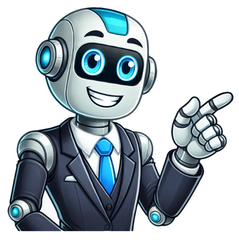
Click to verify



Simply put, it’s a powerful framework that securely grants people and systems the appropriate access to critical resources—whether you're a government agency or a private organization. By providing a comprehensive framework to manage digital identities, credentials, and access restrictions, ICAM ensures that authorized users gain seamless access while keeping intruders at bay. The parts are broken out as follows: Identity Management This involves identifying users in a system and controlling their access to system resources by linking user rights and constraints to the established identity. Processes often include identity verification, registration, and the provision of login credentials such as usernames and passwords. Credential Management This entails the development, issuing, and administration of digital credentials that validate a user's identity when they interact with a system. Credentials can take many different forms, from straightforward username/password pairs to more intricate ones like digital certificates, smart cards, or biometric information. Access Management To control access to only the resources they are permitted to use, this entails managing permissions for authenticated users. Policies, protocols, and technologies are frequently used in access management to govern which resources a person may access or cannot access within a network or system. Key Features of ICAM: ICAM Authentication: Verifying a user, application, or system’s identity. Authorization: Figuring out if a person, program, or system is authorized to carry out a specific operation. Accountability: Keeping track of actions and transactions to identify their origin. Audit and Compliance: Ensuring that the firm complies with compliance and security standards. Single Sign-On (SSO): Enabling users to log in once to access several systems without being requested to do so for each one. Multi-Factor Authentication (MFA): Validating users’ identities through multiple verification methods for more secure access Benefits of ICAM Enhanced Security: Decreases the possibility of unauthorized entry. Operational Efficiency: Simplifies the procedures for permission and authentication. Compliance: Aids in fulfilling statutory requirements. User Experience: Streamlines user contact with systems, especially when SSO is used. ICAM plays a vital role in ensuring that organizations of all types, from government agencies to private enterprises, effectively manage access to their systems and protect sensitive information. How IDMWORKS can help with ICAM At IDMWORKS, we specialize in Identity and Access Management (IAM), a critical subset of ICAM. We provide a variety of services that can assist businesses in setting up, maintaining, and improving their ICAM frameworks. How they can help is as follows: Assessment and Strategy Development An organization's current ICAM infrastructure can be thoroughly evaluated by IDMWORKS to find any gaps and create a strategic plan for growth. This frequently involves a risk analysis, a compliance check, and best practice suggestions. Solution Selection Given the abundance of options available, selecting the best ICAM solutions might be difficult. IDMWORKS can assist organizations in choosing the best vendors and solutions based on their unique requirements, financial constraints, and legal obligations. Implementation and Integration With expertise in deploying ICAM solutions like multi-factor authentication and identity governance, IDMWORKS ensures a smooth integration with your existing IT infrastructure while minimizing disruptions to business operations. Managed Services For organizations lacking internal resources to manage their ICAM systems, IDMWORKS offers managed services, including 24/7 monitoring, regular updates, and incident response. Training and Knowledge Transfer IDMWORKS can train an organization's staff on best practices for managing and operating the ICAM infrastructure. By doing this, it is made sure that the company can manage the system successfully even after the consulting phase has concluded. Compliance and Audit Support ICAM's ability to meet regulatory criteria is essential. Organizations can use IDMWORKS to make sure their ICAM systems are in compliance with applicable rules and regulations and to help them be ready for audits. Custom Development Off-the-shelf solutions may not always fit an organization's specific requirements. In these circumstances, IDMWORKS can provide unique ICAM solutions based on the particular needs of the organization. Ongoing Support and Optimization ICAM is not a project you can "set it and forget." IDMWORKS offers continuing support to ensure the ICAM system stays up-to-date with the latest security threats and compliance requirements. Conclusion: Secure Your Organization with IDMWORKS Embracing ICAM is not just a technical upgrade; it’s a strategic imperative for every organization aiming to navigate the digital world safely and effectively. By leveraging the expertise of IDMWORKS, your organization can significantly enhance security, improve operational efficiency, and ensure compliance with regulatory requirements through a robust ICAM framework. From assessment to ongoing optimization, we guide you through every step of the process to ensure your system is secure and optimized for success. Contact IDMWORKS today to learn more about how we can help you design, implement, and manage a tailored ICAM solution that fits your specific needs. Author: Mark Saks, IDMWORKS, Director – Technical Solutions In the realm of cybersecurity, ICAM stands for Identity, Credential, and Access Management. This crucial framework plays a vital role in safeguarding sensitive data and ensuring secure access to information systems. Understanding the components and implementation of ICAM is essential for organizations looking to enhance their cybersecurity measures. In this article, we will explore the significance of ICAM, its key components, benefits, risks of not implementing it, and real-world examples of its application. So, let’s dive into the world of ICAM and its importance in cybersecurity. What Is ICAM? Identity Credential Access Management (ICAM) is a crucial component of cybersecurity that involves the management of digital identities, authentication, and access control within an organization. ICAM plays a pivotal role in ensuring secure access to resources by verifying the identities of users and granting appropriate levels of access based on their credentials. This helps prevent unauthorized access to sensitive information and systems. By managing user identities effectively, ICAM fosters a more streamlined and secure environment where individuals can securely access the resources they need to perform their roles. ICAM frameworks aid in implementing a layered approach to cybersecurity, where multiple authentication factors are required for access, enhancing overall security posture. For instance, in a real-world scenario, a government agency may utilize ICAM frameworks to authenticate employees accessing classified information, ensuring that only authorized personnel can view the data. What Does ICAM Stand For? ICAM stands for Identity Credential Access Management, a comprehensive approach to managing user identities, access rights, and security protocols in the realm of cybersecurity. This strategic framework involves multiple components that collaborate to restrict unauthorized access and safeguard sensitive data from potential cyber threats. Authentication processes validate a user’s identity to verify their access rights, ensuring that only authorized individuals can access specific resources. Authorization determines what actions a user is allowed to perform within the system, while secure access control mechanisms regulate the flow of information and monitor user activities. By implementing ICAM practices, organizations can fortify their defenses against malicious activities while promoting data integrity and confidentiality. Why Is ICAM Important in Cybersecurity? ICAM plays a pivotal role in cybersecurity by enhancing access control, managing risks, ensuring compliance with security standards, and protecting sensitive information from unauthorized access. ICAM frameworks provide organizations with a structured approach to managing identities and access across digital systems. By incorporating ICAM solutions, businesses can establish granular access controls, limiting user privileges to authorized personnel only. This not only reduces the likelihood of data breaches but also aids in compliance adherence by enforcing stringent access policies and detecting potential security threats promptly. ICAM frameworks facilitate seamless integration with regulatory requirements, ensuring that organizations meet industry standards effectively while maintaining a bolstered security posture. What Are the Key Components of ICAM? The key components of ICAM include robust authentication mechanisms, precise authorization processes, attribute management, and the interaction between subjects (users) and objects (resources) within a system. Authentication plays a crucial role in confirming the legitimacy of users, ensuring that individuals accessing the system are who they claim to be. By having stringent authentication measures in place, organizations can protect sensitive information from unauthorized access. Authorization complements authentication by defining the specific rights and permissions granted to authenticated users, controlling what actions they can perform within the system. Attribute management is essential for categorizing user characteristics, such as roles or clearance levels, which further refines access control. Understanding the relationships between subjects and objects is fundamental in establishing effective access control policies that dictate who can access specific resources and under what conditions. How Does ICAM Work? ICAM operates by establishing policies, adhering to standards, and implementing access control mechanisms to govern the interactions between users, systems, and data. These policies serve as the foundation for regulating user access within an organization’s network, determining who can access what information and under what conditions. By setting clear guidelines and principles, ICAM ensures that only authorized users can interact with sensitive data, reducing the risk of breaches and unauthorized access. Adherence to industry standards guarantees interoperability across different systems, enabling seamless communication and data exchange. Access control mechanisms play a crucial role in enforcing these policies, utilizing authentication methods, authorization processes, and encryption techniques to safeguard the integrity and confidentiality of data. What Are the Steps of ICAM Implementation? The implementation of ICAM involves establishing an ICAM framework, integrating identity providers, verifying user identities, and deploying authentication mechanisms to secure access. Defining an ICAM framework entails outlining the specific guidelines, policies, and procedures that govern the management of identities, credentials, and access within an organization. Incorporating identity providers involves connecting to a reliable source that can validate and authenticate user identities accurately. Moving forward, verifying user identities through identity proofing methods ensures that the individuals accessing the system are who they claim to be. Deploying authentication mechanisms like multi-factor authentication enhances security by requiring users to provide multiple forms of verification before granting access. What Are the Benefits of Using ICAM in Cybersecurity? Implementing ICAM in cybersecurity offers numerous benefits, including improved security measures, streamlined access management processes, and enhanced compliance with regulatory requirements. By leveraging ICAM, organizations can establish robust authentication mechanisms that enhance data protection and prevent unauthorized access. The centralized approach to user management simplifies administration tasks, reducing the risk of human errors. ICAM aids in enforcing least privilege principles, ensuring that users only have access to the resources necessary for their roles. This not only enhances security but also contributes to a more efficient and cost-effective IT environment. Adherence to industry standards such as NIST and GDPR is facilitated through the comprehensive control mechanisms established by ICAM. Improved Security The implementation of ICAM leads to heightened cybersecurity measures by safeguarding user identities, managing digital identity attributes, and enforcing secure access controls within the organizational infrastructure. By ensuring that user identities are securely protected, ICAM plays a crucial role in reducing the risk of unauthorized access or identity theft. Through the management of digital attributes, organizations can establish a strong foundation for verifying and authorizing users’ identities accurately. The rigorous implementation of access controls across the organization’s systems and applications further strengthens the overall cybersecurity posture. Digital identity management serves as a linchpin in bolstering defenses against cyber threats and maintaining the integrity of critical data assets. Streamlined Access Management ICAM enables streamlined access management through role-based access control mechanisms and the implementation of multi-factor authentication protocols that enhance user verification and authorization processes. By assigning access rights based on predefined roles, ICAM ensures that individuals have appropriate levels of access to resources within an organization. This not only simplifies the access management process but also reduces the risk of unauthorized access. In addition, the implementation of multi-factor authentication adds an extra layer of security by requiring users to provide multiple forms of verification before gaining access, making it more difficult for unauthorized users to infiltrate the system. By optimizing access control policies, ICAM helps in efficiently managing and allocating resources, enhancing overall operational efficiency. Enhanced Compliance ICAM facilitates enhanced compliance with regulatory requirements by conducting risk assessments, responding to security incidents promptly, and aligning access control policies with compliance mandates. This approach enables organizations to proactively identify potential vulnerabilities and security gaps, ensuring that necessary measures are in place to mitigate risks effectively. By staying vigilant and continuously evaluating and updating access control protocols, businesses can ensure that they are always in alignment with the latest compliance standards and regulations. This proactive stance not only helps in preventing security breaches but also demonstrates a commitment to upholding the integrity of data and systems, which is crucial for maintaining trust with customers and business partners. What Are the Risks of Not Implementing ICAM? Failing to implement ICAM exposes organizations to risks such as inadequate security monitoring, weakened cybersecurity defenses, and increased vulnerabilities to identity theft and unauthorized access. Not having robust Identity, Credential, and Access Management (ICAM) protocols in place can leave organizations susceptible to a multitude of threats. Without proper ICAM measures, it becomes challenging for organizations to effectively monitor their security systems, leaving them blind to potential breaches and security incidents that could harm their operations and reputation. Weak cybersecurity defenses resulting from the absence of ICAM make it easier for cybercriminals to exploit vulnerabilities and gain unauthorized access to sensitive data and systems. ICAM plays a critical role in safeguarding organizations against the prevalent risks of identity theft and unauthorized access, which can have damaging repercussions in today’s digital landscape. Real-World Example of ICAM in Action A real-world application of ICAM can be observed in federal agencies, where robust identity management practices are implemented to ensure information security and regulatory compliance. This strategic approach involves the meticulous control and monitoring of user identities, privileges, and access rights within the agency’s network. By utilizing ICAM frameworks, federal agencies can streamline processes related to user authentication, authorization, and attribute management. This ensures that only authorized personnel can access sensitive information or critical systems, reducing the risk of data breaches and insider threats. ICAM solutions enable agencies to adhere to strict compliance standards by providing a comprehensive audit trail of user activities and access permissions. The effective implementation of ICAM not only enhances information security but also promotes accountability and transparency within governmental organizations. Case Study: ICAM Implementation in a Government Agency The case study on ICAM implementation in a government agency exemplifies how identity credentials are managed, user privileges are assigned, and access rights are controlled to maintain a secure and compliant operational environment. In this scenario, the government agency streamlined its processes by implementing a centralized ICAM system that allowed them to establish strict protocols for identity verification. By provisioning unique credentials for each user, the agency ensured that only authorized personnel had access to sensitive information. User privileges were allocated based on predefined roles, ensuring that individuals only had the necessary permissions for their specific duties. This granular approach to access control enhanced security measures and reduced the risk of unauthorized data breaches within the agency’s operational framework. How Can Organizations Implement ICAM? Organizations can implement ICAM by establishing robust security controls, integrating identity and access management solutions, and architecting a secure framework to govern access and authentication processes. This approach ensures that only authorized individuals within the organization can access sensitive data, applications, and systems while protecting against unauthorized access attempts. It is essential for organizations to define and enforce role-based access controls, implement multi-factor authentication mechanisms, and regularly monitor user activities to detect any suspicious behavior. Having a centralized identity management system can streamline user provisioning and deprovisioning processes, improving operational efficiency and reducing the risk of security breaches. Assess Current Systems and Processes The initial step in ICAM implementation involves assessing current systems and processes to identify gaps, enhance cybersecurity governance, and improve threat detection capabilities within the organization. During the assessment phase, experts analyze the organization’s existing IT infrastructure, evaluating access controls, authentication mechanisms, and data protection strategies to pinpoint potential weaknesses. This comprehensive review aims to establish a solid foundation for ICAM deployment by ensuring that the right policies and controls are in place to mitigate security risks. By conducting a thorough system analysis, organizations can proactively address vulnerabilities, enhance their cyber resilience, and fortify their defenses against evolving threats in the digital landscape. Develop an ICAM Strategy Subsequently, organizations need to develop a comprehensive ICAM strategy that encompasses security policies, cybersecurity awareness initiatives, and training programs to educate users on secure access practices. Security policies play a crucial role in setting the guidelines and rules for access management, outlining the framework for securing the organization’s digital assets. Concurrently, cybersecurity awareness campaigns aid in keeping employees informed about the latest threats and best practices, instilling a sense of vigilance and responsibility within the workforce. Conducting regular training sessions helps enhance user knowledge of secure access protocols, empowering them to make informed decisions when navigating digital systems. This continuous education not only bolsters the organization’s defenses but also fosters a culture of cybersecurity, making it a shared responsibility among all members of the team. Implement and Monitor ICAM Solution Organizations should implement an ICAM solution that aligns with compliance requirements, conducts regular risk assessments, and monitors security incidents to ensure the effectiveness of access controls and authentication mechanisms. This involves several key steps. Initially, organizations need to assess their specific compliance mandates to tailor the ICAM solution accordingly. Conducting thorough risk assessments helps in identifying potential vulnerabilities and threats that could compromise security. Once the ICAM solution is in place, continuous monitoring of security incidents is vital to detect and respond promptly to any unauthorized access attempts or breaches. By integrating these practices seamlessly, organizations can strengthen their overall security posture and safeguard sensitive data effectively. Frequently Asked Questions What Does Icam Mean? Icam stands for Identity, Credential, and Access Management. It refers to a framework of processes, policies, and technologies used to manage digital identities, credentials, and access to resources. What is the Purpose of Icam in Cybersecurity? The purpose of Icam is to ensure that only authorized individuals have access to sensitive information and resources. It also helps organizations manage and secure their digital identities and credentials. How Does Icam Work? Icam works by verifying the identity of a user, issuing them a unique credential, and controlling their access to resources based on their role and permissions. It also includes processes for revoking access and managing changes in identity or credentials. Can You Give an Example of Icam in Action? An example of Icam in action is when an employee logs into their company’s network using their unique credentials. The Icam system will verify their identity and grant them access to specific resources based on their role and permissions. What Are the Benefits of Implementing Icam? Implementing Icam can provide several benefits, including improved security, easier management of digital identities and credentials, and better control over access to sensitive information and resources. Is Icam Only Relevant for Large Organizations? No, Icam is relevant for organizations of all sizes. It is especially crucial for those that deal with sensitive information, such as personal or financial data. Implementing Icam can help protect against cyber threats and data breaches, regardless of the organization’s size. Okta Looks like you have Javascript turned off! Please enable it to improve your browsing experience. In today’s digital landscape, organizations face unprecedented security challenges. Managing who accesses sensitive systems and information has never been more critical. Enter Identity, Credential, and Access Management (ICAM)—an essential framework for securely managing identities, credentials, and access across networks, systems, and devices. ICAM isn’t just for large corporations or government entities. From small businesses to enterprises, the principles of ICAM are becoming crucial for anyone who handles sensitive information or operates in a highly regulated industry. But what is ICAM, and why does it matter? This guide will break down the fundamentals of ICAM, how it works, and why adopting this framework is important for your organization. By the end, you’ll have a solid understanding of the benefits ICAM brings to your security infrastructure. ICAM stands for Identity, Credential, and Access Management, and it refers to the policies, processes, and technologies used to manage access to resources based on an individual’s identity. The core purpose of ICAM is to ensure that only the right people, with the right credentials, can access the right resources at the right time. Let’s break down ICAM into its three main components: Identity Management: Focuses on identifying and verifying individuals in the system. It ensures that each user is uniquely identifiable and their actions can be tracked. Credential Management: Refers to the process of issuing and maintaining the credentials (such as passwords, biometrics, or tokens) that verify a user’s identity. Access Management: Determines what resources or services a particular user or group can access based on their role or identity. Organizations today operate in a highly interconnected world. With employees accessing networks remotely, third-party vendors needing secure entry, and a rise in cybersecurity threats, the importance of strong access control cannot be overstated. ICAM helps organizations reduce the risk of unauthorized access, insider threats, and data breaches. With the rise of sophisticated cyber-attacks, such as phishing or ransomware, robust identity management is essential. ICAM provides mechanisms to prevent unauthorized users from infiltrating your system. Additionally, it helps monitor and track access, so you know exactly who is in your system and what they are doing. Many industries, such as healthcare and finance, are subject to strict compliance regulations. Laws like HIPAA and GDPR mandate strict controls on who can access sensitive information. An effective ICAM strategy ensures that your organization complies with these regulations, avoiding heavy penalties or legal repercussions. Zero Trust is a security model that assumes threats are both inside and outside the network. It operates on the principle of “never trust, always verify.” ICAM is a key enabler of Zero Trust Architecture, where access is continuously validated based on user identities, their credentials, and behaviors. Learn more about Zero Trust Architecture ICAM integrates various processes and technologies to manage identities and control access. Let’s explore some of the core elements that make up ICAM: Before assigning credentials or allowing access, users need to be vetted. This process is called identity proofing. Whether through a government-issued ID, multi-factor authentication (MFA), or biometric verification, organizations need to ensure the individual requesting access is who they claim to be. Once identity proofing is successful, credentials are issued. Credentials can range from passwords to physical smart cards or biometric data like fingerprints. These credentials must be secure, unique, and easy to manage. Additionally, as organizations evolve, credentials may need regular updates to reflect changing security protocols or job roles. Authentication is the process of verifying a user’s identity when they request access. The most common method is a username and password, but modern systems increasingly rely on multi-factor authentication, which combines something the user knows (password), something the user has (a token), and something the user is (biometrics). Authorization occurs after authentication and determines what actions an authenticated user can perform. Role-based access control (RBAC) is a common method of authorization, where users are given access based on their role within the organization. For example, a manager may have broader access to company data than an entry-level employee. Access auditing involves monitoring who has access to what resources and when. Regular audits ensure that access privileges are appropriate and that there are no anomalies in access behavior. Access logs also help identify potential security breaches or internal threats. By ensuring that only authenticated and authorized users can access sensitive systems, ICAM drastically reduces the chances of data breaches. The framework makes it harder for bad actors to infiltrate networks, reducing risks from external hackers and insider threats. A well-implemented ICAM strategy reduces the manual workload on IT and security teams. Automated systems can manage user credentials, assign access rights, and track activity. This efficiency allows organizations to scale their security measures without excessive manual intervention. ICAM can improve the user experience by streamlining the process of accessing systems. Single sign-on (SSO) and multi-factor authentication reduce the need for multiple passwords and make it easy for employees to securely access everything they need with minimal friction. As previously mentioned, ICAM helps organizations meet industry-specific regulations. Compliance frameworks like NIST SP 800-63 offer guidelines for identity management. By adopting ICAM, you ensure that your organization adheres to these regulations, avoiding penalties and enhancing your reputation as a secure organization. There are several technologies that help enable ICAM systems: Single Sign-On (SSO): SSO allows users to access multiple applications with one set of login credentials, improving security while reducing password fatigue. Multi-Factor Authentication (MFA): MFA requires users to provide two or more verification methods to access a system, significantly enhancing security. Biometrics: Biometrics, such as fingerprint or facial recognition, offer highly secure methods for identity verification, as they are harder to fake or steal. Privileged Access Management (PAM): PAM manages and monitors access to critical systems by users with elevated privileges, reducing the risk of insider threats or abuse of power. Federated Identity Management (FIM): FIM allows a user’s identity to be used across multiple systems, even across organizations, streamlining access while ensuring security. To get the most out of your ICAM strategy, follow these best practices: Credentials should be updated regularly to ensure they remain secure. Conduct audits to ensure that only necessary personnel have access to sensitive systems. Relying on passwords alone is risky. MFA adds an extra layer of security, ensuring that even if passwords are compromised, bad actors can’t easily access systems. Limiting access based on a user’s role helps ensure that people only have access to the information they need to perform their job. This minimizes the risk of unauthorized access. Instead of assuming that internal users are trustworthy, implement a Zero Trust model where all access must be continuously verified. This model helps prevent both external and insider threats. Security awareness training is essential. Educate your staff about the importance of identity management, safe credential practices, and the role they play in keeping your systems secure. As technology advances and organizations continue to shift toward remote and hybrid work models, the need for robust identity management frameworks will only increase. The rise of cloud services, mobile workforces, and increasing cyber threats demand that organizations prioritize ICAM. By implementing ICAM, organizations can protect sensitive data, ensure regulatory compliance, and improve operational efficiency. It’s not just a defensive measure—it’s a proactive strategy for securing the future. In an era where data breaches and cyber-attacks are increasingly common, Identity, Credential, and Access Management (ICAM) has become indispensable. ICAM provides a structured way to manage identities, credentials, and access, safeguarding your organization’s most valuable assets. Whether you’re a small business or a large enterprise, adopting ICAM can drastically improve your security posture. Take the first step towards a more secure future—adopt ICAM today and ensure that only the right people have access to your organization’s critical resources. Official websites use .gov A .gov website belongs to an official government organization in the United States. Secure .gov websites use HTTPS A lock ( ) or https:// means you’ve safely connected to the .gov website. Share sensitive information only on official, secure websites. Additional terms and conditions Traveler reimbursement is based on the location of the work activities and not the accommodations, unless lodging is not available at the work activity, then the agency may authorize the rate where lodging is obtained. Unless otherwise specified, the per diem locality is defined as "all locations within, or entirely surrounded by, the corporate limits of the key city, including independent entities located within those boundaries." Per diem localities with county definitions shall include"all locations within, or entirely surrounded by, the corporate limits of the key city as well as the boundaries of the listed counties, including independent entities located within the boundaries of the key city and the listed counties (unless otherwise listed separately)." When a military installation or Government - related facility(whether or not specifically named) is located partially within more than one city or county boundary, the applicable per diem rate for the entire installation or facility is the higher of the rates which apply to the cities and / or counties, even though part(s) of such activities may be located outside the defined per diem locality. Identity, Credential, and Access Management, ICAM best practices are designed to ensure that authorized individuals have the necessary and correct access to resources and digital assets within a company’s systems. It encompasses the processes and technologies used to manage digital identities, authenticate users, authorize access to resources, and enforce security policies. ICAM best practices and principles have been developed and refined by various government agencies, industry consortia, standards bodies, and cybersecurity professionals over several decades. These efforts have aimed to address the growing need for robust identity and access management solutions to protect sensitive information, secure critical infrastructure, and support digital transformation initiatives. Therefore, ICAM is not attributed to a single creator or organization. Instead, it has evolved as a response to the increasing complexity and security challenges associated with managing digital identities and access to resources within organizations’ information systems. While it’s challenging to pinpoint a specific creator or organization responsible for ICAM, government agencies such as the National Institute of Standards and Technology (NIST) in the United States and international standards organizations like the International Organization for Standardization (ISO) have played significant roles in developing standards, guidelines, and ICAM best practices related to identity and access management. ICAM continues to evolve as new technologies emerge, cyber threats evolve, and organizations seek more effective ways to manage identities, credentials, and access rights in increasingly complex and interconnected environments. ICAM aims to strike a balance between security and usability by ensuring that access controls are robust enough to protect sensitive resources from unauthorized access while still allowing legitimate users to efficiently access the resources they need to perform their duties. It’s a critical aspect of cybersecurity and is particularly important in environments where there are stringent regulatory requirements or where sensitive data must be protected from unauthorized disclosure or modification. Here’s a breakdown of the components within ICAM: Identity Management: This involves the creation, maintenance, and deletion of digital identities for users, devices, applications, and services within an organization’s ecosystem. It includes processes such as user provisioning, identity verification, and identity lifecycle management. Credential Management: Credentials are the means by which users prove their identities to gain access to resources. Credential management involves the issuance, distribution, storage, and revocation of authentication credentials such as passwords, cryptographic keys, biometric data, and security tokens. Access Management: Access management controls who can access which digital assets and what they can do within systems once authenticated. It includes processes for defining access policies, enforcing access controls, and monitoring user activities to detect and respond to unauthorized access attempts. The primary purpose of ICAM best practices is to ensure that the right individuals have the appropriate access to resources within an organization’s information systems while maintaining security, compliance, and efficiency. Here are some key purposes of ICAM: Enhanced Security: ICAM helps organizations strengthen their security posture by implementing robust authentication mechanisms, enforcing access controls, and continuously monitoring user activities to detect and respond to security threats. Risk Management: By centrally managing digital identities, credentials, and access rights, ICAM enables organizations to reduce the risk of unauthorized access, data breaches, insider threats, and other security incidents that could result in financial losses, reputational damage, or regulatory penalties. Compliance: ICAM helps organizations comply with various regulatory requirements and industry standards related to identity verification, access control, data privacy, and cybersecurity. By implementing ICAM best practices, companies can ensure the protection of critical data and meet legal obligations. Operational Efficiency: ICAM streamlines access management processes by automating user provisioning, authentication, and authorization tasks. This improves operational efficiency, reduces administrative overhead, and enhances user experience by ensuring that authorized users can access resources promptly and without unnecessary delays. Interoperability: ICAM promotes interoperability by providing standardized frameworks, protocols, and technologies for managing identities and access across different systems, platforms, and organizations. This enables seamless integration and collaboration between internal and external stakeholders while maintaining security and privacy. Scalability: ICAM solutions are designed to scale with the growth of an organization, allowing it to efficiently manage a large number of users, devices, applications, and services without sacrificing security or performance. ICAM involves several key steps and considerations: Assessment and Planning: Begin by conducting a thorough assessment of your organization’s current identity and access management practices, systems, and infrastructure. Identify existing challenges, security risks, compliance requirements, and business objectives. Develop a comprehensive ICAM strategy aligned with organizational goals and regulatory mandates. Policy Development: Define clear and enforceable policies governing identity management, authentication, authorization, and access control. These policies should establish criteria for user provisioning, credential issuance, access privileges, user roles, and entitlements in alignment with industry and regulatory standards. Technology Selection: Choose appropriate ICAM technologies and solutions based on your requirements, budget, and growth expectations. This may include identity management systems, authentication mechanisms (such as multi-factor authentication), access management platforms, directory services, and identity federation solutions. Consider factors such as interoperability, integration capabilities, and vendor support. Implementation and Integration: Deploy ICAM solutions and integrate them into your existing systems and applications. Configure identity repositories, establish trust relationships between systems, and implement single sign-on (SSO) mechanisms to streamline user authentication and access. Ensure proper synchronization of user data across systems and platforms. User Lifecycle Management: Implement processes for comprehensive digital identity lifecycle management, including user registration, provisioning, de-provisioning, and account termination. Enforce strong password policies, periodic credential rotation, and self-service capabilities for users to manage their accounts and credentials securely. Access Control and Enforcement: Define access control policies based on the principle of least privilege, granting users only the permissions necessary to perform their roles and responsibilities. Implement role-based access control (RBAC), attribute-based access control (ABAC), or other access control models as appropriate. Monitor user activities and enforce policy violations through real-time alerts and automated responses. Training and Awareness: Provide comprehensive training and awareness programs for employees, contractors, and partners to educate them about ICAM principles, policies, and best practices. Foster a culture of security awareness and accountability to ensure that users understand their roles and responsibilities in safeguarding digital identities and access credentials. Continuous Monitoring and Improvement: Incorporate methods for continuous monitoring, auditing, and evaluation of ICAM processes, controls, and technologies. Perform periodic security risk assessments, penetration testing, and compliance audits to identify control gaps and improvement areas. Continuously update and refine your ICAM strategy to face evolving threats and new requirements. By following these steps and incorporating ICAM principles into your organization’s cybersecurity framework, you can enhance security, streamline access management, and mitigate the risk of unauthorized access to critical resources. Identity, Credential, and Access Management (ICAM) is a comprehensive framework encompassing processes, policies, and technologies aimed at ensuring secure and efficient management of digital identities and access to resources within organizations’ information systems. It involves the creation, verification, and management of digital identities, the issuance and control of authentication credentials, and the enforcement of access controls to safeguard sensitive data and systems from unauthorized access. ICAM strives to strike a balance between security and usability, promoting interoperability, scalability, and compliance with regulatory requirements while enhancing operational efficiency through automation and streamlined access management processes. ICAM is essential for mitigating security risks, protecting critical assets, and supporting organizational goals in an increasingly digital and interconnected world. ICAM enables organizations to effectively manage the lifecycle of digital identities, control access to resources, mitigate security risks, and achieve their business objectives in a secure and compliant manner. ICAM adoption is crucial for organizations to effectively manage the increasingly complex digital landscape, where the proliferation of user identities, diverse access requirements, and evolving security threats pose significant challenges. By implementing ICAM, organizations can establish centralized control over identities, credentials, and access rights, enabling them to mitigate security risks, ensure compliance with regulatory mandates, and enhance operational efficiency. ICAM facilitates secure and efficient access to resources, fosters interoperability across systems and platforms, and empowers organizations to protect sensitive data, safeguard critical assets, and support digital transformation initiatives. In today’s interconnected and data-driven environment, ICAM adoption is essential for organizations to strengthen their security posture, maintain trust with stakeholders, and achieve their business objectives effectively. FICAM Architecture version table Version Number Date Change Description 3.3 6/20/2023 Combined separate architecture pages into a single web page. Updated change table to reflect all version updates. 3.2 9/30/2022 Editorial updates.1. Consolidated use cases into a table format.Combined services framework and services description.Updated access management services description to differentiate authentication from authorization and include an overview of difference access models.Map FICAM playbooks to FICAM Roadmap Part B content. **Version 3.2 sunsets FICAM Roadmap Part B content**. 3.1 1/6/2021 FICAM Architecture v3.1 incorporates updates proposed by the Federal CISO Council ICAM Subcommittee.Clarified introduction, goals, and objectives section.Added Privileged Access Management as Access Management Service.Added Identity Governance as Governance Services.Streamlined use case language and order.Updated system component examples.Updated standards and policies.Updated graphics. 3.0 11/27/2019 Version 3.0 for the Architecture represents the baseline changes to FICAM Roadmap Part A released in 2016. Version 3.0 sunsets FICAM Roadmap Part A content. 2.0 12/2/2011 Revised to include new Part B:Implementation GuidanceChapter 6: ICAM Implementation PlanningChapter 7: Initiative 5: Streamline Collection and Sharing of Digital Identity DataChapter 8: Initiative 6: Fully Leverage PIV and PIV-I CredentialsChapter 9: Access Control ConvergenceChapter 10: Initiative 7: Modernize PACS InfrastructureChapter 11: Initiative 8: Modernize LACS InfrastructureChapter 12: Initiative 9: Implement Federated Identity CapabilityInclusion of Glossary appendixEditorial and formatting correctionsTerminology updates to maintain consistency between Parts A and BUpdates to content related to the Federal Public Key Infrastructure to reflect infrastructure upgrades since original publication. 1.0 11/10/2009 Initial publication of the document, including:Chapter 1: IntroductionChapter 2: Overview of ICAMPart A: ICAM Segment ArchitectureChapter 3: ICAM Segment ArchitectureChapter 4: ICAM Use CasesChapter 5: Transition Roadmap and Milestones Introduction FICAM is the federal government’s implementation of Identity, Credential, and Access Management (ICAM). ICAM is the set of tools, policies, and systems that an agency uses to enable the right individual to access the right resource, at the right time, for the right reason in support of federal business objectives. This version of the FICAM Architecture encompasses the enterprise ICAM policies, technologies, and system approaches for government employees, contractors, and authorized partners. Citizen interactions with the federal government - or consumer ICAM - are not covered under this version of the FICAM Architecture. The following diagram is a high-level view of the ICAM practice areas and supporting elements. The FICAM Architecture includes government-wide enterprise architecture views with the flexibility to support each agency’s unique business or mission needs. Use the FICAM Architecture as a tool to continuously improve upon your agency’s approach and align with federal security and privacy initiatives. Copy the graphics and text throughout this playbook to use at your agency to drive ICAM awareness, strategy developments, and communications. What Is ICAM? ICAM is the set of tools, policies, and systems that an agency uses to enable the right individual to access the right resource at the right time for the right reason in support of federal business objectives. Agencies implement ICAM services and solutions to unify their IT services, improve physical access control, and improve information security and decisions. Understanding the building blocks of ICAM is key to understanding the FICAM Architecture. ICAM has three practice areas and two supporting elements. The supporting elements enhance the capabilities of the practice areas. ICAM Practice Areas Identity Management is how an agency collects, verifies, and manages attributes to establish and maintain enterprise identities for employees and contractors. Credential Management is how an agency issues, manages, and revokes credentials bound to enterprise identities. Access Management is how an agency authenticates enterprise identities and authorizes appropriate access to protected services. ICAM Supporting Elements Federation is the technology, policies, standards, and processes that allow an agency to accept digital identities, attributes, and credentials managed by other agencies. Governance is the set of practices and systems that guide ICAM functions, activities, and outcomes. What Is the FICAM Architecture? FICAM is the federal government’s enterprise approach to design, plan, and execute common ICAM processes. The FICAM Architecture is a framework for an agency to use in the ICAM program and solution roadmap planning. The FICAM Architecture focuses on enterprise identity processes, practices, policies, and information security disciplines. A federal enterprise identity is the unique representation of an employee, contractor, or enterprise user, which could be a mission, business partner, or even a device or technology managed by a Federal agency to achieve its mission and business goals (OMB Memorandum 19-17). Who Is the FICAM Architecture for? The FICAM Architecture is for agency personnel. An enterprise architecture is primarily used by: Senior Federal IT and Agency Stakeholders to understand the concepts for identity and access management services and the basic use cases supporting business objectives. Program Managers to find common definitions and frameworks for use in planning. Enterprise and Application Architects to use a common framework for designing and governing IT systems, applications, and implementations. There are four main government-wide initiatives to help agencies implement and manage an Agency ICAM program and technology. Planning and Configuration Guidance The FICAM Architecture and accompanying playbooks provide an overall guide for meeting federal ICAM requirements in an efficient and secure way. It focuses on enterprise identity processes, practices, policies, and information security disciplines. Playbooks offer stakeholders overarching strategies and tactical approaches for implementing technical FICAM topics. Interagency Forum and Subcommittee: The Federal Chief Information Security Officer (CISO) Council is a primary resource for identity management, secure access, authentication, authorization, credentials, privileges, and access lifecycle management. The ICAM Subcommittee aligns identity management activities of the federal government and supports collaborative government-wide efforts. Approved Products Lists (APL): The Federal Information Processing Standard 201 (FIPS 201) Evaluation Program not only tests commercial products for use in Personal Identity Verification (PIV) credentialing systems, physical access control systems (PACS), and public key infrastructures but also publish APLs. Federal acquisition professionals rely on these APLs to purchase commercial products that fully comply with federal ICAM mandates. Federal Public Key Infrastructure (PKI): The Federal PKI is a network of certification authorities (CAs) that issue PIV credentials and person identity certificates; PIV-Interoperable credentials and person identity certificates; and other person identity certificates. CA-issued digital certificates, which employ cryptography, close security gaps in user identification and authentication, encryption of sensitive data, and data integrity. What Is the History of the FICAM Architecture? The FICAM Architecture was created in 2009 to provide a common ICAM segment architecture for federal agencies. The FICAM Architecture was the primary foundation of what later became the FICAM Roadmap and Implementation Plan, enhanced with complementary implementation sections. In 2015, ICAM experts from across the federal government collaborated on an updated FICAM Architecture. This update was intended to be more concise, easy to understand, and visually appealing while reflecting the latest updates in cybersecurity, enterprise architecture, and ICAM policy and technology. This site contains the current version of the FICAM Architecture. The FICAM Roadmap and Implementation Guidance v2.0 is superseded by both the FICAM Architecture updates and other complementary modernized playbooks developed by ICAM committees across government. Goals and Objectives The Goals and Objectives identify the aims and outcomes of a federal agency enterprise ICAM program. The goals and objectives align with ICAM functions and map to government-wide policies, cross-agency priorities, and strategic government initiatives. Goals are aspirational statements designed for senior government leaders, agency executives, and agency ICAM program leadership responsible for setting program strategy. Objectives are action areas where agency execution strategies, action plans, and performance metrics can be developed based on alignment with mission needs. The visual below presents the three goals, each with its own objectives. Goal 1: Modernize security policies and solutions to make risk-based decisions, automate identity and access management processes, and move access protections closer to government data. 1.1 Review, update, and maintain comprehensive ICAM policies and technology solution roadmaps to inform and enforce enterprise strategic planning, risk management, and modernization. 1.2 Adopt and use cloud-ready systems that provide an efficient and secure way to access resources. 1.3 Monitor and respond to user behavior and events by using data as a strategic asset to make adaptive and risk-based decisions. Goal 2: Enable missions to efficiently deliver services to federal and contractor employees and resources. 2.1 Establish and manage identities for all enterprise users and resources. 2.2 Design enterprise solutions to manage access to information and resources. 2.3 Use enterprise identity information discovery and enterprise centralized access management. 2.4 Leverage federated solutions to accept identity and authentication assertions made by other agency and mission partners when efficient. Goal 3: Provide enterprise-level solutions within agencies to improve operations and promote cost-effective and efficient use of resources. 3.1 Streamline ICAM governance and program management within each agency to optimize execution, ensure consistency, and align intent across the enterprise. 3.2 Evaluate, rationalize, and migrate to modern, cloud-smart solutions for ICAM services. 3.3 Promote interoperability and efficiency across the federal government by buying and building ICAM solutions that use open, commercially adopted standards. Services Framework and Service Descriptions The Services Framework is a tool designed for ICAM program managers and information technology enterprise architects. It identifies the services that provide functionality within the scope of ICAM and assists in distinguishing between business requirements and technical solutions. The services framework includes the five practice areas and services within. Practice Area Visual The graphic below illustrates the five ICAM practice areas and provides a list of services that fall within each area. Identity Management Identity Management is how an agency collects, verifies, and manages attributes and entitlements to establish and maintain enterprise identities for federal government employees, contractors, and authorized mission partners. This service does not apply to public or consumer identity management. An enterprise identity record is the set of attributes or characteristics that describes a person within a given context: Your identity within your agency’s Human Resources (HR) system is different from your personal identity at your bank. A person’s identity as a government contractor is different from their identity as an Army Reservist. Although your identity remains the same over time, it evolves as your attributes change, such as when you get a promotion, change your name, receive additional training, or retire. Agencies should manage identity attributes as centrally as possible and distribute them as needed. Examples of identity attributes include: Core identity attributes - First name, last name, and address of record. Contact attributes - Physical location, government phone number, and government email address. Authorization attributes - Clearance, training, and job codes. An entitlement is a specific type of authorization attribute that refers to an application permission. Entitlements management is the act of managing those permissions. An agency may group multiple entitlements into a specific role or group to streamline provision and de-provision activities as well as for auditing and reporting purposes. For example, a new employee may require access to ten core enterprise applications on the first day of work. An agency can create a new employee group with new employee entitlements and automate the provisioning of the ten core applications rather than treat them as individual access requests. Attributes and entitlements are created or aggregated through a number of manual and automated mechanisms. Mechanisms may include: Attributes and entitlements are created or aggregated through a number of

manual and automated mechanisms. Mechanisms may include: Use a single sign-on tool to aggregate application access entitlements. Allow employees to update contact attributes in an employee record. Automate integration between a training system and an identity governance and administration tool to create and update annual security training. Identity proofing is how an agency verifies an enterprise's identity. The complexity of this process depends on the Identity Assurance Level (IAL) required for an identity. Federal agencies require a minimum IAL3 for employees and contractors. For example, a federal employee or contractor presents identity attributes via a driver's license or utility bill. The agency verifies the identity documents and the individual's photo (biometric). An identifier is a unique attribute used to locate an identity in a system: While your agency may issue Personal Identification Verification (PIV) cards to multiple people named John Smith, each individual has a different PIV card number. While your agency may have more than one employee named Jane Smith, each employee has a unique email address tied only to their identity. The Identity Management services in the Federal ICAM architecture include Creation, Identity Proofing, Provisioning, Maintenance, Identity Aggregation, and Deactivation. These services are sometimes collectively known as Identity Lifecycle Management. Service Description Keywords Creation Establish an identity made of attributes that define a person or entity. Identity Record, Authoritative Source Identity Proofing Use identity attributes to connect a digital identity to a real-world entity. Source Document Validation, Remote Proofing, In-Person Proofing Provisioning Create, manage, and delete accounts and entitlements. Identity Lifecycle Management, Workflow, De-provisioning, Account Management, Account Creation, Entitlements Management Maintenance Maintain accurate and current attributes in an identity record over its lifecycle. Identity Lifecycle Management, Updating, Attribute Management Identity Aggregation Find and connect disparate identity records for the same person or entity. Identity Reconciliation, Identity Resolution, Account Linking Deactivation Deactivate or remove enterprise identity records. Identity Lifecycle Management, Suspension, Archiving, Deletion Credential Management Credential Management is how an agency issues, manages, and revokes credentials bound to enterprise identities. A credential is a data structure that authoritatively binds an authenticator to an existing identity using one or more identifiers. Types of authenticators include: Something you know, like a password or PIN. Something you have, like a private key or One-Time Password (OTP) generator. Something you are, like a fingerprint or an iris. The Authenticator Assurance Level (AAL) determines the authenticators associated with a credential. Federal government-wide policy requires a minimum AAL2 for employees and contractors. Examples of credentials include: An agency-issued smart card, such as a PIV or Common Access Card (CAC), that includes a picture and cryptographic key pairs to assert your identity at a federal facility. A combination of credentials, such as a username/password with an OTP generated by a mobile application, to assert your identity to a federal web application. Unlike identities, credentials can expire. If an enterprise identity continues past a credential's expiration date, the issuing agency can issue a new credential. The Credential Management services in the FICAM architecture include Sponsorship, Registration, Generation & Issuance, Maintenance, and Revocation. Service Description Keywords Sponsorship Formally establish that a person or entity requires a credential. Sponsor, Authorizing Official, Affiliation, Request Registration Collect the information needed from a person or entity to issue them a credential. Enrollment Generation & Issuance Assign a credential to a person or entity. Activation, Token, Authenticator Maintenance Maintain a credential throughout its lifecycle. Renewal, Reset, Suspension, Reissuance Revocation Revoke a credential from a person or entity or deactivate an authenticator. Termination Access Management Access Management is how an agency authenticates enterprise identities and authorizes appropriate access to protected services. Policy administration is a combination of laws, regulations, rules, and agency policies that secures access to agency services. Your agency determines the requirements for an individual to access each resource category; they can be as simple or as complex as needed. Examples of access requirements include: "Grant access to anyone on this list of people." "Grant access to any agency employee or contractor with an authenticated PIV card." "Grant access to anyone who is a federal employee, GS-12 or higher, cleared Top Secret, trained in first aid, and certified as a project manager." In providing access services, it can be challenging to conduct an application discovery and inventory for both physical and logical access. For logical access, see the Application Inventory and Identity Risk Analysis section of the Enterprise Single Sign-On Playbook. Authentication Authentication is how you verify the claimed identity of someone trying to access an agency resource. Typically, you'll verify an identity using an authenticator associated with a credential. To determine the appropriate authenticator level, use the Digital Identity Risk Assessment Playbook Authentication is generally a two-step process: Step 1. Authenticate the credential: Did a trusted organization issue the credential? Has the credential expired? Has the credential been revoked, voided, or tampered with? Step 2. Ensure the individual to whom the credential was issued is the same individual presenting it: Do the photo and attributes on the credential match the person who presented it? Does the person know the PIN for the credential? Does the person have the private key on the smart card for the certificate presented to a website? Authorization is how you decide whether you should allow someone to access an agency resource. Access requirements usually dictate whether you'll allow someone to: Read or modify a certain document. Access an agency website. Enter an agency facility or location. Usually, authorization occurs immediately after authentication. When you log in to a service, you present your credentials. The service then confirms that your credentials are valid (authentication) and grants or denies you access based on your assigned permissions (authorization). Authorizations are based on progressive, fine-grained access models. Most agencies implement role-based access and move toward more fine-grained access, such as attribute-based or risk-adaptive access control, as outlined in the Federal Zero Trust Strategy. While there are defined access models, vendors may implement them in different or overlapping ways. Ensure your agency develops use cases and understands how a vendor meets the use case. Granularity Access Model Description Example Least Access Control Lists(ACLs) A static list of entities with their access rights. Allow Jane Doe access to email application More Role-Based Access Control (RBAC) Access based on a user's static pre-defined role. Jane Doe is assigned the user role "New Employee" which grants access to email and sharepoint. More Attribute-Based Access Control (ABAC) Access based on a user's assigned attributes which may be static or dynamic. Allow Jane Doe to access email if on a government device (device attribute) and in the United States (location attribute). Most Risk Adaptive Access Control (RAAC) Access based on dynamic risk factors. If Jane Doe is in assigned work location, allow email access from any managed device. If Jane Doe is not in assigned work location, only allow email access from a government device. Each authorization model has benefits and limitations. The policies and access requirements defined by agency business owners help define the model that best suits their needs. More robust access control models, such as ABAC, can help agencies with improved automation, and they are increasingly adopted by cloud-native and cloud-friendly services. The Access Management services in the FICAM architecture include Policy Administration, Authentication, Authorization, and Privileged Access Management. Service Description Keywords Digital Policy Administration Create and maintain the technical access requirements that govern access to protected agency services. Policy Decision, Policy Enforcement Authentication Verify that a claimed identity is genuine based on valid credentials. Validation, Two-Factor, Multi-Factor Authorization Grant or deny access requests to protected agency services based on access requirements, identity attributes, and entitlements. Policy Decision, Policy Enforcement Privileged Access Management Protect access to accounts that have access permissions that can affect IT system configurations and data security (e.g., superusers, domain administrators, or global administrators). Privileged Identity Management, Privileged Account Management, Administration, Superuser Federation Federation is the technology, policies, standards, and processes that allow an agency to accept digital identities, attributes, and credentials managed by other agencies. Federation has many different applications, including: Accepting an authentication transaction from another organization: Agency A authenticates one of its users and passes identity attributes and transaction details to Agency B. Agency B grants access to an application for that identity. Accepting specific characteristics (i.e., attributes such as identifiers) describing an individual from another organization: An individual can use their agency-issued credential containing an internal identifier(s) to directly log in to a different agency's online service. The online service registers the identifier(s) in its system for future use. The Federation services in the FICAM architecture include Policy Alignment, Authentication Broker, and Attribute Exchange. Service Description Keywords Policy Alignment Develop relationships and a common understanding between parties by establishing authorities, policies, standards, and principles. Trust Relationship Authentication Broker Transform an authentication event into an alternative format, such as an assertion, containing claims about the entity and the authentication transaction, to grant access to a resource. Assertion Service, Federation Assertion, Security Token Service Attribute Exchange Discover and acquire identity or other attributes between different systems to promote access decisions and interoperability. Attribute Definition Governance Governance is the set of practices and systems that guide ICAM functions, activities, and outcomes. To perform effective governance, agencies must collect and analyze data about ICAM functions from many sources, such as policies and entitlements stores. Proper data analytics help agencies monitor compliance with established information security policies. If your agency identifies problems during data collection and analysis, you should remediate these issues as quickly as possible. Real-time monitoring and risk mitigation are crucial to ensure employees and contractors have only the appropriate access, following the principle of least privilege. The Governance services in the FICAM architecture include Identity Governance, Analytics, and Mitigation. Service Description Keywords Identity Governance The systems, solutions, and rules that link enterprise personnel, applications, and data to help agencies manage access and risk. Management Framework, Rules and Procedures, Access Reviews and Re-certifications Analytics Leverage continuous analytics data to identify if someone has entitlements that conflict with access requirements. Data collection, Monitoring, Review, Data Certification, Auditing and Reporting Mitigation Correct the problems and address risks discovered by analysis that may occur during standard operations. Redress, Remediation Use Cases These use cases are designed for ICAM Enterprise Architects and business owners and describe some of the most common ICAM business processes. Each use case includes a high-level summary of the scenario, individuals and systems involved in the use case, illustrations that show the required steps to achieve the end goal, and an icon that indicates the practice area and the service with which the use case most closely aligns. For details about ICAM services, see the Services Framework. While each use case describes a particular ICAM business process, the use cases are all interrelated. The use cases generalize the activities and technologies to make sure they apply across many agencies. You can combine or build upon the ICAM use cases to support your agency's scenarios and needs. When you onboard an employee or contractor at your agency, you collect identity information from the individual and store parts of that information as identity attributes. These attributes serve as a digital proxy for the individual's identity, also known as an enterprise identity. Use Case In this use case, an administrator needs to collect or manage identity data for an employee or contractor for the purpose of creating an enterprise identity record and maintaining it throughout its lifecycle. 1. Collect information The administrator collects identity information from the employee or contractor.This identity information may come from the individual, onboarding documents, or HR systems. 2. Create an enterprise identity The administrator adds the identity information to the authoritative source, a data repository. Result: An enterprise identity in the authoritative source for the employee or contractor. 3. Maintain the enterprise identity The following steps describe identity maintenance your agency should perform on a regular basis. 3a. Identify and aggregate identity data Query your data repositories for any existing identities for an individual. Aggregate these attributes as a single enterprise identity for the individual. 3b. Update the enterprise identity If an individual has updated personal information, there are two ways to update the enterprise identity: The administrator updates the individual's enterprise identity attributes directly in the authoritative sources. The individual uses an agency application to update their personal information, and the application updates the individual's enterprise identity attributes in the authoritative sources. 3c. Delete the enterprise identity When you need to delete an enterprise identity, delete the identity attributes in the authoritative source. Example I want to create a new enterprise identity so that an individual may be established as a federal employee or contractor that will need to be identity proofed, credentialed, and granted access to agency services. Before you can create a credential and assign it to an individual, that person must provide proof of their claimed identity. Identity proofing is the process by which a federal agency collects and verifies information about a person to establish an enterprise identity. The location or information that a person needs to access informs the Identity Assurance Level (IAL), which determines the elements you should require from that person for identity proofing. There are three IALs; however, federal agencies require a minimum of IAL2 for employees or contractors with recurring access to government resources, so these use cases do not include IAL1. This use case describes the high-level steps to proof an identity at IAL2 or IAL3. Depending on the required IAL, you may require increasingly more information from an employee or contractor or partner along with additional verification steps. The information provided by the employee or contractor is also known as identity evidence. Identity evidence may be physical, such as passports, driver's licenses, and birth certificates. IAL2 - first and last name, email address, and address of record, supported by appropriate identity documentation and verified as strong. IAL3 - first and last name, email address, address of record, and fingerprints, supported by appropriate identity documentation and verified as superior. For more information about identity proofing and IALs, see NIST SP 800-63A (Section 2.2). Use Case In this use case, an administrator needs to collect or manage identity data for an employee or contractor for the purpose of creating an enterprise identity record and maintaining it throughout its lifecycle. 1. Collect identity information IAL2 (In-person or remote) - The employee or contractor presents identity information, like first name, last name, and address of record.IAL3 (In-person or supervised remote) - The employee or contractor presents identity information, like first name, last name, and address of record, and biometric data like fingerprints. 2. Verify the identity information IAL2 - The administrator confirms the information provided is valid and current by comparing photo identification to the individual, or confirming contact information, ensuring it matches the provided documentation. IAL3 - The administrator verifies all information with the issuing organization. Result: The individual's identity has been successfully proofed at IAL2, or IAL3. Examples I want to proof the identity of an employee or contractor to verify that the individual is who she says she is so that she can be issued a unique enterprise credential. A prospective employee or contractor has filled out their information in an HR system and requires IAL3 proofing and minimum background investigations. The prospective employee/contractor is then scheduled for in-person proofing. The prospective employee/contractor brings required identity documentation; the information is verified using approved documentation and biometrics are captured. You can assign access entitlements to individuals, roles, and groups. These entitlements define an employee or contractor's access to agency services, so you'll need to assign entitlements before an employee or contractor can access an agency service. Use Case In this use case, an administrator needs to assign entitlements to an employee or contractor. 1. Initiate the request An individual requests entitlements, or joins a team with specific access requirements.The requestor may be the employee or contractor, their supervisor, HR, or a security team member. 2. Review the request The administrator compares the employee or contractor's requested entitlements with the relevant access requirements.If the employee or contractor qualifies for the requested entitlements and has a mission need for access, the administrator approves the request. 3. Assign the entitlements The administrator assigns the entitlements to the employee or contractor.Any time the employee or contractor's role or relationship changes, the administrator updates the entitlements accordingly, including removing entitlements as needed. Examples I want to indicate that an employee or contractor requires and is allowed access to an agency service so that they can access the service when needed. An employee is hired to be part of the financial review team and requires access to financial applications. The employee has a role assigned to their enterprise identity record and associated with their identity attributes. After you identity proof an individual, you'll issue some proof of that individual's claimed identity. A credential (like a physical card) is a type of authenticator that serves as a tool for an employee or contractor to gain access to agency services. Use Case In this use case, an administrator needs to issue a credential to an employee or contractor. Note: The preferred credential for employees and contractors is a PIV card. For cases where you cannot issue a PIV card, you must use a combination of factors to reach at least an Authenticator Assurance Level 2 (AAL2) credential. For more information about authentication and AALs, see NIST SP 800-63B (Section 4). 1. Initiate the request An individual presents a valid government issued ID. 2. Review the request The government ID is verified with the organization that issued it. 3. Generate and assign the authenticator(s) Generate and assign the authenticator to the individual. Example I want to issue an enterprise credential, unique to an employee or contractor, so that they are able to access federal buildings and protected resources to which they require access. A derived credential is a credential derived from an existing credential, with a different form factor, such as a credential on a mobile device. Derived credentials have the same IAL as the existing credential and the same or lower AAL. When an employee or contractor requires authentication but cannot leverage an existing credential, they can use a derived credential. To be eligible for a derived credential, the employee or contractor must already have a valid credential with Authenticator Assurance Level (AAL) 2 or 3. Use Case In this use case, an employee or contractor interacts with the agency services to register or request a derived credential. 1. Initiate the request A request for identity data is initiated to the identity manager. This identity manager could be a person or system, depending on the organization. 2. Authenticate the existing credential The identity manager identifies relevant sources of data on the individual. Sources could include HR systems, security data, and personal databases. 3. Generate the derived credential Generate the derived authenticator and note the change in the user's enterprise identity record. Examples I want to provide an employee or contractor, who has already been issued an enterprise credential, a derived credential so that they can authenticate to enterprise applications. An employee or contractor travels quite a bit as part of their job. Accordingly, they are frequently limited to using a small tablet or their phone to stay connected while on the go. In this case, a derived credential is needed for purposes such as accessing secure agency websites or an agency VPN from their mobile device. Active credentials require regular maintenance. This use case describes the most common credential maintenance activities: Reset a credential - An employee or contractor forgets the password or PIN associated with a credential and requests a reset. Renew a credential - An employee or contractor's credential is expiring or their identity information changes, so they request a replacement credential. You must renew a credential prior to the expiration date; otherwise, the employee or contractor must go through the issuance process again. Revoke a credential - An employee or contractor is no longer eligible for their credential (like separating from the issuing agency). The sponsor, supervisor, or administrator requests a revocation of all associated credentials and enterprise accounts. You should periodically review your employee or contractors' eligibility for credentials to identify potential orphaned data. Use Cases Reset a Credential In this use case, an administrator needs to reset a password or PIN for an employee or contractor credential. 1. Initiate the request An employee or contractor forgets their password or PIN, and requests a reset.If the request is valid, the identity management system approves the request. 2. Issue a reset The system issues a password/PIN reset, which may be a temporary password or a link to a web-based reset form. 3. Reset the credential The employee or contractor resets their password or PIN. Renew a Credential In this use case, an administrator needs to issue a new credential to replace one that will expire soon or has outdated identity information. 1. Initiate the request An individual requests a renewal for an employee or contractor's credential.This individual may be the employee or contractor, their supervisor, or an administrator with approval authority.This could also be an automated process triggered by schedules or specific events. 2. Review the request The identity management system reviews the request and verifies that the employee or contractor qualifies for a renewed credential. If so, approve the request. 3. Replace the credential The system issues a new credential to the employee or contractor, and updates the associated enterprise identity record. Revoke a Credential In this use case, an administrator needs to revoke an active credential. 1. Initiate the request An individual sends a separation notification or a notice of a lost or compromised credential, requesting revocation.This individual may be the employee or contractor, their supervisor, HR, or a security team member. 2. Disable the credential The administrator invalidates the credential.Depending on your agency, an individual or a system may perform this task. 3. Return the credential If the revoked credential is physical or hardware-based, the administrator returns the credential to the appropriate individual.This individual may be a supervisor, HR, or security team member. Examples An employee or contractor may have attempted to use a credential and input the PIN information incorrectly several times up to an agency-defined limit and has locked their account or credential. The employee or contractor requests a PIN reset. The employee or contractor is directed to an unlock service; has to verify information again to prove they are the same person issued the original credential; and follows prompts to unlock their credential, generating a new PIN in the process. Reset - I want to verify the identity of an employee or contractor that has already been issued a credential and reset their PIN or password so that they can continue to access enterprise resources. Renew - I want to verify the identity and eligibility of an employee or contractor, who has a previously issued credential that is near expiration, so that they may be issued a new enterprise credential to maintain their ability to access enterprise resources. Revoke - I want to remove access to enterprise resources for an employee or contractor so that they can no longer use the protected resource. This use case describes the steps to authenticate individuals and authorize access to agency services. Agency services can be anything from applications and files to physical facilities. Use Case In this use case, an Access Control System (ACS) Administrator needs to grant access to an employee or contractor who has an enterprise identity and active credential and needs to access a logical or physical resource. These steps assume the employee or contractor already has credentials to support authentication as well as the access entitlements to support authorization decisions. Authentication - I want to verify the claimed unique identity of a given employee or contractor so that the system can verify the right individual is attempting to access an agency service. Authorization - I want to allow access for only employees and contractors that meet established requirements so that only the people who should have access do have access. 1. Access Attempt An employee or contractor attempts to access an agency service. 2. Authenticate the employee or contractor The employee or contractor presents an authenticator to the ACS that meets the protected resource's minimum assurance requirements:AAL2 (two-factor) - Something you know + something you have, like a one-time passcode.AAL3 (two-factor + hardware) - Something you know + something you have, like a one-time passcode generated by a hardware-based authenticator; or a PIV credential. For more information about AAL values, see NIST SP 800-63B Section 5: Authenticator and Verifier Requirements. 3. Determine the access entitlements and access requirements Upon successful authentication, the ACS identifies 1) The employee or contractor's access entitlements associated with the protected resource, and 2) The protected resource's access requirements. 4. Process the access information The ACS compares the employee or contractor's access entitlements to the protected resource's access requirements to decide whether to authorize access. 5. Grant access If the employee or contractor meets the protected resource's access requirements, the ACS grants access to the protected resource.The ACS logs the access attempt and decision for auditing purposes. Example An employee on the financial review team attempts to access a government financial application that is secured by a single sign-on (SSO) solution. The employee clicks a link to the financial application and is redirected to the SSO portal. The employee authenticates using his/her provided credential, which the SSO determines to be valid. The SSO solution or the financial application system finds the employee's enterprise identity account and compares the roles assigned to those allowed by the financial application. The resulting determination is that the employee has authenticated to the required assurance level and has the appropriate entitlements to access the system and is subsequently logged on. Federal employees and contractors often need to access protected services managed by other federal agencies. Federation is the means by which an agency can accept authentication assertions and associated identity attributes from systems within their agency and at other agencies. This allows federal employees and contractors from across agencies to access protected resources and streamlines the user's experience. Agencies can pass assertions to share attributes about employees and contractors. Use Case In this use case, an employee or contractor from Agency A attempts to access a federated service at Agency B. This use case assumes the employee or contractor already has an account or entitlements to access resources at Agency B, or that they will be provisioned. For more information about granting access to protected resources, see Use Case 7. Grant Access. 1. Request access to federated service An Agency A employee or contractor requests access to a federated service at Agency B.The employee or contractor selects the Agency A authentication service. 2. Redirect to Agency A for authentication The Agency B system redirects the employee or contractor to the Agency A authentication service.Agency A authenticates the employee or contractor. 3. Perform transparent transaction Agency A passes identity attributes and transaction data to Agency B via a signed assertion. 4. Agency B grants access Agency B consumes the assertion data, optionally correlating it with an established account or local identity and makes an access control decision.The Agency B system redirects the employee or contractor to the federated service. Examples I want to allow other federal agencies' employees and contractors (who meet specific requirements) to access some of my agency's resources, which facilitates cross-government collaboration and information sharing. An employee or contractor from Agency A visits a shared service operated by Agency B to service all federal government users. At the homepage, the employee/contractor selects their Agency A icon and is redirected to their Agency A SSO portal. They log in using their Agency A managed credentials and are redirected back to the Agency B shared service. Reference Example This reference example includes sample enterprise ICAM tools (e.g., solutions, applications, and software) aligned with ICAM service areas that illustrate ICAM functionality at an agency. The reference examples are designed for enterprise architects, security engineers, and solution architects to facilitate discussions regarding the technology solutions to integrate with enterprise applications and business requirements. The system's components are representative examples only. Some solutions chosen by your agency may span across more than one service area. The following figure is an example of a small selection of system components only. You can modify the graphic or incorporate it as is and target state system components for enterprise roadmap planning. An authoritative source is a trusted repository of identity attribute data. It's possible to have multiple authoritative sources for attributes. Authoritative sources systems components may include: Human Resource systems such as payroll, time and attendance, and benefits administration Agency or government-wide Learning Management Systems Agency or government-wide Personnel Security systems for security and suitability Directory services, including on-premise or cloud-based directory services Other external or internal sources Identity Management Systems Identity management systems are how an agency manages the identity lifecycle. Identity management system components may include: Identity Governance and Administration tool for provisioning and workflow Role management or role manager applications Identity correlation or aggregation Directory management Virtual directories Credential Management Systems Credential management systems are how an agency manages an authentication token bound to an identity. Credential management system components may include: PIV credential service provider solutions Other non-PKI credential service provider solutions Federated certification authorities Private certification authorities Key management services Enterprise certificate manager Multi-factor authentication managers for software and hardware tokens Password managers Access Management Systems Access management systems are how an agency leverages credentials to authenticate individuals and authorize access to protected resources. Access management system components may include: Enterprise Single Sign-On (SSO) applications Web access management applications Physical or facility access control systems Privileged access management applications Access policy and access rules repositories Policy enforcement points Policy decision points Virtual private networks Cloud access security brokers Network access management tools Governance Systems Governance is the set of components to centralize management, develop insights, and assist in managing ICAM areas and services. Applications across all service areas include auditing, such as standard audit logs or configuration of auditable events. Governance includes the aggregation of individual auditing and reporting into centralized tools to perform real-time or near real-time analysis, identify anomalies, and trigger mitigations for anomalous authentication or authorization events. Tools are increasingly incorporating machine learning or adaptive algorithms. Governance systems components may include: Identity Governance and Administration (IGA) solutions to perform access re-certifications IT Service Management (ITSM) Security information and event monitoring (SIEM) Agency Endpoints Agency endpoints are resources that an agency needs to protect, including physical and digital resources. Agency endpoints may include: On-premise applications Cloud-based applications and platforms Agency private networks Government cloud email services Government facilities Policies and Standards See the ICAM Policy Matrix for the latest set of ICAM policies and standards.