ForgeRock

INDUSTRY BRIEF

The Time Is Now

U.S. Federal Government Agencies Must Take Bold Action to Protect Citizen Privacy

Despite decades of investment in providing services securely to the public,[1] federal agencies are still facing the compromise of sensitive information entrusted to them as well as massive financial losses due to fraud. An uncomfortable truth is that while agencies need to accelerate moving citizens to online channels, many aging and legacy government systems, often developed in-house, are unfit to address these challenges.

The core problem is two-fold: On the one hand, as a federal agency, you can't trust the digital identities used to access services and data. But the problem is much wider – you can't blindly trust any component of the computing infrastructure. That's why industry experts – from the U.S. Defense Information Systems Agency to leading analyst firms – have been working to define a security model known as Zero Trust.[2] In Zero Trust, we assume that all users, devices, and systems are not implicitly trustworthy unless they are proven and the access assignment is necessary.

The second part of the problem is that government agencies have always focused on security while ignoring or downplaying the user experience – but this is no longer acceptable in today's market. Since the shift to more online services accelerated in earnest after the onset of the global pandemic, people have become more accustomed to online shopping, banking, and even online healthcare via telemedicine appointments. They've come to expect a more intuitive, user-friendly, and frictionless experience online – but government services are not there yet.

Fortunately, over the last few years, a compelling category of solutions has emerged after years of research and lessons learned based on the principle of Zero Trust. In particular, recent commercial identity and access management (IAM) solutions with strong consumer or citizen-facing solutions have made considerable progress in creating and utilizing trusted identities to provide secure access to services.

1 https://www.govinfo.gov/content/pkg/PLAW-107publ347/html/PLAW-107publ347.htm
2 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Federal Mandates & Guidance Deadlines are Looming

The May 2021 Executive Order on Improving the Nation's Cybersecurity[3] acknowledges the reality that agency capabilities are not meeting urgent security needs. It states:

> "Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments to defend the vital institutions that underpin the American way of life. The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems."

The Executive Order mandates specific types of security improvement by November 2021.

Zero Trust

The requirement to migrate to more secure Zero Trust Architectures (ZTA)[4] is at the core of the Executive Order. The goal of any Zero Trust (ZT) strategy is to operate under the assumption that your network is already compromised and to minimize uncertainty by enforcing accurate, least privileged, and per-request access decisions in information systems and services. In the event of a breach, Zero Trust aims to limit the ability of an attacker to move laterally in your network by requiring granular access rules and leveraging continuous authentication and authorization when possible. The need to modernize IAM solutions is at the core of the Executive Order, and modern citizen/customer identity and access management (CIAM) solutions are the foundation for Zero Trust. Some of the core capabilities required for successful Zero Trust implementations are found in many modern IAM solutions. These include precise identity management,

adaptive policy-based access control capabilities, and the ability to integrate with and leverage the threat and fraud indicators provided by continuous diagnostics and mitigation (CDM)[5] systems and other sources of intelligence.

Multi-Factor Authentication

The Executive Order also explicitly called out a core Zero Trust Architecture requirement that agencies must meet by November 2021:[6] data must be protected with multi-factor authentication (MFA) and encryption[7] at rest and in transit. MFA and data protection are common components of any IAM product, but are often missing from the homegrown or older solutions that many agencies still rely on.

This late 2021 timeline may sound aggressive, but the requirement is not new. In June 2017, the National Institute of Standards and Technology (NIST) released its Digital Identity Guidelines,[8] which requires MFA for access to all personal data. In May of 2019, the Office of Management and Budget (OMB) issued Memorandum M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management (ICAM),[9] which requires agencies to implement the NIST guidelines. M-19-17 also requires agencies to migrate away from custom homegrown solutions to "ensure that deployed ICAM capabilities are interchangeable, use commercially available products, and leverage open application programming interfaces (APIs) and commercial standards to enable componentized development and promote interoperability across all levels of government."

3 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
4 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
5 https://www.cisa.gov/cdm
6 "Within 180 days of the date of this order"
7 https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines
8 https://pages.nist.gov/800-63-3/
9 https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf

Positive user experiences, along with fair and impartial access, help your agency meet its mission goals. No single authenticator type or method will serve the needs of all citizens accessing government systems. Without compromising security or Zero Trust tenets, your agency must enable citizens to choose the way they wish to incorporate MFA. For example, depending on the authentication assurance level (AAL) required for a specific task, using a social network provider's authenticator may relieve the citizen's burden of managing a large number of authenticators.[10]

Other choices for strong authentication include FIDO2 passwordless and usernameless authentication, on-device biometrics, push notifications from a mobile authenticator app, or even one-time passwords (OTPs) sent via email, text, or voice. Providing citizens with as many options as possible while maintaining AAL compliance can improve the likelihood of faster and more widespread adoption of MFA.

Adopting Cloud Services

The May 2021 Executive Order expanded on the M-19-17 requirement to use commercial products in solutions: it requires agencies to "accelerate movement to secure cloud services" that unburden agencies for day-to-day maintenance costs. This echoes the Federal Chief Information Officers (CIO) Council's Cloud Smart[11] strategy. Adopting cloud services can lower operations and maintenance costs by reducing the need for government contracting teams to maintain IT infrastructure and develop custom in-house solutions. Cloud services can also improve security and scalability, allowing your agency to focus on its core mission.

Authentication and Federation Requirements

Office of Management and Budget (OMB) Memorandum M-19-17 also requires that agencies improve user experience by allowing them to manage their authenticators and leverage federated credentials[12] whenever possible. IAM solutions must support those requirements, which include the need to integrate with federated identity standards[13] such as Security Assertion Markup Language 2 (SAML 2), Open Authorization 2.0 (OAuth 2.0), OpenID Connect, and User-Managed Access (UMA), while meeting NIST 800-63C Digital Identity Guidelines: Federation and Assertions[14] requirements for Federation Assurance Levels (FAL) 1 & 2.[15]

Agencies must also "provide identity verification and access control appropriate to the risk level and performance of the business function." Depending on your agency's service offerings, this could require your IAM solutions to support integration with identity proofing solutions,[16] authentication, and federation at different assurance levels,[17] with the ability to step up proofing or authentication as needed to access more sensitive or valuable information, and to protect their services at different assurance levels.

Conclusion

There are many other federally mandated requirements for IAM, and new guidance and requirements will continue to be released to keep up with emerging technologies and new threat vectors. Your agency's IAM solutions must be able to keep up with and even pioneer those evolving requirements, while simultaneously meeting operational needs and customer expectations. The best way to meet this requirement is by evaluating and adopting commercial IAM instead of relying on in-house development.

To learn more about commercial solutions for citizen and consumer IAM, visit: https://www.forgerock.com/digital-identity/customer-identity

10 https://pages.nist.gov/800-63-3/sp800-63b.html
11 https://cloud.cio.gov/strategy/
12 "Agencies shall leverage federated solutions to accept identity and authentication assertions made by mission and business partners." "Agencies shall leverage existing credentials and identity federations that meet the agency's determined acceptable risk level rather than standing up processes or capabilities to issue new credentials to users."
13 https://www.forgerock.com/platform/access-management/federation
14 https://pages.nist.gov/800-63-3/sp800-63c.html
15 https://www.forgerock.com/resources/whitepaper/forgerock-nist-sp-800-63-3
16 https://www.forgerock.com/resources/whitepaper/reduce-government-services-fraud
17 https://pages.nist.gov/800-63-3/