Security in the Digital Age

Your Guide to Identity & Access Management

carahsoft.

govloop

"How agencies conduct identity proofing, establish enterprise digital identities, and adopt sound processes for authentication and access control ***significantly affects*** *the security and delivery of their services, as well as individuals' privacy."*

-Office of Management and Budget ICAM Memo

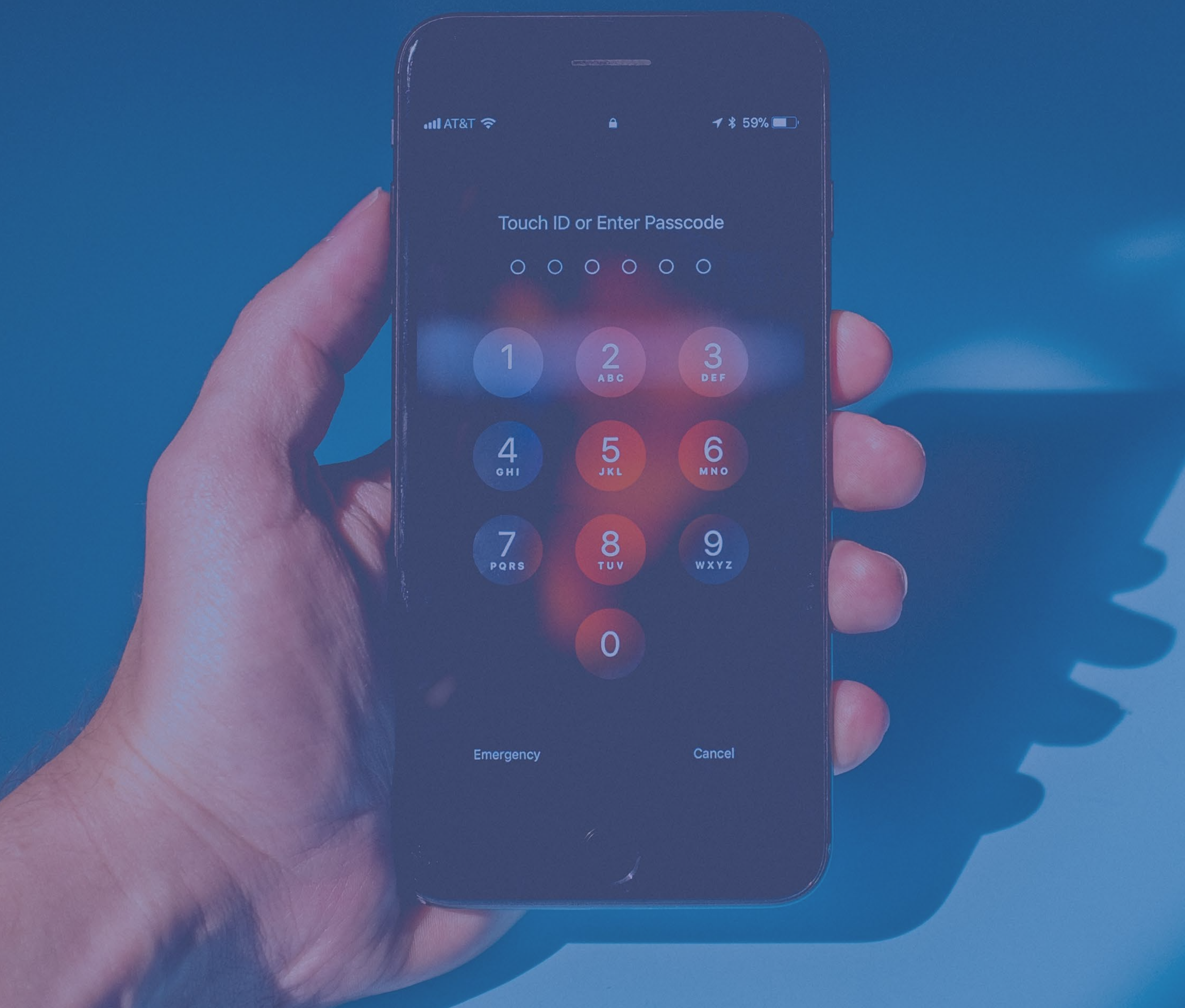


Table of Contents

Carahsoft and GovLoop have partnered to provide resources around the latest federal, state and local identity access management (IAM) initiatives and legislation. The goal is to guide government leaders and stakeholders interested in learning more about improving their cyber posture.

Executive Summary

When cartoonist Peter Steiner illustrated and captioned a now iconic drawing about internet privacy in 1993, he likely had little idea of its potential impact then — let alone nearly 25 years later.

The cartoon depicts two dogs. One is sitting at a desk in front of a computer and talking to another dog seated on the floor. The computer-savvy dog's words about internet anonymity are also used as the cartoon caption: "On the Internet, nobody knows you're a dog."

It's cute, right? Plus, who doesn't love a funny cartoon dog with a sense of humor? But to fully understand the novelty of this illustrated message, consider that "surfing the internet" was a fairly new term in the early 1990s, and the general public was just getting its first taste of a popular web browser.

To say the online world has drastically changed since then is an understatement. We shop, bank, work, date, research and communicate online. If you were to take an inventory of the personal and professional accounts you have online that require you to verify your identity, you probably couldn't list them all.

In many ways, how we secure, manage and verify our digital identities have become as important — if not more important — than how we represent ourselves in person. Our privacy, security and sensitive assets are at stake and are more accessible to us, and to those who wish to harm us. For government agencies, the ability to provide secure and seamless services to millions of people — think tax and public-safety systems — is on the line. It can be easy to get caught up in the excitement of all the possibilities that going digital can offer, but identity and access management (IAM) must be an integral part of that discussion.

IAM is the security discipline that enables the right individual to access the right resource at the right time for the right reason. Ensuring its effectiveness extends beyond the IT and cybersecurity teams. Everyone plays a role, and they come from multiple offices, including finance, human resources, legal, acquisition and physical security.

The IAM market is estimated to reach **$24.12 billion** by 2025.

And although IAM falls under the umbrella of security, functionality and user experience are also central to securing digital identities. Employees are sure to circumvent processes that are too cumbersome, which could harm individuals and organizations.

We developed this guide in partnership with Carahsoft to study today's IAM landscape. We examine what an effective strategy looks like, how to modernize capabilities and government adoption, and use cases highlighting IAM shared solutions and services. You will also hear from IAM experts at the Agriculture Department (USDA), National Institute of Standards and Technology (NIST), and the Defense Information Systems Agency (DISA).

What Does Identity and Access Management Mean for Government?

In recent years, there has been an explosion of online service offerings from government agencies. Internally, employees can manage their pay and benefits, request time off and analyze sensitive data in the cloud. Government customers can access their health records via online portals, make automated payments and even avoid long lines at the Department of Motor Vehicles by going digital.

To ensure the right people have access to these resources at the right time — and for the right reasons — IAM must be an integral part of the design, acquisition, operations and continuous maintenance of these digital services.

IAM also enables trust across organizational, operational, physical and network boundaries because, without it, confidence in the security of the service is lacking. Although IAM may not be as flashy as artificial intelligence (AI), robotic process automation (RPA) and other hot tech, it is the foundational layer that supports these and other capabilities. An emphasis on IAM can also result in better customer experience through secure, user-friendly interactions, such as information sharing or accessing an online service.

In many ways, there has been a resurgence and renewed focus on IAM as agencies move operations outside traditional office boundaries and look to augment the workforce with tools that mimic human behaviors. And like humans, these technologies have identities that need to be verified. (We will discuss this more in our Q&A with USDA's Adam Zeimet and in the section on the current federal landscape).

Although this guide primarily focuses on the digital side of IAM, physical security is also a real concern. The ID cards that government employees and contractors use to access computers are the same cards that give them access to government facilities. There have been discussions about security beyond these ID cards, but they are still the main method that agencies use for identification and authentication. They were designed to work with traditional computing devices, such as desktops and laptops, and they can be clunky and cumbersome when trying to verify users on mobile devices.

"However, as technology evolves, the government must offer flexible solutions to meet changing technology needs and shift the focus from managing the lifecycle of credentials to the lifecycle of identities," according to a May 21, 2019, memo from the Office of Management and Budget (OMB) on the government's identity, credential and access management (ICAM) policy.

We will explore those options, including new ways to help organizations authenticate mobile device users who need secure access to information systems and applications.

Is it IAM, IdAM or ICAM?

Whether you say IAM, IdAM or ICAM, they are essentially the same thing. IAM or IdAM (identity and access management) used to be more common, said Sarbari Gupta, an information security expert and CEO. Actively involved in information security for more than 20 years and co-author of several NIST Special Publications, Gupta said the "C" or credential in ICAM became more commonly used in the federal space because of former NASA ICAM Solutions Architect Tim Baldridge.

Around 2011, NASA's novel approach for using government-issued personal identity verification (PIV) smart cards to connect to Google Apps for Government sparked a lot of buzz. That's because the core method you use to prove who you are is the cornerstone of IAM's strength, Gupta said. You can't talk about IAM without talking about credentialing, such as PIV and common access cards (CAC).

KEYWORDS TO KNOW

Identity

The unique representation of a subject, such as a person, device, non-person entity or automated technology, that is engaged in a transaction involving at least one federal subject or a federal resource, such as federal information, an information system, or a federal facility or secured area.

Source: Whitehouse.gov

Identity proofing

A process in which an applicant provides evidence to a credential service provider reliably identifying themselves, thereby allowing the provider to assert that identity at a useful identity assurance level. Generally, there are two options for identity proofing: in-person and remote (performed over an online, networked session).

Source: NIST

Public identity

The unique representation of a subject that a federal agency interacts with, but does not directly manage, in order to achieve its mission and business objectives. Public identity may also refer to a mechanism of trust used to render services to the American public.

Source: Whitehouse.gov

Digital identity

The unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service but does not necessarily need to uniquely identify the subject in all contexts. In other words, accessing a digital service may not mean that the subject's real-life identity is known. Identity proofing establishes that a subject is who they claim to be.

Source: NIST

Federal enterprise (enterprise identity)

The unique representation of an employee, a contractor, an enterprise user such as a mission or business partner, a device, or a technology that a federal agency manages to achieve its mission and business objectives.

Source: Whitehouse.gov

Authorization

The process of granting or denying a user access to system resources once the user has been authenticated. The amount of information and the amount of services the user has access to depends on the user's authorization level.

Source: Identity Management Institute

Accounting

The process of keeping track of a user's activity while accessing the system resources, including the amount of time spent in the network, the services accessed while there and the amount of data transferred during the session.

Source: Identity Management Institute

Authentication

Proves a user's identity. It is based on the idea that each user will have unique information that sets him or her apart from other users to provide proof of identity. There are primarily four types of authentication methods and they use static passwords that remain active until they are changed or expired; one-time passwords, such as codes delivered thorough SMS texts or tokens used for each access session; digital certificates; and biometric credentials.

Source: Identity Management Institute

Close to **90%** of businesses will use biometric authentication by 2020. Today, **57%** of organizations use fingerprint scanning as large companies attempt to get rid of the need for passwords.

CREATE & MAINTAIN AN IDENTITY

Source: idmanagement.gov

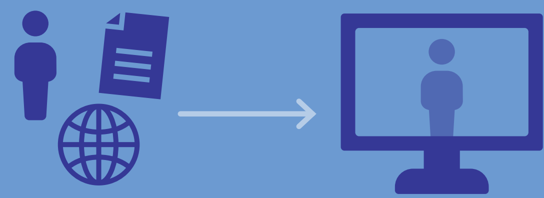
When an employee or contractor onboards at an agency, their identity information is collected and stored to act as their digital proxy in IT systems. This information is stored within an identity record, which may be modified or deleted as needed.

Once this digital identity record is established, it may be pushed to other systems from an authoritative source and provisioned access permissions.

- Employee or contractor
- Personnel admin
- Application
- Authoritative source
- Data repository
- Change to the identity record

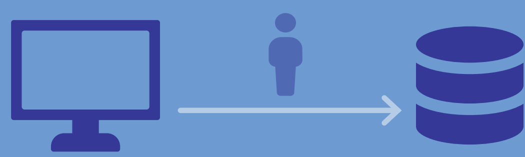
1. INFORMATION POPULATED

Personnel information is populated into the authoritative source. *Sources for this information could include onboarding documents or HR systems.*



2. NEW IDENTITY RECORD CREATED

The authoritative source sends the information to the system's data repository.



3A. MODIFY RECORD *MANUAL*

The administrator receives a change request and updates personnel information in the authoritative source.

3C. DELETE RECORD

The administrator deletes the identity record within the authoritative source when notified that deletion is required.

3B-1. MODIFY RECORD *SELF-SERVICE*

The individual uses an agency application to update their personal information.

3B-2. MODIFY RECORD *SELF-SERVICE*

The agency application updates the individual's identity record within the authoritative source.

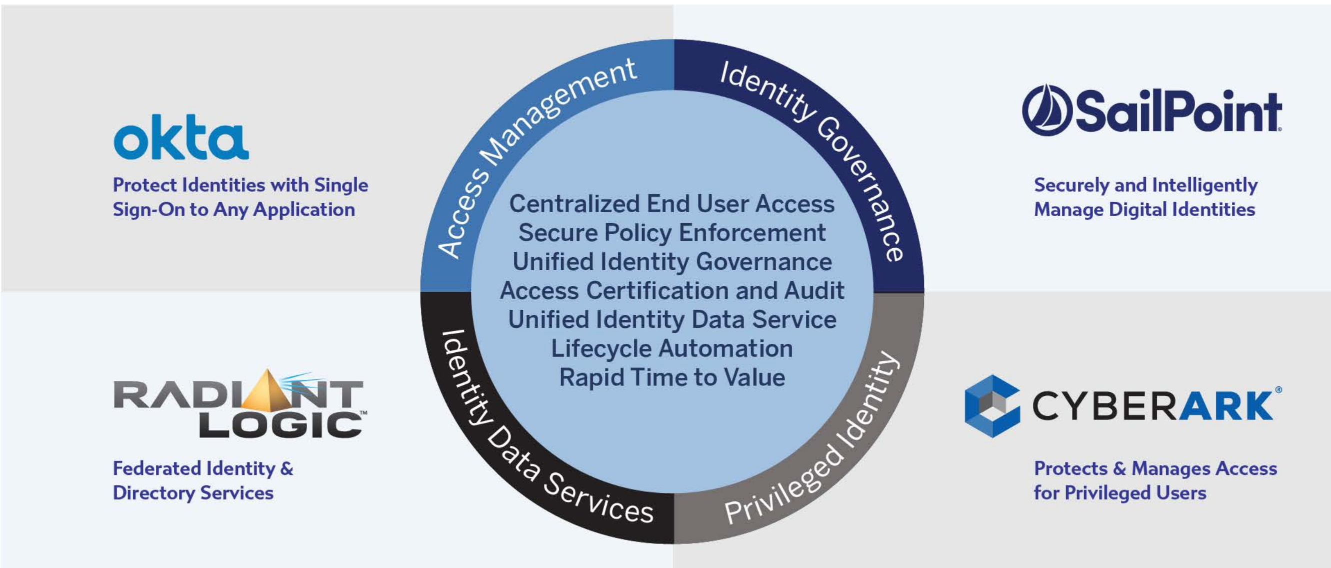
4. DATA REPOSITORY UPDATED

The authoritative source updates the available identity information to the data repository.

Carahsoft Solutions Portfolio
Identity and Access Management

Identity and Access Management have become crucial to organizations' security, helping them stay secure and compliant at the same time and never compromising one for the other. Carahsoft represents best-of-breed solutions, providing agencies with a multi-faceted approach involving security, governance, automation and controls, and federated identity based on virtualization.

See how agencies are benefiting from these solutions in the use cases featured below, and learn more at **carahsoft.com/identity**.



Carahsoft's Identity and Access Management solutions are 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.

CyberArk: Managing Privileged Accounts & Credentials

A federal government agency was struggling with balancing security with productivity as well as rampant password reuse across multiple accounts. They found that their IT admins had more privileges than they truly needed, and there were too many endpoints with local administrator privileges. The agency knew they needed to be better prepared for an audit, and they were also driven by an executive mandate.

The agency wanted a solution that could provide for privileged access security to limit the exposure of privileged credentials; enforce strong passwords, store them in an encrypted vault, and rotate them; and secure infrastructure and assets in the cloud.

They turned to CyberArk to protect their highest-value information assets, infrastructure and applications, deploying CyberArk to secure privileged credentials in a vault, rotate credentials based on policies, and secure and rotate shared service accounts.

The agency also plans on managing the following types of privileged accounts, credentials and secrets with CyberArk in the next 12 to 18 months: Domain admin accounts; Microsoft Windows admin accounts; NIX admin accounts (UNIX and Linux); and database or application admin accounts.

Since adopting CyberArk, the agency reports that they are now more secure, that the time and cost of audit reporting has been reduced, and that the time required to manage and maintain privileged account and credential security has been reduced significantly.

Okta: Improving Security, Reliability, Scalability & User Experience

Okta helps governments around the world serve citizens better with increased security and reduced cost. Lately, they've been noticing a trend in the government agencies they work with.

"We are seeing agencies that hope to modernize citizen- and public-facing properties," said Ted Girard, Vice President Public Sector, Okta. The Centers for Medicare and Medicaid Services (CMS) selected Okta to transition the agency to a modern and flexible identity architecture and to build the Quality Payment Program (QPP) interface, centered around shifting U.S. healthcare to a value-based payment model and away from traditional fee-for-service.

"They chose Okta's Identity Cloud to improve the security, reliability, scalability and user experience for its QPP web presence," Girard explained. The QPP is the external facing system that interacts with all healthcare professionals who provide Medicare and Medicaid services.

"CMS and their users had such a good experience after the portal was modernized, that they have now brought us in to work on internal-facing portals for them," Girard said.

The State Department's Directorate of Defense Trade Controls had a similar experience when they modernized a paper-based system that interfaces with aerospace and defense contractors. They chose Okta as the IAM solution for their custom applications.

"In short, we've noticed that the first things getting modernized are public-facing properties, and then that positive experience leads an agency to want to do this for their employees and contractors too."

Radiant Logic: Building a Modern, Flexible Identity Architecture

The Department of Homeland Security (DHS) consists of numerous different programs and agencies such as FEMA, TSA, and the US Borders and Protection Agencies. Its employees needed fast and secure access to the DHS network for email, facility control, training and attendance systems. However, identity and attribute data was fragmented across multiple data repositories, and incorporating change required manual, repeated steps. In addition, every internal system used a unique collection of the user's digital identity and credential data. Keeping a high degree of access control over this wide array of application types and points of entry presented a constant challenge to the DHS's IT personnel.

To help aggregate all identities for proper authentication and authorization, DHS set up the Trusted Identity Exchange (TIE), enabling and managing the digital flow of identity, credential, and access-management data for DHS employees and contractors. TIE is powered by RadiantOne, a federated identity and directory service based on virtualization. It establishes connections to various internal authoritative data sources and provides a secure, digital interface to other DHS consuming applications — essentially a 'one-stop-shop' of trusted identity information.

This cross-agency federal identity infrastructure can produce the specific composite views required by each application. RadiantOne is now a key enabler for many important DHS initiatives, including the DHS Data Framework, Personal Identity Verification (PIV) Smart Card usage, Single Sign-On (SSO) and fine-grained, attribute-based authorization.

SailPoint: Providing Identity Access Management for Custom Applications

Over the past year, Karen Wrege, CIO, Department of State's Directorate of Defense Trade Controls (DDTC), led a major "cloud first" IT modernization effort to improve efficiency and security for DDTC employees and external customers.

Tasked with modernizing DDTC's IT platform, Wrege's team launched the Defense Export Control and Compliance System (DECCS) in February 2019. This online portal provides industry with consolidated access to needed DDTC applications, and significantly streamlines operations. It also gives thousands of external users access to a system housing millions of Controlled Unclassified Information documents.

After attempting a custom solution, the team explored a COTS IAM solution, looking for one that would provide security for users within and beyond their network, integrate custom and SaaS applications (new + existing technology), and could be procured quickly. Based on meeting the wish list objectives and other government successful government uses cases, Wrege selected Okta as the IAM solution for their custom applications and ServiceNow implementation.

DDTC's new IAM strategy has reduced customer wait times and improved the customer experience. After a successful implementation, the Department of State recently assessed IAM requirements to satisfy the need for on-premises IAM for thousands of domestic employees — and an even greater number of personnel serving overseas. Based on the assessment, the team identified criteria, ultimately selecting Radiant Logic, SailPoint, CyberArk and Okta to support all users internal and external.

Identity and Access Management in the Federal Government Today

CURRENT LANDSCAPE

IAM is not just about doing security to comply with government requirements. Instead, it's a means to ensure the consistency and trustworthiness of government services, especially as digital options expand.

This expansion means that office walls no longer define agencies' perimeters because employees are increasingly accessing resources and data remotely from various devices. In light of these and other changes, OMB issued updates to the federal government's ICAM policy in May 2019. Among other things, the policy calls on agencies to take a risk management approach to identity management and align with NIST guidelines.

Gone are the days when simply adhering to a checklist of security mandates was enough to defend against online impersonators, fraudulent claims and other attacks. Agencies must understand the unique risks they face and use that information to drive what technologies and mitigation strategies can reduce them, according to NIST Special Publication 800-63 revision 3, which establishes digital identity guidelines for federal agencies.

The policy update also calls on agencies to shift from managing who has access inside and outside their perimeter to using identity as the foundation for managing risks resulting from attempts to access federal resources. Having stronger authentication methods in place requires malicious actors to have better capabilities and expend greater resources to successfully subvert the authentication process, according to NIST.

Following the massive Office of Personnel Management (OPM) breach in 2015, the Obama administration launched a 30-day cybersecurity sprint to assess and improve the health of federal IT. That decision set into motion an accelerated effort to ensure all users, especially privileged account holders such as system administrators, use PIV cards to access federal networks and systems.

Those efforts are still being felt today, according to Sabari Gupta, an IAM expert. Even if agencies are not fully compliant with the federal directive requiring PIV cards, they are prioritizing the use of these credentials for account holders who could do the most harm to the organization.

93%

Federal agencies enforce the use of PIV cards among **93 percent** of their privileged users, or those who have access to large amounts of sensitive agency and citizen data.

WHY IS IAM ESPECIALLY IMPORTANT NOW?

The number of digital transactions between the public and government agencies is rapidly increasing. Citizens can skip in-person visits, and with a few clicks or swipes, they can file taxes, apply for food assistance and renew a license.

Although the rapid expansion of digital services has given the federal government faster, more reliable operations and connections with the public, it has also shed light on IAM's critical role in providing a seamless digital experience.

IAM is particularly important now as technologies such as cloud mature and older IT systems become obsolete. "A new set of challenges has emerged, because information about individuals has become more widely available through social media and breaches of personally identifiable information (PII)," according to the OMB memo on ICAM. "Identity management has become even more critical to the federal government's successful delivery of mission and business promises to the American public."

Agencies must adopt identity validation solutions that enhance privacy and mitigate negative impacts on the delivery of digital services and maintenance of online trust.

64%

of U.S. federal IT leaders view identity management as critical to cybersecurity.

HOW DOES IAM SUPPORT IT MODERNIZATION AND OTHER EFFORTS?

As noted earlier in the guide, IAM underpins many government efforts, including conducting background investigations, managing access to federal IT assets on-premise and in the cloud, and deploying emerging technologies such as RPA.

IAM allows for secure and frictionless information sharing with the right people at the right time, and this is especially important as more government services move to cloud-based models. To support the increase of mobile technologies, OMB has made clear that agencies should use derived credentials, which provide strong authentication for mobile devices.

With the rise of automated tools that can take on identities of their own, agencies must be capable of managing digital identities for RPA tools and AI.

For example, software bots can run unattended and work round-the-clock, meaning a person does not have to physically oversee all the work a bot is doing. This is great for productivity, but autonomous bots can raise security concerns.

That's why OMB requires agencies to ensure that digital identities for automated tools are distinguishable, auditable and consistently managed across the agency. "This includes establishing mechanisms to bind, update, revoke and destroy credentials for the device or automated technology," according to the memo.


Modernize faster with Okta
Agencies need innovative solutions to modernize infrastructures, increase security and reduce cost while serving citizens better.
Identity Management is the hidden accelerator for secure digital transformation.
Okta provides FedRAMP compliant cloud identity solutions that help government agencies do more faster.
www.okta.com/solutions/government
okta

INDUSTRY SPOTLIGHT

Mitigating Threats While Enabling the Citizen Experience

An interview with Ted Girard, Vice President of Public Sector, Okta

Agencies today are looking to better reach citizens and improve internal processes, all while staying ahead of modern threats.

But as agencies focus on these efforts, they must be mindful of mitigating dangers to their data.

Credential-based attacks – such as phishing, password spraying, brute force and more – are common vectors that can be mitigated with strong multifactor authentication, built into the workforce/IT experience and also constituent-facing programs.

Whether your agency is building a new citizen-facing portal or unifying a constellation of existing services, there are ways to prevent these credential-based attacks and make web and mobile access secure, compliant and frictionless.

"Today, people are accessing more resources from more locations than ever before, changing the dynamic away from the previous 'castle-and-moat' or perimeter-style approach to security and instead centering controls around the only commonality in today's environment: people – and their identities," said Ted Girard, Vice President of Public Sector at Okta.

"By tackling security from a zero trust lens – and we've heard from a number of customers that identity is often where they start on their zero trust journey – they'll be better equipped to mitigate today's threat actors, especially those employing the common credential-based attacks."

To this end, the Office of Management and Budget (OMB) recently updated its federal identity, credentials and access management (ICAM) policy, encouraging the use of more flexible solutions, supporting pilots for new authenticators and requiring agencies to create an ICAM team.

The memo notes: "While hardening the perimeter is important, agencies must shift from simply managing access inside and outside of the perimeter to using identity as the underpinning for managing the risk posed by attempts to access federal resources made by users and information systems."

"The memo aligns really well with how Okta sees identity's role evolving both from a management and security/privacy perspective in government agencies," Girard explained. "Okta can play a role in supporting major IT modernization projects, as well as in improving security for agencies. Our cloud-based, industry-leading identity and access management platform comes with all of the tools you need to manage a complex user base at scale."

IT and security leaders recognize the need to adopt new, often cloud-based technologies to better support and secure their workforces and constituents, but they're also faced with decades' worth of legacy technologies, regulations and processes that stifle adoption and growth.

"Okta can help make the transition easier and more secure, which is why today dozens of agencies use Okta to consolidate disparate systems, securely adopt cloud services and find new ways to better reach their constituents," Girard concluded.

"Today, people are accessing more resources from more locations than ever before, changing the dynamic away from the previous 'castle-and-moat' or perimeter-style approach to security and instead centering controls around the only commonality in today's environment: people — and their identities."

TAKEAWAY:

Agencies must shift from simply managing access inside and outside of the perimeter to using identity as the basis for their security posture.

IAM FEDERAL POLICIES, GUIDANCE, STANDARDS

OMB's **"Enabling Mission Delivery through Improved Identity, Credential, and Access Management"** memo updates the federal ICAM policy. (May 2019)

NIST Special Publication 800-63 revision 3 provides technical requirements for federal agencies implementing digital identity services. (June 2017)

The White House's **National Strategy for Trusted Identities in Cyberspace** enhances the security and privacy associated with online transactions. (April 2011)

The **Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance** provides a common framework for rolling out ICAM programs across government. It also includes a variety of use cases for managing internal and external identities. (December 2011)

HSPD-12: Policy for a Common Identification Standard for Federal Employees and Contractors is a strategic initiative intended to enhance security, increase government efficiency, reduce identity fraud and protect personal privacy. It requires the development and implementation of a governmentwide standard for secure and reliable forms of identification for federal employees and contractors. (August 2004)

To review other federal policies and standards that impact and shape the implementation of ICAM programs and systems, visit arch.idmanagement.gov/standards.

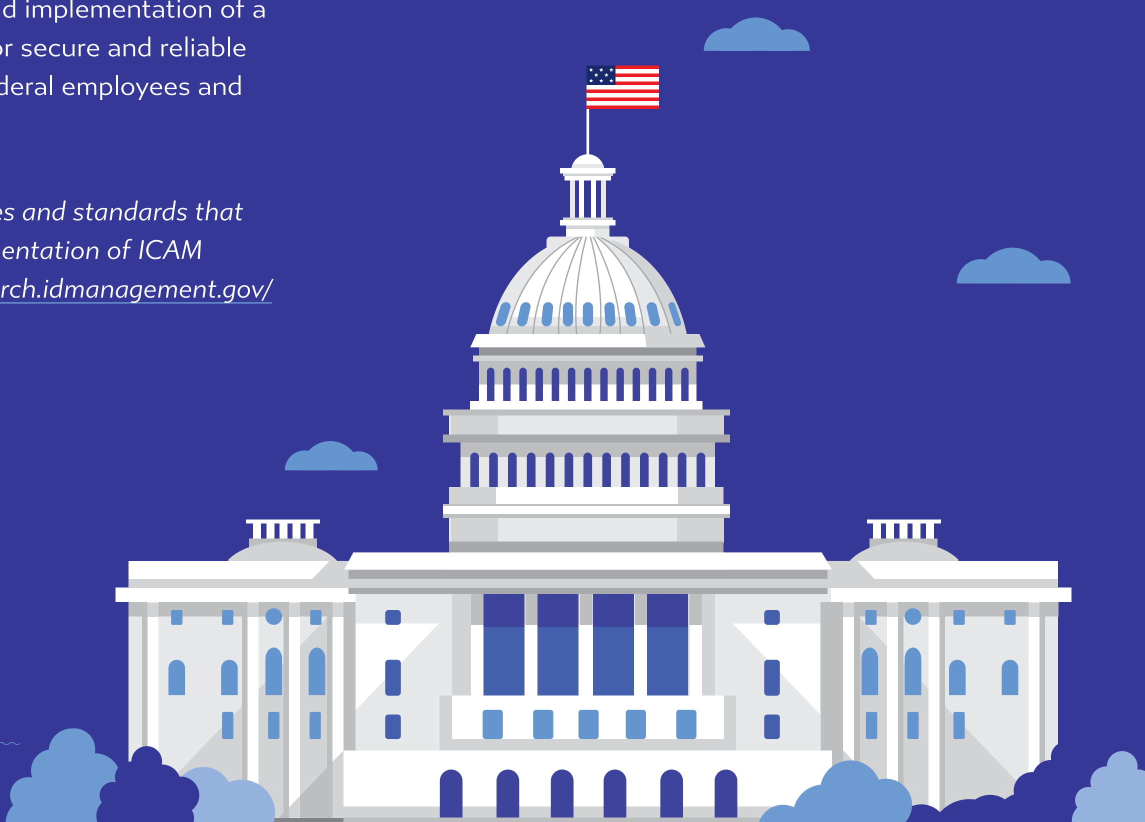
FEDERAL LAWS THAT IMPACT IAM

The **Privacy Act of 1974** covers the privacy of individual federal records, including systems that require the retrieval of records based on PII such as Social Security numbers.

The **Health Insurance Portability and Accountability Act** protects personally identifiable health information by mandating privacy compliance with federal guidelines. IAM is crucial to the use of federated identities, single sign-on (which allows for access to multiple, independent software services based on a one sign-on verification), multifactor authentication and role-based policies.

The **Government Paperwork Elimination Act of 1998** mandated that individuals have the option to submit information and maintain records electronically. The act established the validity of electronic records and signatures.

The **Federal Information Security Management Act of 2002** necessitates that each federal agency has a cohesive program to secure information within the information systems that support operations.



Q&A with David Temoshok, NIST IT Lab's Senior Policy Adviser for Applied Cybersecurity

One agency plays a critical role in creating guidelines for other agencies to follow in the realm of IAM. NIST establishes standards for information systems security across the federal government through a series of guidelines and best practices in NIST Special Publications.

NIST views information system security from an internal standpoint, or how the federal government uses information systems, and an external perspective, in terms of responsibilities the government has to citizens.

"All of our information security deals with identity and access management, whether that is physical access management or logical, on the line access," said David Temoshok, Senior Policy Adviser at NIST's Trusted Identities Group. "We look at the context for that, for how we manage our information systems and access for our employees and other individuals who are privileged to access our systems."

GovLoop interviewed Temoshok to learn more about how NIST addresses IAM across the federal sphere.

The responses below have been lightly edited for brevity and clarity.

GOVLOOP: What issues are top of mind for you as an IAM professional in government?

TEMOSHOK: First, in terms of security, we want to make sure that anyone accessing our resources is in fact who they claim to be. We manage our resources based on privileging who can access resources, and we make sure that we can identify those individuals and confirm or authenticate that they are who they claim to be.

The second factor that our security and access management is centered around is protecting information. We want to make sure that we protect the information that may be necessary in order to determine access. So, privacy and security go together as our top priority issues.

The third thing that I would say is key to us is usability. Security can make things difficult or complex for users, and we want to make sure that our IAM controls always consider usability, so that controls aren't too complex for users.

What are some challenges that agencies face when implementing IAM?

The first would be dealing with the public. For federal agencies that deal with the public and want to move services from a paper-based process to an online process, like the Internal Revenue Service or the Department of Education or the Social Security Administration, they are all looking at providing online services in a secure way. If it's necessary to know who you're dealing with in an online service, and in most cases it is, it becomes necessary to have a legitimate way to prove the identity of that claimed individual.

Identity proofing remotely with the public is very challenging. It means being able to verify identity evidence, in the form of a driver's license or another form of evidence, remotely. Let's just call that assurance. And we recognize that there can be different levels of security or assurance that are needed for different types of transactions.

Again, the key issue for us is the privacy and the protection of personal information that we may collect. So, the challenge as we try to move additional services online to allow access to federal services and transactions to the public, is that we also need to be able to expand our capabilities to be able to securely provide assurance that federal agencies are dealing with who the individuals claim to be. We call that authentication.

What do you think the current trends around IAM are in the federal space?

The trend that we are advancing to the federal government is to move from user ID, PIN and password to multifactor authentication, which involves using two forms or more to identify a user remotely.

I would give an example of those industry initiatives in the form of the specifications developed by the SAS Identity Online Alliance. Those provide for very secure cryptographic controls that are very user-friendly in a digitally accessible program. Those types of devices are commonly available on Amazon and through other outlets, and we encourage that type of use, both for internal use in the federal government, as well as for the public.

"Security can make things difficult or complex for users, and we want to make sure that our IAM controls always consider usability, so that controls aren't too complex for users."

Can you talk about ID and access management in terms of the everyday employee? What do advances in this area mean for the way that they perform their jobs?

In terms of the everyday employee, a little bit of background is necessary. In 2004, the president signed HSPD-12, which required a secure badge and identification capability for physical and local access for all federal employees. It was a common badge and common identifier, and wasn't intended to be agency-specific, but governmentwide. We published the standard for that badge in 2005, called the PIV Standards.

However, with the current workforce being mobile and agencies wanting to be able to have the same access of the PIV card, there's a smart card that's the size of a debit or credit card that has an RFID [radio-frequency identification] chip. Now all laptops and desktop computers have ports that allow these cards to be inserted and read. However, smartphones do not have a similar type of port for a card like that to be able to read the chip on the device.

It's become very key for us to have both security and privacy for access control and to extend that capability to the federal user. There are many jobs in the federal government that require employees to be away from the duty station to fulfill their responsibilities. This allows them to gain access to their online applications and information in a way that is secure, usable and protects their information.

Identity and Access Management in State and Local Governments Today

CURRENT LANDSCAPE

Agencies are searching for cohesive solutions to their IAM needs, especially as they contend with the siloed approaches that led to this need in the first place. According to the National Association of State Chief Information Officers (NASCIO), some states have turned to federated ID frameworks to avoid duplication by using a shared services model for identity and access. Most states are either creating frameworks independently or neglecting the issue altogether.

NASCIO's findings were noted in its 2012 strategic vision for state-based identity, credential and access management efforts. But the lack of federated ICAM models across state and local governments persists.

The nonprofit ACT-IAC, which focuses on improving collaboration between government and industry, found that "sharing among external states is currently limited due to challenges, such as funding and the lack of a common platform." At its core, a federated government framework provides centralized services to citizens, businesses, employees and other government entities across state, local and federal jurisdictions.

"It illustrates how government entities can share services across independent information technology domains and federation with states," according to a 2018 ACT-IAC report.

When you consider the law enforcement sector and how often cases span cities, counties and even state lines, it's imperative that governments can coordinate and easily share information. A federated identity system could lay the groundwork for new systems that allow for these seamless connections.

NASCIO

NASCIO STATE CIO TOP 10 PRIORITIES

2019 Strategies, Management & Process Solutions

1. Security and Risk Management
2. Cloud Services
3. Consolidation/Optimization
4. Digital Government
5. Broadband/Wireless Connectivity
6. Budget, Cost Control, Fiscal Management
7. Customer Relationship Management
8. Data Management and Analytics
9. Enterprise IT Governance
10. **Identity and Access Management**

Source: NASCIO

WHY IS IAM ESPECIALLY IMPORTANT NOW?

At a time when ransomware and other attacks are on the rise, state and local governments must do all they can to secure their data and systems. Increased security within a state correlates with diminished identity theft incidents, fewer data breach cases and better levels of trust. IAM bridges the weak points in an agency's efforts to identify and authenticate users, encrypt sensitive data, and log and audit information.

81%

of hacking-centered breaches are tied to weak or stolen passwords.

States are required to measure and report the results of federally funded programs in areas like health, job creation, voting and welfare. For example, the Education Department's State Longitudinal Data Systems involve the ability to measure student performance and the moving parts that affect educational outcomes from preschool to age 20. State governments must analyze student and teacher data across multiple state departments that are involved with delivering educational services, such as human services, K-12 education, workforce development, corrections and higher education.

There has to be a unique identifier to make sure that students are linked between systems, and that's where identity management can play a significant role.

Communicating identity information among departments is also important so that new updates are easily shared from one agency to the other.

HOW DOES IAM SUPPORT IT MODERNIZATION AND OTHER EFFORTS?

Law enforcement and public-safety organizations, in particular, are working together to increase efficiencies and improve information sharing to better meet community needs. However, there are many risk management considerations for modernizing and applying new technology approaches to drive better outcomes.

Leaders need to be aware of current thinking around digital and data trust, cloud-based services, and analytic and machine learning as they prepare for the next generation of technologies that support a secure, safe, resilient homeland of the future.

That's why investments in IAM are critical. Efforts around the development of FirstNet, a dedicated broadband network for public-safety workers, are a prime example of the important role that IAM plays in enabling first responders.

Registration, verification, authentication and authorization of public-safety officials and other approved users are vital to protecting the integrity and safety of the broadband network. This is not a one-time event, but rather an ongoing exercise to account for changes in roles and responsibilities and changes in employment status.

Delaware is eyeing innovative ways to share opioid information with police departments statewide, according to ACT-IAC. "State agencies are potential building blocks for a national opioid 'data lake' that can be accessed by law enforcement officers throughout the nation."

Consolidating an agency's processes and workflow under the overarching objective of following IAM guidelines can reduce costs for security IT infrastructure. Plus, the entire IT enterprise could be improved, and PII better protected.

STATE AND LOCAL POLICIES, GUIDANCE, STANDARDS

NASCIO published the **State Identity and Credential Access Management (SICAM) Guidance and Roadmap**, which takes a strategic approach to state IAM efforts and highlights the importance of implementing SICAM architecture. According to the publication, "states can, and should, provide a secure, auditable environment for the processing and exchange of information across the entire spectrum of state business." (September 2012)

California released an updated version of its **SICAM guidance**, which has similarities to the NASCIO version. (October 2013)

The New York State Department of Financial Services released **cybersecurity requirements for financial services**, which included access controls and identity management. A cybersecurity program should include limited user access privileges to systems that contain nonpublic information, according to the regulations. (March 2017)

STATE LAWS THAT IMPACT IAM

Virginia's Electronic Identity Management Act, which went into effect on July 1, 2015, was passed to bolster cybersecurity with a standard set of identity proofing methods that rely less heavily on passwords.

Utah passed legislation in 2016 that required the Department of Technology Services to create **a single-sign-on business portal**. The portal involves the Tax Commission, the Department of Workforce Services, the Labor Commission and the Department of Commerce, and it will become a common point of determining eligibility across all agencies dealing with health and human services departments and unemployment. The first phase is expected to be completed by July 2019.

In the past five years, **Michigan has undertaken an enterprise IAM solution** that allows users access to multiple state systems with a single user ID and password. More than 4 million state residents have logins through MILogin, which allows them to renew their driver's, hunting or fishing licenses. There is also a policy in place that all new software programs and major rewrites have MILogin as their front-end identifier, and several systems are going live with the single-sign-on login this year.

LOCAL IAM PROJECTS

Boston revealed a two-year, $2.4 million **citywide IAM project**. The project involves a web portal with single-sign-on access and improved security measures. (April 2019)

Detroit ID, run by the Health Department's Administrative Office, launched in December 2016 to help users open checking and savings accounts, and provide proof of ID to police and other authorities.

The City Key Program in Chicago was launched in December 2017 by the City Clerk's office to provide a means of having a transit card, library card and ID for prescription drugs.

New York City has a program called **IDNYC** that was launched in January 2015. With the ID, a New York City resident can take the high school equivalency exam, open a bank account and access discounts on prescription drugs.

Oakland, California offers the **Oakland City ID** as of February 2013. This is a valid means of providing proof of ID to police and to open a bank account. It also grants access to homeless services and food assistance.

Providence, Rhode Island offers **IDPVD** as of June 2018, which is proof of ID to police and other authorities, proof of residency, and a way to access local discounts.

INDUSTRY SPOTLIGHT

Identity Is the New Perimeter

An interview with Frank Briguglio, Public Sector Identity Governance Strategist, SailPoint

Today in government, the security perimeter and user credentials have expanded to include mobile devices, SaaS applications and technology such as software bots. At the same time, compromised user credentials have become vulnerable to sophisticated cyberattacks. Together, these changes have created a critical need for strong identity governance in the federal government.

But limited budgets and a shortage of trained cybersecurity personnel can make it difficult for government agencies to verify that user access is authorized, secure and compliant.

To learn why strong identity governance strategy can help the public sector move past these challenges and achieve compliance and security objectives while empowering end users, GovLoop sat down with Frank Briguglio, Public Sector Identity Governance Strategist at SailPoint. SailPoint is a leader in Identity Governance and Administration.

Data breaches that expose user identities are on the rise. In 2018, the Identity Theft Research Center reported that hacking was the most used method of breaching data, with 482 data breaches resulting in almost 17 million records exposed.

Briguglio explained that enterprise security is in need of a new paradigm and must evolve from network-centric to identity-centric. The increasingly complex relationships between people and data is redefining perimeter defenses, and it means that the public sector must think about identity in a very different way.

"The traditional network as we know it today can be breached," said Briguglio. "So how do we protect our high-value assets? Really, identity and the access controls are the best way."

According to Briguglio, a strong identity governance strategy is what will help the federal government achieve compliance and security objectives while empowering end users.

The role of identity governance is simple in principle: give the right people the right access to the right data. To do this, trusted and properly managed identity access has to become the primary control.

That's where SailPoint comes in.

"SailPoint offers a modern identity governance and administration platform," Briguglio explained. "We can be deployed on premise, in the cloud as a SaaS solution or as a managed service. We can deploy everywhere, anywhere, to meet the requirements of federal, civilian, our DoD and Intelligence Community agencies."

As the trusted vendor managing more than 2 million identities at 54 agencies, SailPoint helps the federal government meet their compliance requirements by controlling who has access to IT resources and monitoring how that access is used. Their cloud identity governance platform uses automated IT processes to drive efficiencies and maintain stringent regulatory compliance requirements. It also helps agencies apply machine learning techniques to prevent unwanted application and data access that typically leads to data breaches.

Using the right identity access management solution will empower users to manage their passwords and simplify the process for gaining access securely, Briguglio concluded.

"The identity is more important than ever, and to remain secure and compliant, you need to look beyond how you've approached access in the past and modernize your identity governance."

TAKEAWAY:

The identity is more important than ever, and access management is just one piece of the security puzzle. Government security teams must govern broad and govern deep.

Q&A with Adam Zeimet, Branch Chief for ICAM at USDA

The ICAM program at USDA started about 16 years ago with the E-Authentication Initiative. It's evolved since then to support more 120,000 employees and 750,000 public users.

Adam Zeimet, Branch Chief for ICAM at USDA, has been with the program since it started. He talked to GovLoop about central considerations to ICAM at the agency.

The responses below have been lightly edited for brevity and clarity.

GOVLOOP: USDA is making it easier for farmers to access services online, such as paying loans. Are you involved in these efforts?

ZEIMET: Yes. We support a lot of that on the backend. I think that as more of those kinds of citizen interactions move online, we have to focus on how we establish trust in those users and verify them, but also do it in a way where we can prioritize customer-focused experiences. Our CIO likes to say customer-obsessed experiences have probably never been more important than they are now. The challenge for us is enabling enterprise-grade security for these types of systems, but with consumer-grade experiences. The expectation of the user experience that the average user — and especially public citizens — has now is high, and the government is no exception.

What issues are top of mind for you as an ICAM professional in government?

On a broad scale, I want to shape ICAM from being seen as just a domain of cybersecurity, or even just compliance, which is how it's been thought about for a long time. It should be something that is a strategic partner and value-add enabler for the business and the mission that the agencies are trying to serve.

What does being a strategic partner look like? Does that mean that you're a part of the conversation early on when people are talking about launching a digital service or doing something new online?

A lot of these kinds of things come from being a part of the team and not bolting things on afterward. I think that applies to the security aspect, but it applies to the user experience aspect as well. As we move to more and more digital services, especially citizeninteraction-type things, it's impossible to plan those initiatives without planning for how we get the users that need access to the system into it. How do we deliver services directly to users?

I think it's impossible to build and plan those services without accounting for how identity and access should be incorporated into that. Really starting to drive that kind of identity-centric thinking, whether we're planning services or initiatives like moving to the cloud, moving workloads to the cloud outside of the traditional security perimeter, mobile as that applies to employees or citizens: all of those little things require identity-centric planning when security and those user experiences are being planned for.

Are there any trends in this space that we should focus on? Any challenges in particular?

I think cloud mobility, artificial intelligence and robotic process automation are becoming big things. All of those represent a fundamental shift for what IAM programs need to be able to focus on. Especially in government, I think that the era of focusing on smart cards is really over, and we need to be expanding ICAM to look at more of these types of services and how we support them. I think ICAM is an enabling platform for those kinds of initiatives.

As it relates to ICAM, I think user experience and automation and increasingly building in security from the start are some of the key items for what all those things mean for ICAM. ICAM needs to help enable broader digital transformation.

You mentioned AI and RPA, and when I think about those technologies in particular, it's almost like bots have identities. Can you speak to the relationship among AI, RPA and ICAM and how you view your role in enabling that?

To say that bots have a sort of identity is absolutely the right way to think about it. If the entity on the network has access — it is a often quite a bit of access — and the same access that a human might have in various systems. So, it's really essential that those identities — nonperson identities but identities nonetheless — be managed.

The whole goal of RPA is to streamline processes and automate simple tasks to the greatest extent. So with that, a lot of those tasks are going to include access to systems, authenticating things, being accepted or rejected for the types of things that they're trying to do. We have to be able to automate the issuance of those robotic-type identities and the types of credentials that they have and make sure that their credentials are just as strong as the credentials that a human would be using and doing in a way that streamlines those processes.

Is there something you're actively looking at or focusing on now? What kind of state are you in?

I think USDA is just starting to look at those kinds of capabilities and where they can be implemented into the different agency workflows that exist. From an ICAM perspective, I think our goal right now is to modernize our systems and capabilities so that we can have a platform that supports those initiatives when they really begin in earnest.

Are any current projects or efforts related to ICAM under way? What are the objectives of those efforts?

We're working to modernize our ICAM platform specifically around identity lifecycle management and our authentication services. The goal there is to increase automation around identity and around the assignment and granting of access, but also improving user experience.

We recently finished implementing Phase 2 of the Homeland Security Department's CDM [Continuous Diagnostics and Mitigation] program. The CDM program was a huge accelerator for us on these different modernization efforts that we've been undertaking as we try to continuously improve and evolve our ICAM capabilities.

We are also rolling out a Derived PIV credential solution for our mobile devices, which enables us to get away from passwords and get our mobile computing infrastructure compliant with HSPD-12. With the release of OMB's new ICAM policy, we are also looking to expand this to other credential types.

Unsecured privileged accounts add risk to your business anywhere they exist— 100% of advanced cyber attacks involve them. Seamlessly protect privileged accounts across the enterprise— on premises, in the cloud and on your endpoints with CyberArk.

Federal Certifications and Compliances Include:

- DoD UC APL
- Common Criteria Certified
- NIST SP 800-53 / -171 / -82 / -63
- NERC-CIP
- DHS CDM Phase II Privilege Management Solution
- Army Certificate of Networthiness (CoN)
- Available on DoD Cyber Range
- HSPD-12
- In Evaluation for NIAP

CyberArk.com

CYBERARK®

INDUSTRY SPOTLIGHT

Thinking Like an Attacker to Protect Privileged Access

An interview with Kevin Jermyn, Regional Manager, Federal Customer Success, CyberArk

Federal agencies, departments and critical infrastructure today are frequent targets of targeted cyberattacks from the world over. These attackers hope to compromise complex government data, steal personally identifiable information (PII) or disrupt day-to-day operations, making it difficult to safeguard the government's critical infrastructure.

To ensure protection of vital information, data and systems, leadership in the White House, Congress and the Homeland Security Department have worked to develop security mandates and regulations designed to secure agencies from both internal and external threats.

Privileged account protection and threat detection are at the center of many of these requirements due to their powerful role in providing access to critical cyber infrastructure and sensitive information.

To learn more, GovLoop sat down with Kevin Jermyn, Regional Manager, Federal Customer Success at CyberArk. CyberArk is a privileged access security market leader, focused on protecting data, infrastructure and assets in on-premises, cloud, hybrid and ICS environments, and throughout the DevOps pipeline.

"Privileged access can be exploited and used to gain access to sensitive data," said Jermyn. "We've seen time and time again, attackers will get into the network. It's not about keeping them out; it's about limiting what they can do once they are in the network. How do we stop them from escalating privileges and moving laterally?"

Securing privileged access is critical; industry data suggests that nearly all targeted attacks involve the compromise of privileged credentials. Simple, automated privileged access security focused on risk reduction can increase information security and improve operational efficiency.

Designed from the ground up for security, the comprehensive CyberArk Privileged Access Security Solution helps government agencies efficiently manage privileged credentials and access rights, proactively monitor and control privileged activity, intelligently identify suspicious activity and quickly respond to threats. It helps IT security teams automate routine privilege functions and reduce risks of human error – and integrates with more than 100 vendors to help agencies proactively reduce risk.

Privileged access security, done well, complements identity access management and takes security and compliance a step further by helping IT teams get control over privileged accounts and credentials and provide granular visibility on how identities are actually being used. With built-in reporting and auditing features, the CyberArk solution helps agencies meet stringent compliance mandates.

"Privileged access is everywhere within an environment," Jermyn concluded. "Government needs to be thinking about it more broadly than just a user accessing a server. There's a lot more privilege that exists out there. Especially as agencies invest in cloud and DevOps, the privilege-related attack surface expands dramatically."

"We've seen time and time again, attackers will get into the network. It's not about keeping them out, it's about limiting what they can do once they are in the network. How do we stop them from escalating privileges and moving laterally? The way that we do that is think like them, and start to put in controls to block the most common pathways of privileged access, and then go from there."

TAKEAWAY:

Simple, automated privileged access security, focused on risk reduction, can increase information security and improve operational efficiency.

Breaking Down the Benefits of IAM

IDENTITY AND ACCESS MANAGEMENT

What it is: IAM is the security discipline and resources that enable the right individuals to access the right resources at the right times for the right reasons. It has two components: access management, and identity governance and administration. It's about managing user accounts and about the processes that bring new people into the organization, what privileges they receive and how those permissions evolve.

Why it's important: Today, government employees use technology in new ways to collaborate with one another and to access systems and data. But how do IT teams control that access and make sure government systems are secure?

Proper IAM is necessary to ensure that government employees have access to critical data, systems and facilities — and that external actors aren't compromising agencies.

IAM simplifies the management of access to services, implements policy, increases transparency and integrates enterprise identity management infrastructure. It also makes sure that the right people can access the right services at the right time, while managing user identities and providing secure access to devices, IT systems, networks and data for which they are authorized and authenticated. This service provides a common enterprise solution for government organizations.

By 2020, each person with an online presence will create about **1.7 megabytes of new data per second**. This is on top of the **44 zettabytes** of data that will exist in the digital space by that time.

FEDERATED IDENTITY MANAGEMENT

What it is: Federated identity management (FIM) empowers organizations with several technologies, standards and use cases to share applications by allowing individuals to use the same login credentials or other personal identification information across security domains. As IDManagement.gov states, "Federation is the ability of one organization to accept another organization's work. Federation is based on inter-organizational trust. The trusting organization has to be comfortable that the trusted organization has similar policies, and that those policies are being followed."

Why it's important: FIM provides a standardized means for allowing agencies to directly provide services for trusted users that they do not directly manage. Companies and government agencies that collaborate to share information see the value in authenticating identities via federated identity management across domains for secure access.

At the government level, the need for this type of verification exists internally and externally. For instance, an enterprise such as the FBI will use single sign-on to ensure user access within its own system. Yet there are instances when the FBI will also have to access the database of another government agency such as the Justice Department. In this case, a federated identity can grant an agent the ability to enter both seamlessly.

PRIVILEGED IDENTITY MANAGEMENT

What it is: Privileged identity management involves the monitoring and protection of superuser accounts in an organization's IT environment. This oversight is critical to ensure that these superusers' greater access abilities are not misused, abused or infiltrated.

Why it's important: "Privileged accounts provide elevated, often unrestricted access to an organization's underlying information systems and technology, making them rich targets for both external and internal malicious actors," according to NIST. "Often referred to as the 'keys to the kingdom,' these accounts have been used in successful attacks to gain access to corporate resources and critical systems (e.g., 'crown jewels'), resulting in data breaches. Complex organizations face challenges managing privileged accounts, which opens a significant risk to their business. If used improperly, these accounts can cause significant operational damage including data theft, espionage, sabotage, ransom, or bypassing important controls."

By centralizing privileged credentials in one place, PIM systems can ensure a high level of security for them, control who is accessing them, log all accesses and monitor for any suspicious activity.

IDENTITY GOVERNANCE

What it is: Identity governance (IG) enables and secures digital identities for all users, applications and data. It's enacted as a policy-based centralized orchestration of user identity management and access control that helps support enterprise IT security and regulatory compliance. IG creates guiding principles that determine who has access to what information in an organization. Additionally, it imposes the monitoring mechanisms required to evaluate the access and usage rights of individual users on an ongoing basis and flag anomalies.

Why it's important: In the ever-changing government IT landscape, which involves myriad distributed technologies, applications in the cloud, and private and public networks, it becomes all the more important to set appropriate access levels to various users. IG and administration tools help handle user identity lifecycle management.

IG systems generally have ways to manage multiple users. They include password management, access request management workflows that make it easier for users to request access to applications and systems and get approvals, and automated provisioning and deprovisioning at both the user and application levels.

WHAT DOES HAVING AN IDENTITY RECORD ENABLE?

Identity systems don't just benefit system administrators. Users can do some very handy things with an authenticated digital identity. Here's a short list:

- **Pre-filling online forms with verified information speeds up application processing.** There's less redundant effort, and users don't need to worry about basic errors.
- **Authenticated users can access and download data the system holds about them, such as account activity.** With a verified legal identity, the user can access very sensitive medical or financial records and even download them.
- **Identity systems can protect your privacy.** If you need to be 21 or older to access a service, you can authorize an identity system to confirm your age without sharing your exact birth date.

Source: login.gov

Q&A with Brandon Iske, ICAM Lead at DISA

IAM standards have heightened over the years as agencies adapt to increasingly effective cyberattacks and breaches.

Brandon Iske, ICAM Lead at the Defense Information Systems Agency (DISA) has been in the IAM space for close to nine years, serving at DISA for all of that time. GovLoop talked to Iske to pinpoint how DISA focuses on IAM issues and the agency's future plans.

The responses below have been lightly edited for brevity and clarity.

GOVLOOP: What issues are currently top of mind for you as an ICAM professional in government?

ISKE: The Defense Department Criminal Investigative Service has identified ICAM as a top four cyber initiative. So top of mind for me are our efforts in partnership with Design Management and Builders Corporation and the National Security Agency to solve enterprise challenges for DoD. We have a couple of capability enhancements that we're aiming to invest in and enhance that fall in the DISA lane, like automated account management provisioning, with master use of record capabilities, as well as centralized authentication for central identity providers. Those are the efforts that I focus on.

I'm curious about your process for identifying those central priorities.

Within DoD we have a senior-level forum. That is the official forum where over the last couple of years there have been entire team efforts across the services and agencies to define gaps in the identity space. So, most of the capabilities have been vetted through that senior leadership forum as top priorities, and then bubbled up as part of the DoD CIO's top 10 cyber initiatives.

What do you see as some of the current trends around how people talk about ICAM, how it's being implemented and what challenges agencies face?

I think DoD has an opportunity to enhance a lot of capabilities. We've been very focused on defense critical infrastructure and the common access part. You can look at programs like the CDM program in the Homeland Security Department, which has very specific investments and enhancements in the space. But my bottom line is that I think there is a lot of commercial capability out there that we just need to leverage and adopt.

A lot of our challenges aren't always technology challenges; they often involve the business process. We have hundreds of financial systems and need to look at who should have access. Those aren't IT problems; those are business problems. We have to work those business problems, and then have the technology to implement those separations and audit capabilities.

Why do you think ICAM is especially important now, with the rise of digital services and a push for more reliable self-service options for employees and citizens?

I think it's important. I think having a lot of applications in the cloud is a big driver. It's a big disruptor to how we've done things traditionally. I think the new heightened attention to DoD's financial audit has been a big driver as well. So we have a very high assurance authenticator that is our CAC. That has carried us quite far, for decades at this point. But I think there are additional commercial capabilities that help us streamline how we get access to systems. We rely today on a very painful or slow paper process, and so there's a lot of opportunity to enhance that as everyone looks to automate, whether you look across industry or government.

"A lot of our challenges aren't always technology challenges; they often involve the business process."

How would you describe the maturity of policies and standards around ICAM and where do you think they're headed?

I would say the policies and standards are fairly mature; this is a pretty well-defined area. There's a robust vendor marketplace for capabilities in this area, and it's just really our strategy of how we're going to implement and architect that from the department. One of the fundamentals that I'm really trying to drive toward is allowing local control of identity governance tools and automation, plus supporting publishing data and attributes up to the enterprise.

Finally, can you talk about ICAM as it relates to the everyday employee? What exactly does this mean for employees as they do their jobs?

The best case I like to use to explain what we're trying to do is an example from DISA. As we migrated to the new Time and Attendance system, we went through a process: Every employee had to go through an approval process to get access to the system.

From my perspective, if we take a data-centric approach to this, we already have authoritative data sources that know that I'm a DISA employee. Every employee is going to have access to Time and Attendance. There should be an automatic process to provision our accounts and establish those fundamentals.

But today we operate in a very decentralized fashion and rely on paper processes or maybe automated process that are still based on the overall paper process. I think that leads to a delay in being able to accomplish or work on your mission. So, if I need to access some system, it might take me days, weeks, months to get that, depending on the people and the processes that requires. But we're trying to put capabilities in place that automate a lot of that, to the greatest extent possible, to provide near real-time access. Also, if I leave an organization, we want to make sure that my accounts are disabled or deleted in a timely and proper fashion.

Worksheet: Implementing an Identity Management System

An effective IAM program requires thoughtful planning, collaboration and execution. The following worksheet was adapted from the federal government's Login.gov website, and it outlines key questions to ask before implementing an identity management system.

Ask yourself, what are you protecting?

(Not all information requires an identity system to manage access. You can protect the privacy of users and reduce the security risk to your systems by avoiding any unnecessary collection of PII.)

You might not need to implement an identity system if (check all that apply):

- ☐ You do not need to have an ongoing relationship with users.
- ☐ Transactions don't depend on personal information being accurate.
- ☐ You can rely on other forms of security.

If you still think an identity system is needed, consider the following questions:

What transactions will users need?

Will the transactions be ongoing, as when users bookmark benefits or grant applications to fill out later, then return repeatedly to check the application status? Or will they be a one-time or infrequent transaction, as when people download medical or financial records?

What kind of information do you need to protect your customers?

Do you need full name and other personal information so that users can access private information? Or do you only need to verify that a user fits in certain categories, such as the veterans category or the senior citizens category?

What sort of crime might access to this information make possible?

Information that seems innocent on its own might still be valuable to fraudsters and other criminals in combination with other easily accessed information.

What other means of security are available?

Postal tracking numbers, for example, are not secrets because the package will be delivered only to a specific address. The safety of the delivery rests on the security of the building and the conduct of the delivery person, not on the secrecy of the number itself.

What kinds of resources do you already have to identify customers?

Your agency may already have mission-specific information and resources that can be used to identify customers. By integrating resources you know and trust, you can increase the reliability of identification.

Conclusion

Equipping agencies with the resources they need to accomplish their mission — whether it's providing secure transportation, maintaining government facilities or administering reliable social services — is the driving force behind IAM efforts.

The systems that power these services are often critical to government operations, and ensuring the right people can access them for the right reasons is key. Ultimately, IAM helps agencies make these decisions accurately, consistently and in a timely manner.

But to ensure the effectiveness of IAM, it must be a collaborative effort, not just another task for the IT department. Our personal and national security are at stake, and it will take a collective effort to maintain the balance of cybersecurity and accessibility to online services in an increasingly digital world.

ABOUT CARAHSOFT

Carahsoft Technology Corp. is The Trusted Government IT Solutions Provider®. As a top-performing GSA Schedule and SEWP contract holder, Carahsoft serves as the master government aggregator for many of its best-of-breed technology vendors, supporting an extensive ecosystem of manufacturers, value-added resellers, system integrators and consulting partners committed to helping government agencies select and implement the best solution at the best possible value.

Visit www.carahsoft.com, follow @Carahsoft, or email sales@carahsoft.com for more information.

THANK YOU

Thank you to Carahsoft, CyberArk, Okta, Radiant Logic and SailPoint for their support of this valuable resource for public sector professionals.

ABOUT GOVLOOP

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to info@govloop.com.

govloop.com | @govloop

AUTHORS

Nicole Blake Johnson, Managing Editor
Sherin Shibu, Editorial Fellow
Catherine Andrews, Senior Director of Editorial & Production

DESIGNER

Kaitlyn Baker, Creative Manager

Carahsoft's identity access management solutions are available through its reseller partners on a variety of contracts including Carahsoft's GSA Schedule 70, SEWP V, ACCENT, NASPO ValuePoint, National IPA, and numerous state and local contracts. Learn more at ***Carahsoft.com/Identity.***

See the latest innovations in government IT from Carahsoft's vendor partners at Carahsoft.com/Innovation.

govloop

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop