, legacy drag, late cybersecurity, fragmented CX, weak data foundations, skills misalignment, and lack of performance-based metrics.

The playbook to break this cycle is equally clear:

- Tie every initiative to statutory or policy drivers (IDEA, EO 14058, M-22-09) and leverage leading commercial products with integrated professional services and accountable owners, using performance-based contract incentives. [34, 35, 36]
- Modernize in increments, funding strangler patterns that retire legacy and reinvest O&M into DME. [37, 38]
- Start with cybersecurity, Zero-Trust architecture (ZTA), and automated evidence via AI-powered C-ATO to reduce authorization friction as portfolios scale. [39, 40]
- Leverage LC/NC and AI-powered coding assistant software (under enterprise guardrails) to digitize services faster while preserving assurance. [41, 42]
- Make human-centered design, accessibility, and analytics first-class, measurable requirements. [43, 44]
- Implement a cloud-first IT deployment model with Financial Operations (FinOps) analysis to determine the real Total-Cost-of-Ownership (TCO) and the return on investment (ROI).

We believe that when agencies align policy, commercial technology, integrated services, cybersecurity, CX, data, and financial stewardship, digital transformation becomes a repeatable discipline rather than a one-time initiative—delivering better, more affordable mission outcomes for the public.

About the Authors

Gregory A. Garrett is the Chief Operating Officer of Converged Security Solutions (CSS), leading expert teams within business units Evolver and eVigilant. These groups provide advanced IT, AI, cybersecurity, electronic security, and eDiscovery services to federal agencies and Fortune 500 companies.

With over 25 years of executive experience and a background as a CIO, CTO, CISO, and COO, he has managed more than $40 billion in global tech contracts and served in key roles across both large and mid-sized firms.

A retired U.S. Air Force Colonel and accomplished author, Garrett has also contributed extensively to industry thought leadership through 24 books, more than 150 articles, expert testimony, and over 250 speaking engagements.

Dr. Brian McElyea is an accomplished cybersecurity executive recognized for leading largescale digital transformation initiatives and building high-performing Cyber Centers of Excellence that drive mission-aligned security outcomes.

With over two decades of leadership across healthcare, defense, and federal sectors, he has guided global organizations through the complexities of risk management, compliance, and modernization with measurable results.

www.evolverinc.com

Works Cited

- **[1, 10, 15, 24, 37]** GAO. Agencies Need to Continue Addressing Critical Legacy Systems. 10 May 2023.
- **[2, 11, 16, 25, 38]** GAO. Agencies Need to Plan for Modernizing Critical Decades-Old Systems. 17 July 2025.
- [3, 20, 32] General Services Administration. TMF FY24 Annual Report. 29 Dec. 2024.
- [4, 13, 21, 34, 43] Digital.gov. "Delivering a Digital-First Public Experience: 21st Century IDEA." 2018.
- [5, 14, 30, 35] Performance.gov. "Executive Order 14058 on Transforming Federal Customer Experience." 2021.
- [22, 31, 33, 44] Performance.gov. "Federal Website Performance." 2025.
- [6, 34, 37, 39] Office of Management and Budget. M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. 26 Jan. 2022.
- [7, 9] McKinsey. "Common Pitfalls in Transformations: A Conversation with Jon Garcia." 29 March 2022.
- [8] McKinsey, "Losing from Day One: Why even successful transformations fall short." Dec. 2021.
- [12, 17, 26, 36] Office of Management and Budget. M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. 26 Jan. 2022.
- [18, 27, 40] CISA. Zero Trust Maturity Model, Version 2.0. Apr. 2023.
- [19] DoD Chief Information Officer. Department of Defense Zero Trust Strategy. Nov. 2022.
- [23] IBM. "IBM Report: Escalating Data Breach Disruption Pushes Costs to New Highs." 30 July 2024.
- [28, 29, 41] Gartner. "Gartner Forecasts Worldwide Low-Code Development Technologies Market to Grow 23 Percent in 2021." Newsroom Press Release, 16 Feb. 2021.
- [42] Gartner. "Gartner Says Cloud Will Be the Centerpiece of New Digital Experiences." Newsroom Press Release, 10 Nov. 2021.

Additional Sources

- Congress.gov. "H.R.5759 — 115th Congress (2017–2018): 21st Century Integrated Digital Experience Act." 2018.
- U.S. Department of Health and Human Services. "The 21st Century Integrated Digital Experience Act (IDEA)." 18 Sept. 2024.
- U.S. Federal Register. "Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government." 16 Dec. 2021.

www.evolverinc.com