Authentication for Government and Public Sector: M-22-09, FIPS 201, FedRAMP, and What Federal Zero Trust Actually Requires

Industry Guides / Last updated 2026-06-11 / https://www.scrambleid.com/learn/authentication-for-government-public-sector

In one sentence: Federal, state, and local agencies and their contractors are converging on a single authentication direction (phishing-resistant by default, PIV/CAC and FIDO2/WebAuthn as the two ceremonies that meet the bar, derived credentials and ICAM-aligned identity for the contexts where smart cards do not reach), and the architecture has to satisfy M-22-09, NIST SP 800-63-4, FIPS 201-3, FedRAMP, CJIS, and increasingly state and local mandates without leaving the legacy systems behind.

TL;DR (canonical)

- OMB M-22-09 is the load-bearing directive: phishing-resistant MFA for federal staff, contractors, and partners; phishing-resistant options for public-facing services. PIV/CAC and FIDO2/WebAuthn are the two ceremonies that meet the bar.
- PIV and CAC remain the gold standard for federal workforce. Derived PIV (NIST SP 800-157) and FIDO2 fill the mobile, BYOD, partner, and citizen-facing gaps.
- NIST SP 800-63-4 defines the AAL framework. AAL3 properties (verifier-impersonation resistance, verifier-compromise resistance, hardware-bound) are the bar for the highest-assurance federal applications.
- FedRAMP, CJIS, IRS Pub 1075, NSA CNSSI, DoD STIGs, and state-level mandates layer additional requirements on top, but converge on the same phishing-resistant direction.
- The architecture that scales: PIV/CAC primary for federal workforce on managed devices, FIDO2/WebAuthn for partner and citizen access, derived PIV for mobile, with sender-constrained tokens on machine-to-machine paths and ICAM-aligned identity governance across the lifecycle.
- The biggest deployment challenges are legacy systems that do not speak modern protocols, BYOD and partner contexts that cannot use PIV cards, and the citizen-facing surface (where Login.gov, ID.me, and per-agency portals are converging on FIDO2-grade options).

The federal threat landscape

Nation-state credential phishing. APT campaigns against federal employees and contractors are a continuous threat. Phishing-resistant MFA is the highest-leverage control against this category.

Contractor and partner compromise. Defense Industrial Base (DIB) and federal civilian contractors are heavily targeted as a path into agency systems. CMMC and the broader contractor cybersecurity stack tighten the requirements year over year.

Insider misuse. Privileged-user audit and signed authentication events are essential. The recent emphasis on ZT and continuous validation makes this a controllable rather than aspirational property.

Citizen-facing service abuse. Identity fraud against benefits programs, tax filing, unemployment, and healthcare programs is at scale and growing. Identity proofing at signup and phishing-resistant authentication on return access are the dominant mitigations.

Critical-infrastructure attacks. State and local water utilities, transportation, election systems, and emergency services face threat actors with national-security relevance. Authentication on operator workstations and remote access is a chronic gap.

Supply-chain attacks via federal CSPs. A compromised cloud service provider with FedRAMP authorization can affect every agency that uses it. FedRAMP's identity controls (IA-2 series) are part of how this risk is managed.

Federal regulatory and policy stack

Document	What it requires (authentication-relevant)	Practical implication
OMB M-22-09	Phishing-resistant MFA for federal staff, contractors, partners; phishing-resistant options for public-facing services	The single most important federal authentication directive. PIV/CAC and FIDO2/WebAuthn meet the bar.
NIST SP 800-63-4	Identity Assurance Level (IAL), Authenticator Assurance Level (AAL), Federation Assurance Level (FAL)	Finalized July 2025 and supersedes 800-63-3; coordinate with NIST and your auditor on the transition timeline applicable to your compliance regime
FIPS 201-3	PIV credential format and ceremony	The federal smart-card standard for federal employees and contractors
NIST SP 800-157 (Derived PIV)	Derived PIV credentials in mobile and software contexts	Path to phishing-resistant MFA on mobile and BYOD without smart-card readers
NIST SP 800-53 Rev. 5	Authentication controls (IA-2 family); AC and AU families	The control catalog FedRAMP and most agencies derive baselines from
FedRAMP (Low/Moderate/High)	NIST 800-53 baselines, plus FedRAMP-specific overlays	Authentication requirements for cloud service providers serving federal customers

Document	What it requires (authentication-relevant)	Practical implication
CISA Zero Trust Maturity Model	Pillar 1 (Identity); Advanced and Optimal stages require phishing-resistant MFA, continuous validation	The maturity reference for federal Zero Trust progression
Federal ICAM Playbook	Lifecycle (proofing, enrollment, credentialing, access management, governance, federation)	The federal-specific architecture for end-to-end identity
FBI CJIS Security Policy	MFA for CJI access; advanced authentication	State and local law enforcement agencies and their contractors; verify current version
IRS Publication 1075	Authentication for FTI access	State tax agencies and their contractors
NSA CNSSI and DoD STIGs	Configuration and authentication controls for national-security and DoD systems	DoD-specific requirements layered on top
CMMC 2.0	Defense contractor cybersecurity, including authentication controls	DIB-specific
State cybersecurity statutes (varying)	State workforce, contractor, and citizen-facing requirements	Increasingly aligned with federal direction
CISA SLCGP	State and local cybersecurity grant program	Federal funding tied to baseline cybersecurity practices including identity

For a deeper compliance view including specific NIST 800-53 control mapping, see Compliance Mapping: NIST and CISA.

The federal channel mix

Channel	Who authenticates	Typical legacy method	Phishing-resistant pattern (M-22-09 aligned)
Federal employee on managed workstation	Federal staff	PIV smart card (already phishing-resistant in mature agencies)	Continue PIV; add FIDO2 fallback for non-PIV contexts
Federal employee on mobile/BYOD	Federal staff	Username/password + push (often)	Derived PIV or FIDO2/WebAuthn
Contractor on contractor-managed device	Contractors	Variable, often password + push	PIV-I or FIDO2/WebAuthn aligned with M-22-09
Partner agency federation	Cross-agency users	SAML/OIDC with variable assurance	Federated authentication with phishing-resistant primary; assurance level explicit in the assertion

Channel	Who authenticates	Typical legacy method	Phishing-resistant pattern (M-22-09 aligned)
Citizen-facing services (Login.gov, agency portals)	Public	Email/password + sometimes SMS	Phishing-resistant options (FIDO2/WebAuthn) per M-22-09; identity proofing at IAL2 for higher-assurance services
Privileged administrators	Federal admins	PIV + jump host	PIV + JIT elevation + cryptographic step-up + dual control on highest-risk
Defense workforce	DoD military and civilian	CAC	CAC continues; FIDO2 for non-CAC contexts
Mobile-device access to NIPRNet/SIPRNet	DoD users on mobile	Variable per service/agency	Derived CAC; FIDO2 in non-classified contexts
State and local law enforcement (CJIS)	Officers, dispatchers	Variable; many still username/password + token	Phishing-resistant MFA aligned with CJIS Security Policy
State agencies (tax, DMV, benefits)	State staff and citizens	Variable per state	Phishing-resistant for staff; phishing-resistant options for citizens; alignment with state-specific mandates
FedRAMP CSP support staff	CSP personnel with federal access	SSO + MFA per CSP policy	Phishing-resistant SSO; FedRAMP-aligned controls
Machine-to-machine across agency boundaries	Service-to-service across networks	mTLS or shared secrets	mTLS aligned with FIPS-validated cryptography; sender-constrained tokens; FIPS 140 modules
Citizen-facing voice/IVR (benefits hotlines)	Public callers	KBA (SSN, DOB)	Cryptographic caller verification where authenticator exists; KBA only for low-assurance unauthenticated read-only

Authentication patterns by use case

Pattern 1, federal employee on managed workstation

Goal: Continue PIV as the phishing-resistant primary; satisfy M-22-09 in agencies still on partial PIV adoption.

Approach: PIV at logon. PIV-aware applications (or PIV via federation through the agency IdP). For applications that cannot consume PIV directly, federated authentication where the IdP performs PIV and asserts an assurance claim.

Outcome: The federal-employee surface is phishing-resistant by construction. M-22-09 compliance for federal workforce is a configuration question, not an architectural one.

Pattern 2, federal employee on mobile or BYOD

Goal: Phishing-resistance on mobile and BYOD where smart-card readers are impractical.

Approach: Derived PIV per NIST SP 800-157 issued to a hardware-protected key store on the mobile device, or FIDO2/WebAuthn passkeys with appropriate identity binding. Mobile management and posture (MDM) compose with the cryptographic credential.

Outcome: The "M-22-09 except mobile" gap closes. Mobile workforce gets phishing-resistant authentication without depending on smart-card hardware.

Pattern 3, contractor on contractor-managed device

Goal: Phishing-resistance for contractors who cannot or do not have full federal-issued PIV.

Approach: PIV-I (PIV-Interoperable) for contractors with high-assurance binding, or FIDO2/WebAuthn for contractors at lower assurance levels with explicit identity binding. Federated authentication into agency systems with explicit assurance-level assertion in the SAML/OIDC payload.

Outcome: Contractors are part of the phishing-resistant baseline rather than a residual exception.

Pattern 4, citizen-facing services (Login.gov and agency portals)

Goal: Offer phishing-resistant options to the public, per M-22-09; bind authentication to identity proofing at appropriate IAL.

Approach: Passkeys on the citizen portal, with optional identity proofing at IAL2 for services requiring higher assurance (tax filing, benefits, healthcare). Phishing-resistant recovery so the recovery flow does not become the new attack surface. SMS removed from the chain.

Outcome: Citizens have a phishing-resistant option for federal interactions. Identity-fraud-driven attacks on benefits programs lose leverage on authenticated members.

Pattern 5, privileged federal administrators

Goal: Phishing-resistance plus JIT elevation plus dual control on the highest-risk operations.

Approach: PIV as primary. JIT elevation requiring fresh authentication (not session reuse) at elevation. Dual control on highest-risk operations: production system changes affecting agency-wide systems, IAM policy changes, mass data exports. Lockstep (in development) is designed to enforce this once it ships.

Outcome: Privileged credential compromise does not equal day-one impact. The audit trail makes incident reconstruction tractable.

Pattern 6, partner-agency federation

Goal: Cross-agency authentication that respects each agency's identity authority while ensuring uniform assurance.

Approach: SAML or OIDC federation with explicit AAL/IAL/FAL assertions in the assertion. The relying agency enforces minimum assurance properties for the function being requested.

Outcome: Cross-agency workflows do not silently downgrade to the lowest common denominator. Audit shows the assurance level used for each cross-boundary action.

Pattern 7, machine-to-machine across boundaries

Goal: Eliminate long-lived shared secrets on cross-agency and cross-boundary M2M paths.

Approach: Mutual TLS using FIPS-validated cryptography. Sender-constrained tokens (RFC 8705 mTLS or RFC 9449 DPoP). Cloud workload identity (IRSA, Workload Identity, Managed Identity in FedRAMP-authorized environments) where applicable. FIPS 140 cryptographic modules throughout.

Outcome: Long-lived service-account credentials disappear. Cross-boundary authentication composes into the FedRAMP and CMMC audit narrative.

For deeper M2M coverage, see M2M Authentication Without Secrets.

Pattern 8, state and local CJIS

Goal: Satisfy CJIS advanced authentication requirements for law enforcement and their contractors.

Approach: Phishing-resistant MFA aligned with NIST SP 800-63-4 AAL2 properties or higher. Hardware-bound credentials on officer-issued devices and on contractor-managed equipment. Audit and SIEM integration that supports CJIS Security Policy oversight.

Outcome: CJIS access becomes a controllable property of the architecture rather than a series of exceptions.

Pattern 9, voice/IVR for benefits hotlines

Goal: Reduce KBA-driven identity fraud on citizen-facing voice channels.

Approach: For citizens who have authenticated to the agency portal, a cryptographic caller verification ceremony when they call. KBA falls back only to read-only inquiries on unauthenticated callers.

Outcome: Vishing-driven benefits fraud against authenticated citizens collapses on the voice channel as well as the web.

ICAM lifecycle and the federal posture

Federal authentication is best understood inside the Federal ICAM Playbook lifecycle:

1. **Identity proofing** at IAL appropriate to the application. NIST SP 800-63-4 Part A defines IAL1, IAL2, IAL3.
2. **Enrollment** of the credential, binding the cryptographic identity to the proofed person.

3. **Credentialing** with PIV, derived PIV, FIDO2, or other phishing-resistant authenticator.
4. **Access management** including SSO, ABAC/RBAC, and policy enforcement.
5. **Federation** across agency boundaries with explicit AAL/IAL/FAL.
6. **Governance** including provisioning, deprovisioning, attestation, and audit.

The phishing-resistant authentication ceremony is one stage in this lifecycle; the others have to compose with it. Agencies that treat M-22-09 as "buy a passkey product" and skip the proofing, federation, and governance stages produce a brittle posture that fails the next IG review.

Anti-patterns to avoid

1. **Push-OTP MFA in agencies that haven't completed M-22-09.** Push is not phishing-resistant. The directive is explicit.
2. **Citizen-facing services with email-only recovery.** A compromised email becomes the citizen account compromise. Use phishing-resistant recovery.
3. **Federation without explicit AAL/IAL assertions.** A federated assertion that does not carry the assurance level lets the relying party drift into low-assurance access for high-assurance functions.
4. **Long-lived service-account credentials on cross-agency M2M paths.** The compromise of one creates lateral movement across boundaries.
5. **PIV on the workstation, no PIV-aware authentication on the application.** The application drops back to username/password and the PIV investment is wasted on that path.
6. **State/local programs that are CJIS-compliant on workforce and KBA-based on citizen voice channels.** Vishing-driven fraud follows the path of least resistance.
7. **CMMC compliance on the contract but not on the operating reality.** CMMC audits are increasingly real; identity controls are the most consistently flagged.
8. **Treating "Login.gov is mandatory" as the answer.** Login.gov is one phishing-resistant option for citizen-facing services; agencies still need agency-specific architecture for workforce, partner, and machine paths.

Key Takeaway

Authentication for federal, state, and local government has to satisfy a layered policy stack (M-22-09, NIST SP 800-63-4, FIPS 201-3, FedRAMP, CISA Zero Trust, ICAM, CJIS, IRS Pub 1075, CMMC, state mandates) on workforce, contractor, partner, citizen-facing, and machine paths. The phishing-resistant ceremonies that meet the bar are PIV/CAC and FIDO2/WebAuthn, with derived PIV (NIST SP 800-157) covering mobile and BYOD. The architecture that scales is PIV/CAC primary for federal workforce on managed devices, FIDO2/WebAuthn for partner and citizen access, derived PIV for mobile, and sender-constrained tokens on machine-to-machine paths, all wrapped in ICAM-aligned

identity governance across the lifecycle. The biggest deployment challenges are legacy systems, BYOD and partner contexts where PIV cards are impractical, and the citizen-facing surface where M-22-09 phishing-resistance options must be available.

FAQ

What does OMB M-22-09 require for federal authentication?

OMB M-22-09 (January 2022) directs federal agencies to use phishing-resistant MFA for federal staff, contractors, and partners by the end of FY24, and to enable phishing-resistant MFA options for public-facing systems where individuals interact with federal services. PIV and FIDO2/WebAuthn are explicitly identified as meeting the phishing-resistance bar. Push notifications, SMS, and TOTP do not meet it.

Are PIV and CAC the same as phishing-resistant MFA?

PIV (federal civilian) and CAC (DoD) cards built to FIPS 201-3 are phishing-resistant by design, the cryptographic ceremony is a smart-card challenge-response that does not rely on user-entered codes that can be replayed. They remain the gold standard for federal workforce. The challenge is mobility: PIV/CAC works well on workstations with smart-card readers and less well on mobile devices, BYOD, partners, and citizen-facing services. Derived PIV and FIDO2/WebAuthn fill those gaps.

What is derived PIV?

Derived PIV (NIST SP 800-157) is a credential cryptographically derived from a person's PIV credential, issued in software or to a hardware key on a mobile device. It carries the assurance of the original PIV identity proofing and binding while supporting form factors PIV cards cannot reach. Derived PIV is one of the cleanest paths to satisfy M-22-09 for mobile, BYOD, and partner workflows where PIV-card insertion is impractical.

How does FIDO2/WebAuthn fit into federal Zero Trust?

FIDO2/WebAuthn passkeys are explicitly named in M-22-09 as meeting phishing-resistance. CISA's phishing-resistant MFA fact sheet treats FIDO2/WebAuthn and PIV as the two phishing-resistant ceremonies. For partner integrations, contractor systems, citizen-facing services (including Login.gov), and mobile/BYOD workflows that PIV does not cover, FIDO2 fills the gap. Both can coexist; the mature posture supports PIV/CAC as the primary federal-employee credential and FIDO2 for contexts where smart-card-based ceremonies do not work.

Does FedRAMP require phishing-resistant MFA?

FedRAMP baselines incorporate NIST SP 800-53 controls including IA-2(1), IA-2(2), and IA-2(8) (replay-resistant authentication). Phishing-resistant MFA is the cleanest fit for the IA-2 series and aligns with the broader OMB M-22-09 federal Zero Trust direction. CSPs targeting FedRAMP Moderate or High should plan for phishing-resistant MFA on privileged and federal-facing access paths.

What does CJIS require for authentication?

FBI CJIS Security Policy requires advanced authentication for access to CJI (Criminal Justice Information). The 2022 update to the CJIS Security Policy (and subsequent revisions) explicitly require MFA, with a phased transition. Phishing-resistant MFA aligned with NIST SP 800-63 AAL2 properties or higher is the cleanest path for state and local law enforcement agencies and their contractors. Verify current CJIS Security Policy version with the CJIS APB and your state CSO.

What about state and local government?

State and local governments are increasingly held to similar bars by federal grant programs (CISA SLCGP), CJIS for law enforcement, IRS Pub. 1075 for tax data, and state-level cybersecurity statutes. The architecture is the same: phishing-resistant MFA on workforce, citizen-facing services, and partner integrations, with audit and SIEM integration that supports oversight. The funding constraints and legacy-system reality differ from federal; the technical bar increasingly does not.

References (public)

- OMB M-22-09: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
- NIST FIPS 201-3 (PIV): https://csrc.nist.gov/pubs/fips/201-3/final
- NIST SP 800-157 (Derived PIV): https://csrc.nist.gov/pubs/sp/800-157/final
- NIST SP 800-63-4: https://csrc.nist.gov/pubs/sp/800/63/4/final
- NIST SP 800-53 Rev. 5: https://csrc.nist.gov/pubs/sp/800-53/r5/final
- FedRAMP: https://www.fedramp.gov/
- CISA Zero Trust Maturity Model: https://www.cisa.gov/zero-trust-maturity-model
- CISA, Implementing Phishing-Resistant MFA: https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
- Federal ICAM Playbook: https://playbooks.idmanagement.gov/
- FBI CJIS Security Policy: https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center
- IRS Publication 1075: https://www.irs.gov/pub/irs-pdf/p1075.pdf
- CMMC 2.0: https://dodcio.defense.gov/CMMC/

- CISA SLCGP: https://www.cisa.gov/state-and-local-cybersecurity-grant-program
- DoD STIGs: https://public.cyber.mil/stigs/

Related reading

- Compliance Mapping: NIST and CISA
- Phishing-Resistant Web Authentication
- M2M Authentication Without Secrets
- Recovery and Fallback Playbook
- Lockstep: Dual Control
- Omnichannel Authentication
- Enterprise Passwordless Vendors Compared