Conceptual Framework for Cybersecurity-Integrated Performance Excellence in U.S. Digital Public Services

Karyn Ekpo[1], Kenneth Nnadi[2]

[1]University of West Georgia – Richards College of Business, USA
[2]University of Oregon, USA

Abstract:
Agencies of the United States are required to provide quicker, less complex, and fairer digital public services and enhance cybersecurity at the same time. Policy and engineering guidance (e.g., Zero Trust, secure-by-design software, systems security engineering, cloud guardrails) and performance frameworks (e.g., leadership, measurement, customer value, equity) are all well-developed, but are typically operationalized concurrently, yielding poor traceability between security features and service performance (e.g., reliability, burden reduction, accessibility, and public trust). This paper fills this gap in the execution and suggests a conceptual framework that unifies cybersecurity and performance excellence into one management logic of digital public services in the United States. With an integrative review of relevant federal policy and standards, oversight materials, and academic syntheses, we formulate six constructs, Governance & Strategy (GOV), Secure-by-Design capabilities (SBD), Service Operations and Reliability (OPS), Assurance and Compliance (ASSUR), Customer Experience and Equity (CXE) and Outcomes (OUT) and theorize their connections. We provide a measurement crosswalk of leading capability indicators (e.g., Zero Trust pillar maturity, secure-Software Development Life Cycle (SDLC) adoption, SBOM/attestation coverage, telemetry completeness) and lagging service indicators (e.g., uptime/SLO achievement, incident frequency/MTTR, burden/time, satisfaction, trust, accessibility/equity). We define governance cadence and data plumbing that render capability adoption transparent as a service outcome generator, and we state falsifiable hypotheses to inform empirical analysis through agency metrics. The framework is auditable and real-world. It transforms the mandates of modernization into the form of outcomes-focused management, in which the leaders can prove how cybersecurity enhances the performance and legitimacy of the digital public services. It does this by showing paired indicators and exercising rigorous interpretation of the outcomes.

Keywords: Digital public services, cybersecurity-performance integration, Zero Trust Architecture; NIST Cybersecurity Framework (CSF) 2.0, Baldrige Excellence Framework.

1. INTRODUCTION

The U.S. public institutions should simultaneously provide more equitable, rapid and simpler digital services and maintain a better cybersecurity against continuous threats. These are incorporated in executive, budgetary and technical binding mandates. At the service side, there is federal guidance that mandates agencies to design services to be accessible and equitable, and to quantify the outcomes at the transaction level, including burden and trust (OMB Circular, 2021; Young, 2023; Digital.gov, 2025; Marine, 2024). On the security side, policy guides agencies to embrace Zero Trust and modernize telemetry and logging, as well as establishing secure-by-design software practices through the entire supply chain (Young, 2022; House, 2021; Federal Register, 2021; Souppaya et al., 2022). The main issue that this paper addresses is the fact that performance excellence and cybersecurity continue to be operationalized in parallel, as opposed to being an operating logic of digital-based public services.

The performance excellence models provide an available foundation but need clear incorporation with cybersecurity. Baldrige Excellence Framework uses a system that classifies leadership, strategy, customers, measurement/knowledge, workforce, operations, and results in a coherent management system, which is

customized by most of the public organizations (Baldrige Performance Excellence Program, 2021; Schaefer, 2016; Ghafoor et al., 2021). Security, and cybersecurity in particular, is also acknowledged by Baldrige materials as something that customers expect from high-performing organizations, and Baldrige Cybersecurity Excellence Builder bridges the gap between Baldrige and Cybersecurity risk management (Baldrige Performance Excellence Program, 2019, 2021). However, traceability between particular security capabilities (e.g., identity assurance strength, software attestations/SBOM, segmentation and telemetry) and service results (e.g., reliability, burden reduction, equity, and public trust) is often missing between agencies. Federal cybersecurity requirements indicate what is to be built, however, it is indirectly linked to performance of the services (Nnadi et Opoku, 2025; Nnadi et al, 2026). The redefinition of cybersecurity in Executive Order 14028 is based on the idea that it is modernization, with a focus on software supply-chain security, detection/response, and the adoption of Zero Trust (House, 2021; Federal Register, 2021). The mandatory requirements of OMB M-22-09 stipulate a Zero Trust Architecture working to be implemented across identity, devices, networks, applications/workloads, and data, whereas the Zero Trust Maturity Model of CISA v2.0 gives staged capability guidance that has cross-cutting Visibility and Analytics, Automation and Orchestration, and Governance (Young, 2022; CISA, 2023). National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF) 2.0 enhances linkages of leadership and measurement by increasing the Govern function (NIST, 2024). NIST SP 800-218 formalizes the secure-by-design, and the NIST SP 800-160 gives the principles of systems security engineering of trustful sociotechnical systems (Souppaya et al., 2022; Ross et al., 2022). These expectations are converted into cloud patterns and shared responsibilities according to Cloud Security Technical Reference Architecture v2 and the NIST Cloud Computing Reference Architecture (CISA et al., 2022; Lui et al., 2011). What is still under-specified across policy and practice is how these capabilities are regulated and quantified as drivers of service outcome as opposed to parallel compliance pathways.

There is an urgency of an integrated approach brought out by oversight and sectoral maturity models. Government accountability assessment is often found to identify the lack of governance in relation to risk, modernization planning, and traceability of outcomes, which may undermine reliability and public trust unless they are addressed (GAO, 2025). Sectoral models like Cybersecurity Capability Maturity Model (C2M2) demonstrate how capability maturity can be designed, quantified, and gradually enhanced and provide patterns applicable to civilian digital services (CISA, 2022). Academic summaries converge on the necessity to integrate cybersecurity in digitalization to continue creating value and resilience (Metin et al., 2024; Azmi et al., 2018; Calvo-Manzano et al., 2025; Melaku, 2023). The concept of work on public value focuses on the legitimacy, trust, and equitable results, the aspects that are influenced by the existence and applicable security controls (Panagiotopoulos et al., 2019). The literature complementing the present scholarly work on the metrology of organizational performance highlights what agencies measure and how they measure often defines what it can consistently enhance (Bailey, 2015).

This paper constructs an informed conceptual framework that can unite performance excellence and cybersecurity into one theory of change in the context of digital public services in the United States. We also perform an integrative review of authoritative federal policy and standards, performance excellence material, and oversight and scholarly works. We describe constructs and linkages that render cybersecurity capabilities causal in outcomes of services and suggest a governance and measurement crosswalk that may be implemented in public agencies.

In the paper we address what governance systems and competences are associated with cybersecurity and performance excellence in U.S. digital public services, where frameworks are coinciding, overlapping or contradicting and what conceptual or policy gaps exist. The rest of the paper gives definitions and context, synthesizes thematic evidence, finds conceptual and policy gaps, describes our proposed framework and propositions, discusses governance and measurement implications and outlines boundary conditions and evaluation directions.

2. BACKGROUND AND DEFINITIONS

U.S. digital public services and performance expectations:

In the context of the term digital-first, agencies will be responsible for transaction-level evidence burden, satisfaction, trust, and resolution time, and this requires security decisions to be supported in terms of the measurable impact on these service delivery outcomes (OMB Circular, 2021; Young, 2023; Digital.gov, 2025; Marine, 2024). Such requirements cut across federal mission areas and have implications on state and local applications through the diffusion of policy and funding terms. The Baldrige Excellence Framework, as a performance excellence template that is common in the management of public organizations, divides the management into Leadership, Strategy, Customers, Measurement/Knowledge Management, Workforce, Operations, and Results (Baldrige Performance Excellence Program, 2021; Schaefer, 2016). More importantly, Baldrige documentation underscores that customer needs include security, which is a broad concept covering physical, operational, and information safeguards, and it explicitly extends this to cybersecurity (Baldrige Performance Excellence Program, 2021). By framing cybersecurity as part of what customers expect in terms of service quality, Baldrige shifts it from being viewed merely as a compliance obligation to being understood as a core component of value delivery.

Foundations of performance excellence:

Baldrige offers a consistent purpose, strategy, process and evidence alignment. The Criteria Commentary explains the practice expectations covering leadership accountability, strategy implementation, and use of measures in a disciplined manner (Baldrige Performance Excellence Program, 2021). Reviews of academic literature and practice suggest that Baldrige facilitates learning and permanent enhancement in government when mapped onto public-value goals (Schaefer, 2016; Ghafoor et al., 2021). Baldrige Cybersecurity Excellence Builder (BCEB) specially provides the connection between Baldrige and cybersecurity risk management and provides a self-assessment framework that connects organizational context, processes, and outcomes of cyber performance (Baldrige Performance Excellence Program, 2019). This bridge is the focus of the integration task of our paper. BCEB demonstrates the current points of intersection of excellence and cybersecurity, yet agencies lack a traceable operating model that links certain cyber capabilities to service results.

Engineering and policy foundations of cybersecurity:

Cybersecurity has become a new modernization requirement by federal directives. Executive order 14028 triggers government-wide enhancements in the field of software supply-chain security, detection and response, and the adoption of zero-trust (House, 2021; Federal Register, 2021). OMB M-22-09 requires a Zero Trust Architecture of identity, devices, networks, applications/workloads, and data (Young, 2022). The Zero Trust Maturity Model v2.0 operationalization of capability development by Cybersecurity and Information Security Agency (CISA) has maturity stages and three cross-cutting disciplines, such as "Visibility and Analytics, Automation and Orchestration, and Governance" (CISA, 2023). The latest version of the NIST CSF 2.0 upgrades the national level of risk-management and expands the Govern function to encompass leadership, policy, and measurement (NIST, 2024). The practice of secure-by-design and supply-chain attestations is codified in NIST SP 800-218 and systems engineering principles of building reliable sociotechnical systems are provided in NIST SP 800-160 (Souppaya et al., 2022; Ross et al., 2022). In the case of cloud, Cloud Security Technical Reference Architecture v2 and NIST Cloud Computing Reference Architecture transform the policy requirements into architectural patterns and common responsibilities among service models (CISA et al., 2022; Lui et al., 2011).

Oversights, exemplary maturity and academic basis:

The food and drug control reports emphasize oversight, modernization planning, and traceability-to-outcomes-recurring problems having the potential to destroy reliability and public trust (GAO, 2025). The transferable practices portrayed by sectoral maturity models like C2M2 include role clarity, tiering informed by risks, continuous monitoring, and uplift of iterative capability (CISA, 2022). Academic reviews unite around embedding the concept of cybersecurity into digitalization to achieve resilient value, as opposed to mere compliance (Metin et al., 2024; Azmi et al., 2018; Calvo-Manzano et al., 2025; Melaku, 2023). Public value frames performance in terms of legitimacy, trust, equity, and mission results, which are directly

influenced by the presence and usability of security controls (Panagiotopoulos et al., 2019). Supplementary studies regarding the metrology of organizational performance underline the fact that enhancement requires valid and reliable measurements and rigorous interpretation (Bailey, 2015).

3. SYNTHESIS OF LITERATURE AND POLICY CORPUS.

Governance and accountability:

Across various sources, the governance clarity is the starting point of the effective integration of cyber-performance. It deals with whoever owns risk, who owns experience and how do their incentive align. The Baldrige materials indicate leadership accountability to a consistent framework of strategy, clients, measurement/knowledge, workforce, operations, and outcomes (Schaefer, 2016). The BCEB brings this reasoning to the field of cybersecurity, where organizational context, maturity of the process, and outcomes are combined into a unified self-assessment framework (Baldrige Performance Excellence Program, 2019, 2021).

Governance expectations are now proscribed in U.S. cyber policy as part of security itself. CSF 2.0 brings Govern to the level of first-class functions, which enhances leadership accountability and integration of measurement (NIST, 2024). OMB M-22-09 appoints agency leadership as the implementation of Zero trust outcomes in identity, devices, networks, applications/workloads, and data whereas CISA ZTMM v2.0 governance is one of three cross-cutting disciplines (along with visibility/analytics and automation/orchestration) (CISA, 2023; Young, 2022). This is important because oversight evidence demonstrates that the frequent lack of consistency in risk governance and modernization planning limits the likelihood that the cyber capabilities will be transformed into dependable services (GAO, 2025). The transferability of governance practices, such as role definition, risk-tiering, and iterative capability uplift, employed in mature and tested critical-infrastructure models are applicable to civilian digital services (CISA, 2022).

The connection between the cybersecurity capabilities and the service results should be possessed by governance and not just supervised by two independent scorecards. Baldrige with its leadership/measurement disciplines and CSF with its Govern provides the anchor whereas ZT governance cadences make it operational (Baldrige Performance Excellence Program, 2021; NIST, 2024; CISA, 2023).

Secure digital service delivery capability stack:

The capability literature is focused on a layered stack that has the capacity to provide reliable digital services. The stack includes:

Cross-cutting visibility/automation/governance (including identity, devices, networks, applications/workloads, data) in the form of zero trust pillars (Young, 2022; CISA, 2023). SSDF activities like planning, protecting, producing, and responding, with the help of artifact integrity (e.g., SBOM, attestations) supported by secure software engineering (Souppaya et al., 2022). The principles of systems security engineering that involves the construction of inbuilt credibility across the life-cycle phases and socio-technical frontiers (Ross et al., 2022). Cloud TRA v2 and the NIST Cloud Computing Reference Architecture present cloud guardrails such as identity control planes, network segmentation patterns, logging/telemetry pipelines, key management, and shared-responsibility clarity that are captured in Cloud TRA (Lui et al., 2011). Executive Order 14028 prompted an integrated security response and supply-chain software detection/response (House, 2021; Federal Register, 2021).

This stack is consistent with academic syntheses, where cybersecurity needs to be integrated into digitalization to obtain resilience in operations and value creation and not an added compliance activity (Metin et al., 2024; Azmi et al., 2018; Calvo-Manzano et al., 2025; Melaku, 2023). The stack is not a goal on its own but a path to performance excellence. The capabilities have to be defined in a manner that can be tracked to the results of reliability, burden, equity, and trust.

Measurement and evidence: the connection between leading capabilities and lagging outcomes:
Service policy demands effort, satisfaction, trust, and timeliness of resolution, all of which are transaction-level CX metrics, as well as access and equity consideration (OMB Circular, 2021; Young, 2023; Digital.gov, 2025; Marine, 2024). Leading indicators are presented in the cyber policy and engineering guidance, which ought to describe those results; ZT pillar maturity, SSDF adoption, SBOM/attestation coverage, code defect density, patch latency and telemetry completeness (Young, 2022; CISA, 2023; Souppaya et al., 2022; CISA et al., 2022).

According to the sources in Baldrige, improvement is based on valid constructs and reliable measures, i.e., valid measures indicating the process to be improved, and reliable measures that can be interpreted by the leadership (Baldrige Performance Excellence Program, 2021; Bailey, 2015). The weak traceability of the modernization controls to service results is identified in the oversight reports (GAO, 2025).

Measuring credibly requires: (1) formulate ability metrics in the ZT/SSDF/cloud stack; (2) formulate service metrics in CX/equity/reliability terms; (3) model pathways of causality (e.g., the strength of identity assurance to less failure at login/transaction completion to less burden, stronger trust).

Workforce and culture, matching incentives to outcomes:
The aspects of performance excellence rely on the ability of the workforce and learning disciplines (Baldrige Performance Excellence Program, 2021; Schaefer, 2016). The former SP 800-160 highlights the necessity of multi-disciplinary teams, capable of making system-spanning decisions, whereas the latter of SSDF lists positions and checkpoints throughout the SDLC (Ross et al., 2022; Souppaya et al., 2022). Zero Trust implementation also expects interfunctional collaboration between identity, platform, application and data teams wherein telemetry and automation workflows are shared (Young, 2022; CISA, 2023). Reviews show that digital transformation initiatives are stalled with measurements placed on opposing goals on security and delivery teams, whereas secure-by-design can make delivery faster when incentives are set to prevent defects and ensure a fast recovery (Metin et al., 2024; Azmi et al., 2018; Calvo-Manzano et al., 2025). The incentives offered to the workforce must be based on the ability to adopt capabilities (e.g., SSDF gates, ZT controls) in relation to service KPIs (e.g., completion rate, mean time to resolve incidents affecting users), so that teams are able to view security as a performance thing and not a limiting factor.

External dependencies and Software supply chain:
Executive Order 14028 and SSDF emphasize the integrity of the supply-chain software, out the artifacts signing, provenance, and vulnerability response (House, 2021; Federal Register, 2021; Souppaya et al., 2022). Cloud reference guidance defines the boundaries of shared responsibility with the focus on centralized identity, logging, and key management to avoid the integration risk (CISA et al., 2022; Lui et al., 2011). The models of sectoral maturity demonstrate the tiering and monitoring of third-party risk which is part of capability governance (CISA, 2022). In their findings, oversight often attributes the problem of information modernization to vendor and integration practices (GAO, 2025). Supply-chain assurance must manifest as capability measures (e.g. percent of critical systems including attested components, SBOM coverage), as well as service-related risks (e.g. dependency-based outages to completion times and trust) (Ogunsola et al, 2026)

Equity, public value and ethics in secure service delivery:
The public value views focus on legitimacy and trust as the result of service designs and governance (Panagiotopoulos et al., 2019). The CX policy focuses on equity, access, and burden, and it is essential that anti-fraud controls, proofing, and MFA minimize the exclusion and increase the assurance (OMB Circular, 2021; Young, 2023; Digital.gov, 2025; Marine, 2024). Academic reviews warn that hard-to-use security measures lead to higher rates of abandonment and reduced legitimacy, therefore usable security patterns can raise completion and satisfaction (Metin et al., 2024; Melaku, 2023). BCEB and CSF 2.0 make provisions to establish cybersecurity as a customer need and a governance requirement, not a back-office activity (Baldrige Performance Excellence Program, 2019; NIST, 2024).

Equity-aware security should be treated as a core design requirement, not a trade-off. This means identity proofing, authentication, and fraud controls must be built to reduce unnecessary burden and improve completion rates for underserved users, while still maintaining strong security assurance.

Collectively, these themes point to a clear pattern. U.S. policy and standards define *what* security capabilities agencies must build, while performance frameworks describe *how* leaders should operate to achieve desired results. What is missing is a traceable link between these capability requirements and the service outcomes they are intended to produce. This gap motivates the analysis and conceptual framework that follows, where we outline the key constructs, their relationships, and the measurement connections between them.

4. GAP ANALYSIS: CONCEPTUAL AND POLICY MISALIGNMENTS

Management and Attribution Gap:

Current federal guidance is mature on both sides of the problem space. On the cybersecurity side, agencies are directed by Zero Trust, Secure-by-Design principles, systems security engineering, and the NIST CSF 2.0 Govern function. On the service-delivery side, they are guided by transaction-level and equity-focused customer experience requirements. However, agencies often plan and review these areas on different timelines, which means that the adoption of security controls is not consistently tied to measures of burden, satisfaction, trust, or resolution time (CISA, 2023; Souppaya et al., 2022; NIST, 2024; OMB, 2021).

Even though EO 14028, M-22-09, ZTMM v2.0, and cloud reference architectures specify what should be implemented and who is responsible, the full end-to-end attribution chain of policy, control, KPI, outcome, and leadership scorecard is still not clearly defined (House, 2021; Federal Register, 2021; Young, 2022; CISA, 2023; CISA et al., 2022; Lui et al., 2020). As a result, oversight bodies often view modernization activities as disconnected from demonstrable outcomes (GAO, 2025).

Implication: Agencies need a governance crosswalk that integrates Baldrige leadership and measurement principles with the CSF Govern function. This crosswalk would own the attribution path by requiring every capability initiative to declare its related service outcomes and the evidence trail that leads to executive review (Baldrige Performance Excellence Program, 2021; NIST, 2024; Baldrige Performance Excellence Program, 2019).

Measurement and Evidence Gap:

Cyber teams and service teams tend to track different types of indicators. Cyber teams focus on leading indicators such as Zero Trust pillar maturity, SSDF adoption, SBOM coverage, code-defect density, patch latency, and telemetry completeness. Service teams track lagging indicators such as uptime and SLO performance, user time and burden, satisfaction, trust, accessibility defects, and equity gaps (Young, 2022; Souppaya et al., 2022; CISA, 2023; CISA et al., 2022; OMB, 2021).

However, measurement theory indicates that indicators cannot drive improvement unless their construct validity is established and shared interpretation rules exist (Bailey, 2015). At present, few agency playbooks define analytic routines such as pre/post comparisons, interrupted time series, difference-in-differences, or mediation analysis to validate claims about how security improvements affect performance (NIST, 2024; CISA, 2023).

Implication: Agencies should identify paired indicators and standard analysis designs, such as control-adoption cohorts or difference-in-differences on CX measures, to help leadership interpret security capability signals in relation to service outcomes during regular reviews (Baldrige Performance Excellence Program, 2021).

Operating-Model and Incentives Gap:

Baldrige emphasizes combined leadership, measurement and learning and the BCEB offers a cyber self-assessment bridge (Baldrige Performance Excellence Program, 2021; Baldrige Performance Excellence Program, 2019; Schaefer, 2016). ZTMM v2.0 has uplifted Governance, which is visible and automated (CISA,

2023). However, control-compliance incentives, instead of reliability or burden reduction, are found in many agencies that do not have a consistent cadence between SSDF gateways, release/change procedures, and CX check points (Souppaya et al., 2022; GAO, 2025).

Implication: Introduce one quarterly capability and outcome indicator portfolio by service and streamline incentives such that security adoption becomes performance-related and not a liability (NIST, 2024; Baldrige Performance Excellence Program, 2021).

Supply-Chain Integration Gap:
SSDF and EO 14028 reinforce provenance, integrity and vulnerability response; cloud references provide a clear distinction of shared responsibility and guardrails (House, 2021; Federal Register, 2021; Souppaya et al., 2022; CISA et al., 2022; Lui et al., 2011). Nonetheless, vendor attestations, SBOM coverage, and defect trends are seldom turned into service-level risk indicators (e.g. estimated outage probability or time-of-completion impact). Monitoring connects third-party practices to a lack of modernization; the models of sectoral maturity demonstrate how to rank the risk of vendors (GAO, 2025; CISA, 2022).

Implication: Consider supply-chain artifacts first-class indicators with the crosswalk (capability side) and variables in reliability/CX models (outcome side).

Equity and Usability Gap:
The CX policy focuses on equity, access, and burden (OMB Circular, 2021; Young, 2023; Digital.gov, 2025; Marine, 2024). Studies caution that improperly done proofing and MFA will increase abandonment and trust loss; consumed security increases completion and satisfaction (Metin et al., 2024; Melaku, 2023). Anti-fraud and proofing patterns are not always intended to have distributional effect, however.

Implication: Bring equity to the openness of security design: gauge holes in completion, language/accessibility flaws, and redesign designs to reduce load without sacrifice in assurance (Panagiotopoulos et al., 2019).

Language and Semantics Gap:
The same constructs in terms of security, CX, and management communities have different terminologies (e.g., assurance as audit evidence vs. user confidence; reliability as SLO performance vs. resilience as mission continuity). Even though BCEB and CSF 2.0 aid in it, a common glossary/crosswalk is not typical practice (Baldrige Performance Excellence Program, 2019; NIST, 2024).
Implication: Operationalize definitions and map across framework to minimize interpretive drift in forums of governance.

Sealing the gaps will elucidate the agenda; (1) management and attribution, (2) measurement and evidence, (3) operating model and incentives, (4) supply-chain integration, (5) equity and usability, and (6) language and semantics. These are the design requirements the framework fulfills.

5. PROPOSED CONCEPTUAL FRAMEWORK

The framework conceptualizes cybersecurity capabilities as the cause of digital service performance with oversight and measurement in one logic of management. It aligns (i) U.S. cybersecurity policy and engineering guidance like Zero Trust, secure-by-design software, systems security engineering, cloud guardrails with (ii) performance excellence disciplines and CX/equity requirements (Young, 2022, 2023; CISA, 2023; Souppaya et al., 2022; Ross et al., 2022; CISA et al., 2022; NIST, 2024; OMB Circular, 2021; Baldrige Performance Excellence Program, 2019, 2021). Effectively, Governance & Strategy (GOV) implements Secure-by-Design Capabilities (SBD), these capabilities boost Service Operations and Reliability (OPS) and credibility of Assurance and Compliance (ASSUR), which together enhance Customer Experience and Equity (CXE) and downstream Outcomes (OUT), which are public trust, mission effectiveness, and efficiency (Panagiotopoulos et al., 2019).

Constructs:
Assurance (ASSUR) refers to the procedures and evidence demonstrating that controls and suppliers perform as intended. Examples include authorization and continuous ATO artifacts, audit and oversight results, SBOMs and signed attestations, vulnerability remediation evidence, and third-party risk monitoring. Confidence or perceived reliability is part of Customer Experience and Outcomes (CXE/OUT), not an element of ASSUR.

We define six constructs that together explain how cybersecurity becomes a driver of performance excellence in U.S. digital public services.

Governance and Strategy (GOV) capture leadership accountability, risk appetite, prioritization, portfolio decisions, and the crosswalk that links cybersecurity scorecards with performance scorecards. This construct is grounded in the CSF 2.0 Govern function and Baldrige leadership and measurement disciplines, which together provide executive ownership of outcomes (NIST, 2024; Baldrige Performance Excellence Program, 2019, 2021).

Secure-by-Design (SBD) capabilities include the maturity of identity, devices, networks, applications and workloads, and data, along with the cross-cutting practices of visibility and analytics, automation and orchestration, and governance. SBD is also supported by SSDF practices, software attestations and SBOMs, systems security engineering, and cloud guardrails with clear shared responsibility (CISA, 2023; Young, 2022; Souppaya et al., 2022; Ross et al., 2022; CISA et al., 2022; Lui et al., 2011).

Service Operations and Reliability (OPS) refer to the operational expression of SBD in production environments. It includes change and release discipline, SLO/SLA management, incident frequency and impact, mean time to recovery, and continuity or load resilience (CISA et al., 2022; GAO, 2025).

Assurance and Compliance (ASSUR) include activities that confirm trustworthiness and control posture of systems and suppliers. This encompasses authorization and continuous ATO packages, audit and oversight findings, third-party risk monitoring, and software provenance evidence such as SBOMs and signed attestations (House, 2021; Federal Register, 2021; Souppaya et al., 2022; GAO, 2025).

Customer Experience and Equity (CXE) capture user burden and effort, satisfaction, trust, accessibility, language support, and the speed of resolution at the transaction level, including distributional analysis across populations (OMB, 2021; Young, 2023; Digital.gov, 2025; Marine, 2024).
Outcomes (OUT) reflect institutional trust, mission effectiveness, and the underlying metrological discipline as perceived by the public (Panagiotopoulos et al., 2019; Bailey, 2015).

System Orientation
GOV provides the strategic orientation for the system. It establishes risk appetite, funds capability epics, and sets expectations for foundational practices such as Zero Trust, SSDF, and cloud guardrails. The Govern function of CSF 2.0 reinforces this role by linking cybersecurity management directly to organizational performance outcomes (NIST, 2024; Young, 2022; CISA, 2023; Souppaya et al., 2022; CISA et al., 2022).

Secure-by-Design and Operational Reliability
OPS is strengthened through Secure-by-Design (SBD) capabilities. These include mature identity assurance, segmentation, high-quality telemetry, code integrity, and automated response functions. Together, these reduce failure modes and shorten time-to-mitigation, resulting in more reliable services (Ross et al., 2022; Souppaya et al., 2022; CISA et al., 2022).

SBD also enables robust Assurance (ASSUR). SSDF artifacts, such as SBOMs, attestations, and software provenance evidence, provide credible inputs for authorization, auditing, and vendor oversight. Strong assurance supports timely vulnerability remediation and reinforces organizational confidence in taking and managing risk (House, 2021; Federal Register, 2021; Souppaya et al., 2022; GAO, 2025).

Reliability and Customer Experience

Improved OPS translates into better Customer Experience and Equity (CXE). Reduced incident frequency, faster recovery, and reliable scaling improve task completion rates, lower user burden, and increase satisfaction and trust (OMB, 2021; Young, 2023). ASSUR further supports CXE by reducing the likelihood and severity of supplier-driven failures and ensuring rapid notification and recovery during incidents (GAO, 2025; Souppaya et al., 2022).

CXE then feeds back into GOV. Measures such as burden, equity gaps, and perceived trust inform leadership prioritization and risk appetite. This feedback loop enables leadership to allocate resources where they create the greatest public impact (Baldrige Performance Excellence Program, 2021; OMB, 2021; Young, 2023).

Outcomes

CXE gains ultimately shape OUT, which reflects public trust, equitable access, and mission effectiveness. Service criticality (e.g., benefits disbursement vs. informational tasks) and population vulnerability (e.g., identity-proofing difficulty) moderate these pathways and inform where capabilities must be deeper or more rigorous (Panagiotopoulos et al., 2019; CISA et al., 2022; OMB, 2021; Marine, 2024).

Propositions

From this reasoning, we propose several falsifiable hypotheses for empirical testing:

P1: Capability - Reliability: Greater Zero Trust maturity and SSDF adoption are associated with reduced incident frequency and lower MTTR (Young, 2022; CISA, 2023; Souppaya et al., 2022).

P2: Reliability - Experience: Declines in incident rates and MTTR correspond to higher completion rates and reduced burden for users (OMB, 2021; Young, 2023).

P3: Assurance as Mediator: ASSUR mediates the positive effects of SBD on CXE. Higher SBOM/attestation coverage and telemetry completeness improve CXE by strengthening security provenance and failure response (Souppaya et al., 2022; GAO, 2025).

P4: Identity Burden Trade-Off: Usability-optimized identity assurance increases completion and trust. Poorly designed proofing or MFA reduces both (Metin et al., 2024; Melaku, 2023; Digital.gov, 2025).

P5: Governance Amplification**:** SBD and OPS effects are greater when governance cadence is strong, through rapid decision cycles, resource reallocation, and disciplined CSF Govern execution consistent with Baldrige leadership principles (NIST, 2024; Baldrige Performance Excellence Program, 2019, 2021).

P6: Supply-Chain Signal**:** Higher supplier attestation and SBOM coverage correlate with fewer dependency-driven outages and faster recovery, strengthening user and institutional trust (House, 2021; Federal Register, 2021; Souppaya et al., 2022).

Measurement Crosswalk

To treat cybersecurity as a driver of results, agencies must pair leading capability indicators with lagging service outcomes.

Capability Indicators: Zero Trust pillar maturity, Visibility/automation/governance maturity, SSDF adoption, SBOM/attestation coverage, Code defect rates, High-risk vulnerability age and patch latency, Telemetry completeness, and Cloud guardrail adherence (identity centralization, segmentation, key management, etc.) (Young, 2022; CISA, 2023; Souppaya et al., 2022; CISA et al., 2022).

Outcome Indicators: SLO achievement, Incident rates and MTTR at the transaction level, Throughput/load stability, CX metrics (burden, satisfaction, trust, resolution speed), Accessibility and language-support defects, and Equity measures: drop-off rates, device/network dependence (GAO, 2025; OMB, 2021; Young, 2023; Digital.gov, 2025; Marine, 2024)

Causal Pairings: Strong identity assurance (e.g., FIDO2, step-up) should predict higher first-attempt login success, lower drop-off, and lower time-to-complete.

SBOM/attestation coverage should predict fewer dependency-driven outages, faster time-to-patch, and stronger post-incident trust.

Telemetry completeness and automation should reduce MTTD and MTTR, stabilizing completion and satisfaction during incidents (Young, 2022; CISA, 2023; CISA et al., 2022).

Following metrology standards, the interpretation of indicators requires clear operational definitions, cohort rollouts, pre/post or quasi-experimental comparisons, and transparent uncertainty reporting (Bailey, 2015; Baldrige Performance Excellence Program, 2021).

Governance and Cadence

The management cadence integrates cybersecurity and service outcomes into a single rhythm of execution.
Executive leadership owns the policy-to-outcome crosswalk and associated risk appetite. Modernization epics must declare paired indicators linking capabilities to service results (NIST, 2024; Baldrige Performance Excellence Program, 2021). A single funded portfolio co-stewarded by the CIO, CISO, CDO, and CX lead drives predictable gains in both capability and user experience (Young, 2022; CISA, 2023; Souppaya et al., 2022; OMB, 2021).
Product owners report paired indicators using pre/post or cohort-based analyses. Assurance transforms SBOM/attestation data and incident records into decision-quality signals for leadership (CISA et al., 2022; Souppaya et al., 2022; GAO, 2025).
The cadence includes:
Annual strategy refresh: mapping EO 14028, M-22-09, and CSF Govern to capability epics with CX/equity targets.
Quarterly joint reviews: examining paired indicators by service and reallocating investments or vendor actions.
Monthly service councils: reviewing release impacts (identity proofing, automation, segmentation) with distributional equity checks (House, 2021; Federal Register, 2021; NIST, 2024).
The approach is operationalized through guardrails such as SSDF gates in CI/CD, no-regression rules for priority populations, contractual SBOM/attestation/telemetry requirements, and platform-level cloud guardrails that reduce variance (Souppaya et al., 2022; CISA et al., 2022; Lui et al., 2011).

Evaluation and Validation

The framework is evaluated based on coherence, completeness, and non-redundancy, its alignment with CSF Govern and federal CX/equity requirements, and its traceability to measurable outcomes (NIST, 2024; Baldrige Performance Excellence Program, 2021; OMB, 2021; GAO, 2025).
To support empirical testing, we outline analytic designs that agencies can apply to operational data:

1. Pre/post comparisons with cohort controls
2. Interrupted time series to detect level or slope changes in completion, burden, and reliability
3. Mediation analyses for SBD to (OPS/ASSUR) to CXE
4. Moderation analyses by service criticality and population vulnerability

(Bailey, 2015; CISA et al., 2022; Marine, 2024)
Evidence artifacts include a traceability register linking policy clauses to epics, indicators, and outcomes; assurance binders (SBOMs, attestations, CI/CD gates, vulnerability SLAs); CX/equity dossiers; cloud-guardrail adoption evidence; and periodic BCEB self-assessments to ensure cybersecurity remains embedded in enterprise excellence (Souppaya et al., 2022; CISA et al., 2022; OMB, 2021).

6. IMPLICATIONS (POLICY, MANAGERIAL, TECHNICAL)

Policy implications:

U.S. directives already define what should be practiced (ZT, SSDF, logging, supply-chain assurance) and what should be measured for CX and equity. The lever that is still lacking is a cohesive narrative on governance that considers capabilities of cybersecurity as vectors of service performance. CSF 2.0 - Govern is to be operationalized expressly as a policy bridge to Baldrige leadership/measurement and must mandate that all modernization epics announce a paired set of indicators: a capability measure and an outcome measure (NIST, 2024; Baldrige Performance Excellence Program, 2019, 2021). Only the Zero Trust plans which indicate their expected impact on measures burden, trust, satisfaction and resolution time should be approved, in addition to the accessibility/equity lenses (OMB Circular, 2021; Young, 2023).
Supply-chain evidence (SBOMs, attestations, signed builds) paperwork should also be raised by policy stewards to first-class performance signals that drive the reliability and CX expectations in line with Executive

Order 14028 requirements in terms of service-level risk forecasting (House, 2021; Federal Register, 2021; Souppaya et al., 2022; GAO, 2025). Lastly, cloud guardrails (identity centralization, segmentation, telemetry pipelines, key management) are supposed to sit as platform policy, an enterprise services that will decrease the per-program variation and minimize time-to-assurance (CISA et al., 2022; Lui et al., 2011).

Managerial implications:

The leaders are to convene a quarterly forum to examine modernization using paired indicators, rather than separate cyber/CX scorecards (Baldrige Performance Excellence Program, 2021; NIST, 2024). The portfolio of epics funding (identity, telemetry/automation, SSDF, cloud guardrails) should be co-owned by the CIO/CISO/CDO/CX "quadrad", which is not based on the maturity of the control alone but also on expected service gains (Young, 2022; Souppaya et al., 2022; CISA, 2023).

The incentives in the workforce should be based on rewarding defect prevention and quick recovery to achieve user outcomes. An example is recognition for teams that can lower the MTTR and at the same time lower transaction load (Ross et al., 2022; OMB Circular, 2021). Pre/post or cohort analyses for significant control changes, such as the introduction of phishing-resistant authentication, a new proofing flow, or automated containment, also need to be conducted by program managers, with distributional checks to monitor equity swirls (Bailey, 2015; Young, 2023).

To be oversight ready, keep a traceability register between policy clauses - controls - capability indicators - outcome indicators - observed effects; this directly solves the recurring issues with GAO regarding linking modernization to results (GAO, 2025). Periodically use BCEB to ensure that the enterprise excellence routine is incorporated with cyber performance (Baldrige Performance Excellence Program, 2019).

Technical implications:

Architects must implement the capability stack as platformed guardrails instead of modified service features. These include centralized identity planes with phishing-resistant elements and risk-based step-up, software integrity pipelines with signed compiles and SBOM, network categorization patterns, and normal accounted logging/telemetry with automation hooks (CISA et al., 2022; Souppaya et al., 2022; CISA, 2023). Such guardrails are required to expose quality of decision telemetry which can be attached to user journeys (login success, completion, time-to-resolve) and could read along effects causally in the leadership forum (Young, 2023; OMB Circular, 2021).

In engineering practice, operationalized SSDF gates in CI/CD (threat modeling, code signing, provenance checks, remedies against vulnerabilities SLAs) and treat attestation of the suppliers as a queryable data structure (e.g., a dependency risk score of a particular service, which predicts the probability of incident occurrence and restoration time) (Souppaya et al., 2022; GAO, 2025). Use systems security engineering to keep track of mission requirements to security properties throughout the life cycle so that security controls are provided as the source of reliability and equity, but not extensions (Ross et al., 2022).

Lastly, make identity proofing and MFA patterns more usability friendly. Consider ways to increase assurance with reduced burden for high priority groups. Track proofing failure, non-use of patterns, and drop-off, and redesign where necessary (Young, 2022; Digital.gov, 2025; Marine, 2024); Melaku, 2023; Metin et al., 2024). Bottom line is the "what" is guided by policy, the "how" by management and the "with what" by engineering. The combination of paired indicators in a single cadence (when joined) generates a controllable route between adoption of cybersecurity capabilities and achievable improvements in reliability, burden, equity, and trust by the public, meeting the performance excellence requirement and the federal cybersecurity agenda (NIST, 2024; Young, 2022; OMB Circular, 2021; Baldrige Performance Excellence Program, 2019).

7. LIMITATIONS AND BOUNDARY CONDITIONS

U.S.-centric scope: The framework is based on the U.S. policy/standards (EO 14028, M-22-09, CSF 2.0, A-11), which enhances the relevance in terms of federal application but reduces the generalization possibilities. To make obligations, capacities, and oversight regimes applicable to non-U.S. contexts, it will be necessary to adapt them (Young, 2022; NIST, 2024; OMB Circular, 2021).

Policy drift and version specificity: Guidance develops (e.g. CSF amendments, CX reporting amendments). The discoveries are related to the versions used in the paper, agencies should monitor the updates and re-base the crosswalk when the texts of authoritarians are updated (NIST, 2024; Young, 2023).

Theoretical (non-experimental) nature: It is a behind desk design science artifact. It hypothesizes processes and speculations but does not experiment on causality. The evaluation should be followed by the quasi-experimental designs and cohort rollouts with the agency data (Bailey, 2015; GAO, 2025).
Validity and interpretability of measurement: The pairing of indicators is based on construct validity, quality of data and disciplined interpretation. Paired metrics may incorrectly lead the management in the absence of accepted definitions and uncertainty notes (Baldrige Performance Excellence Program, 2021).
Information and communications limitations: Other agencies do not have end-to-end logging, SBOM coverage, or CX transaction data at the required granularity, which restricts the ability to trace capabilities to outcomes (CISA et al., 2022; Souppaya et al., 2022; GAO, 2025).
Old and federated environment: Decentralized portfolios and old systems may undermine the implementation of Zero Trust and slow down the use of SSDF, outcomes are predetermined by guardrails of platforms and the clarity of shared responsibility (Lui et al., 2011; CISA, 2023).
Supply-chain opacity: The attestation of vendors can also be partial or not standardized, which limits assurance as evidence of the quality of decision-making. The crosswalk requires contractual reimbursements and levels of oversight to operate (Souppaya et al., 2022; GAO, 2025; CISA, 2022).
Boundary of equity and usability: Security controls also have the disadvantage of increasing access burden. To prevent regressions, agencies will need to track the distributional impacts and re-design proofing/MFA designs (OMB Circular, 2021; Young, 2023; Melaku, 2023).
Applicability boundary: The framework focuses on transactional digital services, but identity, application logic, and telemetry can be influenced by agencies. A variant based on contracts and reduced form may be needed by informational sites or fully outsourced services (CISA et al., 2022; Baldrige Performance Excellence Program, 2019).

8. CONCLUSION

The paper develops a conceptual model of design science that combine cybersecurity and performance excellence within digital public services in the United States. Combining authoritative policy and engineering guidance with performance and public-value literatures, we define constructs which are, governance, secure-by-design capabilities, service operations, assurance, customer experience and equity, and outcomes and theorize causal pathways among constructs. One such contribution is a measurement crosswalk to align leading capability indicators (e.g., Zero Trust maturity, SSDF adoption, SBOM/attestations, telemetry completeness) with lagging service indicators (e.g., reliability, burden, satisfaction, trust, equity) so that leaders can manage the concept of security as a result driver as opposed to a side-by-side compliance initiative. We offer an operating cadence and evaluation plan that we use to implement it and prepare empirical testing. Weaknesses are that the study is based in the U.S. and is conceptual (non-empirical) in nature. Future research must confirm propositions with agency data, investigate distributional consequences of security patterns on priority groups, and improve crosswalk strategies and service situations and modernization stages.

REFERENCES:

1. Azmi, R., Tibben, W., & Win, K. T. (2018). Review of cybersecurity frameworks: context and shared concepts. *Journal of cyber policy*, *3*(2), 258-283.
2. Bailey, D. (2015). The metrology of organizational performance: How baldrige standards have become the common language for organizational excellence around the world. *Retrieved November*, *17*, 2015.
3. Baldrige Performance Excellence Program, (2019). BALDRIGE CYBERSECURITY EXCELLENCE BUILDER v1.1. Key questions for improving your organization's cybersecurity performance. https://www.nist.gov/system/files/documents/2019/03/24/baldrige-cybersecurity-excellence-builder-v1.1.pdf

4. Baldrige Performance Excellence Program, (2021). 2021–2022 Baldrige Performance Excellence Framework Criteria Commentary, https://www.nist.gov/system/files/documents/2020/12/14/2021-2022-criteria-commentary-bnp.pdf
5. Calvo-Manzano, J. A., San Feliu, T., Herranz, Á., Mariño, J., Fredlund, L. Å., & Moreno, A. M. (2025). CyberESP: An Integrated Cybersecurity Framework for SMEs. *Journal of Software: Evolution and Process*, *37*(9), e70050.
6. CISA, (April 2023) Zero Trust Maturity Model V 2.0. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf
7. CISA, (OCTOBER 2022) DAMS SECTOR CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2) Version 2.0, https://www.cisa.gov/sites/default/files/2023-01/dams-c2m2-2022-508.pdf
8. Cybersecurity and Infrastructure Security Agency (CISA), United States Digital Service (USDS), and Federal Risk and Authorization Management Program (FedRAMP), (2022). Cloud Security Technical Reference Architecture V.2 https://www.cisa.gov/sites/default/files/2023-02/cloud_security_technical_reference_architecture_2.pdf
9. Digital.gov., (2025). Requirements for delivering a digital-first public experience. Understand the policy framework: 21st Century Integrated Digital Experience Act and OMB Memo M-23-22 https://digital.gov/resources/delivering-digital-first-public-experience
10. Federal Register, ((2021). Improving the Nation's Cybersecurity. https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity
11. GAO, (May 2025). SPECTRUM IT MODERNIZATION NTIA Should Fully Incorporate Cybersecurity and Interoperability Practices, https://www.gao.gov/assets/gao-25-107509.pdf
12. Ghafoor, S., Mann, R. S., & Grigg, N. (2021). The strengths and opportunities for improvement of the Baldrige Performance Excellence Program. *Quality Management Journal*, *28*(3), 128-144.
13. House, W. (2021). Executive Order 14028, Improving the Nation's Cybersecurity. https://www.cisa.gov/topics/cybersecurity-best-practices/executive-order-improving-nations-cybersecurity
14. Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). NIST cloud computing reference architecture. *NIST special publication*, *500*(2011), 292.
15. Marine, J. (Sep 23, 2024), Delivering a digital-first public experience: One agency's plan, Learn how GSA is approaching the requirements in OMB memo M-23-22. https://digital.gov/2024/09/23/delivering-a-digital-first-public-experience-one-agencys-plan
16. Melaku, H. M. (2023). A dynamic and adaptive cybersecurity governance framework. *Journal of Cybersecurity and Privacy*, *3*(3), 327-350.
17. Metin, B., Özhan, F. G., & Wynn, M. (2024). Digitalisation and Cybersecurity: Towards an Operational Framework. *Electronics*, *13*(21), 4226.
18. NIST, (2024) The NIST Cybersecurity Framework (CSF) 2.0 https://doi.org/10.6028/NIST.CSWP.29
19. Nnadi, K. and Opoku, J. A. " Cybersecurity Curriculum Alignment with Industry Needs: A Literature Review of Educational Models Integrating Labs, Certifications, and Research." Sarcouncil Journal of Engineering and ComputerSciences 4.12 (2025): pp 64-76
20. Nnadi, K., Okrah, Y. A. & Opoku, J. A. "Cloud Security Posture Management in Resource-Constrained Organizations: A Review of Azure, AWS, and Hybrid Approaches." *Sarcouncil Journal of Applied Sciences* 6.1 (2026): pp 9-21.
21. Ogunsola, O., Adikorley, I. J. N., & Opoku, J. A. Mitigating Cognitive Load in Supply Chain Decision-Making: An AI-Driven Framework for Enhanced Operational Efficiency.
22. OMB Circular., No. A-11 (2021). SECTION 280 – MANAGING CUSTOMER EXPERIENCE AND IMPROVING SERVICE DELIVERY, https://www.performance.gov/cx/assets/files/a11_2021-FY22.pdf
23. Panagiotopoulos, P., Klievink, B., & Cordella, A. (2019). Public value creation in digital government. *Government Information Quarterly*, *36*(4), 101421.
24. Ross, R., Winstead, M., McEvilley, M. (November 2022). Engineering Trustworthy Secure Systems. NIST Special Publication 800-160v1r, https://doi.org/10.6028/NIST.SP.800-160v1r1

25. Schaefer, C. (October 2016), Improving Government Performance: The Great Promise of the Baldrige Excellence Framework , https://www.nist.gov/system/files/documents/2016/10/27/improving_government_performance_the_great_promise_of_the_baldrige_excellence_framework.pdf
26. Souppaya, M., Scarfone, K., & Dodson, D. (2022). Secure software development framework (ssdf) version 1.1. *NIST Special Publication*, *800*(218), 800-218
27. Young, S. D. (2022). Moving the US government toward zero trust cybersecurity principles. *Memorandum M-22-09*. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
28. Young, S. D. (2023). Delivering a Digital-First Public Experience. *Memorandum M-23-22*. https://www.whitehouse.gov/wp-content/uploads/2023/09/M-23-22-Delivering-a-Digital-First-Public-Experience.pdf