CYBER

IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (ICAM)

Enterprise-level services for mitigating digital identity risk and demonstrating federal compliance

Harmonize your enterprise-wide approach to identity governance, architecture, and acquisition with Peraton's ICAM services. Elevating your organization's digital transformation strategy to improve the trust and safety of digital interactions and business transactions with the public across is critical to digital service delivery. Shift your operating model beyond simply managing access inside or outside of your organization's perimeter to using identity as the foundation for managing risk.

ICAM IS ESSENTIAL TO SECURITY

Digital channels are routinely used to conduct business with the public and other governments. Organizations need robust ICAM to manage digital or electronic identities, especially in today's climate where data breaches are commonplace, and defending against cyberattacks is more critical now than ever. The rise of synthetic identity, based on a combination of fabricated data with real identity attributes, is a growing source of fraud for both businesses and government.

Peraton ICAM management services help enterprises utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation—all while adhering to mandated ICAM policies.

BENEFITS

- **Identify sensors, monitor devices, and manage access to sensitive/ non-sensitive data**
- **Manage risk, meet mission success, and provide secure services to the pubic**
- **Shift focus from a network-based perimeter to a risk-based ICAM approach to meet the requirements of cloud and mobile devices, while monitoring for insider threat and other malicious activities**
- **Meet the strategic, technical and operational ICAM challenges presented by the Cloud Smart strategy to maximize the security of your cloud investment**

According to the Office of Management and Budget (OMB) policy memorandum M-19- 17, each agency must manage the risk to services and public user data at a level equal to the risk of the digital offering as well as to the sensitivity of the data collected.

National Institute of Standards and Technology's (NIST) Digital Identity Guidelines provides specific guidance related to the digital id entity risk (inclusive of privacy) that agency relying parties apply while executing all relevant Risk Management Framework (RMF) life cycle phases.

Homeland Security Presidential Directive 12 (HSPD-12) and phase 2 of the Continuous Diagnostic and Mitigation (CDM) program are incorporated with M-19-17.

Navigating through these policies remains a challenge. The adoption of derived personal identity verification (PIV) credentials for mobile devices and cross-government identity federation and interoperability across all federal agencies further advances the HSPD-12 policy to reduce identity fraud and protect personal privacy.

Our approach to risk-adaptive assessments during authentication and authorized access aligns CDM with HSPD-12 to curtail these challenges and enable mission delivery through improved ICAM.

PERATON'S ICAM SERVICES SOLVE THE FOLLOWING PROBLEMS

User-password fatigue

Peraton issues PIV cards as a means of access containing cardholder specific access, with appropriate security levels for all applicable federal applications; with no password necessary.

Slow administrative access application management

We design agile solutions and provide risk-based adaptive authentication, instant authorization or revocation checkpoints, and easier access to shared resources, applications, and facilities.

Lack of user compliance visibility

Peraton's ICAM services help agencies adjudicate claimed identities, manage and maintain credentials, and administer polices for access-control decisions and agency resource enforcement.

Inability to manage access across devices

Peraton evolves HSPD-12, CDM, and federal ICAM architecture to provide digital identities for Internet of Things (IoT) devices and robotic process automation (RPA) tools across enterprise, mobile, and cloud environments.

Tedious application integration maintenance

We incorporate automated technology (e.g., IoT and RPA) to initiate updates.

OUR APPROACH

Before delivering digital interactions and business transactions with the public, we can provide the following assessments to make sure you establish processes based on the digital identity risk and associated assurance levels of NIST Digital Identity Guidelines for Digital Identity Risk Management (DIRM).

ICAM transformation assessment

A higher-level, business-focused, three to four week assessment. Helps identify the protection level required within your organization to protect your assets and data, and enable the use of ICAM to meet your agency's mission based on OMB guidance.

ICAM DIRM assessment

A more detailed, technical risk assessment based on the NIST SP 800-63-3 Digital Identity Guidelines and NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations.

Peraton's ICAM services utilizes DIRM, which harnesses artificial intelligence technologies to generate risk scores of the identity subject's behavior from the moment they sign on and continuously monitored throughout their interactions with your IT environment.

We provide higher assurance levels of identity to provide the risk threshold to grant or deny actions requested by the identity subject, as well as risk-based adaptive authentication methods to provide an opportunity for the user to lower their risk score.

PROVEN RESULTS

- Peraton has quickly personalize, provision, and manage nearly 7 million active credentials for federal enterprise employees and contractors that comply with HSPD-12
- We support more than 100 federal agencies in vetting, issuing PIV or common access cards (CAC), and integrating those credentials into local and physical access control systems—most notably, we've delivered more than 30,000 derived CAC credentials to mobile devices for a Department of Defense customer based on the Defense Information Systems Agency's Purebred architecture
- We established an identity verification service for an independent federal agency so their customers can opt-in for remote identity proofing for enhanced services from this agency's web portal
- We built an iOS mobile app for in-person identity proofing when remote identity proofing fails. Today, this iOS app is used at more than 3,000 retail locations across the country, with more than 10 million customers having used this identity verification services
- Our support for a major federal identity program includes a suite of applications deployed at hundreds of locations, offering sufficient commonality and flexibility to meet the needs of most federal users. These capabilities have helped the program become the largest civilian federal credentialing program, serving over 85% of civilian federal agencies

ABOUT PERATON

Peraton has deep experience in ICAM— designing, engineering, implementing, and delivering large-scale complex solutions. Our company has a storied legacy and combined 50 years of experience, with more than 4,600 security and ICAM professionals to help government customers improve the trust and safety of digital transactions with the public.

Scan the QR code to learn more at peraton.com/capabilities/cyber

Peraton