ForgeRock

INDUSTRY BRIEF

U.S. Federal Agencies and Cyber Security Mandates

Improve the User Experience to Reduce Risk, Lower Costs, and Ensure Equitable Access

The May 2021 Executive Order on Improving the Nation's Cybersecurity[1] gave Federal agencies a November 2021 deadline to demonstrate adherence to a Zero Trust network architecture, including implementing strong authentication and identity federation, along with adopting cloud services. While cybersecurity mandates are important, your agency must not ignore the need to improve the user experience. The recent acceleration to more online services stemming from the COVID-19 crisis, as well as the maturity of the millennials, has shown that systems that do not offer a great user experience will not be used. You cannot assume that citizens will put up with multiple security hoops that sacrifice experience – just for the privilege of interacting with government services online. Poor online adoption will drive additional in-person or telephone interactions, increasing costs and reducing the efficiency of existing resources.

The reason all of these federal imperatives have been issued is because many if not most federal agencies are working with legacy identity and access management (IAM) systems that are not cloud-ready – and are not designed to withstand the sophisticated levels of threat we are facing today.

1 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Agencies are operating with legacy hardware and software. Access management is handled by legacy or homegrown IAM solutions. These legacy IAM systems are siloed, inflexible, and unable to scale to support cloud migration and applications and standards like OpenID Connect (OIDC), Open Authorization 2.0 (OAuth 2.0), Fast ID Online 2 (FIDO2), Security Assertion Markup Language (SAML), System for Cross-domain Identity Management (SCIM2), and User Managed Access (UMA).

Your agency faces numerous risks by not modernizing your citizen-facing IAM solutions:

- Your agency is more vulnerable to both cyber-attacks and fraud,[2] both of which increased during the pandemic.[3] The citizens your agency serves suffer from identity theft, loss of privacy, delayed or lost benefits, fraud, missed opportunities, lost time from work, and numerous other burdens due to inadequate citizen-facing IAM solutions.
- Your agency faces mounting costs for supporting and maintaining legacy systems, costs for responding to increased fraud and attacks, and the greater costs required to provide phone, paper, and in-person services to customers who are not being adequately served by the current online solutions.
- Your agency is also subject to negative audit findings[4] and congressional oversight hearings when they fail to meet all federal requirements.
- Inadequate user experiences prevent user adoption, resulting in increased costs to your agency.

Core Capabilities and Considerations for Federal Agencies

Your IAM solution needs to meet your agency's operational needs while enabling the delivery of critical services in a way that protects both the agency and your customers – both now and in the future – as new threats emerge and new requirements and guidance are issued to meet those threats.

Security & Interoperability

Your citizen/customer identity and access management (CIAM) solution needs to meet the following criteria:

- Fits into a Zero Trust Architecture
- Meets all relevant federal security and IT requirements
- Implements current standards
- Includes processes for evolving products to meet new federal requirements and adapt to changing threat landscapes

Certification from a trusted third party can verify product capabilities and provide confidence that current security and interoperability requirements can be met. Organizations such as the Federal Risk and Authorization Management Program (FedRAMP),[5] Kantara,[6] the National Information Assurance Partnership (NIAP),[7] and the OpenID Foundation[8] can help your agency obtain gold-standard SOC2 Type II audit reports.

Digital transformation proceeds along a roadmap, so modern CIAM solutions must also integrate easily with older systems and standards and add security on top of those older protocols when possible.

Your CIAM solution must also be flexible enough to meet emerging cybersecurity requirements such as the new Executive Order directive to log and share data that can be used to detect both fraud and zero-day attacks. Your agency must plan to meet the new software supply chain security requirements by creating a Software Bill of Materials and ensuring that their developers follow secure coding practices.

Operational Needs

Government to Citizen (G2C) Considerations

Identity proofing is necessary for preventing government services fraud – but for many users, this can be extremely challenging, especially when they are using older technology, have disabilities, or have minimal credit histories. Your CIAM solution must therefore provide the ability to orchestrate flexible omnichannel identity proofing flows[9] that integrate seamlessly with third-

2 https://www.nextgov.com/ideas/2021/06/what-i-learned-helping-lead-oversight-5-trillion-pandemic-relief/175004/
3 HIGH-RISK SERIES : Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas (gao.gov)
4 https://www.oversight.gov/reports
5 https://marketplace.fedramp.gov/#!/products
6 https://kantarainitiative.org/trustoperations/classes-of-approval/
7 https://www.niap-ccevs.org/Product/index.cfm
8 https://openid.net/certification/
9 https://www.forgerock.com/resources/whitepaper/reduce-government-services-fraud

party identity proofing solutions. This will maximize the number of people who can be successfully proofed and allow equitable access to the convenience provided by online services. An omnichannel solution should allow a user to create an account at a customer service office and complete it online – or vice-versa – provide options for online or call center support, and integrate with solutions such as document verification kiosks and address verification controls. The solution should provide flexible proofing controls and options to meet the needs and capabilities of the diverse populations that your agency serves.

Any proofing or authorization solution should also allow your agency to meet the requirement to minimize the collection of personally identifiable information (PII), to adequately protect any that is collected, and to support user consent to the collection and use of that data, including the ability to revoke consent. To enhance privacy, the solution should also allow the use of pseudonymous identities and attribute references where appropriate. For example, if an individual's state of residence is required but not the street address, then only the name of the state should be provided. Likewise, if accounts can be created only by individuals that are legal adults, then an 'over 18' attribute can be used rather than a date of birth.

Your agency should embrace identity federation to reduce the burdens of repeated identity proofing and the challenges with managing multiple credentials. Your IAM solution should provide the flexibility to connect with approved commercial and government cloud service providers that meet the National Institute of Standards and Technology (NIST) Identity Assurance Level (IAL) and authentication assurance level (AAL) requirements. Social logins can be combined with a validated ID, identity proofing, and authentication to make it easier for citizens to register for or gain access to federal systems. Leveraging authentication methods that users are familiar with, like social logins and common mobile authenticator applications, will increase security through majority adoption. Your solution should also support secure password recovery and other self-service options to deliver the level of service and experience customers have come to expect. Your agency should encourage your constituents to move away from paper, phone, and in-person channels by improving their experience and confidence in the security of the online system.

Accessibility Requirements

One significant difference between government and commercial IAM implementations is that government CIAM solutions must enable access to services to everyone eligible to receive them, including customers with disabilities and accessibility challenges.

Providing support for both delegation and "508 compliance" can help meet those needs.

Any citizen-facing content for your CIAM application, including user registration and account management pages, must meet[10] the W3C Web Content Accessibility Guidelines (WCAG) 2.0[11] in order to comply with Section 508[12] of the Rehabilitation Act.[13] Following WCAG guidelines makes it easier for anyone with a disability to be able to interact successfully with online content. The General Services Administration (GSA) has resources for 508-compliant procurement[14] and testing[15] on their Section 508 website that can be used to assist your agency in acquiring a CIAM product that can help meet accessibility requirements.

Consent-based delegation is required when a solution built to meet the 508 requirements cannot provide accessibility and online self-service options to everyone who needs government services. CIAM solutions that support delegation workflows allow a user to set up an account, perhaps with assistance, and then explicitly delegate management of that account to someone else, such as a trusted caregiver or legal representative or firm. Support for explicit delegation provides a far more secure and auditable mechanism for caregivers to provide assistance, without the security problems that result from sharing credentials.

10 How to Meet WCAG (Quick Reference) (w3.org)
11 https://www.w3.org/TR/WCAG20/
12 IT Accessibility Laws and Policies | Section508.gov
13 Rehabilitation Act (access-board.gov)
14 Accessibility Requirements Tool | Section508.gov
15 Accessibility Testing for Websites and Software | Section508.gov

Conclusion

To provide secure and seamless access to citizen services, increase efficiency, and reduce costs, your agency will need to demonstrate that it is adhering to federal cybersecurity mandates for security and interoperability. This includes strong authentication, identity federation, user-managed access, and integration with identity proofing solutions.

At the same time, your agency needs to make the end user experience easy to understand and capable of accommodating citizens with disabilities and those without internet access. The best way to meet these requirements is by evaluating and adopting a commercial IAM that can reduce fraud, strengthen security, and provide frictionless citizen experiences.

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