carahsoft® The Trusted Government IT Solutions Provider®

Identity and Access Management Buyer's Guide **for Government**

Discover modern identity and access management solutions that help agencies operate more securely and efficiently.

FEATURING: ***Solution Areas*** • ***Policies & Executive Orders*** ***Contract Vehicles*** • ***Upcoming Events*** carahsoft. The Trusted Government IT Solutions Provider®

Securing Government Systems with Trusted Identity and Access Management Solutions

Explore Carahsoft's extensive portfolio of identity and access management solutions designed to protect government systems by ensuring the right users have the right access at the right time. Our IAM offerings enable organizations to reduce risk and maintain compliance using proven technologies from leading vendors.

Discover identity and access management vendors that align with your organization's goals, offering capabilities such as Identity Governance, Privileged Access Management, Identity Proofing and Verification, and Machine Identity and AI Management.

Learn More:
www.carahsoft.com

Welcome to the Identity and Access Managment Buyer's Guide!

The Identity and Access Management (IAM) market within the public sector is unique in its complexity, scale, and mission-critical nature. Government agencies must navigate stringent regulatory requirements, high assurance identity needs, and serve an incredibly diverse user base which includes federal employees and contractors as well as citizens accessing essential services. With the growing adoption of zero trust architectures, digital identity has become the cornerstone of secure modernization efforts across defense, civilian, and state and local government organizations.

The core challenge this market faces is enabling trusted access. This means verifying who is accessing *what, when*, and from *where* in a landscape increasingly defined by cloud services, remote work, and persistent cyber threats. Solving this challenge is not just about technology, but about building secure, scalable, and user-friendly identity ecosystems that can support everything from cross-agency collaboration to fraud prevention and secure citizen engagement.

Carahsoft plays a critical role in helping government agencies meet these demands by serving as the trusted government IT solutions provider. Through strategic partnerships with leading identity vendors and a deep understanding of public sector procurement, compliance, and mission requirements, Carahsoft helps agencies identify, acquire, and deploy the identity solutions they need to meet today's security and access challenges. From facilitating market education to streamlining contract vehicles, Carahsoft empowers agencies to build secure, identity-first architectures that protect data and support the public good.

Steve Jacyna
Sales Director, Carahsoft

Table of Contents:

Identity and Access Management Solutions

As Government IT modernization advances and interconnectivity initiatives expand, the need for identity and access management (IAM) solutions is more crucial than ever. Unauthorized access and identity-based attacks are on the rise across the Public Sector, posing significant risks to critical systems, cloud applications, and sensitive data.

The dedicated IAM team at Carahsoft specializes in providing modern access control and identity security solutions to Federal, State, and Local Government, as well as Education and Healthcare organizations. We aim to help agencies secure user identities, streamline

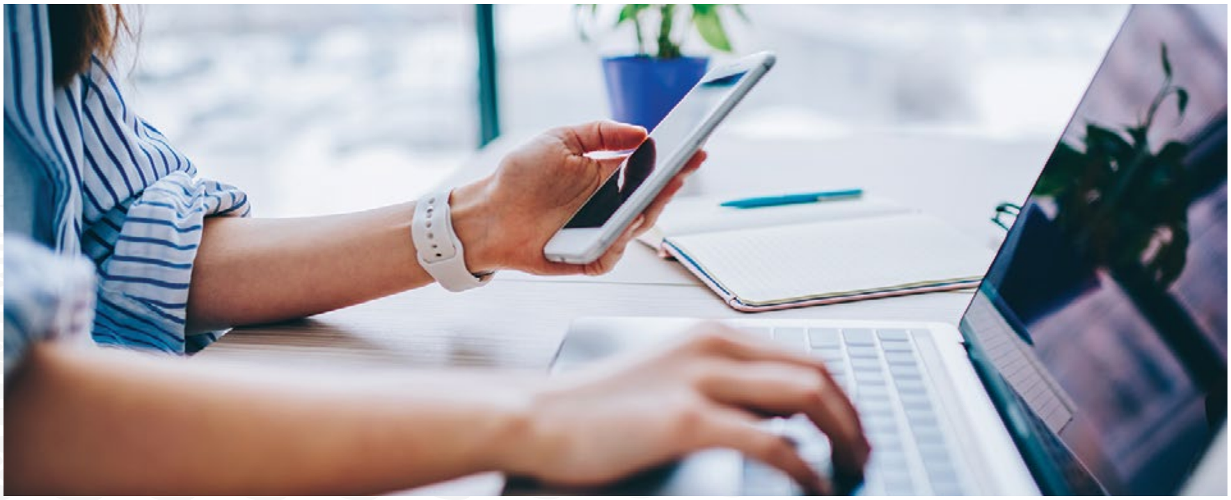
authentication, and enable Zero Trust architectures with proven technologies. Our certified Government Product Specialists assist customers in building comprehensive IAM solution stacks to meet evolving Government compliance and security requirements.

Carahsoft has established strategic, long-term relationships with the industry's leading IAM and identity security providers to offer Government entities proven, cost-effective solutions for identity governance, privileged access, single sign-on, and multifactor authentication—ensuring agencies can protect their most critical resource: trusted digital identities.

Identity & Access Management

Identity and Access Management Solutions empower IT teams to enhance access security by ensuring that only authorized personnel with privileged access gain entry to organizational resources. Reinforce your department's security framework and streamline access with innovative IAM solutions. Choose a provider to learn more about their products and services.

okta	PingIdentity	AXIAD	Beyond Identity	IDENTITY AUTOMATION	intercede
HID	BeyondID	KEEPER	yubico	RSA	RADIANT LOGIC
Aquera	THALES	uberether	1Password	CyberFOX	DASHLANE
imprivata	KEYFACTOR	nuggets	RESILIANT	semperis	SESSION GUARDIAN
ENTRUST					



Identity Governance

Identity Governance Solutions help organizations strengthen accountability and compliance by ensuring the right users have the right access at the right time. Through automated oversight and continuous monitoring, these tools enable agencies to manage roles, enforce least-privilege policies, and maintain visibility across user lifecycles. Reinforce your department's security posture and streamline compliance with innovative Identity Governance solutions. Select a provider to learn more about their products and services.

SailPoint | SAVIYNT | RESILIANT | veza | EchoMark | okta
opentext | SecuPi | SESSION GUARDIAN | SILVERFORT | SpyCloud | ENTRUST

Privileged Access Management

Identity Governance Solutions help organizations strengthen accountability and compliance by ensuring the right users have the right access at the right time. Through automated oversight and continuous monitoring, these tools enable agencies to manage roles, enforce least-privilege policies, and maintain visibility across user lifecycles. Reinforce your department's security posture and streamline compliance with innovative Identity Governance solutions. Select a provider to learn more about their products and services.

BeyondTrust | CYBERARK THE IDENTITY SECURITY COMPANY | Delinea | KEEPER | OLERIA | okta
opentext | ENTRUST

Identity Proofing and Verification

Identity Proofing and Verification solutions enable organizations to confidently confirm that users are who they claim to be before granting access to systems or data. Using advanced authentication methods such as biometrics, document validation, and real-time fraud detection, these solutions reduce identity-related risks and support compliance with federal security standards. Strengthen your department's digital trust and streamline user onboarding with innovative Identity Proofing and Verification solutions. Explore below to discover leading Identity Proofing and Verification products and services.

Socure | LexisNexis® RISK SOLUTIONS | 1KOSMOS | NextgenID | PingIdentity. | CertiPath
TRUSONA | ID.me | THALES | ENTRUST

Machine Identity and AI Management Solutions

Machine Identity and AI Management Solutions help organizations secure and manage the identities of applications, services, and AI systems that connect and communicate across digital environments. By automating certificate management, credential rotation, and policy enforcement, these solutions ensure every machine identity is authenticated, authorized, and continuously monitored. Strengthen your department's cybersecurity posture and maintain trust across automated systems with innovative Machine Identity and AI Management solutions. Select a provider to learn more about their products and services.

CYBERARK® THE IDENTITY SECURITY COMPANY™ | okta | PingIdentity. | veza® | SILVERFORT | SailPoint.
Delinea | ENTRUST

PingIdentity.
Trust Every Digital Moment
Secure every identity.
Power every digital experience.
Trust Starts Here

Policies and Executive Orders

OMB Memorandum M-22-09

On January 26, 2022, The Office of Management and Budget (OMB) released Memorandum M-22-09, which outlines a government-wide strategy to transition all federal agencies to a Zero Trust Architecture (ZTA) by the end of Fiscal Year 2024. The memorandum mandates a shift from perimeter-based security models to a framework that assumes no implicit trust and requires continuous verification of users, devices, and applications.

The strategy is structured around five key pillars, including: Identity, Devices, Networks, Applications and Workloads, and Data, supported by cross-cutting themes of visibility, automation, and governance. Agencies are required to submit implementation plans, designate zero trust leads, and collaborate with the Cybersecurity and Infrastructure Security Agency (CISA) to ensure consistent progress.

A central focus of the memorandum is the enhancement of identity and access management across the federal enterprise. Agencies must implement centralized identity systems capable of integrating with applications and platforms, enforce phishing-resistant multi-factor authentication (MFA) at the application layer, and incorporate device-level signals into access decisions. The strategy emphasizes the use of enterprise-managed identities, consolidation of authentication systems, and adoption of modern, open standards to support interoperability. Additionally, agencies are encouraged to transition toward attribute-based access control (ABAC) models to enable dynamic, risk-based authorization decisions. These measures aim to reduce the attack surface, improve detection of anomalous behavior, and ensure secure, seamless access to federal systems and data.

carahsoft. ENTRUST

Securing Public Trust: Multi-Factor Authentication as the Frontline Defense for Government Systems

Protecting sensitive data and citizen services through layered identity verification and layered access controls

Phishing-Resistant Passwordless MFA

Entrust provides modern authentication methods, including passkeys, device-bound biometrics and smart credentials that help prevent phishing attacks and credential theft. Governments can deliver secure, digital-first access to critical services without relying on vulnerable passwords.

Adaptive Risk-Based Authentication

Entrust's fully customizable adaptive risk engine evaluates device, location and behavioral signals in real time. Low-risk activity flows without interruption, while medium- and high-risk scenarios trigger additional verification or block access. This ensures strong fraud prevention while keeping the user experience smooth for legitimate activity.

Integrated Identity Lifecycle Security

From onboarding through daily access, Entrust secures the full identity journey. AI-driven signals, biometrics and MFA protect enrollment, digital signing and credential recovery, ensuring that trusted identities are maintained across every stage of engagement.

Global Reach and Proven Scale

Entrust protects over 100 million workforce and consumer identities, secures 690K websites and encrypts 24M+ SWIFT messages daily. Their MFA solutions are trusted by governments and enterprises in 150+ countries.

Compliance & Operational Efficiency

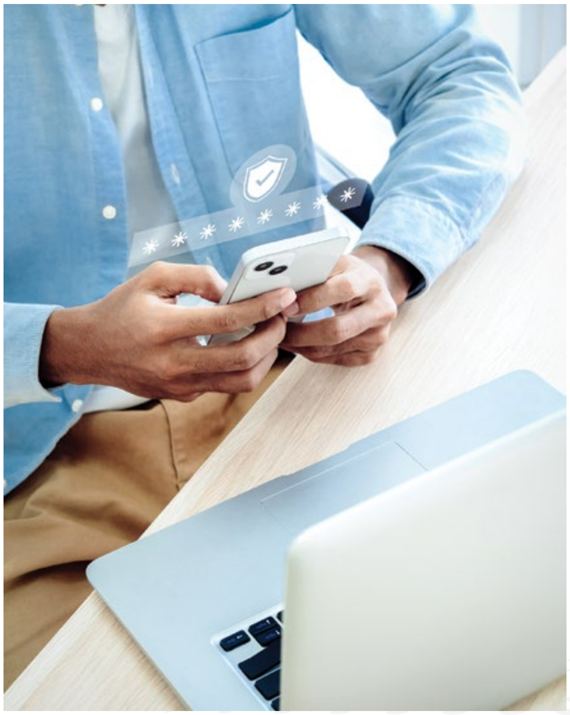
Regulatory compliance is non-negotiable, and managing multiple identity vendors drives unnecessary cost and complexity. Entrust delivers one complete platform with no-code workflows and a full suite of authenticators and signals, helping agencies meet mandates while streamlining operations at scale.

Learn More:
www.carahsoft.com/entrust

OMB Memorandum M-19-17

OMB 19-17, titled Enabling Mission Delivery through Improved Identity, Credential, and Access Management (ICAM), was released May 21, 2019. Established a comprehensive federal policy framework to modernize and secure digital identity practices across executive agencies. Recognizing the evolving technological landscape and the increasing complexity of digital interactions, the memorandum mandates a shift from perimeter-based security models to identity-centric risk management. It emphasizes the need for agencies to adopt a unified ICAM strategy that aligns with the Federal Identity, Credential, and Access Management (FICAM) architecture, integrates with the Continuous Diagnostics and Mitigation (CDM) program, and supports secure, efficient access to federal resources.

A central component of the memorandum is the enhancement of identity and access management practices. Agencies are required to implement standards-based identity proofing, credentialing, and access control mechanisms, including the use of Personal Identity Verification (PIV) credentials and derived credentials for logical and physical access. The policy mandates the adoption of NIST Special Publication 800-63 for digital identity guidelines and encourages the use of federated identity solutions to promote interoperability across agencies. Additionally, agencies must establish governance structures, maintain comprehensive ICAM roadmaps, and ensure lifecycle management of digital identities for both human and non-person entities. These measures aim to strengthen trust, improve operational efficiency, and safeguard federal systems and data from unauthorized access.



1KOSMOS

Credential Service Provider (CSP)

1Kosmos transforms onboarding with secure, self-service identity verification and a privacy-preserving digital wallet—binding verified identity to phishing-resistant authenticators for streamlined access. The 1Kosmos CSP proactively blocks identity fraud and account takeovers, protecting users while ensuring a frictionless user experience.

Mobile Device or Laptop:

Self-service identity verification and phishing-resistant authentication anywhere, anytime, and with any device.

Flexible Deployment:

1Kosmos delivers deployment flexibility, allowing organizations to seamlessly integrate any CSP component—verification, wallet, or authentication—meeting them exactly where they are and evolving alongside their needs.

FR

1Kosmos is the only FedRAMP High authorized, Kantara full-service NIST 800-63-3 and FIDO2 certified digital identity wallet solution.

Scan me to learn more

1kosmos.com

NIST 800-63-4

The NIST SP 800-63-4 Digital Identity Guidelines provides a comprehensive framework for federal agencies to establish, manage, and authenticate digital identities in alignment with the Federal Information Security Modernization Act (FISMA) and Office of Management and Budget (OMB) policies. The guidelines define assurance levels for identity proofing (IAL), authentication (AAL), and federation (FAL), and introduce a risk-based Digital Identity Risk Management (DIRM) process. Agencies are required to assess the impact of identity-related failures, select appropriate assurance levels, and tailor controls to address privacy, usability, and threat resistance. The guidelines emphasize continuous evaluation and improvement, requiring agencies to monitor performance metrics, user experience, and evolving threats.

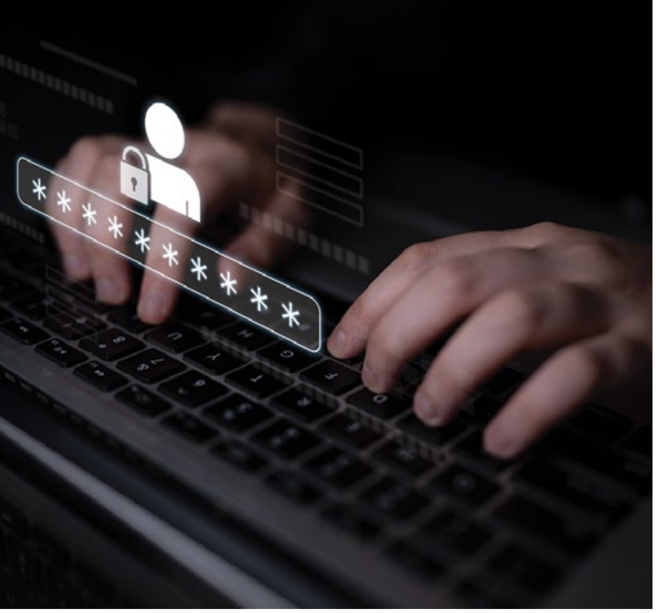
Federal agencies must implement robust identity and access management practices, including phishing-resistant multi-factor authentication, secure authenticator binding, and federated identity architectures. Agencies are expected to document their identity systems through a Digital Identity Acceptance Statement (DIAS), coordinate with cybersecurity and fraud prevention teams, and ensure compliance with privacy regulations such as the Privacy Act and NIST's Privacy Framework. The guidelines also mandate integration with enterprise risk management processes and encourage the use of AI/ML responsibly within identity systems. Overall, SP 800-63-4 sets a high standard for secure, interoperable, and user-centric digital identity management across the federal government.

Executive Order 14028

Executive Order 14028: Improving the Nation's Cybersecurity, released in May 2021, is the most influential piece of federal Zero Trust policy yet. The executive order directed agencies to implement Zero Trust Architecture and strengthen the software supply chain. It required service providers to report cyber incidents and threat information that could impact the government, instructed the NIST to publish standards for testing of vendor software source code, and created cybersecurity event log requirements for Federal departments and agencies.

Executive Order 14144

Executive Order 14028, published on May 12, 2021, provided essential foundational steps to strengthening cybersecurity within the United States and emphasized the importance of Zero Trust Architecture (ZTA). Building upon EO 14028, The Biden Administration issued Executive Order 14144 Strengthening and Promoting Innovation in the Nation's Cybersecurity on January 16th, 2025, to address the rapid evolution of cyber threats, notably those from foreign nations. The order is focused on defending digital infrastructure, securing the services and capabilities most vital to the digital domain, and building the capabilities necessary to address key threats.



Success Stories

As mission requirements evolve, agencies are taking a more strategic approach to managing identities and access. Explore how government organizations have achieved their goals through Carahsoft's identity and access management vendor ecosystem.

CYBERARK®
THE IDENTITY SECURITY COMPANY®

U.S. Education Authority delivers business-class identity security with CyberArk

The Chico Unified School District (CUSD) safeguards digital resources across 21 schools, serving 12,000 students, and manages over 23,000 devices with the CyberArk Identity Security Platform. Upon implementation, the district enhanced protection against cyber threats, ensured secure access for users, and maintained the privacy and integrity of student and staff information.

The Challenge:

CUSD is a high-performing public school district in California's Sacramento Valley, serving over 12,000 students and employing 1,800 staff. With a small IT team, the district must manage identities and access across a sprawling environment of 100 servers, 3,500 Windows devices, and more than 20,000 Chromebooks. Like many educational institutions, CUSD faces increasing cyber threats, limited resources, and growing pressure to secure valuable student data.

John Vincent, Director of Technology at Chico Unified School District, noted that schools have become prime targets for ransomware and identity-based attacks. To address this growing threat, the district needed to resolve vulnerabilities in password management, third-party access, and remote work environments. Rising cybersecurity insurance costs further motivated CUSD to adopt a more robust and layered security strategy.

The Solution:

CUSD implemented multiple capabilities of the CyberArk Identity Security Platform to transform its approach to privileged access management, workforce access, and vendor security. The district strengthened password policies, deployed adaptive multi-factor authentication (MFA), and began vaulting credentials to reduce risk and improve visibility.

CyberArk's platform enabled CUSD to enforce least privilege access, monitor privileged activity, and streamline secure access for staff and vendors. The district also recognized the growing importance of identity security in the age of AI, where false identities can be generated from publicly available data. CyberArk's tools helped CUSD build a multi-layered defense strategy that aligned with cybersecurity best practices and insurance requirements.

Key Takeaways:

CyberArk helped Chico Unified School District secure access to sensitive student and staff data, manage privileged credentials across thousands of devices, and meet cybersecurity insurance standards. The platform's ease of use and layered security approach empowered the district's small IT team to protect its environment efficiently and proactively.with hidden escalation paths. It also offers the team pertinent next steps for improving overall identity hygiene and shrinking the attack surface and enables them to ensure appropriate security controls are applied wherever needed.

BeyondTrust

Large State Entity Adopts Identity Security Insights to Reveal Data Across Domains and Reduce Risk

A large state entity has focused on strengthening identity security for years, including investing in BeyondTrust's Remote Support, Privileged Remote Access, Endpoint Privilege Management and Password Safe solutions. As the team continued to mature their approach to identity security, they faced the growing need to gain more holistic visibility and control over all the parts of their expanding identity landscape.

The Challenge:

Without a holistic view of their entire identity landscape, areas of their environment remained hidden and unmanaged—particularly accounts that were seemingly insignificant. However, many of these ostensibly low-privilege accounts posed risk to the organization, as they had indirect or hidden privilege pathways, which could also enable the ability to move laterally and gain deeper access.

Additionally, the environment contains over 5,000 non-human identities, many of which were unmanaged/unknown. Many of their service accounts and other machine identity credentials were static and hadn't been changed in over a decade. The lack of visibility across platforms also made it challenging to provide an audit trail that incorporated all identity data.

The Solution:

BeyondTrust's Identity Security Insights provided enhanced visibility, enabling the team to understand which of their over 477K accounts and 60K human identities were not under the purview of existing solutions. The solution revealed the following data on other hidden risk within the agency's environment:

- 17,000 compromised passwords that were not considered directly privileged and, therefore, were not subject to controls such as frequent rotation because the accounts were not recognized as highly privileged
- 31,000 password collisions (multiple accounts with the same password)
- 124,000 dormant accounts

Key Takeaways:

By adding a discovery and visibility dimension to the agency 's overall identity security strategy, Identity Security Insights has enhanced the depth of existing solutions. It has enabled the team to understand the True Privilege™ of every account—including low-privilege accounts with hidden escalation paths. It also offers the team pertinent next steps for improving overall identity hygiene and shrinking the attack surface and enables them to ensure appropriate security controls are applied wherever needed.

Beyond Identity
FOR GOVERNMENT

Beyond Identity

Identity Defense for Government. Now FedRAMP Moderate, in Process for High

Identity is your largest attack surface.
Beyond Identity turns it into your strongest defense.

Instead of detecting security incidents after they occur, Beyond Identity prevents adversaries from taking advantage of weak identity protections to gain access in the first place. Beyond Identity eliminates all weak access controls with device-bound credentials and continuous, adaptive access controls that can't be intercepted, spoofed, or replayed.

Stop Attacks Before Access Is Granted

BEYOND IDENTITY PREVENTS:

- Phishing
- Push Bombing
- Brute Force
- Credential Stuffing
- Credential Reuse
- Token Replay
- Device Spoofing
- Unauthorized Unmanaged Device Access
- Adversary-in-the-middle
- Social Engineering
- AI Impersonation

Align With Government-Wide Security Directives

Built to meet the latest mandates without deployment complexity:

- Executive Order 14028
- OMB Memorandum M-22-09
- Executive Order 14144
- CISA Zero Trust Maturity Model
- NIST 800-207
- DoD Zero Trust Strategy
- CISA Zero Trust Model Optimal
- SOC 2 Type 2

This is uncompromising identity defense.

LEARN MORE:
https://www.beyondidentity.com/solutions/government

Beyond Identity

An Ivy League Win-Win: Eliminating Identity Incidents While Simplifying Logins

A leading Ivy League research institution, renowned for its contributions to science, technology, and business, faced rising identity and device security challenges. With a complex, distributed IT environment and phishing attacks targeting high-value faculty accounts, the institution sought to modernize its authentication model while reducing risk in ways that government agencies can closely relate to.

The Challenge:

The university faced a relatively high phishing rate. While student accounts were considered lower value, compromise of faculty or research staff accounts posed significant institutional risk. Faculty and research staff hold credentials tied to sensitive projects, grants, and IP. Past incidents highlighted the stakes: in one case, a lost device containing institutional data led to data loss and forced the university to fund identity protection services for affected individuals.

The institution attempted to build its own passwordless model but ran into challenges with certificate management, revocation, and smart card deployment. With remote work expanding, reliance on network-based trust was no longer viable.

As their IT Security Solutions Architect noted,

"It's more costly to not solve these problems. In the event of compromised accounts, data breaches, and reputational harm – these are more costly than trying to find business practices and the technical tools to try to solve them."

They also wanted to meet NIST and Zero Trust mandates, present year-over-year risk reduction to their board, and ensure cross-college interoperability so faculty could access applications without disruption. For this instruction, zero trust meant not just protecting identities, but the devices getting access – managed and unmanaged.

The Solution:

Beyond Identity helped the institution execute its vision of zero trust and cyber defense at the identity layer. Identity management was mature, but extending trust to devices, including unmanaged ones, and eliminating phishable factors closed a critical gap.

As the IT Security Solutions Architect explained:

"When computers are interacting with our systems, I want to make sure they're not spreading malware, they're backed up, they have file level encryption. Some bar needs to be met before granting access. Otherwise, we can protect identities all we want but a compromised device from someone installing a Trojan game will toss it all out the window."

Beyond Identity enabled:

- Device-bound, passwordless authentication without easily misplaced hardware keys
- Continuous, risk-based access controls based on device posture
- Single-device access, reducing login time
- Centralized policy enforcement through their existing SSO, improving interoperability

Other vendors lacked configurability, requiring costly migrations or didn't support the passwordless vision.

"This is one of the rare cases where we do both at the same time – easier and more secure. Making the right thing to do the easy thing to do."

Key Takeaways:

- Most users now log in within 10 seconds vs. ~30 seconds with password + Duo MFA.
- Zero security incidents related to identity-based attacks
- No unknown devices logging in, including unmanaged student devices.

"This is a rare win-win in which the end-user has benefited from an institutional security program," concluded the IT Security Solutions Architect.

For government agencies, the lesson is clear: enforcing device trust and eliminating spoofable credentials achieves both compliance and usability while making identity compromise impossible.

See how Beyond Identity supports Government Agencies: *www.beyondidentity.com/solutions/government*

KEEPER

West Virginia University Improves Password Management and Visibility with Keeper Security

West Virginia University (WVU)'s Information Technology department needed an easy-to-use, secure and collaborative password management solution to replace an existing tool that no longer met their security or usability needs.

The Challenge:

WVU's IT department was struggling with an outdated password management system that hindered usability and posed growing security and administrative burdens. Users found the system's interface cumbersome, leading them to resort to risky alternatives like shared spreadsheets. Meanwhile, administrators faced limited visibility and insufficient access controls, making tasks like offboarding inefficient and insecure.

Compounding these issues, costs had climbed over time while vendor support deteriorated. A significant security lapse in 2022 further underscored that the legacy solution no longer offered acceptable protection.

The Solution:

WVU transitioned to Keeper Password Manager (Enterprise with Platinum Support), recognized for its intuitive interface, cross-platform compatibility and comprehensive training resources. The university leveraged Keeper Commander to easily import all of the IT teams critical records, while shared folders, one time share and account transfer features enabled secure collaboration and streamlined offboarding. These enhancements, combined with auto-fill capabilities via KeeperFill, promoted secure and efficient user workflows.

On the administrative and security front, Keeper's Role-Based Access Controls (RBAC) delivered precise control over access permissions. Keeper's zero-trust, zero-knowledge architecture, featuring multi-layer encryption, significantly elevated WVU's security posture.

Key Takeaways:

Organizational Impact

WVU achieved enhanced password hygiene, centralized visibility, improved productivity, and lower help-desk workload—all with confidence in governance and security.

Enhanced Usability & Adoption

Keeper's clean, intuitive UI and cross-platform support (Windows, Mac, Linux, iOS, Android) dramatically improved user adoption compared to the legacy system.

Strong Security Architecture

Keeper's zero-trust, zero-knowledge framework, which employs multi-layered encryption (vault, folder and record levels) ensured best-in-class security.

Compliance & Trusted Support

Keeper is SOC 2 and ISO 27001 compliant - with the longest-standing compliance in the industry - as well as FedRAMP and StateRAMP Authorized. Keeper's transparent pricing model paired with world-class customer support ensures that WVU is maximizing their investment.

PresenceID™

Government-Grade Identity Security — Now for Every Organization

Identity proofing and credentialing, trusted nationwide

High-Assurance Identity Proofing & Credentialing

Meeting standards and guidelines of HSPD-12, FIPS 201-3, NIST SP 800-63, the Kantara Initiative, and more.

Nationwide Network of Identity Stations

250+ ADA-compliant kiosks across 50 states providing convenient nationwide access.

Self-Service Stations with Patented SRIP Technology

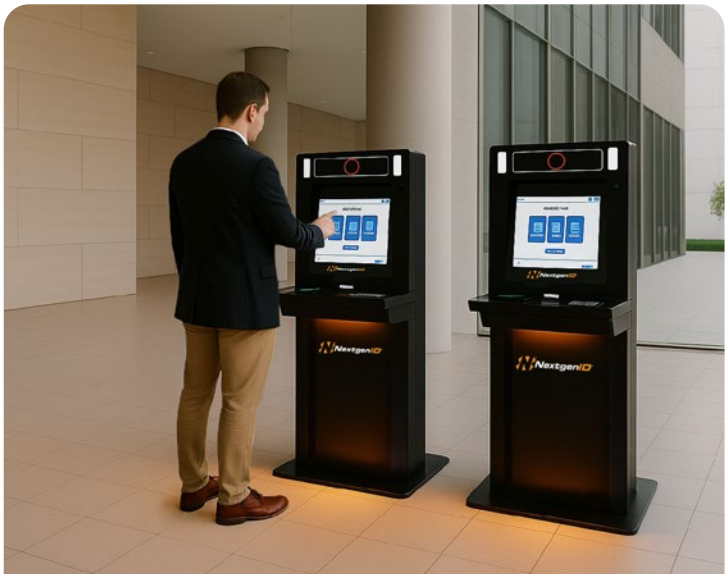
Identity Stations operate like ATMs - available self-service at your convenience or with a remote agent to help you.

PresenceID™ A NextgenID Network

NextgenID®

NextgenID delivers trusted, high-assurance credentials through its PresenceID™ network of self-service kiosks and patented Supervised Remote Identity Proofing (SRIP).

www.nextgenid.com • www.presenceid.com



Health &amp; Human Services Uses NextgenID Solutions to Streamline Nationwide Enrollment

The U.S. Department of Health and Human Services (HHS) modernized credential enrollment for over 80,000 employees by utilizing NextgenID's self-service kiosks, Secure Remote Identity Proofing (SRIP) software, and the PresenceID™ nationwide network. Shifting from centralized, in-person enrollment to decentralized and remote options cut costs, accelerated onboarding, and improved accessibility.

The Challenge:

HHS's traditional model relied on a limited number of PIV Card Issuance Facilities (PCIFs), resulting in bottlenecks, long wait times, and significant travel burdens — especially for a growing remote workforce. The COVID-19 pandemic only heightened the need to establish high-assurance identity proofing without in-person appointments.

Staffing and technical constraints further increased onboarding costs and delays, affecting critical work across the FDA, CDC, NIH, and CMS.

The Solution:

HHS launched a NextgenID pilot to validate SRIP and self-service enrollment for three of its sites. With the model quickly and convincingly proven, HHS moved directly into production to support an agency with 40,000 enrollments.

NextgenID's rapid deployment paired American-made self-service kiosks with SRIP software to standardize workflows, reduce travel and wait times, and support high-volume enrollments. Most critically, it enabled HHS to designate its enrollment staff as SRIP agents, meeting strict credentialing requirements without the need for lengthy third-party onboarding.

To extend its reach, HHS expanded to over 15 kiosk locations (including Indian Health Services), enabled multi-tenant use for broader government efficiency, and joined the PresenceID™ nationwide network, allowing employees to enroll at sites across the U.S. Most enrollments now take 5–10 minutes via QR code.

Key Takeaways:

Travel cost and time savings:
eliminates long-distance trips to PCIFs and reduces wait times.

Faster onboarding:
self-service flow typically completes in 5–10 minutes via QR code.

Flexibility and compliance:
HHS designates its own staff as SRIP agents, meeting stringent requirements without lengthy third-party onboarding.

Lower overhead and predictable costs:
complete managed service with transaction-based pricing from NextgenID.

Scalable, networked footprint:
15 federal locations plus two Indian Health Service units today; multi-tenant kiosks and the PresenceID™ nationwide network, with plans to expand to as many as 90 sites.

RADIANT LOGIC

Modernizing Identity and Access Management at the Department of the Navy with RadiantOne

The Department of the Navy (DON) used RadiantOne Identity Data Platform to enable a unified network initiative and centrally manage its identity and access management (IdAM) infrastructure. By normalizing and integrating identity data across environments, the DON laid the foundation for a more secure, agile, and future-ready identity strategy.

The Challenge:

The DON requires accurate identity information to ensure security and operational flexibility in a hybrid environment. However, connectivity proved to be a challenge—ships often operate in low-connectivity environments for extended periods. The Program Executive Office for Enterprise Information Systems (PEO EIS) sought an integrated identity solution capable of providing at least an 80% improvement in modern IdAM capabilities.

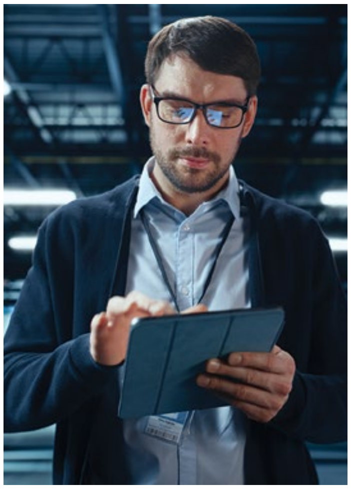
As service members changed roles within the DON, they accumulated multiple personas in the identity system based on their assigned location. This created challenges in authentication, authorization, and overall IAM processes. Additionally, the Navy's two major networks, the on-shore NMCI network and the ship-based CANES network, were not syncing, making onboarding and offboarding difficult and time-consuming.

The Solution:

To address these challenges, the DON seized the opportunity to establish a foundational identity infrastructure capable of supporting long-term strategic initiatives. RadiantOne's Identity Data Platform became a central component of this digital transformation. Using advanced virtualization, the platform abstracts and integrates identity data from both on-shore and off-shore networks, creating a universal identity repository accessible by mission-critical applications.

This integrated identity platform enabled the Navy to:

- Create a universal directory linking and correlating all personas into a single individual across networks.
- Enable syncing across NMCI and CANES, ensuring real-time updates between on-shore and offshore environments.
- Facilitate finer-grained identity management decisions, supplying real-time grouping and data for streamlined authorization.
- Build a foundation for an ICAM suite, supporting access management, identity governance, and privileged access management.



Key Takeaways:

Challenge:
Fragmented identity management across disconnected Navy networks, multiple personas per user, and low-connectivity environments.

Solution:
RadiantOne's Identity Data Platform to normalize, integrate, and virtualize identity data into a universal, real-time directory.

Impact:
Centralized IdAM, streamlined onboarding/offboarding, secure operations across hybrid networks, and a scalable foundation for modernization.

RSA

Protecting Sensitive Police Department Data with RSA's Phishing-Resistant Hardware Passkeys

A 360-question data security audit conducted by a government security agency on a week's notice would be a daunting prospect for any law enforcement entity. But one police department in the southeastern U.S. passed with flying colors, thanks to identity and access management capabilities from RSA.

The Challenge:

Could there be a greater challenge for a local police department than learning that auditors are on the way to check for compliance with Criminal Justice Information Service (CJIS) security policies? How about learning that they'll be there within the week?

It's a development that would have left many scrambling to prepare—but for one midsized police department, it proved to be a relatively light lift, thanks to its deployment of FIDO2 phishing-resistant, passwordless authentication from RSA.

The Solution:

RSA had worked with the police department over time to modernize and strengthen its approach to securing sensitive criminal justice data. The department started with basic multi-factor authentication (MFA) and ultimately evolved to phishing-resistant hardware authenticators based on the FIPS 140-3 Level 3 standard.

As a result, an audit that was expected to take at least a week—if not several weeks—was completed in just five hours. The police department's IT team avoided having to dedicate extensive staff resources for the duration of the review. That proved even more important shortly after the state audit, when the FBI arrived to conduct its own federal audit of CJIS compliance.

The Future:

With RSA's advanced identity management technology—such as the RSA iShield Key 2 series authenticators, the police department is positioned to continue protecting sensitive data against phishing, breaches, and emerging threats. Its investment also ensures efficiency and cost savings: the authenticator firmware is field-upgradable by users, keeping it future-proof against new risks.

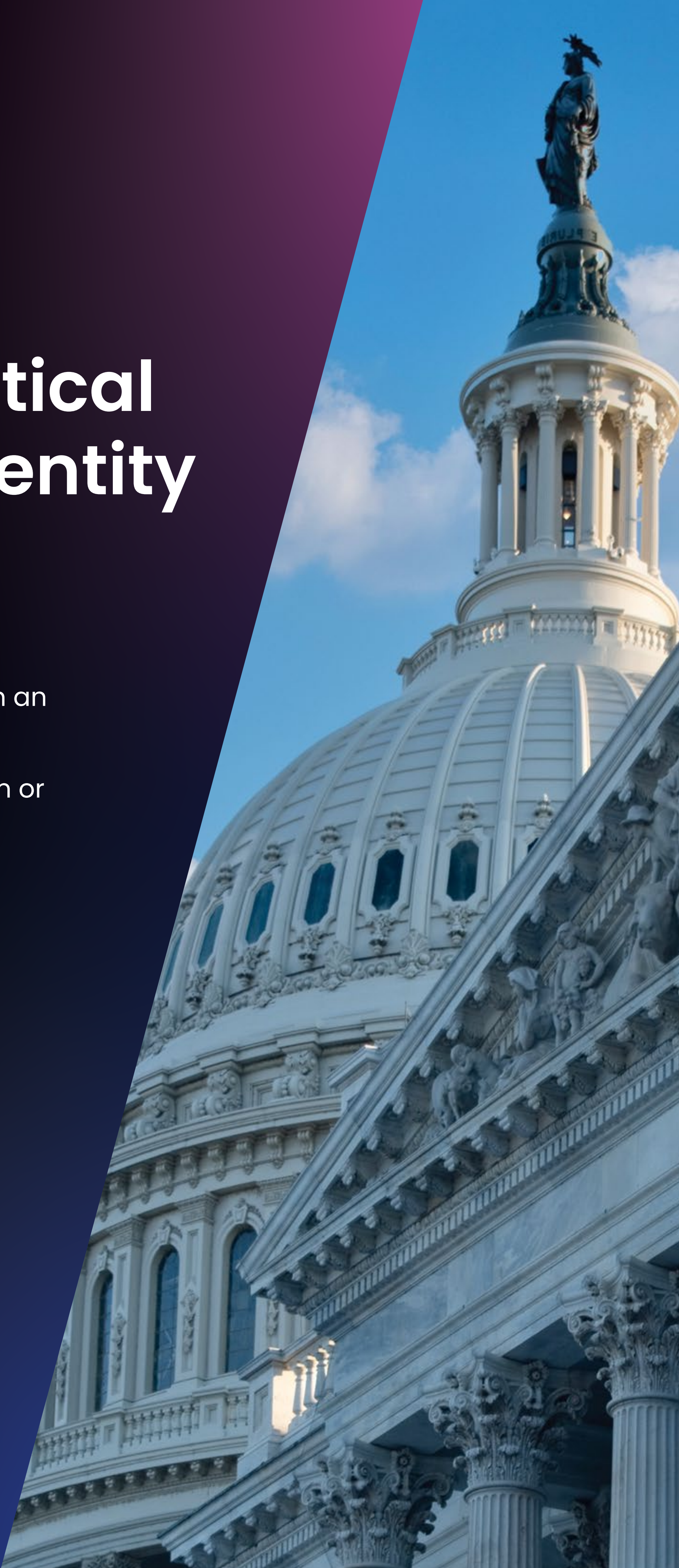
Looking ahead, the department will continue its cloud transformation with RSA, moving from a hybrid environment toward fully cloud-based identity and access management operations.

Key Takeaways:

Challenge:
Passing state and federal audits on short notice to validate compliance with CJIS data security policies.

Solution:
Deployment of phishing-resistant, passwordless multi-factor authentication (MFA) with hardware-based authenticators managed in the cloud.

Impact:
Stronger data protection, faster audits, and an exemplary reputation for securing sensitive criminal justice information.



SailPoint

SailPoint in the public sector: Efficiencies gained from an ICAM enterprise solution

The alignment of existing infrastructure with a new enterprise Identity, Credential, and Access Management (ICAM) solution from SailPoint enables a military department to automate workflows and make access decisions driven by AI and machine learning. The successful SailPoint onboarding allowed an Integrated Logistics Systems Supply (ILS- S) Program Management Office (PMO) team to quickly and efficiently produce system artifacts, provide system demonstrations, and establish a solid foundation for the project, enabling a smooth transition to development.

The Challenge:

- Maintain existing user capabilities while simultaneously prepopulating new user data constructs to align with the enterprise solution.
- Create a synchronization system within ILS-S so that changes to existing data would be accurately reflected in the tool during testing and roll-out to production.
- Limit the impact for users on the Go-Live date with disruption to less than 1% of the over 18,000 active users in ILS-S.

The Solution:

Public sector infrastructure must secure against emerging cybersecurity threats by protecting access to sensitive data, applications, and systems. This requires a cybersecurity approach that includes modern identity security, also known as strong identity governance.

Strong identity governance manages the lifecycle of digital identities for users, applications, and data – allowing agencies to provide automated access to the right identities at the right time with the right permissions, while mitigating potential security and compliance risks.

SailPoint identity security and an ICAM aligned strategy is the foundation for digital modernization and helps organizations increase visibility, better manage digital identities, reduce security threats, and follow best practices for access and policy modeling.

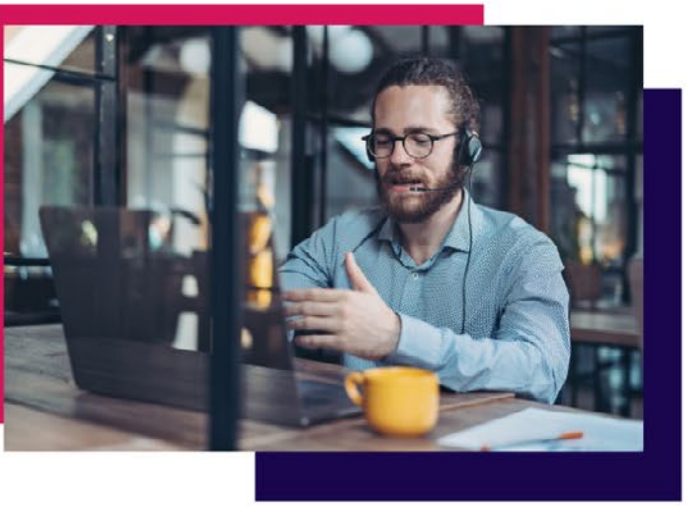
Key Takeaways:

By employing an agile methodology and ensuring thorough testing at every stage, ILS-S was able to successfully integrate SailPoint's ICAM solutions without compromising users' capabilities. This served as a great example of how careful planning, flexibility, and rigorous quality assurance can enable smooth migrations to advanced identity management systems. SailPoint's ICAM solution helps assist ILS-S to maintain audit readiness and limit NFRs by ensuring user access is validated through the proper chain-of-command and permissions. In the public sector, SailPoint provides options for SaaS or on-perm environments.

TRUSONA

One IT Help Desk Call Could Breach Your Network

Stop Social Engineering With Trusona's ATO Protect Suite



THE CHALLENGES

- Cybercriminal gangs like Scattered Spider and the Com are targeting the weak spot of organizations – the IT help desk.
- Armed with stolen credentials they need just one successful call to reset MFA and get access to your network.
- Ransomware is planted, data is stolen and millions of dollars are lost.
- Retailers, airlines & hotel chains have all been compromised in recent months.

THE SOLUTION

- Trusona's ATO Protect stops attacks at the first call, enabling help desk agents to robustly verify callers.
- ATO Protect includes Agent Verify, that helps employees verify legitimate support calls.
- ATO Protect can be rapidly deployed with minimal effort or can integrate into your helpdesk software.

Contact Trusona now and see how to stop one call breaching your network.

TRUSONA.COM

TRUSONA

Trusona ATO Protect at Grand Canyon Education, Inc.

Trusona Inc's ATO Protect solution gave Grand Canyon a quick to deploy, easy to use capability to quickly and robustly verify callers into their IT help desk and remove the threat of social engineering account take over.

The Challenge:

In September 2023, MGM Resorts International, the gaming giant, experienced a major ransomware attack that brought its operations to a screeching halt and cost over $100M. It was a social engineering attack by the now notorious group Scattered Spider who gained super administrator privileges by providing the MGM Help Desk with basic employee information.

The relative ease of the MGM attack got the immediate attention of Michael Manrod, CISO at Grand Canyon Education, Inc. Mike realized that any organization, including his own, was vulnerable to such an exploitation, even more so when the new power of Generative AI is unleashed.

"Multifactor authentication (MFA) carried us a long way, but now that it's everywhere, it naturally creates a cyber evolutionary force, driving adversaries to have to solve it. I think the future is that of a layered approach. No one solution solves the whole problem."
Mike Manrod, CISO GCE

The Solution:

Mike still had the issue that his IT Helpdesk agents could not know for sure who was on the other end of the line. He reached out to Trusona to explore their solution to social engineering of the IT Helpdesk – ATO Protect – which explicitly solves that problem.

Trusona's ATO Protect allows help desk agents to easily capture a government issued identity document from the caller and verify the data on it, plus the number they are calling from and the device they are using against authoritative data sources. An overall picture of risk is presented to the agent and the whole system is resistant to Generative AI, SIM swapping and Man in the Middle attacks. Mike says:

"We were really excited about the driver's license validation aspect, you know, let's take a trusted authority like a driver's license bureau. Let's take a trusted identification with multiple attributes that can be verified and then put it on a clock so that if somebody somehow tries to socially engineer those chains, we detect and report on that too."

Mike was also cognizant that any solution needed to be scalable, quick to deploy and not impose a significant process overhead on his team of support staff. GCU has now deployed ATO Protect for employee IT helpdesk interactions and is exploring expanding the service to their much larger student body.

Key Takeaways:

- The IT help desk is the weak spot of most organizations – one call can lead to a devastating network breach.
- Agents need an easy-to-use method to rapidly and robustly verify caller identity and weed out social engineering scammers.
- Trusona ATO Protect can defend both the IT help desk and regular employees from spoof support calls

"Bypassing the human verification is something super critical we need to get on top of, and it's something we can't afford to wait on, and it's low-hanging fruit."
Mike Manrod, CISO GCE

"We're now in a social engineering battle that is all about identity, not about authentication."
Ori Eisen, Trusona CEO

uberether

Accelerating Federal IAM Transformation with UberEther

A large federal defense agency partnered with UberEther to modernize its Identity and Access Management (IAM) systems, streamline compliance, and overcome legacy infrastructure challenges.

The Challenge:

This agency faced increasing compliance mandates and legacy systems that were no longer sustainable. Outdated identity workflows, fragmented access controls, and data complexity were creating operational inefficiencies and compliance risk. The agency needed a secure, scalable IAM solution that could be deployed rapidly within its cloud environment.

The Solution:

UberEther implemented its IAM Advantage platform inside the agency's secure cloud tenant. Within two days, UberEther configured SailPoint, Radiant Logic, and PingFederate for secure authentication, optimized identity governance, and unified identity aggregation. This turnkey solution unified siloed identity sources and transformed outdated records into clean, actionable user profiles. The deployment included automation of identity lifecycle events and integration with government-issued PKI credentials. The result was a streamlined, compliant authentication process, improved separation of duties, and a scalable architecture ready to support future mission requirements.

Key Takeaways:

Deployed in Days:
IAM Advantage fully operational within 2 days

Integrated Governance & Authentication:
Centralized identity control across systems

Automated Lifecycle Management:
Reduced manual overhead and errors

Compliance-Ready Architecture:
Built for high-assurance, mission-critical environments

Contract Vehicles

Carahsoft offers a number of contract options for purchasing Identity and Access Management solutions. Our contracts offer purchasing options for civilian, defense, state, and local government customers. Customers can purchase solutions off of these major contract vehicles:

GSA Multiple Award Schedule (MAS)

Carahsoft holds a GSA Multiple Award Schedule (MAS) that allows customers to procure a wide variety of Identity and Access Management solutions. Carahsoft holds Contract #47QSWA18D008F and allows customers to purchase everything from identity to automation & orchestration solutions.

ITES-SW2

The purpose of the ITES-SW 2 acquisition is to support Army, Department of Defense (DoD) and all Federal Agency enterprise Information Technology (IT) infrastructure and info-structure goals by leveraging Commercially available-Off-The-Shelf (COTS) software products and maintenance in 14 product categories in addition to related incidental services and hardware.

NASA SEWP V

The NASA SEWP V GWAC (Government-Wide Acquisition Contract) provides the latest in Information Technology (IT) products and product-based services for all Federal Agencies.

SEWP provides the best value and cost savings through innovative procurement tools and processes; premier customer service and outreach; and advocation of competition and cooperation within the industry.

NASPO ValuePoint Cooperative Purchasing Organization

The NASPO ValuePoint Cooperative Purchasing Organization (formerly WSCA-NASPO) provides the highest standard of excellence in public cooperative contracting. By leveraging the leadership and expertise of all states with the purchasing power of their public entities, NASPO ValuePoint delivers best value, reliable, competitively sourced contracts.

Since 1993 NASPO ValuePoint has been the cooperative purchasing arm of NASPO (the National Association of State Procurement Officials) encouraging, fostering and guiding the nation's most significant public contract cooperative. NASPO ValuePoint is a unified, nationally focused cooperative aggregating the demand of all 50 states, the District of Columbia and the organized US territories, their political subdivisions and other eligible entities spurring best value, innovation and competition in the marketplace.

Solutions from more than 200 providers are available through the contract, encompassing:

- Software Licenses
- Product Support
- Maintenance Services
- End User Computing
- Cloud Subscription Services
- Training
- Professional Services

OMNIA, Partners – Cobb County

Carahsoft holds a OMNIA Partners, Cobb County, GA Technology Products, Solutions and Related Services contract (#23-6692-01) that provides full access to a portfolio of value-driven contracts, spend visibility analytics, and subject matter experts.

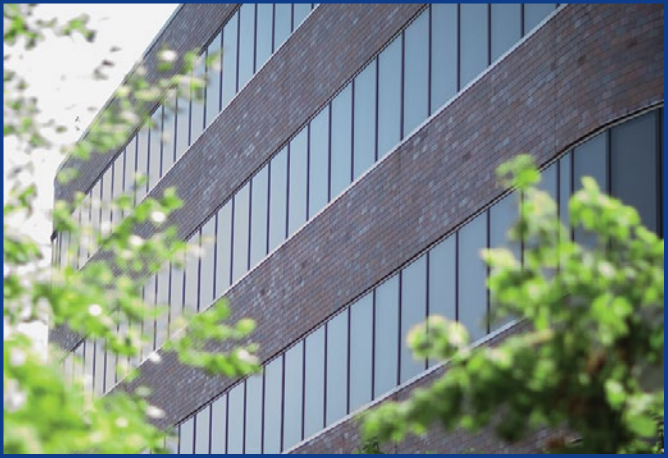
OMNIA, Partners – Education Software Solutions and Services

Carahsoft Technology Corp., The Trusted Government IT Solutions Provider®, today announced that it has been awarded a Region 4 Education Service Center (ESC) contract (#R191902) for Educational Software Solutions and Services available now through OMNIA Partners. This contract makes these solutions available to state and local government agencies, education institutions, non-profits, municipalities, and additional public sector organizations through Carahsoft and authorized reseller partners.

Educational Software Solutions and Services are available through this contract and Carahsoft's reseller partners to public sector organizations in all 50 U.S. states and the District of Columbia, and the contract is established for a five-year period of performance through April 30, 2025. All solutions on this contract are offered at special discounts off their manufacturer list price, and additional price reductions can be provided on a deal-by-deal basis.

Upcoming Events

Carahsoft is prepared to support and guide the Federal, State and Local Government, as well as Education and Healthcare organizations through this new year in collaboration with our robust network of identity and access management partners and solutions. Check out these top events to learn more about what to expect in identity and access management throughout this year.



AFCEA West 2026

February 10-12, 2026 | San Diego, California

Join defense, government, and industry leaders at WEST 2026, taking place February 10–12, 2026 in San Diego, CA. Co-sponsored by AFCEA International and the U.S. Naval Institute, this flagship event unites senior military officials, policymakers, and technology innovators to explore the future of maritime, space, and cyber operations. Attendees will gain mission-critical insights on fleet modernization, AI integration, and C4ISR advancements through keynotes, panel discussions, and an expansive technology showcase. Designed to foster collaboration across the Sea Services, WEST 2026 is where strategy, innovation, and national defense priorities converge.

Datadog GovSummit

April 16, 2026 | Washington, D.C.

Explore the future of government technology at the Datadog GovSummit 2026, taking place April 16, 2026 in Washington, D.C. This premier forum, hosted in partnership with Carahsoft, unites public sector technologists and IT leaders to tackle digital transformation challenges at scale, including modernization, security, compliance, and operational visibility.

Attendees will gain practical insights from interactive sessions, technical walkthroughs, and expert-led discussions that showcase real-world use cases and best practices for observability and mission success. Designed for federal, state, and local government practitioners as well as systems integrators, GovSummit offers valuable learning and networking opportunities to advance secure, efficient, and resilient IT strategies.

TechNet Cyber

June 2-4, 2026 | Baltimore, Maryland

Join government, defense, and industry cybersecurity professionals at TechNet Cyber 2026, taking place June 2–4, 2026 at the Baltimore Convention Center in Baltimore, MD. Hosted by AFCEA International, this flagship event brings together strategic, operational, and technical leaders from across the cyber domain, including experts from U.S. Cyber Command and the Defense Information Systems Agency (DISA).

Attendees will explore how to strengthen cyber defense through innovation, integration, and gaining insights from keynotes, interactive sessions, and a dynamic exhibit hall showcasing the latest technologies shaping the future of cyberspace operations.

Identiverse

June 15-18, 2026 | Las Vegas, Nevada

Join thousands of identity and security professionals at Identiverse 2026, taking place June 15–18 at Mandalay Bay in Las Vegas, for four days of world-class learning, networking, and innovation. With over 250 speakers, 100+ identity topics, and 70+ hours of content, this premier event delivers cutting-edge insights into AI, zero trust, privacy-enhancing technologies, and non-human identity management.

Attendees can earn up to 20 CPE credits, engage in hands-on workshops, and explore the vibrant expo floor featuring 150+ solution providers. From executive leaders to technical architects, Identiverse offers a dynamic platform to shape the future of digital identity in a rapidly evolving landscape.

Identity Week America

September 2-3, 2026 | Washington D.C.

Discover the future of identity at Identity Week America, returning September 2–3, 2026 to the Walter E. Washington Convention Center in Washington, D.C. With over 3,000 attendees, 250 exhibitors, and 250 expert speakers, this premier event unites leaders from government, enterprise, finance, healthcare, and tech to explore cutting-edge identity solutions.

Attendees will gain exclusive insights into the latest innovations in digital identity, biometrics, cybersecurity, and trust frameworks through dynamic sessions and hands-on exhibitions. Whether you're a startup or a global brand, Identity Week offers unmatched networking, learning, and partnership opportunities under one roof.

Gartner Identity & Access Management Summit

December 7-9, 2026 | Las Vegas, Nevada

Explore the future of identity at the Gartner Identity & Access Management Summit 2026, bringing together IAM leaders, security architects, and IT executives from government and enterprise organizations. This premier Gartner event delivers in-depth analysis and strategic guidance on the evolving identity landscape, including Zero Trust, identity governance, authentication modernization, and identity threat detection.

Attendees will gain actionable insights from Gartner analysts and industry experts through research-driven sessions, peer discussions, and solution showcases. Designed for organizations navigating complex digital ecosystems, the summit offers unparalleled opportunities to learn, network, and shape IAM strategies aligned to business and mission outcomes.

Like to know more about our **Identity & Access Management** offerings?

Scan the QR

or contact us:
(571) 590-3490
Cybesecurity@Carahsoft.com
carahsoft.com/solve/cybersecurity

carahsoft

Carahsoft Technology Corp. partners with thousands of vendors, resellers, system integrators and MSPs to proactively market, sell and deploy a comprehensive range of IT solutions for public sector customers across the U.S. and Canada.

Scan to view our solutions, latest events, trending topics and more.

carahsoft.com 11493 Sunset Hills Road, Suite 100 | Reston, Virginia 20190