HIRSCH ▸ SOLUTIONS BRIEF

Tackling Cybercrime in the U.S. Federal Government with Hardware Security Keys

The Federal Government, Data Security, and Cyber Threats

The U.S. federal government continues to be a high-profile target for cyber threats, facing an evolving landscape of ransomware attacks, state-sponsored cyber warfare, and AI-driven phishing attempts. In 2023 alone, federal agencies reported thousands of cybersecurity incidents, reinforcing the need for strong authentication measures.

The Cybersecurity and Infrastructure Security Agency (CISA) has doubled down on Zero Trust Architecture (ZTA) as a guiding principle for all federal agencies. The Office of Management and Budget's OMB M-22-09 mandates phishing-resistant multi-factor authentication (MFA) across federal systems, emphasizing the need for FIDO2-based security keys.

Evolving Cybersecurity Challenges

- **Rise of AI-driven phishing attacks:** Attackers are leveraging AI to bypass traditional authentication methods, making hardware-based security keys critical.
- **Cloud adoption and identity security:** Federal agencies now store over 60% of their sensitive data in the cloud, yet many still lack full encryption and secure authentication protocols.
- **Quantum computing threats:** Agencies are preparing for the impact of quantum computing on encryption standards, driving interest in post-quantum cryptography-ready security solutions.

Strengthening Federal Identity Security

To address these concerns, agencies are integrating modern authentication solutions, including:

- **Common Access Card (CAC) and Personal Identity Verification (PIV):** Secure smart cards used in physical and logical access control.
- **FIDO2 Security Keys:** Providing phishing-resistant authentication aligned with federal Zero Trust policies.

Understanding Smart Cards, CAC, PIV, and FIDO2 Security Keys

U.S. Federal Government Smart Card Programs

Smart cards remain the gold standard for federal identity security. The U.S. government has expanded the use of CAC/PIV credentials across defense, civilian agencies, first responders, and transportation security personnel.

FIDO2 Adoption in Government

With the login.gov initiative, the U.S. General Services Administration (GSA) is pushing for stronger authentication across all government portals. FIDO2 security keys have emerged as a preferred solution for phishing-resistant, passwordless authentication.

Recent government initiatives include:

- **NIST 800-63 updates**: Reinforcing phishing-resistant MFA as a requirement.
- **Federal Zero Trust Strategy (OMB M-22-09):** Mandating FIDO2 security keys for government workers and contractors.
- **CISA's Zero Trust Maturity Model:** Encouraging agencies to integrate hardware-backed authentication.

Hirsch: The First to Deliver FIPS 140-3 Security Keys

Introducing the Most Secure, FIPS 140-3 Validated MFA Key

- First manufacturer to achieve FIPS 140-3 certification for government-grade authentication
- Meets the highest federal security standards for strong authentication
- TAA compliant and independently tested for government and defense applications
- Designed for mission-critical environments where security is non-negotiable

Indestructible Protection. Anywhere, Anytime.

- IP68-rated for extreme durability, built for defense, field ops, and secure workplaces
- Tamper-resistant, water-resistant, and designed to withstand extreme temperatures
- Ensures compliance for remote workers, first responders, and high-security personnel

Cost-Effective Without Compromise

- More affordable than competing FIPS 140-3 solutions without sacrificing security
- Eliminates reliance on passwords—stronger, faster, phishing-resistant authentication
- Reduces risk while maintaining federal compliance (NIST, FedRAMP, CISA)

uTrust FIDO2 GOV Security Keys

Hirsch's FIDO2 Security Solutions

Hirsch's uTrust FIDO2 GOV Security Keys deliver:

- FIPS 140-3 and NIST compliance
- Multi-protocol support (FIDO2, PIV, OTP, PGP)
- Phishing-resistant authentication for high-security environments

Federal agencies must prioritize phishing-resistant authentication to secure their systems against evolving threats. Hirsch's uTrust FIDO2 GOV Security Keys offer the highest assurance levels to protect federal identities, credentials, and access control.

Visit hirschsecure.com or call +1.888.809.8880 to request a demo.

Sources:

https://www.rsa.com/wp-content/uploads/meeting-presidential-mandates-with-rsa-id-plus-phishing-resistant-mfa-for-federal-agencies-rsa-solution-brief.pdf

https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

HIRSCH

SOLUTIONS BRIEF