

Advancing Cybersecurity

WITH
ICAM

INSIDE:

DISA: Improving Zero Trust	3
Infographic: Cybersecurity with ICAM	7
Modern Tech: Tier Zero Assets	8

SPONSORED BY



From the editor's desk



Sarah Sybert, Managing Editor

Strengthening Security, Streamlining Access in an Evolving Digital World

Protecting sensitive data and ensuring secure access to systems is more important than ever. This is where identity, credential, and access management (ICAM) comes into play.

ICAM helps organizations verify and manage who has access to what data, ensuring only authorized personnel can access sensitive information. It's a key component in any robust cybersecurity strategy, especially as government and industry move toward zero trust.

There's a growing push for federating ICAM systems across different agencies and organizations, allowing them to seamlessly work together while maintaining strict security protocols. This is especially important for defense and government sectors, where multiple systems and partners need to communicate securely but independently.

Cyber leaders are also improving access in disconnected or tactical environments. By implementing localized ICAM instances, users in remote locations or deployed forces can maintain secure access, even if they're disconnected from the central network.

There's also an ongoing effort to integrate newer authentication technologies, like passkeys and biometric systems, into the ICAM landscape to make access even more secure and user-friendly.

ICAM is becoming more sophisticated and essential for ensuring secure, efficient access to systems and data. As organizations face increasingly complex cybersecurity threats, the need for strong ICAM solutions that can adapt to various environments and technologies has never been greater. ✨

Table of Contents



Ross Gianfortune,
Senior Staff Writer



Nikki Henderson,
Staff Writer



ARTICLE

DISA Boosts ICAM to Enhance Zero Trust

Federation and cloud adoption helps DISA drive unified user access, addressing tactical needs and insider threats.

BY ROSS GIANFORTUNE



INFOGRAPHIC

Enhancing Cybersecurity with ICAM

ICAM streamlines access control, strengthens security, and ensures compliance across systems and networks.



PARTNER INTERVIEW

Securing Tier Zero Assets for Modern Cybersecurity

Organizations are protecting tier zero assets and implementing robust ITDR to maintain a zero-trust security posture.

Chris Roberts, Director, Quest Federal Engineering



ARTICLE

NIST's Latest Guidance Bolsters Identity Management

NIST is advancing zero trust and identity management with new guidance on cybersecurity, authentication and digital identity.

BY NIKKI HENDERSON

DISA Boosts ICAM to Enhance Zero Trust

Federation and cloud adoption helps DISA drive unified user access, addressing tactical needs and insider threats.

BY ROSS GIANFORTUNE

The Defense Information Systems Agency (DISA) is accelerating zero-trust implementation by focusing on identity, credential and access management (ICAM) solutions. Brian Hermann, the agency’s director of the Cybersecurity and Analytics Directorate, said the agency is progressing ICAM implementation through federation and cloud adoption.

“Thus far, we’re going to use the lessons that we learn out of [ICAM implementation in military services] to go ahead and do the federation across all the other ICAM solutions that exist within the department,” said Hermann during a media roundtable. “Learning the lessons that we’re learning right now on federation is a good thing, and we expect by the end of this fiscal year to have completed the federation activities with all of the military departments.”

According to Hermann, the Defense Department is actively pursuing a federated ICAM approach, connecting disparate systems across the services to provide a unified view of user access. Hermann said that the launch of a federation hub is enabling interoperability between different ICAM solutions within the DOD. The hub allows for a comprehensive understanding of user access rights and prevents conflicting roles across systems, he added, and that the technical challenges are minimal.



DISA headquarters in Fort Meade, Maryland.

“We would hate for somebody to be authorized for access to something but not be able to reach back to something that would grant them access,” Hermann said. “ICAM is really about that user pillar of zero trust.”

(ctd.)



Brian Hermann

Director, Cybersecurity & Analytics
Directorate, DISA

Tactical ICAM and Attribute-Based Access Control

To address connectivity and resiliency challenges in tactical environments, DISA is implementing localized ICAM instances that synchronize with the enterprise system, Hermann said. Operations have a “reach back” that allows deployed forces to retain access even in disconnected scenarios.

“If that tactical location becomes disconnected from the enterprise in its totality, they still have the most recent synchronization of data that they can use to work from so thus far, that has been the way that we solve for the tactical issue is that there’s a local instance of the identity provider function,” said Hermann. “We have a single place where all the identities across DOD are managed out of and we, DISA, synchronize that data with anybody else that has a separate instance of identity.”

Hermann said that the different needs across DOD require difference tactical solutions for resiliency. The Navy and Marine Corps, for example, have different requirements than the Army or Air Force, he said.

“Each of the military services has a need for potentially a different kind of a tactical situation [like] a float versus a tactical [or] a land-based environment,” Hermann said. “There’s also potentially some different identity requirements associated with combatant commands and even some of the combat support agencies.”

Hermann added that DISA’s ICAM responsibility extends to partners, including the defense industrial base and coalition partners and allies.

“U.S. Transportation Command needs to be able to partner with transportation companies that will never have DOD-provided credentials, so we have the ability to work with those partners with multi-factor authentication,” he said. “We have a process for granting them access.”

Master User Records and Insider Threats

ICAM is helping DISA to combat insider threats. DISA is implementing a master

user record with strict privileged access control, providing a central location for user access information. While not currently connected to insider threat analysis, Hermann acknowledged its potential for future use.

“It’s important — if something happens, and somebody was concerned about [an insider threat] having access to something — [DISA system administrators] might want to look at what ... damage could have been done,” Hermann said. “You can have a track record of changes and things that have been done, as well.”

Balancing Enterprise and Specific Use Cases

DISA is also conducting pilots to assess whether enterprise ICAM solutions can meet the needs of various components, minimizing the need for separate ICAM instances, Hermann said. This approach aims to maximize efficiency and reduce the complexity of federation.

“One of the things that we’re trying to do is to have the right number of ICAM instances across the department based on the use cases that each of the components needs, but not to have too many,” Hermann said. “We are working

with some components across the department to determine whether or not the enterprise solution can meet their needs and avoid having a separate instance of ICAM for them.”

Cybersecurity and ICAM

Hermann added DISA has established a standard architecture for ICAM solutions, requiring privilege management functions for system administrators. DOD OCIO, DISA and the National Security Agency governs the architecture, he added, and DISA works with other DOD components to buttress cybersecurity in the department.

“We have a pretty robust operational control layered on top of the accreditation process and partly my team here at DISA PEO Cyber, we provide the data and analytics environment to a separate organization within the agency that provides defensive cyber operations and cyber security service provider functions as well,” Hermann said. “It’s something that that we take very seriously.” 🌟

Photo credit: pixadot.studio/Shutterstock



“One of the things that we’re trying to do is to have the right number of ICAM instances across the department based on the use cases that each of the components needs, but not to have too many.”

— Brian Hermann, Director, Cybersecurity & Analytics Directorate, DISA

Enhancing Cybersecurity with ICAM

ICAM streamlines access control, strengthens security, and ensures compliance across systems and networks.

ICAM is essential for securing digital identities, ensuring that only authorized users can access sensitive systems and data while reducing cybersecurity risks. It strengthens compliance, improves operational efficiency, and enables seamless, secure access across organizations and federated networks.

GOVERNANCE

Governance refers to the framework of policies, processes and controls that align with security and compliance and ensure the effective management of identities, credentials and access management.

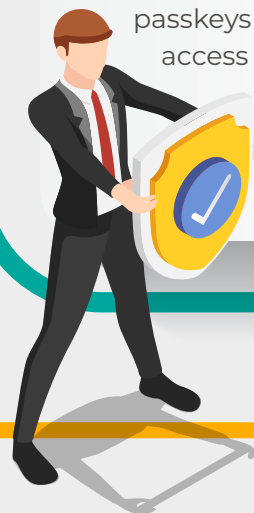
IDENTITY MANAGEMENT

Identity management is the process of creating, maintaining, and securing digital identities to control user access to systems, applications and data.



CREDENTIAL MANAGEMENT

Credential management is the process of issuing, storing and verifying authentication credentials – think passwords, biometrics and passkeys – to ensure secure access to systems and data.



ACCESS MANAGEMENT

Access management is the process of defining, enforcing and monitoring user permissions to ensure that only authorized individuals can access specific systems, applications, and data.



PARTNER INTERVIEW



Securing Tier Zero Assets for Modern Cybersecurity

Organizations are protecting tier zero assets and implementing robust ITDR to maintain a zero-trust security posture.

How are identity-based attacks evolving, and why is securing tier zero assets critical to modern cybersecurity?

Roberts In any system, credentials, user information and attributes are maintained in a database. Tier zero assets are the critical components of the system. Attackers want to get to that data beyond that directory protocol.

Multifactor authentication (MFA) prevents bad actors from accessing these key identity systems, but the job of the hackers has gotten easier because of the advanced tooling that commercial software industry has produced.

They are leveraging hybrid attacks to poke and prod on-prem components, gateways, access points and the SASE points to bypass MFA and privileged account management and get access to some piece of the directory infrastructure. We provide privileged access management that uses time, location and role-based access. (ctd.)



Chris Roberts
Director,
Quest Federal
Engineering

What are the key technical and operational challenges in recovering identity systems after a ransomware attack?

Roberts If we look at the CrowdStrike outage last year as an example, that happened below the hardware, below where everyone loads their security software.

Because CrowdStrike was the security software, and they're a preferred partner of Microsoft, they had kernel-level access. This made the issue far more complex, affecting system control and recovery at a much deeper level.

If you think of it when recovering a system, especially an identity system, the questions for most operators are, 'can I bring it back online from a backup?

Can I be reasonably certain that that backup was not also compromised? Where did we get compromised? How do I restore and read without reintroducing the same malware all over again? And then in the meantime, how do I keep my organization running?'

How does identity threat detection and response (ITDR) fit into a modern zero-trust security strategy?

Roberts Identity Threat Detection and Response (ITDR) is a unified set of technologies that brings together various indicators across an organization. I – as a CISO, network operations center analyst or security operations center analyst – can

“Having an identity system that is secured from a single source of truth standpoint is critical. If I am not confident of the identities and the validity of those identities, then zero trust gets compromised.”

— Chris Roberts, Director, Quest Federal Engineering




use ITDR to connect those pieces, identify potential threats and determine when deeper investigation is needed.

If the event meets a certain number of criteria, then I shut down that credential, port or workstation. There's an automated response to that process. I automatically do something in the environment, and then I flag it for review. In other words, shoot first, ask questions later.

How does all of this align with federal zero trust and IT modernization efforts?

Roberts The federal zero-trust effort basically says, unless I can validate who you are, where you are and what you're supposed to be doing, you don't get to do anything. You can't read, you can't write and you surely can't execute.

So, having an identity system that is secured from a single source of truth standpoint is critical. If I am not confident of the identities and the validity of those identities, then zero trust gets compromised. 

NIST's Latest Guidance Bolsters Identity Management

NIST is advancing zero trust and identity management with new guidance on cybersecurity, authentication and digital identity.

BY NIKKI HENDERSON

Recent guidelines and updates to standards are advising on zero trust and identity, credential and access management (ICAM) to support federal government's next stages of cybersecurity. Here's a look at some of those.

Guide for Implementing a Zero Trust Architecture

At the end of the last year, the National Institute of Standards & Technology (NIST) publicly released the initial draft of the practice guide, Implementing a Zero Trust Architecture, for comment. This latest document outlined best practices from the National Cybersecurity Center of Excellence (NCCoE), which worked with 24 vendors to demonstrate end-to-end zero trust architecture.

"The NCCoE and its collaborators have used commercially available technology in lab environments to build 19 interoperable, open standards-based ZTA implementations that align to the concepts and principles in NIST SP 800-207, Zero Trust Architecture," according to the document. "The implementations include ZTA approaches for enhanced identity governance, software-defined perimeter, microsegmentation and secure access service edge."

According to Alper Kerman, cybersecurity engineer and project manager at NCCoE, the guidance outlines the technical information for each sample implementation and serves as a resource for technology implementers by



providing models they can replicate. Agencies will save time and money in the future by applying lessons learned from the implementations.

"In it, we describe how we utilized ICAM capabilities throughout the 19 example lab implementations that we built," Kerman told GovCIO Media & Research. (ctd.)

Ryan Galluzzo

Digital Identity Program Lead, NIST



Digital Identity Guidelines

Last summer, NIST updated its draft Digital Identity Guidelines following a four-month-long comment period and yearlong external engagement period.

NIST Digital Identity Program Lead Ryan Galluzzo said there are four volumes of the agency's Special Publication 800-63-4. The first digital identity guidelines cover identity risk management. The second, or Volume A, covers identity proofing and verifications of how you prove an identity. Volume B covers authentication, and Volume C covers federation.

The updated guidance primarily aims to enhance privacy and accessibility throughout the identity-proofing process for individuals seeking government services. Galluzzo said the draft version of the guidelines also lays out requirements for phishing resistant authentication and next steps to improve the guidance.

"We're more interested in the establishment of an identity, how you authenticate that identity on an ongoing basis and how to effectively convey in a secure manner information about who that identity is," said Galluzzo at an industry event in Washington, D.C. "Our guidance, the digital identity guidelines, covers everything from public facing access, to public service systems, to back-end access, to higher risk applications like your admin side."

NIST is working to include additional types of authenticators, such as passkeys and platform-based authenticators. These are embedded within devices and enable cryptographic authentication, which can then be seamlessly integrated into web applications. The agency aims to establish appropriate policies to secure and manage these emerging tools.

"We're looking at things like syncable authenticators. How can we go get devices? How can we build out a representative identity and access management system that looks like a federal agency?" said Galluzzo. "Then how can we deploy mobile device management software to those devices to be able to help us manage things like syncable authenticators, or things like derived authenticators in a way that allows us to take advantage of their usability features

but does not compromise security.”

Galluzzo said NIST wants to replicate the issues federal agencies face and experiment with new technology solutions to inform how the agency can improve its guidance moving forward.

Personal Identity Verification Guidance

NIST is updating its entire suite of personal identity verification (PIV) guidance.

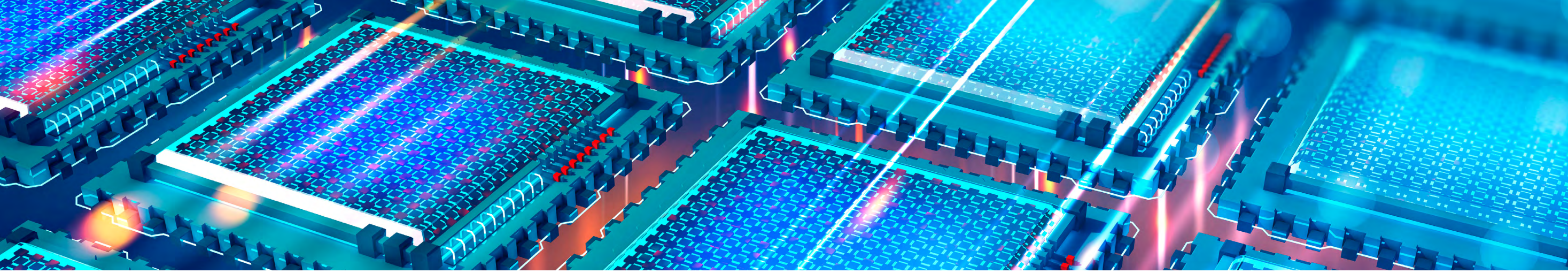
Federal employees and contractors primarily use PIVs as credentials to enforce authentication and access controls for zero-trust models in government.

NIST SP 800-217 guidelines for Personal Identity Verification (PIV) Federation and NIST SP 800-157-1 guidelines for Derived PIV Credentials released in November 2024 provide tailored guidance for applying federation controls and alternative authenticators to PIV scenarios.

“We are also finalizing NISTIR 8480 Attribute Validation Services for Identity

“We’re more interested in the establishment of an identity, how you authenticate that identity on an ongoing basis and how to effectively convey in a secure manner information about who that identity is.”

— Ryan Galluzzo, Digital Identity Program Lead, NIST



Management: Architecture, Security, Privacy and Operational Considerations,” Galluzzo told GovCIO Media & Research. “This draft report delves into the architecture, security, privacy and operational considerations surrounding attribute validation services (AVS), offering considerations for government agencies seeking to implement these critical services. AVS can be used to validate specific attributes for access control or identity-proofing scenarios.”

Preparing for the Future Cyber Landscape

NIST is looking to the future technology landscape and developing guidance to secure federal agencies as quantum and artificial intelligence evolve.

Government is bracing for “Q-Day,” when quantum technology will become so advanced that it can crack current encryption methods and threaten the information systems that

make up the nation’s digital services and critical infrastructure across sectors. NIST released new quantum standards last year, marking a milestone in the government’s effort to migrate systems to post-quantum cryptography.

Galluzzo told GovCIO Media & Research that he’s seen challenges around ICAM as it relates to post-quantum cryptography — in particular, transitioning authentication mechanisms to upgraded algorithms while not losing backward compatibility needed to support legacy applications and services.

NIST has also been monitoring the evolution of generative AI and deepfakes, which have been used to target identity proofing, Galluzzo added.

“Such attacks, if not detected, can undermine confidence in the issuance

and use of authenticators and degrade the ability to detect and prevent identity-based attacks,” said Galluzzo. “Ongoing threats such as phishing of authenticators and — in particular — assertion [or] token theft and forgery. These have been actively exploited to conduct both high scale and highly targeted attacks on U.S. infrastructure.”

NIST has several ICAM initiatives on the horizon, like advancing verifiable digital credentials (VDC).

“Take any physical credential you use in everyday life — your driver’s license, your medical insurance card, a certification or diploma — and turn it into a digital format stored on your smartphone that can be presented and cryptographically verified either online or in person. That’s a verifiable digital credential,” Galluzzo and Bill Fisher, security engineer at NIST’s NCCoE, wrote in a 2024 NIST article.

While VDC is still nascent, NIST is accelerating the adoption of mobile driver’s license standards. Galluzzo said these efforts will eventually move from an initial focus on protecting financial services to government applications and health care services. There is still a lot to learn on how these concepts will fit into existing and emerging online services.

“We are in the process of standing up a lab focused on testing emerging authentication and federation technologies, with a specific emphasis on scaling phishing resistant authenticators such as passkeys and improving our ability to federate PIVs across agencies and organizations,” said Galluzzo. “These, combined with our efforts to complete the Digital Identity Guidelines and the PIV materials, remain the crux of our efforts.” ✨