Safeguard Agency Missions with a Comprehensive ICAM Solution Set

There's a cyber war being waged against federal agencies. Today's threatscape involves persistent attacks architected to forge past traditional firewalls via application and identity breach. As agencies embrace the cloud, IoT, and other digital tools for innovation, a treasure trove of credential data is generated that can be used to breach government systems. Now, the cybersecurity perimeter has no boundaries and secure access must be supported anywhere, anytime, from any user or device.

Safeguarding agency credentials is only possible when there is insight into identity data. Yet barriers to visibility exist. For example, disparate security solutions and a lack of federated data sources like active directory and LDAP create silos of identity data that can't be shared across agencies or departments. A cybersecurity skills gap and reliance on manual security tools creates a false sense of security that leads to privacy violations and identity breach. These challenges come at a time when the OMB has outlined hardened identity, credential, and access management (ICAM) policies based on zero trust and architected to bring personal identity verification (PIV) and common access cards (CAC) into the digital world.

Align with New ICAM Requirements

Agencies are being mandated to modernize their ICAM capabilities to support secure, modern agency operations, in compliance with NIST standard 800-63 Foundation for Identity. This includes the ability to manage access based on contextualized insight into users, privileges, and devices of both employees and contractors. Agencies must ensure deployed ICAM capabilities are interoperable across all levels of government. They must also outline agency-wide performance expectations for security and privacy risk management throughout the identity lifecycle.

71 OUT OF **96** federal agencies had programs at high risk for cyberattack according to a 2018 OMB assessment.[1]

Protect Identities Inside—and Outside Agency Perimeters

To meet these ICAM requirements, federal agencies need to shift their operating model beyond the perimeter, safeguarding privacy, identity, and access with governance and federation. Core to ICAM success is the ability to identify, credential, monitor, and manage users who access federal resources, information systems, facilities, and secured areas. Policies and controls must be enforced to prevent entitlement creep and unauthorized access.

Goals include:

- **Zero Trust:** Trust nothing inside or outside federal agency perimeters and force verification to authenticate users via SSO and MFA.
- **ICAM Governance and Administration:** Enforce the principle of least privilege to ensure users only have access to the resources needed to complete their job.
- **Federation First**: Consolidate authoritative data sources to create a more efficient system.

Easing Identity Management and Governance

Federal agencies can accelerate ICAM compliance with a best-of-breed, integrated, and automated solution set designed to close security gaps. Carahsoft Solutions Portfolio simplifies ICAM with a multi-faceted approach involving security, governance, automation, controls, and federated identity based on virtualization. Carahsoft's ICAM solution set is available through its reseller partners on a variety of contracts, including Carahsoft's GSA Schedule 70, SEWP V, NASPO ValuePoint, National IPA, and numerous state and local contracts.

Identity Access Management (IAM): Okta is a FedRAMP Authorized cloud identity solution that protects and enables federal employees, contractors, and partners with advanced, contextualized identity access management. It goes beyond simple access cards and passwords to grant or deny access based on a host of factors, not just roles, to include location, device, type, and timing of a request.

- Single Sign On
- Multi Factor Authentication
- Lifecycle Management
- Universal Directory
- API Access Management
- Advanced Server Access

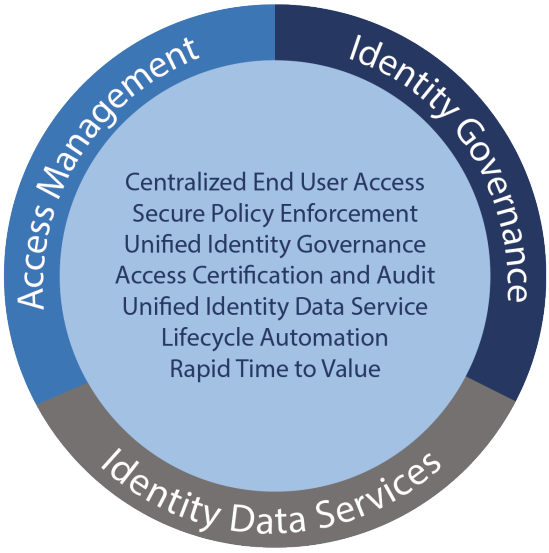
Identity Governance and Administration: SailPoint safeguards applications, users, and data with governance and compliance. It helps agencies manage and document user behavior with tools for employee roll-off risk management with managerial oversight, access requests, access certifications, separation of duties, entitlement provisioning, and password management.

- Direct Connector between Okta and SailPoint
- Centralized Visibility
- User Self-Service
- Governance Model
- Audit and Access Certification
- Reporting and Analytics

Identity Data Services: Radiant Logic works as an aggregator to eliminate silos of identity information. It connects all the places identity exists to provide a rich profile of identity information that can be shared with Okta and SailPoint for real-time decision making. Through virtualization, Radiant Logic consolidates and rationalizes all identity data to create a global list of users with no duplicates which speeds up deployments, reduces integration costs, and provides flexibility for dynamic environments.

- Active Directory Consolidation
- Federated Identity and Directory Services
- Authoritative Data Source Consolidation
- Unified Identity Infrastructure
- SSO Integration

okta



SailPoint

RADIANT LOGIC

Siloed identity data spread across the federal enterprise puts ICAM initiatives at risk and consumes agency resources with manual oversight that's error-prone and out of alignment with new ICAM requirements. Carahsoft Solutions Portfolio simplifies the task of validating identity and access control across users, devices, locations, and roles. It enhances privacy without compromising service delivery, for secure, compliant, modernized operations that keeps agencies focused on mission delivery.

Contact Carahsoft to learn more.

SIMPLIFY ICAM COMPLIANCE

Code-free ICAM integration

Secure data and application access

High availability and scalability

Federated access, centralized control

About Carahsoft

Carahsoft Technology Corp. is The Trusted Government IT Solutions Provider®. As a top-ranked GSA Schedule and SEWP Contract holder, Carahsoft is the largest government partner, distributor and master government aggregator for many of its best-of-breed vendors, managing their public sector reseller networks and driving demand for their offerings.

carahsoft®

CARAHSOFT TECHNOLOGY CORP. | 11493 SUNSET HILLS ROAD | SUITE 100 | RESTON, VA 20190 | 703.871.8500 | WWW.CARAHSOFT.COM

1. FCW, Senate Turns up a Decade of Federal Cybersecurity Failure, June 26, 2019