IBM Center for The Business of Government

2025

GOVERNMENT'S DIGITAL DNA

Identity and Access Management for Public Sector Security

Dr. Andrew B. Whitford
University of Georgia

IBM Center for The Business of Government

Government's Digital DNA: Identity and Access Management for Public Sector Security

Dr. Andrew B. Whitford
University of Georgia

NOVEMBER 2025

IBM Center for
The Business
of Government

TABLE OF CONTENTS

FOREWORD

In an era where digital transformation is reshaping the landscape of public administration, the importance of robust Identity and Access Management (IAM) systems cannot be overstated. As U.S. government agencies navigate an increasingly complex cybersecurity environment, the need to secure sensitive data, protect critical infrastructure, and maintain public trust has never been more pressing.

This IBM report, *Government's Digital DNA: Identity and Access Management for Public Sector Security*, authored by Professor Andrew B. Whitford of the University of Georgia, offers a timely and insightful exploration of how IAM serves more than ever as a cornerstone for effective governance in the face of evolving threats and technological advancements. The report assesses prior and current events impacting IAM in government, introduces new findings, and makes recommendations for adapting IAM in the context of emerging technologies like artificial intelligence and advanced analytics.

Professor Whitford's analysis underscores the critical role of IAM in aligning with federal mandates, such as the Federal Information Security Modernization Act (FISMA) and the principles of Zero Trust Architecture (ZTA). By emphasizing continuous verification, least privilege access, and real-time monitoring, IAM systems provide a vital defense against insider threats, sophisticated cyberattacks, and emerging risks like AI-enabled breaches and quantum computing vulnerabilities. The report also highlights the growing convergence of information technology and operational technology, which introduces new complexities for securing interconnected systems that underpin public services and critical infrastructure.

Through a detailed examination of six key challenges facing identity management in the public sector, this report not only identifies the hurdles but also proposes six actionable recommendations to guide the future of IAM. These insights are particularly valuable as agencies strive to balance security, compliance, and operational efficiency in a rapidly changing digital landscape. By addressing the integration of advanced technologies and the evolving nature of governance, Professor Whitford's work provides a forward-looking framework for policymakers, practitioners, and scholars alike.

The IBM Center for The Business of Government is proud to present this report as part of our commitment to advancing knowledge and practice in public administration. We believe it will serve as a critical resource for government leaders seeking to strengthen cybersecurity, enhance public trust, and navigate the complexities of modern governance.

Daniel J. Chenok
Executive Director
IBM Center for
The Business of
Government
chenokd@us.ibm.com

Alice Fakir
Vice President
Cybersecurity Services
Federal Lead, IBM
Alice.Fakir@ibm.com

EXECUTIVE SUMMARY

This report examines the critical role of Identity and Access Management (IAM) in safeguarding U.S. government systems, data, and infrastructure. Implemented effectively, IAM ensures that only authorized individuals access sensitive resources using principles of least privilege, aligned with federal mandates like the Federal Information Security Modernization Act (FISMA) and Zero Trust Architecture (ZTA).

By exploring emerging technologies and frameworks, this report aims to guide public sector leaders in strengthening identity, privacy, and security measures to protect national security, public trust, and operational integrity. The report provides actionable insights and recommendations to defend against evolving threats and enhance governance in an increasingly complex digital landscape.

Challenges

The report identifies six key challenges in implementing effective IAM systems in the public sector, ordered from operational to systemic:

1. **Heavy Reliance on Third-Party Vendors**: Government agencies depend on vendors for IAM provisioning, creating a complex ecosystem of corporate partnerships. While essential, this reliance introduces risks due to the growing role of external actors in managing critical systems.
2. **Cross-Functional Burdens of Identity Policy Review**: IAM policies require continuous, cross-functional review involving IT, legal, and business units, straining resources and demanding frequent updates akin to total quality improvement processes.
3. **Fragmentation of Identity Verification Systems**: The absence of a unified national identity system, coupled with decentralized initiatives like Real ID, complicates consistent identity verification across agencies.
4. **Balancing Privacy and Security in System Design**: Integrating privacy and security requires protecting sensitive data and addressing privacy-by-design approaches.
5. **Emergent Threat Vectors**: Quantum computing, AI-based intrusions, deepfakes, and IoT vulnerabilities expand the threat surface, undermining current cryptographic and verification methods.
6. **Operationalizing Zero Trust Architecture**: ZTA demands a cultural and operational shift to continuous verification, disrupting traditional workflows and clashing with informal organizational norms.

Recommendations

To address these challenges, the report proposes six recommendations, progressing from immediate operational improvements to long-term structural changes:

1. **Leverage Public-Private Partnerships**: Strengthen vendor and consortia collaborations to harness external expertise, particularly for cloud and AI-driven solutions.
2. **Institutionalize Identity Governance**: Establish enduring identity policies integrated with HR and compliance teams to ensure consistent, credible commitments to security.
3. **Adopt Hybrid IAM Architectures**: Implement systems combining centralized oversight with decentralized flexibility to meet diverse agency needs while maintaining policy coherence.
4. **Treat IAM as Foundational Secure Infrastructure**: View IAM as critical public infrastructure, akin to utilities, to prioritize its integration and resilience given implementation challenges.
5. **Prioritize Privacy-Enhancing Technologies**: Adopt privacy-by-design principles to balance security and user trust, addressing the gap between technical solutions and operational awareness.
6. **Develop Executive-Level Fluency in IAM and ZTA**: Understand identity ecosystems and Zero Trust principles to drive informed decision-making and compliance across agencies.

Conclusion

Effective IAM is essential for securing government operations in a digital era marked by complexity and uncertainty. By addressing these challenges and implementing the recommended strategies, agencies can strengthen security, ensure compliance, and build public trust. The report underscores successful IAM strategies must address inevitable tradeoffs, and anticipate and manage human behavior and incentives, to achieve resilient and adaptive governance.

The Need For New Identity Management Methods and Tools

Identity and Access Management is critical for U.S. government departments and agencies because it ensures that only authorized individuals can access sensitive systems, data, and resources, thereby safeguarding national security, public trust, and operational integrity.

IAM systems establish robust mechanisms to authenticate user identities, enforce least privilege access, and monitor activities to prevent unauthorized access or data breaches. In a government context, where agencies handle classified information, citizen data, and critical infrastructure, proper IAM implementation mitigates risks from insider threats, cyberattacks, and human error.

For example, IAM aligns with federal mandates like the Federal Information Security Modernization Act (FISMA) and Zero Trust Architecture, requiring strong identity verification, multifactor authentication, and continuous monitoring. By implementing IAM, agencies can protect sensitive information, ensure compliance with regulations, streamline secure access for employees and contractors, and maintain accountability, all of which are vital for effective governance and public safety.

The increasing demand for enhanced IAM systems in government stems from fundamental shifts in how public organizations secure sensitive data and manage access to critical systems. IAM systems serve as essential frameworks for ensuring that access to resources is appropriately granted but requires that they be continuously monitored. These systems typically include tools such as multifactor authentication, centralized identity repositories, and role-based access controls, all of which are designed to address the growing complexities of cybersecurity in public governance.

The move toward zero trust architectures (ZTA) reflects a broader transformation in cybersecurity policy, where verification is ongoing rather than episodic. This shift places IAM systems at the center of efforts to comply with federal mandates and protect against evolving threats. ZTA is discussed further in the next section as a means of managing threats to identity in the broader cybersecurity ecosystem.

At the same time, changes in security paradigms—including heightened risks from insider threats and increasingly sophisticated external attacks—underscore the inadequacy of perimeter-focused approaches. Further complicating these challenges are emerging technological threats, such as AI-enabled breaches, quantum computing risks, and vulnerabilities arising from interconnected networks. Together, these developments demand that governments address key tradeoffs of risk and opportunity, and develop IAM solutions that are not only adaptive but also scalable.

Appendix 1 discusses various frameworks through which IAM is typically organized.

The Demand for Identity: Individual, Organizational, and Societal

The place of identity in modern life can be seen through three lenses: the individual, the organizational, and the social.[1] In a nutshell, it is impossible to think about identity as an "information processing system" without fully considering all three levels.[2]

Helping People Improve their Lives

- **Improving Employment Outcomes:** New employees provide proof of identity when starting jobs. In some cases, this happens for the purposes of background checks. In most cases, it establishes their eligibility to work. In the broader context, it allows for the creation and continuation of official employment records (e.g., worker's compensation). For instance, this includes the U.S. Citizenship and Immigration Services (USCIS) Employment Eligibility Verification process to certify a person is eligible to work in the U.S.[3]
- **Enhancing Economic Opportunities:** In the U.S., people must verify their identity when utilizing various financial services, such as when opening bank accounts, applying for loans or mortgages, establishing investment accounts, or purchasing insurance. Identity verification and authentication is especially important in the case of large transactions; for instance, financial regulations like Know Your Customer (KYC) (and overseers like the U.S. Department of the Treasury's Financial Crimes Enforcement Network)[4] play key roles in preventing fraud, money laundering, tax evasion, and the financing of terrorism.
- **Ensuring Access to Public Benefits:** Eligible individuals who want to receive Social Security benefits must prove their identity. The Social Security Administration has rigorous verification processes to try to ensure the provision of benefits to the rightful beneficiaries—an important task given the rise over time in identity theft and fraudulent claims.[5] Such processes require the provision of varieties of documents such as birth certificates, drivers' licenses, passports, naturalization documents, proof of name changes, and SSNs.

Helping Organizational Missions

- **Mitigating Risk in National and Public Safety:** Public agencies face the ever-present challenge of securing the nation against a host of threats, ranging from cyberattacks to terrorism. In adopting robust identity and access management systems, agencies manage access to sensitive resources, thereby reducing the probability of catastrophic breaches. This strategy reflects a calculated effort to avoid "regret scenarios," where the cost of inaction or insufficient controls would far outweigh the investments required for preventive measures.
- **Reducing Vulnerabilities in Public Service Delivery:** The effective delivery of public goods is central to government legitimacy, yet inefficiencies and fraud remain persistent risks. By deploying IAM technologies, agencies streamline authentication and authorization processes, ensuring that resources reach the correct beneficiaries. This approach minimizes the regret tied to system inefficiencies, misallocations, and the erosion of trust that results from perceived failures in service provision.

1. These lenses are akin to the classic micro-meso-macro distinction. Blalock, Hubert M. 1981. *Social Statistics*. Revised Edition. McGraw-Hill Series in Sociology. New York: McGraw-Hill.
2. Marr, David. 1982. *Vision: A Computational Investigation into the Human Representation and Processing of Visual Information*. Henry Holt.
3. The USCIS Form I-9 is located at: https://www.uscis.gov/sites/default/files/document/forms/i-9.pdf.
4. For more information on such rules, see: https://www.fincen.gov/resources/statutes-and-regulations/cdd-final-rule.
5. Anderson, Keith B, Erik Durbin, and Michael A Salinger. 2008. "Identity Theft." *Journal of Economic Perspectives* 22 (2): 171–92. https://doi.org/10.1257/jep.22.2.171.

- **Protecting Sensitive Data and Avoiding Regulatory Risks:** Agencies are stewards of vast repositories of sensitive information, ranging from classified intelligence to citizen records. The implementation of IAM systems provides a proactive framework for safeguarding this information, while also ensuring compliance with regulatory mandates. The minimization of regret, in this case, arises from preempting the financial, reputational, and political costs that accompany breaches or compliance failures.
- **Preventing Coordination Failures in Interagency Collaboration:** Effective interagency collaboration is often central to addressing complex policy problems, such as disaster response or national security. However, without adequate safeguards, such coordination can exacerbate risks, particularly when sensitive information is shared. IAM systems reduce these risks by providing secure, federated identity management frameworks, ensuring that collaborative efforts proceed without exposing agencies to the vulnerabilities of information mismanagement. In this sense, regret is minimized by anticipating and preventing operational breakdowns.
- **Enhancing Accountability to Preclude Organizational Failures:** Public organizations are held to high standards of accountability, yet they frequently grapple with the risks of mismanagement, misuse of authority, or corruption. IAM systems address these challenges by ensuring transparency through audit trails and access logs. This mitigates the risk of undetected malfeasance, reducing the likelihood of regret stemming from failures in oversight or governance.
- **Guarding Against Technological Obsolescence and Emerging Threats:** As government agencies continue their transition into the digital age, the risks associated with technological obsolescence and emerging threats, such as AI-based attacks, become more pronounced. IAM systems enable scalability and adaptability, ensuring that agencies remain resilient in the face of these challenges. This commitment to proactive risk management minimizes regret by safeguarding agencies against the vulnerabilities that accompany stagnation or technological lag.

Making Societies Resilient

- **Enforcing Laws and Securing the Nation:** Applications in both national security and law enforcement include biometric technologies such as fingerprints, facial recognitions, and iris scanning. It also includes digital databases for cross-referencing personal information, including genetic information. Increasingly, advanced surveillance systems vendors such as Flock Safety have expanded capabilities for identifying individuals via license plate recognition or other visual recognition technologies.[6]
- **Facilitating Fair Elections and Ensuring Participation:** Election integrity depends on the use of various methods or technologies for identity verification and authentication, including photo IDs, fingerprint scanners, and signature matching techniques. Voting systems also require identity management techniques to ensure the sanctity of the vote, including digital certificates, multifactor authentication, and blockchain-based solutions.[7]

6. See https://www.flocksafety.com/resources/license-plate-reader-cameras-overview.
7. Fidler, David P. 2017. *Transforming Election Cybersecurity*. Council on Foreign Relations. http://www.jstor.org/stable/resrep29928. Aniche, Chijioke, Chika Yinka-Banjo, Precious Ohalete, and Sanjay Misra. 2021. "Biometric E-Voting System for Cybersecurity." In *Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons or Opportunities*, edited by Sanjay Misra and Amit Kumar Tyagi, vol. 972. Studies in Computational Intelligence. Springer International Publishing. https://doi.org/10.1007/978-3-030-72236-4_5. Abba, Abdullahi Lawal, Mohammed Awad, Zakaria Al-Qudah, and Abdul Halim Jallad. 2017. "Security Analysis of Current Voting Systems." 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA), November, 1–6. https://doi.org/10.1109/ICECTA.2017.8252006.

- **Changing how Personal Information is Authenticated and Managed:** As digital identity systems become the cornerstone of personal identification, effective implementation depends on building systems that genuinely serve user needs while maintaining robust protections against misuse and public trust through transparency and accountability measures.

Threats to Identity: Now and Future

For the U.S. National Institute of Standards and Technology (NIST), "threat actors" can be defined as "The instigators of risks with the capability to do harm."[89] An enhanced definition is "threat actors are groups or individuals who, with malicious intent, aim to exploit weaknesses in an information system or exploit its operators to gain unauthorized access to or otherwise affect victims' data, devices, systems, and networks, including the authenticity of the information that flows to and from them"[10]

Regardless of level (individual, organizational, or social), the point is that someone wants to disrupt the identity verification and authentication system for reasons inconsistent with the purposes of the system and those who benefit from it.

Consider the following threats that all such systems now face and must account for in their design and operation:

Cyberattacks and Data Breaches—For NIST, a cyberattack is "Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself."[11] Better identity verification systems help reduce vulnerability to cyberattacks.[12] However, such attacks and the data breaches they facilitate make personal data vulnerable, leading to identity theft and fraud—and thus further fragilities in the cybersecurity ecosystem. This includes advanced persistent threats (APTs) that bypass authentication mechanisms or capture authentication credentials.[13]

More Zero-Day Exploits—Each new system or technology response brings the likelihood of new (undiscovered) zero-day fragilities.[14]

Biometric Data Theft and Spoofing—Even if biometric data (fingerprints, facial recognition) are used for identity verification, the compromise of such information brings unique risks. Such data cannot be changed, and while they are generally secure, the rise of deepfakes and other technologies can lead to facial recognition spoofing, fingerprint duplication, or voice imitation.[15]

8. Coley Felt and Will LaRivee, Exploring the Global Digital ID Landscape: Clear Leaders, Varied Paths, and Steps to Realize Their Potential (Washington, D.C.: GeoTech Center, The Atlantic Council, 2025), p.2.
9. This is a standardized definition from Johnson, Christopher S., Mark Lee Badger, David A. Waltermire, Julie Snyder, and Clem Skorupka. 2016. *Guide to Cyber Threat Information Sharing*. NIST SP 800-150. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-150. See also https://csrc.nist.gov/glossary/term/threat_actor.
10. *An Introduction to the Cyber Threat Environment*. 2022. Communications Security Establishment = Centre de la sécurité des telecommunications.
11. This is a standardized definition from McCarthy, James, Ya-Shian (Orcid)0000-0003-3234-4345 Li-Baboud, Joseph Brule, and Karri Meldorf. 2023. Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services. NIST IR 8323r1. National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.IR.8323r1. See also https://csrc.nist.gov/glossary/term/cyber_attack.
12. Garbis, Jason, and Jerry W. Chapman. 2021. *Zero Trust Security: An Enterprise Guide*. Apress.
13. U.S. Cybersecurity & Infrastructure Security Agency. 2021. Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations. Alert CodeAA20-352A. U.S. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a.
14. Dempsey, Kelley, Nedim Goren, Paul Eavy, and George Moore. 2018. Automation Support for Security Control Assessments: Software Asset Management. NIST IR 8011-3. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8011-3.
15. Mitra, Sinjini, and Mikhail Gofman, eds. 2017. *Biometrics in a Data Driven World: Trends, Technologies, and Challenges*. Taylor & Francis, a CRC title, part of the Taylor & Francis imprint, a member of the Taylor & Francis Group, the academic division of T & F Informa, plc.

These are common current threats to any system that relies on strong identity verification and authentication. In addition, two less-discussed threats demonstrate the technological aspects of such systems.

Advanced Forgery—Over time, technology has made it much easier to create credentials, documents, or other forms of identification that can pass traditional verification checks. Part of this is mechanical: printers and sophisticated software are now accessible. Perhaps more importantly, those seeking to breach the system now can access a multitude of personal data online.[16]

Man-in-the-middle (MITM) Attacks—The interception of communications between the authentication system and the user can allow access to sensitive data. Even more advanced forms of authentication are potentially vulnerable. A notable example is the redirection of data (Internet traffic) from one country to another.[17]

These are all made more difficult to mitigate by important technological changes to the threat surface such as the continuing rise of the Internet of Things (IoT) and the evolving integration of mobile devices. There are probably at least 15 billion IOT devices in the world now, and the number could double by 2030. Each new device increases the interconnectedness of the IoT ecosystem, bringing new vulnerabilities. Each new device contains a range of personal identity data (e.g., a home router, a TV sound bar), with potential risk to our identity systems.[18] For example, mobile devices now play a central role in identity verification and authentication. Yet, their security can be less than adequate.[19]

Future Threats to Identity—While some of these threats may seem futuristic or technologically advanced, the world keeps moving. It is worthwhile to list a few of the potential threats on the horizon noted by researchers and other policy analysts. All identity verification and authentication systems must be built to anticipate future threats as well as mitigate current ones.

16. Vaudenay, Serge. 2007. "E-Passport Threats." *IEEE Security & Privacy Magazine* 5 (6): 61–64. https://doi.org/10.1109/MSP.2007.164.
17. See https://www.theregister.com/2013/11/22/net_traffic_redirection_attacks/.
18. Choo, Kim-Kwang Raymond, Keke Gai, Luca Chiaraviglio, and Qing Yang. 2021. "A Multidisciplinary Approach to Internet of Things (IoT) Cybersecurity and Risk Management." *Computers & Security* 102 (March): 102136. https://doi.org/10.1016/j.cose.2020.102136.
19. Gontovnikas, Martin. 2021. "The 9 Most Common Security Threats to Mobile Devices in 2021." Auth0 by Okta Blog, June 25. https://auth0.com/blog/the-9-most-common-security-threats-to-mobile-devices-in-2021/.

Three key future challenges can be addressed by making risk management trade-offs:

- **Artificial intelligence:** AI can make deepfakes and other biometric spoofing more convincing, and can also make social engineering more effective through personalization. It may expand the reach of malware and other software exploits by democratizing coding. Machine learning algorithms can be trained to probe systems for vulnerabilities.[20] Governments can look to implement responsible AI frameworks as one means of addressing such risks.
- **Threats to new solutions like blockchain:** Even if governments enhance identity verification and authentication through the use of new strategies such as decentralized identity (using the blockchain), those solutions may face unique threats such as attacks on their underlying (protocol-level) infrastructure.[21] Building secure infrastructure can help governments to mitigate these threats.
- **Quantum computing:** Developments in quantum computing threaten current cryptographic standards. The breach of encryption algorithms would place all identity verification and authentication systems at risk,[22] making post-quantum cryptography a key tool for governments to address.

Managing Threats to Identity Within the Broader Cybersecurity Ecosystem

In one specific way, IAM has risen to the forefront of daily operations in all organizations; these systems are core components of all modern cybersecurity efforts. They help facilitate the move toward broader cybersecurity goals in multiple ways:

- Through the prevention of unauthorized access
- Through the verification of users and other entities with the systems (including programs, machines, or other devices)
- By helping meet goals of compliance with broader laws, regulations, and directives
- Through managing processes of remote access or system access outside of traditional conceptualizations
- By enabling dynamic (if not real-time) access control, perhaps by detecting an emerging risk profile

20. Kaur, Ramanpreet, Dušan Gabrijelčič, and Tomaž Klobučar. 2023. "Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions." *Information Fusion* 97 (September): 101804. https://doi.org/10.1016/j.inffus.2023.101804.
21. Yi, Xiao, Daoyuan Wu, Lingxiao Jiang, Yuzhou Fang, Kehuan Zhang, and Wei Zhang. 2022. "An Empirical Study of Blockchain System Vulnerabilities: Modules, Types, and Patterns." *Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, November 7, 709–21. https://doi.org/10.1145/3540250.3549105.
22. Hossain Faruk, Md Jobair, Sharaban Tahora, Masrura Tasnim, Hossain Shahriar, and Nazmus Sakib. 2022. "A Review of Quantum Cybersecurity: Threats, Risks and Opportunities." 2022 1st International Conference on AI in Cybersecurity *(ICAIC)*, May 24, 1–8. https://doi.org/10.1109/ICAIC53980.2022.9896970.

For many years, traditional approaches to cybersecurity have started (and perhaps, ended) with the assumption that things *inside* the organization (e.g., inside its network) are trustworthy. This meant that the primary focus was on external threats—an approach that over time was invalidated due at least partly to growing experience with insider threats and advanced persistent threats (APTs).[23]

Zero Trust Architecture (ZTA) provides a different way of thinking about cybersecurity: it builds on the principle of "never trust, always verify to address tradeoffs made necessary to secure key government systems." Because no one and nothing are ever deemed trustworthy, ZTA requires verification from everyone and anything trying to access system resources (e.g., programs, machines, data, buildings) regardless of what gates they have passed through to get to where they are currently. Every access point and every access request must be verified.

DEFINING ZERO TRUST ARCHITECTURE

Zero Trust Architecture (ZTA) is a cybersecurity framework that assumes no inherent trust within or outside an organization's network, requiring continuous verification of all users, devices, and systems before granting access to resources. Unlike traditional perimeter-based security models, ZTA operates on the principle of "never trust, always verify," emphasizing rigorous identity authentication, least privilege access, and real-time monitoring. Core components include multifactor authentication (MFA), micro-segmentation to limit lateral movement, and comprehensive logging to detect and respond to threats.

ZTA is enabled by advanced technologies like encryption, behavioral analytics, and policy enforcement to ensure secure access to data and systems, regardless of location or device. In the context of U.S. government agencies, ZTA aligns with federal mandates, such as Executive Order 14028, to enhance cybersecurity resilience against sophisticated cyber threats, protecting sensitive data and critical infrastructure by minimizing implicit trust and enforcing strict access controls.

From a broader perspective, this makes ZTA a different cybersecurity paradigm because it changes the fundamental model or approach that shapes understanding and practice. It turns the standard model inside-out and requires a new mindset.

Because ZTA builds on an evolving understanding of cybersecurity and changes the overall model to understanding threats, it is more than just a set of tools or technologies. Just like IAM is more than an information technology solution built on passwords and keycards, so does ZTA require the participation of many different constituencies in the organization. Quoting a key report in the current efforts to expand ZTA:

23. Garbis, Jason, and Jerry W. Chapman. 2021. *Zero Trust Security: An Enterprise Guide*. Apress. Finney, George. 2022. *Project Zero Trust*. John Wiley and Sons. Pillai, Binil, and Abbas Kudrati. 2022. *Zero Trust Journey Across the Digital Estate*. First edition. CRC Press. Gilman, Evan, and Doug Barth. 2017. *Zero Trust Networks: Building Secure Systems in Untrusted Networks*. First edition. O'Reilly Media. Haber, Morey J., and Darran Rolls. 2020. *Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution*. Apress L.P.

> *Identity, authentication, and authorization are critical to making resource allocation decisions. Given that making and enforcing access decisions are the two main responsibilities of a ZTA, the organization will want to use its existing or a new ICAM solution as a foundational building block of its initial ZTA implementation.*[24]

The identity verification and authentication problems begin and end with the lack of easily implementable technologies and processes for answering three questions: Who am I? What do others know about me? Am I secure? These different lenses—at the individual level, inside the organization, and in the broader security context—reveal why and how the identity problem pervades so many work problems and situations.

This means that governments face substantial tradeoffs. Effectively, organizations cannot trust (in the canonical sense) anyone or anything without sufficient proof. Regardless, organizations must get things done, so they invent new processes (fueled by new technologies) to help fill the "trust gap." Those inventions then must satisfy the interests and live within the capabilities of the people who must work with them daily.

While this report centers on the identity problem, broadly conceived, the problems of finding IAM systems that support security initiatives like ZTA are important enough to warrant special emphasis. For that reason, the next section turns into four themes defining IAM's evolution and future promise.

24. Borchert, Oliver, Gema Howell, Alper Kerman, Scott Rose, Murugiah P Souppaya, and others. 2023. Implementing a Zero Trust Architecture. Volume B. Approach, Architecture, and Security Characteristics. 3rd Preliminary Draft. NIST Special Publication 1800-35B. Implementing a Zero Trust Architecture NIST SP 1800-35 Practice Guide. National Institute of Standards and Technology National Cybersecurity Center of Excellence. https://www.nccoe.nist.gov/publications/practice-guide/implementing-zero-trust-architecture-nist-sp-1800-35-practice-guide-1.

Four Current Trends In Identity And Access Management Themes

The last section of this report introduced three lenses through which we can look at the identity problem: at the individual level, at the organizational level, and the social level, all of which must be managed within the security realm.

This section highlights four current themes that help frame where things stand in the context of how governments are handling the identity question, especially given the rise of IAM systems and the ZTA security paradigm. These trends provide further context for the challenges and recommendations that follow in the next section:

- Centralized and decentralized forces
- Governance across multiple agencies
- The changing space of third-party actors
- The shifting technology landscape

Each theme helps to situate how government is experiencing a whirlwind of directives, obligations, and considerations in reaching for higher operational outcomes. These kinds of disruptive changes come in two parts:[25] innovation itself and change to the organization's competitive landscape. Governments should look at organizational "response strategies" (what competitors are doing) and "performance trajectories" (how they are moving over time), making appropriate tradeoffs among complex choices.

Centralized and Decentralized Forces

Consider two ways that government agencies might implement (or "actuate") IAM systems. In the first, a top-down (centralized) system is put in place: *command-and-control to the rescue!* In the second, a bottom-up (decentralized) system is implemented: *empowerment!*

Implementing any government program is always a tug-of-war between these competing forces.[26] Yet, for IAM systems, this tension between centralized and decentralized forces is more than just two different ways to make new program come alive—it is a tightrope that managers must navigate as IAM systems and the ZTA paradigm reshape the internal and external lives of agencies.

On one hand, centralized IAM systems give managers a single control point for verifying and authenticating user identities and access across the agency. For managers, this single control point simplifies the core aspects of the job: enforcing policies, managing user accounts (called "provisioning"), and auditing. On the other hand, those same organizations are moving toward new ways of enabling their workforces given new patterns of work and work requirements. Agencies routinely adopt cloud-based services (SaaS) and remote work models. Decentralized IAM distributes identity management across systems and platforms. The benefits are flexibility, scalability, and tailored access control given changing conditions in a fluid digital landscape.

25. Christensen, Clayton M., Rory McDonald, Elizabeth J. Altman, and Jonathan E. Palmer. 2018. "Disruptive Innovation: An Intellectual History and Directions for Future Research." *Journal of Management Studies* 55 (7): 1043–78. https://doi.org/10.1111/joms.12349.
26. O'Toole, L. J. 2000. "Research on Policy Implementation: Assessment and Prospects." *Journal of Public Administration Research and Theory* 10 (2): 263–88. https://doi.org/10.1093/oxfordjournals.jpart.a024270.

Strongly decentralized systems are often called "self-sovereign identity" systems.[27] While the strongest forms appear infrequently inside government settings, the winds of change are bearing in that direction. As digital identity expert and author Phillip Windley notes:

> *While people often talk about decentralization as an unalloyed good and the answer to every ill, the truth is that decentralization is just an implementation strategy. The goals of Web3 include self-sovereignty (autonomy and independence) and censorship resistance. Decentralization is a good way to achieve these things, but I can imagine decentralized services (in the technical sense) that don't achieve either of these. It's ok to use "decentralization" as shorthand for these goals, but recognize the goals, not the implementation technique.*[28]

This tension between centralization and decentralization is truly seen when IAM intersects with ZTA. ZTA requires central oversight to enforce "never trust, always verify"—this is foundational in the ZTA paradigm. Yet, the goals of ZTA can be facilitated when agencies use decentralized methods in diverse and dynamic workforce environments. Decentralization brings the power of granular access control; increasingly, it enables awareness of multiple access points for users and devices within discreet locations, as well as adaptive verification and authentication. On the other hand, decentralization can also introduce more bureaucratic processes and opportunities for human error.

In general, the authentication architecture question comes down to three basic choices: policy-based architectures (with centralized evaluation and enforcement), token-based architectures (which gives a measure of decentralization to the process of requesting and being granted access),[29] and something in between (a hybrid path). Again, the right path is a matter of choice given the context that often involves multiple data users, devices, locations, and points of entry for government systems.

This is the tradeoff: centralization and decentralization each have benefits and costs. In the end, a hybrid model can build both elements into IAM systems and ZTA platforms given the agency's specific security and operational needs. The answer may not be one or the other—it may involve both.

27. Windley, Phillip J. 2023. *Learning Digital Identity: Design, Deploy, and Manage Identity Architectures*. First edition. O'Reilly Media, Inc.
28. Windley, Phillip J. 2023. *Learning Digital Identity: Design, Deploy, and Manage Identity Architectures*. First edition. O'Reilly Media, Inc. P. 339.
29. Oauth is a widely discussed and utilized authorization – and can be used for authentication when paired with the Open ID Connect standard authentication protocol.

Governance Across Multiple Agencies

All agencies, firms, and other organizations trying to choose and implement the right IAM system or ZTA platform face problems of technical coordination. These involve answering questions like the following:

- Which solution works best for us now? In the future?
- What do we need to know to find that solution?
- How should our technical workforce be trained?
- How should our users (or clients or stakeholders) be enabled to navigate this solution?
- Who is a trusted partner for implementing this solution?
- What standards must we live up to?

Just as there are centralizing and decentralizing forces in play, so too do those types of forces affect the implementation of identity strategies. This section reviews several centralizing forces in terms of key organizational actors. NIST is the foundational actor in this space for developing standards; CISA supports the implementation of those standards. In the case of multiple executive orders, identity verification and authentication became more important to the everyday operations of all federal agencies, governed by key players including those listed in the Box below.

Key Agencies Addressing Identity and Access Management in the U.S. government

NIST—Social scientists have long tried to understand the roles of standards-setting organizations (SSOs) in helping solve problems of technical coordination.[30] Sometimes those SSOs are international, such as the International Organization for Standardization (ISO), the Institute of Electrical and Electronics Engineers (IEEE), or the World Wide Web Consortium (W3C). Others play key domestic roles, including the American National Standards Institute (ANSI) or the Telecommunications Industry Association (TIA).

The most important one for U.S. purposes, though, is the U.S. National Institute of Standards and Technology (NIST). For over a century, NIST has played core roles in research and development (including foundational research in the cryptographic underpinnings of all modern IAM systems), collaboration with academia and industry (including spurring changes in industry that feed back to affect agencies through the vendors they contract with), and (most importantly) standards development that are vital for technology development, deployment, and interoperability.[31] Within NIST, the National Cybersecurity Center of Excellence is a focal point for much policy development.[32]

30. Simcoe, Timothy. 2014. "Governing the Anticommons: Institutional Design for Standard-Setting Organizations." *Innovation Policy and the Economy* 14 (January): 99–128. https://doi.org/10.1086/674022.
31. Logar, Nathaniel. 2009. "Towards a Culture of Application: Science and Decision Making at the National Institute of Standards & Technology." *Minerva* 47 (4): 345–66. Schooley, James F. 2000. *Responding to National Needs: The National Bureau of Standards Becomes the National Institute of Standards and Technology, 1969-1993.* U.S. Department of Commerce.
32. See https://www.nccoe.nist.gov.

Key Agencies Addressing Identity and Access Management in the U.S. government (cont.)

CISA—The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) plays a distinctly different role. Effectively, CISA focuses on many practical and operational aspects in the context of both IAM systems and broader cybersecurity initiatives (including infrastructure resilience).

CISA provides tools, alerts, and resources to many organizations (rather than the foundational guidelines that NIST offers), especially in critical infrastructure sectors, where advanced persistent threats are a key focus. CISA offers a range of types of services ranging from survey capabilities to visualization tools to tabletop exercises,[33] along with maintaining a central repository for guidance about implementing ZTA for federal agencies,[34] and has extended guidance about the integration of mobile devices into such implementations.[35]

Together CISA and NIST are key actors in the IAM and ZTA space. What agencies are doing now and what they are expected to do in the future will depend on NIST and CISA guidance. Both are important, and their collaborative efforts define and elaborate how IAM systems are focal points in cybersecurity.

Other Key Actors—Implementing IAM systems and ZTA calls for enhanced cybersecurity capabilities through the adoption of a ZTA strategy. Moreover, federal government organizations were required to implement (or at least, determine how to implement) ZTA in a timely fashion. It made ZTA a major pillar, reflecting a move away from perimeter-based defense.

A host of other directives or guidance from the Office of Management and Budget, the General Services Administration, and other core support agencies help complete the picture of how the landscape has changed for the everyday lives of managers in all federal agencies. The centralizing impacts of these directives, via the daily work of NIST and CISA, show the importance of such factors for overcoming natural information and coordination challenges.

33. See https://www.cisa.gov/resources-tools, https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages, and https://www.cisa.gov/resources-tools/services/cisa-vulnerability-scanning.
34. See https://zerotrust.cyber.gov/.
35. See https://www.cisa.gov/sites/default/files/2023-01/Zero_Trust_Principles_Enterprise_Mobility_For_Public_Comment_508C.pdf.

The Changing Space of Third-Party Actors

Because recent policy drives the adoption and implementation of ZTA, and because ZTA depends on IAM systems, IAM has become foundational to the work of all federal agencies. Because it is foundational, federal managers are brought into technical spheres that are often unfamiliar and daunting. This section focuses on the changing space of third-party actors—namely, corporate vendors and suppliers.

Two feedback loops change how the federal government is taking on the IAM and ZTA challenges. First, private sector organizations around the world are also undergoing the changes called for by NIST and others; Gartner estimates that the worldwide IAM market will grow from $15.61 billion in 2021 to $31.99 billion in 2027.[36] Those firms also use vendors, so vendors are central players in the broader social move toward stronger controls for identity verification and authentication. Second, those same actors help drive the best practices that agencies must live up to when implementing IAM systems or ZTA platforms.

Effectively, NIST and other standards organizations work in collaboration with vendors. They utilize that experience and expertise to ensure proposals are technically sound and applicable. This helps NIST expand the relevance and application of its guidance. These experiences are effectively public-private partnerships. This is sensible as a two-way street: vendors work both sides of the aisle (public and private), and NIST's guidance sets the standard for everyone in the community. Accordingly, vendors play a unique and fundamental "lynchpin role" in broader IAM and ZTA conversations. Vendor participation is a feature, not a bug.

The Shifting Technology Landscape

In general, much of what managers are currently experiencing in terms of new mandates and requirements has been driven by recent technological changes, such as:

- **The availability of cloud-based solutions:** While government agencies have been moving core operations to the cloud for almost two decades,[37] cloud-based IAM solutions are relatively new. This includes verification and authentication services for on-premises resources and users, and the ability to offer those services for users using cloud/SaaS based services. Increasingly, cloud-based solutions grant agencies the ability to scale and manage access in a flexible way that cannot be offered easily with on-premises solutions.[38]
- **Multifactor authentication (MFA):** IAM practices now regularly require some version of MFA rooted in the core principles of knowledge, inherence, or possession. Consider the latter two: both require sophisticated technological solutions that have long necessitated substantial work to ensure they are authentic and secure.[39] This is only more complicated in the case of security token-based possession verification and authentication.

36. Archambault, Rebecca, Henrique Teixeira, Brian Guthrie, David Collinson, and Nathan Harris. 2023. Market Guide for Identity Governance and Administration. ID G00775672. Gartner. https://www.gartner.com.
37. Wyld, David C. 2009. *Moving to the Cloud: An Introduction to Cloud Computing in Government*. E-Government Series. IBM Center for The Business of Government. https://www.businessofgovernment.org/sites/default/files/CloudComputingReport.pdf.
38. Eryurek, Evren, Uri Gilad, Valliappa Lakshmanan, Anita Kibunguchy-Grant, and Jessi Ashdown. 2021. *Data Governance: A Definitive Guide.* O'Reilly Media, Inc.
39. Romine, Charles H. 2013. "Standards for Biometric Technologies." Testimony before the Subcommittee on Government Operations, Committee on Oversight and Government Reform, U.S. United States House of Representatives. Washington, D.C., June 9. https://www.nist.gov/speech-testimony/standards-biometric-technologies. Romine, Charles H. 2022. *Personal Identity Verification (PIV) of Federal Employees and Contractors*. NIST FIPS 201-3. National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.FIPS.201-3.

- **Artificial intelligence and machine learning:** Increasingly, systems use versions of AI and machine learning in their IAM systems for enhanced security of systems. For instance, adaptive MFA can create real-time risk scores for each authentication experience, requiring more and different steps based on that context-based score.[40] Also, AI and ML can be used for real-time threat detection and automated response based on patterns in user behavior patterns inside systems.[41] User entity and behavior analytics (UEBA) are already here, although they may not be very evenly distributed (a la William Gibson).
- **Zero Trust network access (ZTNA):** Inside the ZTA paradigm, one technological focus is on user-to-server security (often referred to as ZTNA), which requires technological innovations to secure identity verification regardless of location or network in use.[42]
- **Micro-segmentation:** In contrast, micro-segmentation (often referred to as Zero Trust Network Segmentation, or ZTNS) often centers on server-to-server security. By dividing networks into small and distinct zones to limit lateral movement, this aspect of ZTA requires multiple layers of access controls—each with its own technological requirements.[43]

These five broad examples show how much has changed in IAM systems since the beginning when a simple username and password were the "keys to the kingdom." Indeed, in 2014, Osmanoglu argued that the previous decade had seen unprecedented increases in the threat environment that had made IAM a fundamental part of all organization's plans for the coming decade.[44] Arguably, the following decade has seen the same expansion—not just in threat environment, mostly through expansion of every agency's "attack surface,"[45] but also in changes to how organizations can mitigate those threats. The five examples above show the changes in the day-to-day life of organizations.

Much of the most advanced research on IAM and ZTA focuses now on decentralized identity models: the idea is to give users more control over their identity data, reducing reliance on centralized authorities, often rooted in technologies, such as the blockchain. Appendix 2 focuses on these four versions of decentralized identity because in some ways they may be the most disruptive for how we think about who we are, what others know about ourselves, and whether that information is secure.

The broader context of IAM is defined by the tension between centralization and decentralization, the arbitration of new standards for performance by NIST and others, and the changing landscape of third-party actors (mostly vendors) who bridge the different implementation environments of government and the private sector. Within this broader context, managers increasingly face new and significant technological challenges often driven by evolution in cyber threat space, new expectation for business practices, and rapidly changing technology. These structural changes are reshaping how government organizations approach identity verification and authentication, and also the overall cybersecurity paradigm.

40. Syed, Naeem Firdous, Syed W. Shah, Arash Shaghaghi, Adnan Anwar, Zubair Baig, and Robin Doss. 2022. "Zero Trust Architecture (ZTA): A Comprehensive Survey." *IEEE Access* 10: 57143–79. https://doi.org/10.1109/ACCESS.2022.3174679.
41. Bécue, Adrien, Isabel Praça, and João Gama. 2021. "Artificial Intelligence, Cyber-Threats and Industry 4.0: Challenges and Opportunities." *Artificial Intelligence Review* 54 (5): 3849–86. https://doi.org/10.1007/s10462-020-09942-2.
42. Garbis, Jason, and Jerry W. Chapman. 2021. *Zero Trust Security: An Enterprise Guide*. Apress.
43. Garbis, Jason, and Jerry W. Chapman. 2021. *Zero Trust Security: An Enterprise Guide*. Apress.
44. Osmanoglu, T. Ertem. 2014. *Identity and Access Management: Business Performance through Connected Intelligence*. Syngress.
45. Haber, Morey J., and Darran Rolls. 2020. *Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution*. Apress L.P.

Six Challenges for Identity In The Public Sector

In light of the discussion above and the history and context as outlined in the Appendix, six important challenges face governance in an age of threats to identity. Discussed in the following order—from lower strategic magnitude to highest consequence—the public sector is increasingly asked to support decision-making (by both political actors and career civil servants) under the twin conditions of complexity and uncertainty. These challenges start with "operational" (or at least localized) burdens, and end with system-level threats that carry the broadest implications for national governance and public trust.

CHALLENGE 1: Government's heavy reliance on third-party vendors for IAM provisioning

As argued above, corporate vendors are now pivotal actors within these systems. Vendors offer ranges of consulting services, whether those vendors be full-service teams from well-known large corporations or consultancies or small tactical teams that specialize in the most difficult cybersecurity threats. Those teams are fundamental for bridging the different implementation environments of government and the private sector. This is the changing space of third-party actors.

Yet, while this heavy reliance on third-party vendors for these ranges of services is a fundamental challenge, vendor participation is a feature, not a bug, in these policy arenas. As with contracting out more generally, the tension between "making" and "buying" is fundamental for all organizations, yet IAM and its requirements and risks is a somewhat unique space. The most important aspect of this challenge is that this reliance is not going away; indeed, with recent changes to the public sector and its workforce, government reliance on these vendors is only increasing.

CHALLENGE 2: The cross-functional governance burdens of identity policy review

IAM is built on identity policies—not just technological layers. These rules packages are policies in the most canonical sense. They determine the "who gets what, when, and where" of information flows and decision-making authority. As with Laswell's original formulation, policy review distributes highly valued things (status and security), across individuals and groups, across time (affecting dynamic decisions, and thus requiring updates), and across spaces (both geographic and digital).

Consequently, policy review has been, remains, and will continue to be a cross-functional effort. Policy review is more than just the domain of information technology—it builds on the expertise and involvement of legal teams and business units, many of whom have little time or interest in adjudicating the security concerns of large and complex organizations. These dynamics means that routine review must happen annually, biannually, or even more frequently. Essentially, policy review is like total quality improvement (TQI)—it has become a continuous process—and like TQI it challenges every level of the organization to get almost everything right at every point in time.

CHALLENGE 3: The persistent fragmentation and lack of architecture to guide identity verification systems

As noted earlier, the U.S. lacks a single comprehensive national identity verification system. Unlike many other countries, proposals for a national identity system have been largely rebuffed. While Real ID and initiatives to change the conditions under which voters are eligible to participate in federal elections represent attempts to unify access requirements, those attempts are largely limited to special conditions and thus do not broadly solve the overall problems represented in the IAM process.

For instance, witness recent debates about changes to identity proofing in the context of access to Social Security benefits. While the long-run effects of those changes are unknown, and likely to remain unknown for years, the debates about those changes and the speed at which aspects of the original proposals changes reflect this persistent fragmentation of identity verification systems in the U.S. Those rifts are unlikely to be reconciled in meaningful ways soon.

CHALLENGE 4: The difficulty of addressing privacy and security in system design to build a resilient public infrastructure

It is important to recognize the overall difficulty of including both privacy and security in the design of complex systems—whether they be narrowly for traditional information technology purposes or more generally the allocation of resources and services to citizens. One set of information that used to determine and protect security is the same as the set of information that politicians and the populace secure.

While many see this is a design and implementation problem, as evidenced by the move toward "privacy by design" approaches that embed privacy into the underlying architecture of the system, such moves often just replace one conundrum with another. Even if governments protect information within the system by masking such things from the eyes of observers, such moves may make it difficult to assess the veracity of the information being accessed for information or decision-making purposes. If information is a strategic resource, the tendency will be to make privacy subservient to what some may consider higher-order goals.

CHALLENGE 5: The speed and breadth of emergent threat vectors like quantum computing, AI-based intrusions, and IoT vulnerabilities

As suggested throughout the report, these challenges threaten many if not all aspects of current IAM systems. On one hand, developments in quantum computing threaten current cryptographic standards. At the same time, facial recognition spoofing and the rise of deepfakes mean that even visual identity verification is fraught with uncertainty. The continuing rise of IoT means that the threat surface is expanding exponentially. Finally, AI may expand the reach of malware and probe systems for vulnerabilities.

While it is important to recognize that emerging technologies have long been a concern in regulatory spaces, the nature of these changes is unprecedented. Their combination represents the greatest aspect of this challenge. Alone one emerging technology would be a source of concern; together they reinforce and reciprocate in terms of the direction and magnitude of threat assessment. Cutting off one vector just means many other vectors will emerge in its place.

CHALLENGE 6: Operationalizing Zero Trust Architecture

Even more broadly, Zero Trust as a solution is meant to change the fundamental model or approach. ZTA is an attempt to turn the standard model inside-out: from the ring fence to the inside of the castle. As such, ZTA requires a fundamentally new security mindset.

Yet, ZTA is more than just a security mindset: it is a broader transformation in organizational operations rooted in cybersecurity policy. Because verification is ongoing rather than episodic, those who require verification face frictions that fundamentally disrupt (and not always in a good way) what they do on a day-to-day basis. Moreover, this includes not only workers but also devices or even agentic AI needing ongoing verification.

While it is tempting to believe that humans are at the root of the problem—that workers simply cannot be bothered to reenter security tokens repeatedly in MFA environments—this view misses the broader point: ZTA cannot replace the norms and folkways that have evolved in all public sector operations as lubricants that allow workers to get things done. The formal structures of organizations (that now live in identity policies) are likely to run aground on the substantial shoals of the informal organization that define how people get the work done.

Six Recommendations

As with the challenges above, these six recommendations outline where things might go next, given how these threats to identity implicate the evolution of governance in the public sector.

These recommendations generally follow the challenges, and include actions that can give decision-makers near-term operational leverage as well as those that will require the kinds of deeper structural commitments in a world of uncertainty and change.

RECOMMENDATION 1: Agencies should leverage public-private consortia and vendor partnerships.

NIST and other players make this clear: these changes are effectively public-private partnerships. Whether government is developing standards or guidance, much of what is important happens outside agencies, so agencies much look outward to achieve their goals with respect to such initiatives. Regardless of preferences or the tenor of the times, vendors have played and will continue to play a unique and fundamental "lynchpin role."

Some aspects of where things are going will help in this regard, such as the growing reliance on SAAS or cloud services for achieving public goals. It is unlikely that most agencies will develop and deploy their own agentic AI solutions; they will depend on the many thousands of AI researchers working outside the government to help them make what they need to solve their problems.

Yet, such moves face substantial headwinds, especially in changing preferences about the roles of universities and other nonprofit actors in oversight or advisory committees, the difficulty of contracting or grants making in uncertain times, or the need for expertise within agencies to oversee such activities. Some are concerned about generational losses in such changes—that it will take decades to rebuild what we had.

RECOMMENDATION 2: Leaders should institutionalize identity governance functions.

One of the most difficult problems for any leader is to institutionalize changes that fundamentally alter the rules of the game. These "credible commitments" make it clear that what is changing will persist if there is a change in political tides. Similarly, because IAM systems require continuous updating of policies, those identity policies must be integrated with human resources processes, policy review, and compliance in ways that will persist over time.

For instance, the rules for who can access what data under what conditions are themselves credible commitments. Without those commitments, it is easy to see how actors might decide differently about what decisions have a clear and strong evidentiary basis. If data access changes on a whim, and if actors then gain the ability to change data in ways that can affect decisions, how should future decision-makers think about the data they are using? And why would they not demand the same ability as those previous actors?

The institutionalization of identity governance functions as "credible commitment" reflects why commitments can be so powerful but also why they can be so rare—they are the foundation for commitments to broader values like trust, resiliency, and principled agility.

RECOMMENDATION 3: Agencies will move toward the adoption of hybrid IAM architectures.

Federal agencies will continue to move toward hybrid IAM architectures because they are practical: they help balance the demands from some for centralized oversight with the operational realities of decentralized governance. Agencies will look for ways to "have their cake and eat it too" with the adoption of both centralized and decentralized elements in their IAM systems.

It is important to recognize that this is not just convenient, but probably structurally necessary. Agencies are already broadly adopting remote location models, cloud applications, and third-party services. As such, the days are long past where everything is co-located. Yet, ZTA requires centralized identity verification and access decisions; ZTA serves the needs for policy coherence and centralized oversight.

Consequently, the answer is not necessarily one or the other—it may be both. Hybrid models build both centralized and decentralized elements into IAM systems. Agencies navigate this tension by treating decentralization as a gain, not a design flaw; decentralization is an implementation strategy.

It is inevitable, though, that mistakes will be made. Decentralization and centralization are never fully reconciled. They just live in a state of healthy tension.

RECOMMENDATION 4: Leaders and those they lead must treat IAM as secure foundational public infrastructure.

This is the hardest push for organizations living with day-to-day challenges to just get the work done. IAM is now at the beginning, middle, and end of the vast exercise of running large, complex organizations. As such, leaders and their followers must see it as foundational public infrastructure, akin to providing running water and electricity for their workers and those they serve. In a different era, those public services were seen as luxury goods, perhaps even cosmetic. It took decades for services like running water and electricity to diffuse across the population.

Perhaps agencies should expect no less for the spread of principled IAM systems to make their ways through the systems they deploy in the service of the public interest. However, given the threat surface it is almost guaranteed that that such changes may take years—for successful implementation to ensure that bad things do not happen to good people. That calculus also implies that more than one mistake will be made, and that consequently agencies will be called to account for the how's and why's of those mistakes.

Treating IAM as foundational public infrastructure does not mean mistakes will not happen. Such changes just help agencies minimize risk.

RECOMMENDATION 5: Leaders should prioritize privacy-enhancing technologies and privacy-by-design principles.

Throughout this report, one continuing theme has been the move toward expanded attention to privacy-enhancing technologies that help IAM systems attain both privacy and security. Computer scientists and technologists agree that such adoptions help IT professionals help protect their systems from threats that break down trust and user willingness to participate.

It is remarkable that while the technical community is working so hard to make it possible to achieve these goals, and that they are doing so because the higher-order principles of these changes are so widely agreed-upon, operations leaders are broadly unaware of why such changes are necessary and good. In some ways, technologists are more aware of the normative value of such changes than are the users themselves.

As with Recommendation 1, this prioritization may build from a basis of fluency: users knowing more about the stakes will help grease the wheels of change. There is a long history of users being willing to give up privacy for ease of use (or narratives about ease of use). This means that fluency may not be enough.

RECOMMENDATION 6: Leaders should seek to develop executive-level fluency in identity ecosystems and Zero Trust principles.

Executive orders, NIST standards, and CISA guidance can help build a foundation for this kind of fluency. In addition, IAM and ZTA will require the participation of many constituencies—perhaps everyone in the organization—so nontechnical managers throughout agencies are now being drawn into these systems through mandates and compliance.

Fluency throughout agencies is lacking. Few operations-level leaders truly understand what is going on, so the lack of broad attention to (and confusion about) these changes is understandable. Peter Drucker and others have long indicated that the clarity of organizational communications is paramount in any effort at broad organizational change. Clarity is lacking here.

CONCLUSION

These recommendations and challenges reinforce a central theme of identity and access management in government: tradeoffs matter. Making good policy is rarely about finding the best solution to a problem. Usually, it is about understanding how people (in government, or the public) will react to that solution. This research broadly centers on how public agencies, composed of people who all have their own goals, can become more than just the sum of their parts in implementing successful IAM strategies.

If people watch what others are doing and change their behavior based on those expectations, any IAM policy will create new incentives; people will change how they act, but it is not easy to predict how they will change. Those incentives may help the IAM policy work well, or they may create problems.

The real challenge is to find the right balance. Good IAM policies help people work together and work better. Great IAM policies also plan for when people do not follow the rules perfectly. The best policies do not ignore tradeoffs—they expect them and then manage them.

APPENDICES

Appendix 1—Different Systems to Structure Identity

This appendix reviews the status of identity verification and authentication across three different levels—from the broadest to the most specific—in terms of how researchers and practitioners view its purposes and utility. The main message here is that each layer depends on the previous one—that foundational choices matter in important ways for how organizations operate in society.

Common ID Systems in the U.S.

First, the U.S. has made specific choices about the operation and implementation of identification systems. Those choices show how the U.S. has struggled to balance two goals: making the systems operate efficiently and preserving important individual liberties such as privacy and autonomy. This tension between administrative benefits and individual costs has put the U.S. on a unique path compared to many other industrialized democracies.

As noted in the first section, the most notable forms of identification commonly used in the U.S. remain the Social Security Number (SSN) and state-issued driver's licenses/identity cards. The former is the de facto national identifier due to its uniqueness, permanence, and broad utility. The latter also serves as a standard form of identification. Passports are only necessary if a U.S. citizen chooses to travel outside the country. In 2023, about 47 percent of the U.S. population owns a valid passport,[46] compared to about 97 percent having an SSN.[47]

Unlike other countries, the U.S. lacks a single comprehensive national identity verification system (a national ID card). This is probably due to concerns about privacy,[48] the U.S. federal structure's emphasis on state autonomy,[49] and opposition from various groups.[50] As such, proposals for a national identity system have been largely rebuffed.

The most dramatic step toward such a system is the Real ID Act of 2005, which standardized state-issued IDs to enhanced (federal) security standards. Its purpose was to create a trustworthy identity verification system that allowed for security benefits, mostly in the contexts of air travel or entering federal buildings. Real ID does bring multiple benefits, and it is a major step forward in terms of making security more uniform. As author Magdalena Krajewska notes:

46. See https://travel.state.gov/content/travel/en/about-us/reports-and-statistics.html.
47. See https://www.ssa.gov/policy/docs/population-profiles/never-beneficiaries.html.
48. American Civil Liberties Union. 2002. National Identification Cards: Why Does the ACLU Oppose a National I.D. System? American Civil Liberties Union. https://www.aclu.org/documents/national-identification-cards-why-does-aclu-oppose-national-id-system. Electronic Privacy Information Center. 2007. DEPARTMENT OF HOMELAND SECURITY DOCKET NO. DHS 2006-0030. Notice of Proposed Rulemaking: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes. COMMENTS OF: ELECTRONIC PRIVACY INFORMATION CENTER (EPIC). Electronic Privacy Information Center. https://archive.epic.org/privacy/id_cards/epic_realid_comments.pdf.
49. Krajewska, Magdalena. 2020. "Implementing the REAL ID Act: Intergovernmental Conflict and Cooperation in Homeland Security Policy." *Publius: The Journal of Federalism* 50 (3): 398–422. https://doi.org/10.1093/publius/pjaa010.
50. Moore, Stephen. 1997. National Identification System. Cato Institute. https://www.cato.org/testimony/national-identification-system.

> *These eighteen benchmarks are primarily concerned with security standards. They include a mandatory facial image capture and retention, and requirements for documentation of date of birth, SSN, address, and lawful status. The standards also include improvements in the security of the license-issuing process, such as conducting name- and fingerprint-based criminal history and employment eligibility checks on all covered DMV employees.*[51]

Real ID remains deficient in important ways, however. First, Real ID has decentralized issuance given the role of the states and localities in determining the quality of documentation necessary for receipt of such identities. Second, Real ID is voluntary participation: nobody is forced to receive this documentation for any (necessary) purpose. Moreover, as Krajewska notes, advanced forms of identity verification and authentication (e.g., biometrics) are largely missing:

> *Real ID does not create a federal database. Notably, Real ID does not require or even suggest the use of radio frequency identification chips. In fact, Real ID also does not require sophisticated biometric technology; it requires only that all applicants for Real ID-compliant documents be subject to digital facial image capture. A digital facial image can be used in biometric matching only when it is subjected to facial recognition analysis.*[52]

In contrast, institutions like the World Bank and the World Economic Forum use digital identity systems to improve social welfare around the world. The World Bank's Identification for Development (ID4D) initiative emphasizes digital IDs for enhancing service delivery and administrative efficiency.[53] It focuses on the developing world due to widespread use of mobile devices.[54] Consequently, the World Bank developed a framework for creating inclusive and trusted digital identification systems that centers on universal coverage, robust and secure design, and building trust by focusing on privacy and the rights of users.[55] The ID4D initiative is being implemented in over 50 countries.

The World Economic Forum launched its Platform for Good Digital Identity project in 2018 to bring together existing and new digital identity solutions in a three-year project with over 100 coalition partners.[56] The focus was on meeting the needs of diverse groups by providing safe and trustworthy identity systems. Notably, WEF argues that because "ID strategies will vary across jurisdictions, use cases, cultures and more . . . that there is no 'one-size-fits-all set of recommendations' but instead a strong case for decentralized identity methods over the more

51. Krajewska, Magdalena. 2020. "Implementing the REAL ID Act: Intergovernmental Conflict and Cooperation in Homeland Security Policy." *Publius: The Journal of Federalism* 50 (3): 398–422. https://doi.org/10.1093/publius/pjaa010, p. 403.
52. P. 402.
53. See https://id4d.worldbank.org.
54. Silver, Laura, Aaron Smith, Courtney Johnson, Jingjing Jiang, Monica Anderson, and Lee Rainie. 2019. *Mobile Connectivity in Emerging Economies*. Pew Research Center. https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/03/PI_2019.03.07_Mobile-Connectivity_FINAL.pdf.
55. See https://id4d.worldbank.org/guide/1-principles.
56. See https://www.weforum.org/press/2018/09/world-economic-forum-launches-shared-platform-for-good-digital-identity/.

common models used throughout the world."[57] This comparison highlights the complexity in establishing a single, authoritative, universal source of identity for verification and authentication. Individuals, organizations, and societies may need and demand identity systems, but the varieties of use cases and contexts complicate the provision of such systems.

Establishing methods of verification and authentication provide real and continuing benefits—but variance often seems at odds with the overall goals and efficient operation of such systems. This is for good reason. As Maple, et al. emphasize, privacy and security exist in a state of tension in such systems.[58] On one hand, engineering solutions tend to focus on security. On the other, privacy is often demanded by users (and sometimes, beneficiaries) of such systems. In a nutshell, the same information that we often use to determine and protect security is the same information that many want us to secure.

"Privacy by Design" Approaches

Privacy is one reason that designers have moved more towards "privacy by design" approaches, embedding privacy into the underlying system architecture. In a canonical sense, privacy-by-design centers on seven principles to guide that architecture:[59]

1. Proactive not reactive; preventative not remedial
2. Privacy as the default setting
3. Privacy embedded into design
4. Full functionality—positive-sum, not zero-sum
5. End-to-end security—full lifecycle protection
6. Visibility and transparency—keep it open
7. Respect for user privacy—keep it user-centric

Focusing on the tone rather than the mechanics of these goals, one can see the focus on design principles that make privacy the central aspect. Of course, these are laudable goals, although perhaps difficult to always achieve in practice.[60] Yet, there has been expanded attention to privacy-enhancing technologies that help these systems attain both privacy and security.[61]

57. World Economic Forum. 2023. *Reimagining Digital ID*. World Economic Forum. https://www3.weforum.org/docs/WEF_Reimagining_Digital_ID_2023.pdf.
58. Maple, Carsten, Gregory Epiphaniou, and Mirko Bottarelli. 2021. "Trustworthy Digital Infrastructure for Identity Systems: Why Should Privacy Matter to Security Engineers?" *Computer Fraud & Security* 2021 (6): 6–11. https://doi.org/10.1016/S1361-3723(21)00063-4.
59. Cavoukian, Ann. 2010. "Privacy by Design: The Definitive Workshop. A Foreword by Ann Cavoukian, Ph.D." *Identity in the Information Society* 3 (2): 247–51. https://doi.org/10.1007/s12394-010-0062-y.
60. Koops, Bert-Jaap, and Ronald Leenes. 2014. "Privacy Regulation Cannot Be Hardcoded. A Critical Comment on the 'Privacy by Design' Provision in Data-Protection Law." *International Review of Law, Computers & Technology* 28 (2): 159–71.
61. Heurix, Johannes, Peter Zimmermann, Thomas Neubauer, and Stefan Fenz. 2015. "A Taxonomy for Privacy Enhancing Technologies." *Computers & Security* 53 (September): 1–17. https://doi.org/10.1016/j.cose.2015.05.002.

In sum, the search continues for ways to answer the three fundamental questions—Who am I? What do others know about me? Am I secure? However, this effort runs into two basic constraints:

- Is the technology secure, reliable, and sustainable?
- Will users accept the chosen balance between security and privacy?

The next section explores how governments are solving this problem in the narrow sense: through the design and implementation of identity and access management systems.

Identity Verification and Authentication

All organizations (e.g., public agencies, firms) require robust systems for identity verification and authentication (IVA). Agencies have compelling reasons to build robust systems—but they work in environments where decentralization, privacy, and security concerns have hampered easy solutions. The following highlights how robust IVA systems are critical for helping organizations meet key corporate and technical goals.

Key Organizational Goals

Supported by a Robust IVA System

Organizations still suffer when they lack robust systems because those systems help them attain other key corporate goals, such as:

1. **Operational efficiency and cost savings:** Organizations want their employees, users, or other stakeholders to have timely access to the tools and information they need for their work or contributions. Robust systems streamline provisioning and deprovisioning, thus reducing costs and increasing productivity.[62]

2. **User experience, management, and productivity:** Because organizations want those users to have seamless and secure access to different assets, applications, or services, their identity verification and authentication systems determine how users contribute to or even diminish broader goals like security and privacy. Below, I describe how capabilities like Single Sign-On (SSO) make the user experience more convenient.[63]

3. **Remote work management and security:** With the rise of remote work and work from home, organizations now must verify identity when providing access for a workforce that can be located anywhere.[64]

62. Johnson, Mick. 2020. What Is Provisioning and Deprovisioning? Okta. https://www.okta.com/blog/2020/07/what-is-provisioning-and-deprovisioning/.
63. Windley, Phillip J. 2023. *Learning Digital Identity: Design, Deploy, and Manage Identity Architectures*. First edition. O'Reilly Media, Inc.
64. Souppaya, Murugiah P, and Karen A Scarfone. 2016. Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. NIST SP 800-46r2. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-46r2.

Important Technical Goals

Supported by a Robust IVA System

Perhaps less recognized but equally important, organizations need robust identity systems to achieve important technical goals:

1. **Audits, monitoring, and reporting:** Organizations need robust systems that provide comprehensive audit trails and reporting capabilities so they can answer questions like "who accessed what resources and when."[65]

2. **Fraud detection and prevention, especially by insiders:** One core principle of modern security methods is that insiders, once they have access to a system, may represent the biggest threat.[66] Organizations want to detect and prevent those fraudulent activities.

3. **Compliance with regulations:** Most firms face regulatory requirements, especially concerning data protection and privacy, that require assurance of sufficiently robust identity systems. Of course, public agencies also need to comply with national directives and guidance (e.g., executive orders)[67] but also operate within other contexts with rigorous limitations (e.g., the California Consumer Privacy Act).

Narrow Identity and Access Management

Most organizations use Identity and Access Management[68] systems for managing digital identities and access rights. While descriptions vary, IAM systems are often described in terms of seven core laws/principles:[69]

1. **User consent:** Digital identity systems should only reveal information identifying a user with the user's consent.
2. **Limited disclosure:** The system should disclose only the minimal amount of identifying information; the information should be limited to a specific purpose and time.
3. **Fewest (justifiable) parties:** Any identifying information should be passed only to those who need to know it for completing the transaction.
4. **Directional/directed identity:** Systems should provide identities or personas for each context, avoiding universal identifiers.

65. Stouffer, Keith. 2023. Guide to Operational Technology (OT) Security. NIST SP 800-82r3. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r3.
66. Garbis, Jason, and Jerry W. Chapman. 2021. *Zero Trust Security: An Enterprise Guide*. Apress.
67. See https://www.fpc.gov/elements-of-federal-privacy-program/breach-response/.
68. IAM systems are often referred to as IdAM (Identity and Access Management) or ICAM (Identity, Credential, and Access Management). These are often used interchangeably.
69. Cameron, Kim. 2005. "The Laws of Identity." Kim Cameron's Identity Weblog, May 13. https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf. Hovav, Anat, and Ron Berger. 2009. "Tutorial: Identity Management Systems and Secured Access Control." *Communications of the Association for Information Systems* 25. https://doi.org/10.17705/1CAIS.02542.

5. **Pluralism of operators and technologies:** Do not assume a universal identity or a single expression of identity; assume multiple identity providers and technologies.
6. **Human integration:** The user is part of distributed system and should be integrated into the system's processes.
7. **Consistent experience across contexts:** Users should experience the same experience a across multiple contexts and operators in a digital identity system.

While many principles have been offered to describe how to best design and operate an IAM system, Cameron's laws are a good starting place for considering how the systems have changed over time—and where they are headed.

As IAM systems process users (or devices or entities playing "roles") and their requests, they walk through steps meant to secure the system and its data, protect privacy rights in the system, and attain principles like those above. In a nutshell, IAM systems:

1. **Identify** the user.
2. **Authenticate** the user (using one or multiple methods, such as passwords, biometric data, smart cards, security tokens, RFIDs, etc.). This is often called "AuthN."
3. **Authorize** the user's access to resources or data, and what things they can do with those resources or data. These are determined by predefined aspects that are unique to the users and the requests they might make. They are determined by policies, roles, or other attributes. This is often called "AuthZ."
4. **Administer** the policies that underly the AuthN and AuthZ processes. This includes the management of users and roles, and deciding the policies that determine what resources and data can be accessed, utilized, or changed.
5. **Audit** all aspects of these processes, not just for compliance purposes but also to ensure that current and future security and privacy goals are met.

IAM systems have grown over time as we learn more about existing and emerging threats. Organizations of all sizes—with diverse users and many applications—face greater complexity. Enhanced regulatory compliance requirements have brought new complexities for system designers. New understandings of what we need in terms of authentication has made our systems more complete. Many systems face different dynamic claims on their resources. Of course, IAM systems face substantial integration challenges, both with other legacy systems and also with the multiplicity of new services (e.g., SaaS) and devices/entities (e.g., IoT devices).

Here are additional important ways in which IAM systems quickly become very complex.

First, an early point of failure is if the user is not who they say they are. To make this easy, think in terms of Jolene rather than a device named 00-B0-D0-63-C2-26 or a program named "backofficeentity." Someone or something inside the IAM system is responsible for:

1. Checking Jolene's documents (birth certificate, driver's license, passport, etc.) to authenticate their identity. Verify the documents!
2. Checking Jolene's recorded attributes in those to make sure that they are truly who they say they are. Are the data consistent?
3. Verifying their identity via the password or multifactor authentication technology, or perhaps even using a retinal scan, to ensure they are the person making the request. Verify Jolene's identity!
4. In some cases, checking to make sure that Jolene is alive. Is the biometric evidence consistent with other markers of the person. Does Jolene have a pulse?

These steps are often collectively referred to as "identity proofing"—a process that might be the same for each Jolene or it might vary based on the risk associated with the request Jolene has made of the system.[70]

Second, the organization's privacy and security goals require continuous updating of its policies to ensure that Jolene can only access the proper resources and data. One important aspect of this second complexity is that policy review is a cross-functional effort.

Third, each resource must be assessed to ensure that user has sufficient authority given the policy in place to use the data resource of specific features. This might take the form of metadata that indicate the nature of the data, how sensitive the data are, who owns them, and what constraints exist about their usage.

Together with a continuous policy review process and data management, identity proofing means that IAM systems are more than just simplistic mechanisms for access control. Gone are the days when a keycard and a password were all that was needed to guard the gates. Instead, IAM is now at the beginning, middle, and end of the vast exercise of running large, complex organizations—and the U.S. federal government is one the largest and most complex of them all.

70. In general, proofing is a rigorous and complicated process. See Romine, Charles H. 2022. *Personal Identity Verification (PIV) of Federal Employees and Contractors*. NIST FIPS 201-3. National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.FIPS.201-3.

APPENDIX 2—Four Versions of Decentralized Identity

***Federated Identity*—**This system manages identity, allowing user access to different resources, data, applications, or services by relying on a single set of credentials.[71] Federated identity systems are built on "mutual trust relationships" ("federations") that bridge different systems and organizations.

Think of this as a simple version of technological advancements to support decentralized identity systems. Our user Jolene from above wants to access a service or application within a federation, so the service provider requests Jolene's identity information from their home organization (the trusted "identity provider"). That home organization verifies the Jolene's credentials and confirms that verification by sending a token to the service provider that contains enough (but not too much) information to authorize Jolene's access. The service provider grants Jolene access to that resource, data, application, or service based on a trust relationship with the identity provider that is encapsulated in a token; Jolene does not need a separate username and password.

In practical terms, an SSO system is often the same as federated identity. Strong versions of federation allow a person to access multiple organizations. Indeed, sometimes federated identity systems do not allow SSO (having the SSO would improve the user experience).[72]

Federation helps organizations and users by:

- Admitting that users need access to multiple resources or enterprises
- Simplifying the verification and authentication experience for users
- Reducing the number of attack surfaces and enhancing control
- Improving user privacy since users share less personally identifiable information (PII) with fewer entities
- Making organizations work better, if only through interoperability

The mechanics of federated identity management are beyond the scope of this report. In general, organizations (also called "relying parties") decide both patterns of federation (e.g., ad hoc, hub-and-spoke, networks) and providers of federation (specific identity providers, or IdPs). NIST SP 800-63B governs how Jolene, our user, relates to the third-party IdP. NIST SP 800-63A governs how the relying party relates to the IdP (how the IdP conveys "assertions" about Jolene).

This complex of relationships addresses basic IAM challenges: it streamlines user authentication across multiple systems, it enhances security, it protects privacy and simplifies administration. In a world of many decentralized activities, it makes it easier for organizations to control who gets access to what. However, there are always threats—and those threats require mitigation. Threat actors may be minimized by encryption technologies (for now), but IdPs still have access to substantial information about users (e.g., by aggregating across the various services for which SSO/federation has been supplied).[73]

71. Windley, Phillip J. 2023. *Learning Digital Identity: Design, Deploy, and Manage Identity Architectures*. First edition. O'Reilly Media, Inc.
72. Windley, Phillip J. 2023. *Learning Digital Identity: Design, Deploy, and Manage Identity Architectures*. First edition. O'Reilly Media, Inc. p. 208.
73. See NIST SP 800-63C "Privacy Considerations", https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63c.pdf.

***Blockchain-based Identity*—**In contrast, the push for self-sovereign identity has led many to call for the use of blockchain technology in IAM systems. The hallmarks of such strategies center on blockchain's primary attributes: decentralization, security, and limitations on tampering.[74]

A blockchain is a distributed ledger that exists in multiple locations in a network. In this ledger, the list of records ("blocks") grows with use; those blocks are securely knitted together using cryptographic hashes.[75] In an IAM setting, Jolene's identity data would be stored on a blockchain; this information could be varied but might even include credentials or biometric data.[76] Our user Jolene would control that identity data; they could grant access to it using private keys for security. A requestor (or "relying party") might access that information with Jolene's permission for secure and direct verification.[77]

The primary benefits of such a strategy might include:

- Increased transparency and trust because blockchain transactions can be traced and are permanently recorded
- Reduced role of a central identity management authority
- Security and privacy benefits of reduced risk of identity theft/ fraud

Think of blockchain-based identity as a natural response (perhaps by users) to the evolution of SSO and federated identity management. SSO and federation brings great user experience benefits—but likely at a perceived cost to those same users.[78] While blockchain-based IAM solutions remain relatively rare, organizations may also benefit by removing single points of failure.[79]

Blockchain represents a push toward user-centered approaches to identity. Indeed, the WEF initiatives documented above also embrace blockchain. Of course, no technology is inherently immune to future threat actors. Users must still choose which PII attributes to pass along to others—and users almost certainly lack clear guidance about how to navigate that choice.[80] Even if this approach addresses key security challenges to current identity systems, future threats to the underlying hash algorithm remain. Yet, the WEF and other initiatives, including NIST guidance, show why there is so much attention to the potential use of this technology in settings when verification is critical and frequent, such as in government.

74. Hu, Vincent C. 2022. *Blockchain for Access Control Systems*. NIST IR 8403. National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.IR.8403.
75. Werbach, Kevin. 2018. *The Blockchain and the New Architecture of Trust*. Information Policy Series. MIT Press.
76. Arenas, Rodelio, and Proceso Fernandez. 2018. "CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials." *2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*, June, 1–6. https://doi.org/10.1109/ICE.2018.8436324.
77. Lesavre, Loïc. 2020. *A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.01142020.
78. Gilani, Komal, Emmanuel Bertin, Julien Hatin, and Noel Crespi. 2020. "A Survey on Blockchain-Based Identity Management and Decentralized Privacy for Personal Data." *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, September, 97–101. https://doi.org/10.1109/BRAINS49436.2020.9223312.
79. Pashalidis, Andreas, and Chris J. Mitchell. 2003. "A Taxonomy of Single Sign-On Systems." In *Information Security and Privacy*, edited by Gerhard Goos, Juris Hartmanis, and Jan Van Leeuwen, vol. 2727, edited by Rei Safavi-Naini and Jennifer Seberry. Lecture Notes in Computer Science. Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-45067-X_22.
80. Rana, Rima, Razieh Nokhbeh Zaeem, and K. Suzanne Barber. 2019. "An Assessment of Blockchain Identity Solutions: Minimizing Risk and Liability of Authentication." *IEEE/WIC/ACM International Conference on Web Intelligence*, October 14, 26–33. https://doi.org/10.1145/3350546.3352497.

Differential Privacy—A related but different situation that flows from the discussion of federated identity and blockchain-based solutions is that of differential privacy: a way for ensuring data privacy and confidentiality. While it is different, its connectedness can be seen in any setting where the anonymity of individual data is a key concern.

In a nutshell, many of the most worrisome aspects of identity for individuals involve the collection of large amounts of data that with data aggregation mechanisms like AI or ML can then be used at the individual level.[81] Rather than centering on transparency, differential privacy relies on obfuscation: it involves adding random noise to data or queries about data to mask information about individuals. When used for statistical purposes, the procedures of differential privacy ensure that the overall results are about the same regardless of whether any one person's data are included. This limits the exposure of details about specific individuals, thus enhancing privacy.[82]

As noted throughout the first part of this report, one of the main reasons why countries like the U.S. lack strong forms of identity is the concern that organizations should not have that degree of information about individuals. Of course, the modern era is one in which many companies know more about individuals than those same individuals know about themselves, but also social views seem to vary by setting.[83]

Even so, differential privacy affords certain benefits to the potential users of such large collections of data, including:

- A mathematical guarantee of privacy for the subjects of their research, perhaps increasing participation
- The ability to use or share data, maintaining data utility
- Increased public trust and perhaps compliance
- By increasing participation, a broader array of techniques such as machine learning for large data applications

Differential privacy remains in its infancy, but it is worthwhile for all government organizations to become familiar with the potential benefits of such technologies—and perhaps even the advent of regulations that require the use of such masking. Overall, it provides strong privacy assurances while allowing for meaningful data analysis. Such technologies do not solve the tensions over security and privacy, but they make the identification of individuals much less likely.

Federated Learning—This is the fourth stop in the march of innovation. With the advent of machine learning methods, the locations of model training and data are of particular concern for software developers, modelers, and the owners of the underlying data. Essentially, this design approach implements models across multiple decentralized devices or servers, and thus keeps data localized.[84] Federated learning is valuable when data privacy is paramount, or the centralization of data is not advisable.

81. Whitford, Andrew B., and Jeff Yates. 2022. "Surveillance and Privacy as Coevolving Disruptions: Reflections on 'Notice and Choice.'" *Policy Design and Practice*, June 15, 1–13. https://doi.org/10.1080/25741292.2022.2086667. Yates, Jeff, and Andrew B Whitford. 2022. "Surveillance as the Past and Future of Public Administration." *Perspectives on Public Management and Governance*, November 8, gvac022. https://doi.org/10.1093/ppmgov/gvac022.
82. Eryurek, Evren, Uri Gilad, Valliappa Lakshmanan, Anita Kibunguchy-Grant, and Jessi Ashdown. 2021. *Data Governance: A Definitive Guide.* O'Reilly Media, Inc.
83. Whitford, Andrew B., and Jeff Yates. 2022. "Surveillance and Privacy as Coevolving Disruptions: Reflections on 'Notice and Choice.'" *Policy Design and Practice*, June 15, 1–13. https://doi.org/10.1080/25741292.2022.2086667.
84. Mothukuri, Viraaji, Reza M. Parizi, Seyedamin Pouriyeh, Yan Huang, Ali Dehghantanha, and Gautam Srivastava. 2021. "A Survey on Security and Privacy of Federated Learning." *Future Generation Computer Systems* 115 (February): 619–40. https://doi.org/10.1016/j.future.2020.10.007.

Here is a simplification of how federated learning works in practice:

- Instead of bringing data to the model (or server where the algorithm is located, the model is sent to the data, perhaps at a local server or even located on a mobile device.
- The system then adds up all of these locally implemented models but does not access the underlying (raw) data, which might be located anywhere in the world. Think of this as an "averaging" process.
- The new working model is sent back to various locations for further training again (and again).

Just like the other items listed above in the march of innovation, federated learning enhances privacy (especially of sensitive data), reduces costs, is scalable and efficient, and aids with regulatory compliance (e.g., privacy laws). Moreover, it likely improves model-building by leading us toward more generalizable models that are robust because they are trained in the real world.

Indeed, NIST regularly encourages collaborative research (sometimes via challenges and competitions) to help uncover new methods and technologies for enhancing privacy and de-identifying data. The primary targets of NIST's Privacy Engineering Program are now data deidentification and differential privacy.[85]

How the Four Fit Together

Federated identity, blockchain-based identity, differential privacy, and federated learning are distinct yet complementary approaches that collectively address critical challenges in identity and access management (IAM) by tackling data security and privacy protection in interconnected ways. These four components work together to create robust IAM systems by addressing two core structural challenges: secure data management and privacy preservation. Federated identity enables centralized, interoperable authentication across systems, ensuring secure access while reducing redundant identity silos, whereas blockchain-based identity decentralizes identity management, empowering users with greater control over their data through cryptographic security.

Meanwhile, differential privacy safeguards sensitive data during analysis by adding controlled noise, ensuring individual identities remain protected, and federated learning keeps data localized on devices, minimizing centralized data storage while enabling collaborative model training. Together, they enhance cybersecurity by securing identity verification (federated and blockchain-based identity) and protecting data privacy (differential privacy and federated learning). By integrating these approaches, IAM systems achieve a cohesive balance, ensuring secure, privacy-preserving handling of critical data across diverse environments, from centralized servers to distributed networks.

85. See https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering.

ABOUT THE AUTHOR

Dr. Andrew B Whitford
Department of Public Administration and Policy
School of Public and International Affairs
University of Georgia
204 Baldwin Hall
Athens, GA 30602

E: aw@uga.edu
W: https://www.andrewwhitford.com/

Andrew Whitford is the Crenshaw Professor of Public Policy in the School of Public and International Affairs at the University of Georgia. His research concentrates on strategy and innovation in public policy and organization studies.

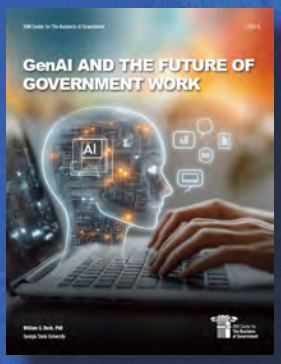
He has published four books on topics including financial regulation, the regulation of emerging technologies, public health science agencies, and narcotics policy. His book *Above Politics: Bureaucratic Discretion and Credible Commitment* was published in 2016 in the Political Economy of Institutions and Decisions series of Cambridge University Press. The book received the American Political Science Association's 2017 Gladys M. Kammerer Award for U.S. national public policy, the International Political Science Association's 2017 Levine Prize for comparative administration and public policy, and the 2016 Book of the Year Award of the Section of Public Administration Research (SPAR) of the American Society of Public Administration.

His research papers have appeared in peer-reviewed journals such as the *Administrative Science Quarterly*, the *Journal of Public Administration Research and Theory*, the *Journal of Policy Analysis and Management*, the *American Journal of Public Health*, *Government Information Quarterly*, and the *American Journal of Political Science*. Current research topics include the use and regulation of emerging technologies.

He also served as Founding Co-Editor of the Cambridge Elements Series in Public and Nonprofit Administration, and is an elected Fellow of the National Academy of Public Administration. He received the 2017 Herbert A. Simon Award for "significant contribution to the scientific study of bureaucracy." He has lectured and conducted research around the world. He is currently Visiting Honorary Professor in the School of Public Policy at University College London and Research Fellow in Arizona State University's Center for Organization Research and Design.

The IBM Center has published two reports by Dr. Whitford. *Designing Competitive Bidding for Medicare*, written with John H. Cawley of Cornell University, was published in 2004. *Transforming How Government Operates: Four Methods for Changing Government* was published in 2020.

Recent Reports from the IBM Center for The Business of Government



GenAI and the Future of Government Work

by William G. Resh

Embedding Strategic Foresight into Strategic Planning and Management

by Bert George

Resilience in action: Crisis leadership through innovation, collaboration, and human-centered solutions

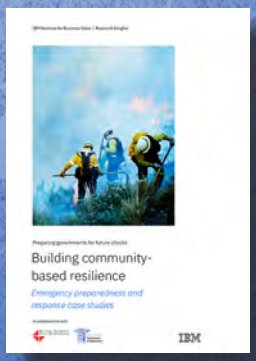
by Julia Carboni

Leadership Framework for an Agile Government

by Pallavi Awasthi and Kuang-Ting Tai

The Opportunity Project

by Joel Gurin and Matt Rumsey

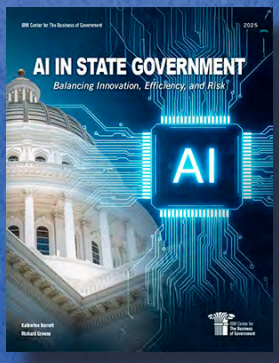


Building community- based resilience

by Authors of Case Study

IBM Center Research Announcement

by Dan Chenok



AI in State Government

by Katherine Barrett and Richard Greene

For a full listing of our reports, visit businessofgovernment.org/reports

About the IBM Center for The Business of Government

Through research stipends and events, the IBM Center for The Business of Government stimulates research and facilitates discussion of new approaches to improving the effectiveness of government at the federal, state, local, and international levels.

About IBM Consulting

With consultants and professional staff in more than 160 countries globally, IBM Consulting is the world's largest consulting services organization. IBM Consulting provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build, and run those solutions in a way that delivers bottom-line value. To learn more visit ibm.com.

For more information:
Daniel J. Chenok
Executive Director
IBM Center for The Business of Government

600 14th Street NW
Second Floor
Washington, D.C. 20005
(202) 551-9342

website: www.businessofgovernment.org
e-mail: businessofgovernment@us.ibm.com

IBM Center for The Business of Government