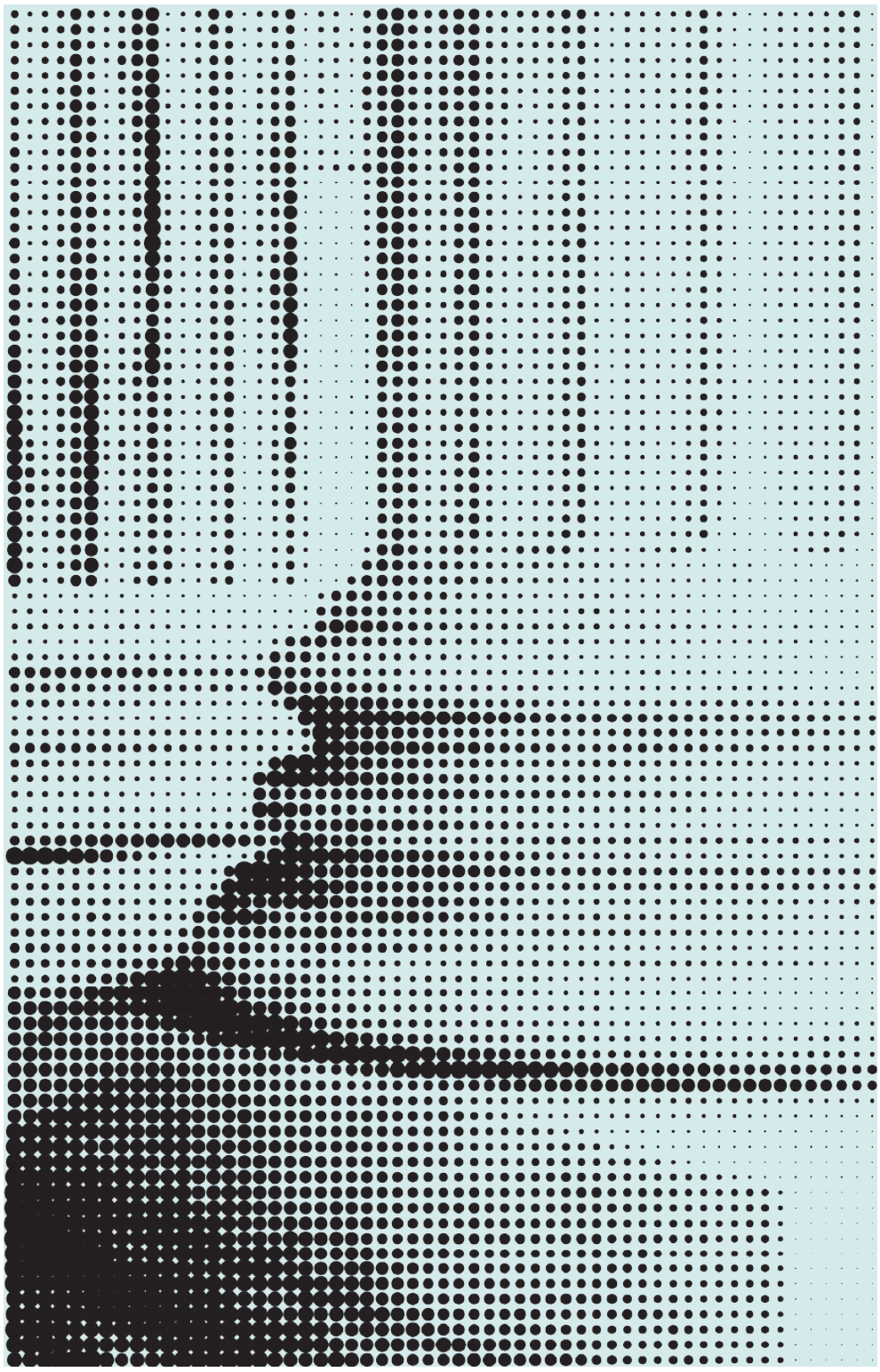
Whitepaper

January 2021

FICAM:

Securing Identities, Credentials, and Access in Federal Government Agencies



Okta Inc.

100 First Street

San Francisco, CA 94105

info@okta.com

1-888-722-7871

okta

Contents

Introduction

Your agency handles a wealth of personal data and classified resources: addresses, social security numbers, as well as medical and financial information. To keep these assets secure, you need a strong identity management strategy that includes the most effective technology—and the best place to start is with FICAM. Otherwise known as Federal Identity, Credential, and Access Management, FICAM refers to the U.S. government's approach to Identity, Credential, and Access Management (ICAM). Its tools, policies, and systems guide agencies in providing the right individual with the right resource at the right time.

There are numerous federal laws, policies, and standards that influence the design of FICAM programs. One of these—**the OMB 19-17 Memorandum**—sets out the federal government's position on identity, credential, and access management (ICAM) and issues multiple strategic goals for agencies to work towards. These goals are intended to modernize digital operations, thereby improving security and better serving citizens and partners.

To achieve these objectives, agencies should implement FICAM solutions that they can manage with confidence. The U.S. **General Services Administration** lists solution providers that can help government entities to securely meet the FICAM roadmap outcomes—and Okta is among them.

In this whitepaper, we'll explore what OMB 19-17 means for your agency. Plus, we'll discuss how an Okta and Amazon Web Services (AWS) partnership can help you to comply with FICAM requirements and perform at full potential.

Breaking down the OMB 19-17 Memorandum

The OMB 19-17 Memorandum contains six sections. Here's what you need to know about each of them:

I. Contextualize identity in the federal government

This section offers a crucial definition of **identity**, describing it as the unique representation of a person, device, or technological subject that interacts with a federal subject or resource (e.g., federal information, systems, and facilities).

It also provides two different contexts for identity:

Federal enterprise identity

Identities that agencies manage to achieve business goals, such as employees, contractors, enterprise users, and their devices.

Public identity

Identities that agencies don't directly manage but interact with to achieve their goals, such as users at partnering agencies.

These are your need-to-know definitions of what identity is and how it occurs in federal government. The subsequent sections of OMB 19-17 outline various mission statements for agencies.

Where FICAM meets FedRAMP

While not discussed in OMB 19-17, it's essential to consider the **Federal Risk and Authorization Management Program (FedRAMP)**. FedRAMP provides government agencies with a standardized approach to assessing cloud products and services—and defines the security requirements and processes that solution providers must follow to get approved for government use. Therefore, it's important that agencies look for FedRAMP authorization when choosing their solution partners.

II. Manage identities, credentials, and access in modern government

Advances in technology have made digital operations faster and more efficient, but these performance gains come with serious challenges—from severe cyber threats to breaches of personally identifiable information (PII). As technology evolves, so do the methods used by malicious actors.

In response, the federal government is paying greater attention to risk management. This means adopting policies that improve privacy and security while helping to conduct operations and deliver services without friction.

To make these improvements, agencies must identify, credential, monitor, and manage all subjects who access federal resources. After all, their methods for proofing identities and controlling access is crucial to delivering secure services that uphold user privacy.

The OMB 19-17 also encourages agencies to shift their approach to FICAM away from the outdated Levels of Assurance model. Instead, they should use a new model based on risk management perspectives. This means implementing **NIST Special Publication (SP) 800-63-3**, —otherwise known as the government's Digital Identity Guidelines—along with any successive versions.

In addition, agencies must consult identity management guidance from the **Office of Personnel Management (OPM)**, **Department of Homeland Security (DHS)**, and **National Security Agency (NSA)**. With these three resources, government bodies can form a well-rounded approach to identity proofing that puts privacy and security first.

III. Adapt the government's approach to Homeland Security Presidential Directive 12 (HSPD-12)

HSPD-12 is the federal policy for issuing reliable forms of identification to agency users. Personal identity verification (PIV) credentials are the required means of identity proofing, vetting, and binding the identity of a credential holder to an authenticator.

The OMB 19-18 Memorandum makes it clear that agencies need flexible solutions to serve changing technology needs and manage the identity lifecycle.

To that end, they must take the following actions:

1. Follow the OPM requirements on issuing, suspending, and revoking PIV credentials.

2. Use PIV credentials as the primary means of identification and authentication.

- Use Derived PIV Credentials for federal employees, contractors, and other enterprise users. Enable apps and devices to accept these credentials.
- Work with the Federal CIO Council, the Federal Privacy Council, and NIST to try alternative identity management solutions that meet the intent of HSPD-12.
- Implement measures to manage access control—including those to revoke privileges and to revoke or destroy credentials in a timely fashion. This will help to prevent unauthorized access attempts from former staff or when the credential is lost.

3. Support cross-government identity federation and interoperability.

- Grant relevant partners and agencies access to information systems, facilities, and secured areas.
- Implement electronic verification processes for PIV credentials held by other agencies.
- Accept existing PIV credentials where possible, rather than issuing new ones.
- Strike agreements with partners to support identity federation.

4. Use PIV authentication apps to continuously vet and evaluate personnel.

- Make risk-adaptive decisions regarding access to federal resources.

5. Implement PIV digital signature capabilities.

6. Use PIV credentials to encrypt data in transit and shared between federal staff and contractors.

IV. Shift the operating model beyond the perimeter

Identity is the **new security perimeter**, so agencies should place it at the heart of their risk management strategy. This means taking steps in governance, architecture, and acquisition:

Governance

☐ Designate a FICAM office, team, or other dedicated structure to enforce and own risk management across the agency. Include leaders in various role functions—Information, Finance, HR, General Counsel, Physical Security, and Privacy. Chief Operating Officers (or equivalents) should also arrange regular coordination between these mission owners.

- ☐ Create and maintain a thorough FICAM roadmap for policy, process, and solutions. In addition, it's a good idea to incorporate relevant federal guidelines and sketch out roles and responsibilities for all users.
- ☐ Outline agency-wide performance expectations for security and privacy risk management, adding ICAM improvement goals into strategic plans and reviewing progress with the OMB.
- ☐ Follow the digital identity risk management requirements set in NIST SP 800-63. This includes making risk-informed decisions about technologies and operational processes, collaborating with government bodies at various levels, and sharing feedback on risk management implementation with the Federal CIO Council, Federal Privacy Council, and NIST.

Architecture

- ☐ Use flexible and scalable identity and access solutions, such as multi-factor authentication (MFA), that work across the agency and support changing mission needs.
- ☐ Deploy interchangeable FICAM capabilities, use APIs and commercially available products, and follow commercial standards to encourage interoperability.
- ☐ Create processes to bind, update, revoke, and destroy credentials for each user, device, and technology.
- ☐ Build privacy-enhanced data validation APIs for public and private identity proofing services to use. This improves the assurance of identity verification measures.
- ☐ Use federated solutions to accept partners' identity and authentication conditions, accept risk assertions made by partners, and confirm that partners use commercially available standards to the extent possible.

Acquisition

- ☐ Encourage all contractors to abide by HSPD-12 and OPM requirements.
- ☐ Use products and services that comply with OMB policies, NIST standards, and supporting tech specifications.
- ☐ Follow the NSA and DHS's guidelines for selecting authentication factors.
- ☐ Obtain digital certificates to identify and authenticate federal enterprise identities.
- ☐ Use the Continuous Diagnostics and Mitigation (CDM) program to deploy tools and tactics that meet FICAM goals—and work continuously with the CDM program to understand new requirements and identify future capabilities to build.

V. Improve digital interactions with the American public

Citizens need services they can trust. To build public confidence, agencies must power digital interactions that work reliably and honor user privacy.

That requires taking the following steps:
1. Proof citizen and partner identities in line with NIST and FICAM requirements.
2. Limit the collection of PII to what's legal, relevant, and necessary.
• Protect data according to the level of risk it poses.
3. Create processes based on identity risk and assurance levels to associate non-government authenticators to digital identities.
4. Use existing PIV credentials and federations that meet your acceptable risk levels.
5. Use federal or commercial services that support NIST SP 800-63-3 requirements for AAL multi-factor authenticators to deliver identity assurance and authentication to the public.
• Share proofing confirmations across agencies to reduce process redundancies. • Get direct feedback from users to see if there's demand to have more service providers as federation partners. • Use shared service providers that follow authenticator assurance level requirements, and that are resilient to compromise or service failure.

VI. Enumerate government-wide responsibilities

The OMB 19-17 concludes by listing the government agencies leading the charge with improving digital identity management:

- **Department of Commerce**
- **Office of Personnel Management**
- **General Services Administration**
- **Department of Homeland Security**

The memo outlines the formal responsibilities each of these organizations has when it comes to shaping FICAM policies and supporting other agencies. You're free to consult with each organization to clarify their FICAM position, and the OMB provides a **contact email** to direct all policy assistance questions.

Achieving your FICAM initiatives with Okta and Amazon Web Services

The right solution partners can bring your FICAM vision to life. OMB stresses the importance of building a flexible, scalable architecture that can evolve to meet tomorrow's performance and security requirements—any provider you choose must meet this need.

The **Okta Integration Network** has 6,500+ connections to apps that improve user experience and security capabilities. You can avoid vendor lock-in and explore the app connections that best fulfill your FICAM needs at any given moment.

Our integration with **AWS** lays the foundation for secure, audited infrastructure and processes. It helps your agency to:

- **Migrate to the cloud:** Apply Okta's **MFA** to secure access to **Amazon WorkSpaces** and other AWS applications that people need for work.
- **Secure access to cloud resources: Advanced Server Access** enables secure, identity-led access management for **AWS EC2**. Its flexible, "least privilege" access model provides stringent protection while adapting to fit environments of any size.
- **Modernize and secure applications:** Okta's **Single Sign-On**, built-in PIV credentials, and Common Access Card (CAC) secure access to AWS tools such as **AWS CLI**, **AWS EKS**, and Lambda.

For additional peace of mind: Okta is FedRAMP authorized with Moderate Authority to Operate. Agencies that need FedRAMP Moderate, Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG) IL2, or DoD SRG IL4 compatibility can **configure Okta's settings** to ensure compliance.

Supporting your identity and access management goals

Driving digital change in line with the **FICAM roadmap** helps you to meet—and exceed—your agency mission in **several ways**, from complying with federal law and strengthening your security posture to streamlining access to digital services and improving trust and interoperability.

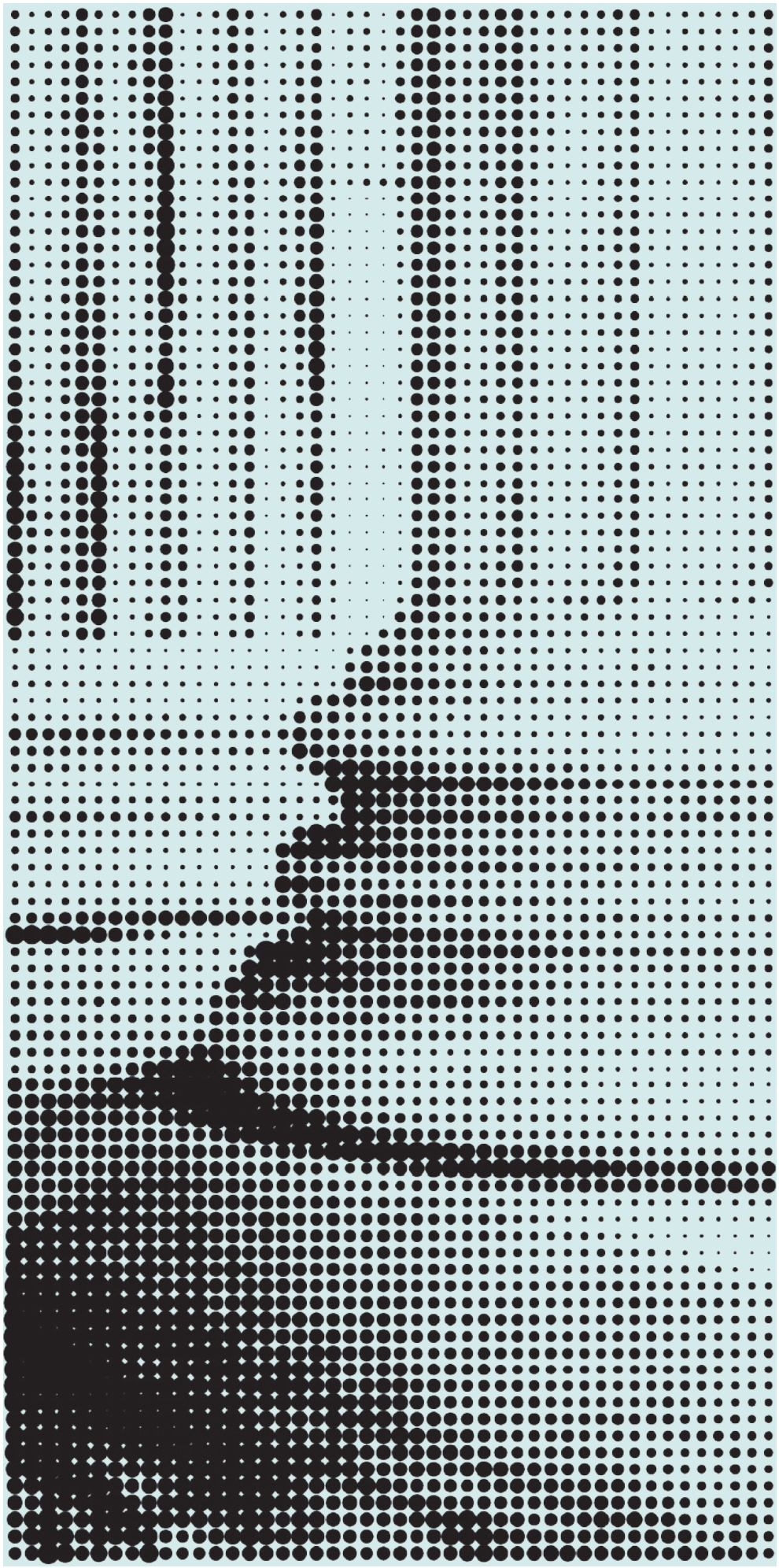
These are all important benchmarks for your agency. Pursuing them through FICAM leads to more secure and user-friendly services, though modernizing the right way requires a solution provider you can trust.

Whatever your objectives, Okta is here to help. **Contact us today**.

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 6,000 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business.

Over 6,100 organizations, including 20th Century Fox, JetBlue, Nordstrom, Slack, Teach for America and Twilio, trust Okta to help protect the identities of their workforces and customers. To learn more, visit **okta.com**.



okta