



National Science Foundation

WHERE DISCOVERIES BEGIN

**National Science Foundation
Identity, Credentials, and Access Management
Technology and Processes**

**November 2023
Version 4.0**

NSF DIVISION OF INFORMATION SYSTEMS

2415 Eisenhower Avenue
Alexandria, VA 22314



CONTENTS

1	BACKGROUND.....	1
2	PURPOSE	1
3	ROLES AND RESPONSIBILITIES	1
4	POLICY.....	2
4.1	Identity and Credential Management	3
4.2	Access Management.....	3
4.3	Governance.....	4
4.4	Enforcement	4
4.5	Review.....	4
4.6	Authority	4
4.7	Revision History.....	4
5	IDENTITY, ACCESS, AND CREDENTIAL MANAGEMENT	4
5.1	Identity and Credential Management	4
5.1.1	NSF Issuance Processes and Procedures	5
5.1.2	NSF Card Lifecycle Processes/Procedures	6
5.1.3	Maintenance Services	7
5.1.4	NSF Identity life-cycle management	8
5.1.5	NSF Identity Attribute Correlation	9
5.1.6	NSF Identity Deactivation	11
5.2	Access Management Services	13
5.2.1	NSF Entitlement or Role Management.....	13
5.2.2	NSF Role Provisioning Workflow.....	14
5.2.3	NSF Organization Move Workflow.....	15
5.2.4	NSF Role Re-Certification.....	15
5.2.5	NSF Authentication Internal User	16
5.2.6	NSF Authentication for External User.....	18
5.2.7	Authorization	23
5.3	Federation.....	25
5.3.1	Federation Integration.....	25
5.3.2	Attribute Exchange by Identity Providers.....	27
5.3.1	Authorizing Federation User for NSF business applications.....	27



5.3.2	Research.gov Federation Policy Alignment	27
5.4	Digital Identity Risk Management	27
6	GOVERNANCE	27
6.1	Auditing & Reporting.....	27
6.2	Redress	27
6.3	Recovery.....	28
7	TECHNOLOGY SOLUTION ROADMAP	29
	APPENDIX 1: FEDERAL POLICIES	30
	APPENDIX 2: STANDARDS, GUIDANCE, AND REFERENCES.....	31



1 BACKGROUND

The National Science Foundation (NSF) began to implement Identity, Credential, and Access Management (ICAM) (NSF internally referred to as Identity and Access Management (IAM)) in 2009 as originally outlined in the Homeland Security Presidential Directive 12 (HSPD-12). Moreover, the agency found itself able to meet the standards set in the Office of Management and Budget (OMB) Memorandum 11-11 (hereinafter, OMB M-11-11) regarding the Continued Implementation of HSPD-12. When the Federal Chief Information Officer Council (CIO Council) released the final Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance in December 2011, NSF found itself well positioned to institute the recommendations as most, if not all, already got implemented. Since that time, the Foundation kept abreast with changes in the federal guidelines and incorporated any needed or relevant changes as required.

NSF continually referenced National Institute of Standards and Technology (NIST) in both Federal Information Processing Standards (FIPS) and Special Publications (SP), notably, FIPS 200 and SP 800, on top of the FICAM Guidance. Thus, the Foundation is pleased to respond to OMB M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, as part of the quarterly Integrated Data Collection (IDC) Submission process.

2 PURPOSE

The purpose of this paper is to present the current state of NSF's ICAM deployment. It is a high-level overview of the process and technology employed in ICAM. This document serves as part of the Integrated Data Collection (IDC) requirement fulfillment regarding OMB M-19-17.

3 ROLES AND RESPONSIBILITIES

Identity Management and Card Issuance roles include:

NSF Chief Information Officer (CIO) – Oversees the establishment of policies and procedures for ICAM.

NSF Division of Information Systems (DIS) Director – Responsible for all activities within the DIS division.

DIS Security, Architecture, Policy and Plans (SAPP) Branch Chief – Oversees related ICAM processes with a focus on identity management.

Division of Human Resource Management (HRM) – Manages the process of requesting Personal Identity Verification (PIV) requests for new employees and re-issues for current employees.

DIS Change Control Board (CCB) - Serves as the governing body responsible for decision-making, prioritization, and information gathering related to the review and approval of changes in the NSF IT environment. Reviews and approves changes and updates to ICAM policies and systems.

NSF Personnel Security and Suitability Team (PSS) Team - Responsible for assuring all staff and contractors are appropriately vetted for employment at NSF using government-wide standards established by the U.S. Office of Personnel Management (OPM) National Background Investigations Bureau (NBIB).



Contracting Officer Representative (COR) - Manages the process of requesting PIV requests for contractors.

DIS ICAM Lead – Responsible for planning, overseeing, and implementing ICAM program and system changes and updates to ensure they are completed in a timely fashion, within budget, and obtain necessary governance review and approval.

Administrative Manager/Sponsor— the individual who substantiates the NSF relationship to the Applicant and provides sponsorship to Applicant. The employer/sponsor shall authorize the request for a PIV credential.

Enrollment Official— the individual who initiates the chain of trust for identity proofing and provides trusted services to confirm employer sponsorship, bind the Applicant to their biometrics, and validate the identity-source documentation. The Enrollment Official delivers a secured enrollment package to the Identity Management System (IDMS) for adjudication.

NSF Personnel Security Specialist—individual that adjudicates NSF applicants through background checks and identity proofing to establish organizational chain of command within the Identity Management System (IDMS). Personnel Security ensures the accuracy of PIV profiles. This includes establishing approved Employer/Sponsor.

Issuing Authority (Issuer) —the entity that issues the PIV credential to the Applicant after all identity proofing, background checks and related approvals have been completed.

4 POLICY

The National Science Foundation (NSF) will deploy ICAM following the federal guidelines as described in:

- *OMB Memorandum M-19-17 Enabling Mission Delivery through Improved Identity, Credential, and Access Management* (May 2019);
- *Homeland Presidential Security Directive 12 (HSPD-12): Policies for a Common Identification Standard for Federal Employees and Contractors* (August 2004);
- *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance* (version 2, December 2011);
- *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (August 2013);
- *FIPS 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors* (August 2013);
- *NIST Special Publication 800-157: Guidelines for Derived Personal Identity Verification (PIV) Credentials* (December) 2014;
- *NIST Special Publication 800-63-3: Digital Identity Guidelines* (June 2017); and
- *NIST Special Publication 800-116 Rev. 1: Guidelines for the Use of PIV Credentials in Facility Access* (June 2018).
- *Executive Order 14028: Improving the Nation's Cybersecurity* (May 2021)
- *OMB Memorandum M-21-07 Completing the Transition to Internet Protocol Version 6 (IPv6)* (November 2020)



National Science Foundation

- *OMB Memorandum M-22-09 Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (January 2022)
- NIST Special Publication 800-207: *Zero Trust Architecture* (August 2020)
- See also Appendix 1: Federal Policies and Appendix 2: Standards, Guidance, and Reference.

NSF ICAM deployment is tailored to the agency's specific circumstances, conditions, and needs within allowable tolerances of the guidance.

NSF's ICAM will also incorporate a Zero Trust Security Model where practical. This is an integrated security model for end-points that includes but is not limited to:

- Users
- Applications
- Data
- Servers
- Devices, and
- Networks

This model provides real-time and contextual security, along with the ability to predict, understand and manage appropriate access while detecting threats and breaches.

In accordance with Zero Trust Architecture, NSF is focused on ensuring eligible staff members are issued a PIV card and can use PIV to log in to agency systems. NSF has achieved a high percentage of multi-factor authentication (MFA) enforcement using Personal Identity Verification (PIV) for agency-internal digital identities. NSF uses phishing resistant MFA for the initial authentication of local devices, e.g., laptops, for personnel with PIV cards. NSF continues to evaluate its current MFA and is looking for alternative phishing-resistant MFA in situations where PIV card usage is not available.

In the long-term NSF plans to change from machine-based enforcement to user-based enforcement.

4.1 Identity and Credential Management

NSF uses Identity and Credential Management practices to establish, maintain, and terminate identities. The set of practices includes: Sponsorship, Eligibility, Enrollment, Adjudication, Physical Issuance, EPACS Enrollment, and LACS Option. NSF ICAM also incorporates the Lifecycle Processes/Procedures that include Storage, Renewal, Reissue (Broken Chain of Trust), Maintenance Services, and Destruction & Close-out Credential Management

NSF Human Resource Management and NSF Security and Emergency Management (SEMS) retain principally responsibility for the issuance and maintenance of identities and credentials.

4.2 Access Management

NSF Access Management policy ensures only those with the proper need for access are permitted the ability to perform an action on a particular resource. The associated services for access management include: Policy Administration, Entitlement Management, Provisioning, Authentication (for both internal and external access), and Authorization.

The NSF ICAM Team and NSF SEMS provide oversight of these services.



4.3 Governance

Please see Section 6 for details regarding Governance.

4.4 Enforcement

ICAM policy directly impacts NSF security, both physical and virtual, and individuals who fail to comply with IT and ICAM security policies may be subject to disciplinary action.

4.5 Review

The NSF ICAM Policy is subject to a yearly review as stipulated in OMB Memorandum M-19-17 pursuant to Homeland Security Presidential Directive 12 (HSPD-12).

4.6 Authority

NSF DIS issues this policy. The policy is in alignment with industry best practices and in compliance with the references listed in the Background section.

4.7 Revision History

Version	Date	Section	Description	Changes by
1.0	11/30/2020	Initial Release	Initial Version	DIS
2.0	11/15/2021	Removed references to IAM platform and replaced with ARM platform in both text and graphics throughout.	Revised Version	DIS
3.0	11/15/2022	Updated federal policies list informing this document; Incorporated more Zero-Trust Architecture alignment; extended MFA description; clarified acronyms and initializations; completed full tech edit.	Revised Version	DIS

5 IDENTITY, ACCESS, AND CREDENTIAL MANAGEMENT

5.1 Identity and Credential Management

Identity and Credential Management is the set of practices allowing NSF to establish, maintain, and terminate identities. These practices include: Sponsorship, Eligibility, Enrollment, Adjudication, Physical Issuance, EPACS Enrollment, and LACS Option. NSF ICAM also incorporates the Lifecycle Processes/Procedures that include Storage, Renewal, Reissue (Broken Chain of Trust), Maintenance Services, and Destruction & Close-out

The ID Card Office issues four distinct types of access cards including:

- **Personal Identity Verification (PIV)** – PIV cards are issued to employees (general schedule (GS) and Intergovernmental Personnel Act (IPA) staff) and contract personnel (including AAA Fellows) who require physical or logical access for a period of 6 months or longer. The PIV is utilized for physical access through card readers that allow access to NSF-controlled space. The PIV card is utilized for logical access, through mechanisms provided by the Division of Information Systems (DIS) that allow for log-in to NSF IT systems and applications.



- **Windows Administrator (WADM)** – WADM holders can safely install properly licensed or publicly available software that has been pre-approved by NSF on systems belonging to NSF users. WADM access is restricted to individuals with legitimate business purposes; permission is granted through the Security, Architecture, Policy and Plans Branch (SAPPB) of the Division of Information Services (DIS).
- **Facility Access Card (FAC)** – The FAC is issued to qualifying individuals who only require physical access to the main NSF facility and for whom the full Personnel Security adjudication process would be inappropriate or impractical. The FAC allows for physical access to NSF controlled space but does not have the capabilities for logical access to NSF information technology systems. The NSF Facility Manager and/or NSF SEMS may request FACs for appropriate personnel, such as building maintenance or security contractors. It should be noted that the FAC is not considered an official form of federal identification, however identity and authorization standards must be met per NSF I-9.
- **Personal Identity Verification-Interoperability (PIV-I)** – The PIV-I card is a PIV-card variation for qualifying individuals who have been vetted through Personnel Security to access NSF premises and systems but are not directly contracted to the agency. Identity and employment authorization standards must be met per NSF I-9. The PIV-I allows for both physical and logical access to NSF systems, therefore the individuals' position duties should explicitly require both. These individuals could include; onboarding employees with current and active PIV cards from an external federal entity (i.e., on-detail), short-term seasonal employees and contractors (i.e., interns), or individuals with no NSF contract who are appointed to render services to the agency (i.e., building managers, custodians, volunteers).

The NSF ID Card Office services effectively manage the full NSF ID card lifecycle, assist with ePACS (electronic Physical Access System) management, and reporting.

5.1.1 NSF Issuance Processes and Procedures

5.1.1.1 Sponsorship

All access card issuance processes begin with sponsorship from an approved federal representative. For employees, sponsorship is initiated by a Human Resources (HR) representative who submits the relevant onboarding information to the NSF ID Card Office. For contractors, sponsorship is initiated by a Contracting Officer's Representative who then submits a completed NSF 1690 form to the NSF ID Card Office. For an external agency's federal workers (e.g., individuals coming to NSF for a detail), sponsorship is initiated by an NSF Federal Sponsor who then submits a completed NSF 1690 form to the NSF ID Card Office.

5.1.1.2 Eligibility

The NSF ID Card Office reviews the documents and information submitted during sponsorship to determine the appropriate access card for each individual, if any, based on FIPS 201.2 and NSF SEMS policy. The NSF ID Card Office may suspend enrollment temporarily if determines more information or approval is required to proceed. Any such suspension will be accompanied by a written request to the sponsor, agency contact (such as NSF SEMS or NSF PerSec), or governing agency system/contact (employment authorization requests through the Department of Homeland Security's (DHS) SAVE for foreign national contractors per FIPS 201.2).



5.1.1.3 Enrollment

The Enrollment Official in the NSF ID Card Office reviews the documents that establish both identity and employment authorization a second time. See Roles and Responsibilities: Enrollment Official section of this document for an overview. Per NSF SEMS policy, NSF employees are able to reject/retake profile photos during the enrollment process.

5.1.1.4 Adjudication

Once enrollment is completed, the NSF ID Card Office will confirm their adjudication status as relayed by NSF PerSec. If confirmation of a positive interim or final determination cannot be relayed from NSF PerSec, it may be necessary to initialize an adjudication process which then suspends any further issuance procedures. The NSF ID Card Office provides fingerprinting services for NSF adjudications.

5.1.1.5 Physical Issuance

The Issuing Authority confirms all elements of the issuance process are successfully completed/approved. They then print, program, and store the access card securely until the individual is available/scheduled for issuance. Once the individual presents themselves for issuance, it is the Issuing Authority's responsibility to establish a biometric match. Once established, the Issuing Authority activates the access card and prompts the individual to encode it with a secure PIN known only to themselves. The individual then takes the access card to the ePACS enrollment station located in the NSF ID Card Office for physical access to the NSF facility. If the access card does not require physical access, they proceed to IT Help Central for logical access.

5.1.1.6 EPACS Enrollment

The NSF ID Card Office technician at the ePACS enrollment station must complete a biometric and PIN match in order to enroll an access card into the ePACS system. Once enrolled the technician fills in required information in the individual's profile and grants him basic access to the facility. Any access request beyond this basic access must be provided in writing through email to the NSF ID Card Office and NSF Security. If approved in accordance with NSF SEMS policy, the technician will add this access to the individual's profile.

5.1.1.7 LACS Option

Logical access is provided by IT Help Central, ITHC. The NSF ID Card Office ensures that the eligible access card is active and secured with a PIN. The PIN is created at the time the PIV card issued, and it is created by the holder and verified by the security office.

5.1.2 NSF Card Lifecycle Processes/Procedures

As the HSPD-12 NSF ID Card Office is responsible for the full life cycle of the cards issued and the many activities beyond issuance performed to maintain the card. Other functions performed include PIV Card Renewal, PIV Card Name Change, PIV Card Lost, PIV Card PIN Reset (LACS), and PIV Card Damaged or Not Working. The processes are described in the following sections and are applicable to all other smart/access cards.

5.1.2.1 Storage

It may become necessary for the NSF ID Card Office to store printed access cards temporarily, such as during physical issuance before pick-up or a found/recovered card. It is the responsibility of the NSF ID Card Office to ensure that these stored cards are secured under standards dictated by FIPS 201.2, and that access to them is limited to NSF ID Card Office personnel and other authorized entities as dictated by NSF Security policy.



5.1.2.2 *Renewal*

Access card renewal requires confirmation the individual card holder is: active in good standing, is in possession of their unexpired access card, and passes a 1:1 match to their profile per FIPS 201.2. Per NSF policy, federal employees eligible for renewal receive a new expiration date set by the Not To Exceed (NTE) date specified by HR up to a maximum of six years from the date of issuance. For contractors, the expiration date is determined by the NTE date established by the COR or sponsoring official (this date should be listed in the contractor's NSF 1690 or a follow-up extension in writing/email). In order to ensure a current biometric match, the NSF ID Card Office technician may require an updated profile picture is collected.

5.1.2.3 *Reissue: Broken Chain of Trust*

If the cardholder experiences an expired, lost or stolen access card, the chain-of-trust is broken. The individual will need to re-enroll in order to get their card re-issued. The NSF ID Card Office should disable and revoke the credential immediately upon receiving a report of a lost/stolen access card. Expired access cards get disabled in a weekly audit every Friday. Re-enrollment for re-issuance entails overwriting all biometrics and documents associated with the individual's profile. Additionally, re-issuance of lost/stolen access cards require a written/email request from an Administrative Manager or Supervisor in the case of employees, or the COR/sponsor in the case of contractors.

5.1.3 Maintenance Services

5.1.3.1 *Name Change*

In accordance with FIPS 201.2, all efforts will be made to ensure a current 1:1 match with the profile data associated with every individual's access card. This includes an individual's current legal name. Name changes can be prompted by marriage, divorce, and/or court approved modification. The individual undergoing a legal name change should bring documented proof of this change to the NSF ID Card Office. The NSF ID Card Office will then update the card holder's profile and provide them with a new access card.

5.1.3.2 *PIN Reset*

An individual may require a PIN reset if their current one becomes locked or lost. A biometric match along with a current access card can be used to re-establish a connection to a card holder's profile data. This can be performed either at the NSF ID Card Office or at the self-service kiosk in ITHCS.

5.1.3.3 *Damaged*

A non-functioning access card may be replaced if the individual returns the damaged card to the NSF ID Card Office. The NSF ID Card Office technician will confirm the card is the current card issued to the individual and is no longer functional. If the damaged card is not returned or cannot be confirmed to match their current issuance record, then the card is considered lost. The NSF ID Card Office technician will clean and test the returned card before approving a replacement.

5.1.3.4 *Destruction & Closeout*

PIV card destruction is required whenever a staff member is leaving the agency or when a previous PIV card is rendered obsolete. Examples of obsolete cards include PIV card renewals, non-operational PIV cards (troubleshooting will not solve the issue), and name changes. The NSF ID Card Office will maintain a record of all destroyed access cards.

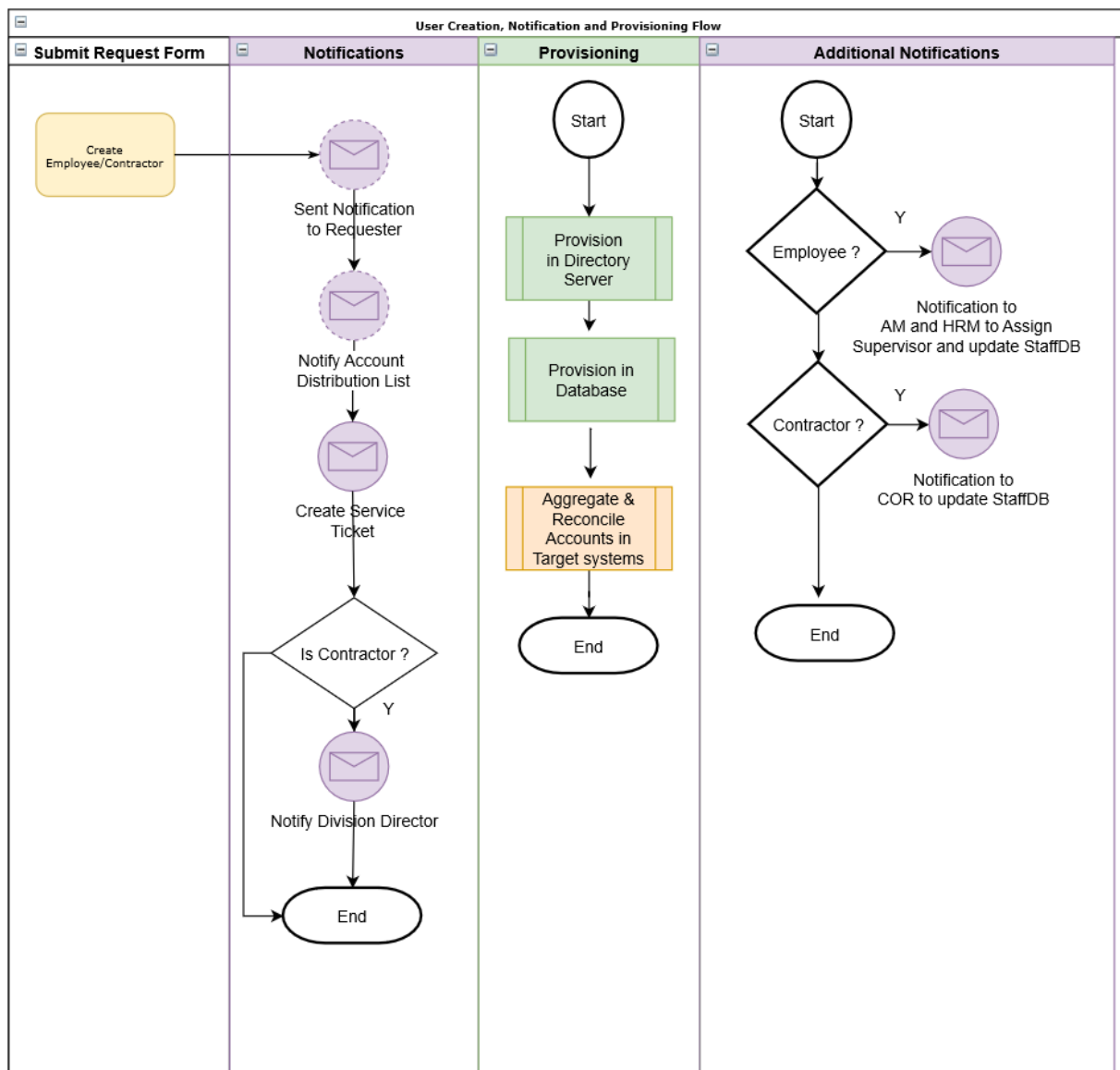


5.1.4 NSF Identity life-cycle management

The NSF Enterprise Identity and Access Management (IAM) platform provides the lifecycle management of user identities and serves as the primary system for identity creation, maintenance, and authoritative source to host identity attributes for business applications to consume.

Identity attributes from different sources are aggregated/read into IAM platform to trigger identity life cycle events. Life cycle events are carried out by different systems in the IAM platform. The following diagram depicts various resource/target provision events triggered during the new user creation event.

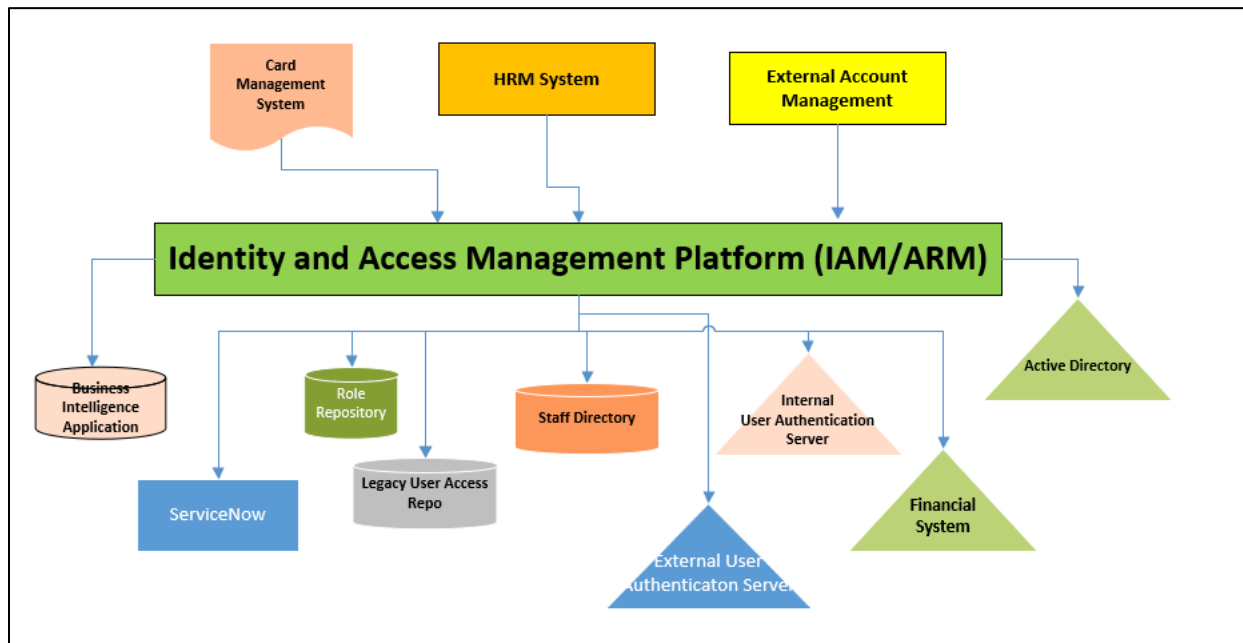
In creating and managing identities, the Divisional Administrative Manager (AM), Contracting Officer's Representative (COR) and Human Resource Management (HRM) division plays a major role.





5.1.5 NSF Identity Attribute Correlation

NSF Identity information is provisioned/synchronized into various systems to support authentication, authorization, and profile attribute access to various applications. Following diagram depicts how IAM platform is integrated with various authoritative sources to aggregate the identity information into the identity warehouse and synchronizes the identity attributes and status to various access control system and application.



5.1.5.1 Card Management System

PIV data comes from the Card Management System and is managed through a file update periodically to load the PIV card attributes associated with the user. NSF Account and Role Manager (ARM) application is integrated with the NSF Fusion Server to provide Continuous Diagnostic and Mitigation (CDM) data on a periodic basis to DHS Dashboard. ARM application generates periodic CDM data feeds of ACCOUNT, BEHAVE, CRED, Identity, PRIV and TRUST Attributes.

5.1.5.2 NSF Account and Role Manager (ARM)

NSF Account and Role Manager (ARM) is a system that collects basic information about the user account and creates an account and provision to various repositories to support authentication, authorization, and profile attribute access to numerous applications.

5.1.5.3 HRM Systems

Supervisor Data: the HR Enterprise Data Warehouse system provides supervisor information to the IAM platform and it is the authoritative source for this information, the information is added to the users'



profile. Admin Managers from various divisions use this information and assign employees to their supervisors.

The HR Enterprise Data Warehouse system also provides authoritative attribute, job title

The IAM platform is designed to perform the following functions pertaining to supervisors:

- Synchronize supervisor data from the HRM system
- Trigger Life Cycle event when a Supervisor changes or leaves the agency
- Provides the Administrative Managers (AM's) the ability to update a user's supervisor record

Learning Management System: LearnNSF is the Learning Management System at NSF that manages user training programs and status. It is an externally hosted system providing data relevant to the training details and training completion status.

Data from LearnNSF is regularly fed into an internal HRM data warehouse repository. For capturing attributes that relate to the identity functional area, a custom-built web services connector is used to aggregate/read in relevant information from the HRM data warehouse.

5.1.5.4 Business Intelligence Application

IAM synchronizes the authorization information with the NSF Business Intelligence (BI) system to enable the BI application to provide access control to various dashboards and reports.

5.1.5.5 Legacy User Access Repository

Business Applications use a database repository to host permissions and user entitlement assignment. Applications makes use of customized stored procedure and database lookup to perform authorization check for a given internal user.

5.1.5.6 Internal User Authentication Server (Directory Server)

The INTDS directory server is an internal user repository used by the authentication services to authenticate internal staff users.

5.1.5.7 External User Authentication Server (Directory Server)

The EXTDS directory server is an external user repository used for authentication service for external users.

5.1.5.8 Active Directory (AD)

NSF's enterprise AD holds user's network account status as well as other network account attributes such as the account name that are relevant for credential management. IAM synchronizes the identity attributes from NSF IAM platform whenever an identity goes through the life cycle events. Users' accounts/records in AD are aggregated into the existing NSF IAM Platform using an AD connector using secure protocols.

5.1.5.9 Financial System

The financial system uses a directory server to manage users' permissions, only users with a current profile in the server are granted access to the financial systems.

5.1.5.10 Staff Directory

StaffDB is a database repository hosting user profiles and provides directory services to NSF employees. It uses the identity attributes synchronized from NSF IAM platform whenever an identity goes through the identity life cycle event.



5.1.5.11 ServiceNow (NOW)

NOW is a personalized Web portal that connects NSF internal customers to IT Service Desk services. IAM synchronizes the identity attributes from NSF IAM platform whenever an identity goes through the identity life cycle event that manages authentication to NOW portal and authorization information for specific functionalities.

5.1.5.12 Role Repository

A centralized database schema used as a repository to host roles & permissions associated with an individual identity, these permissions are managed through Role Management system.

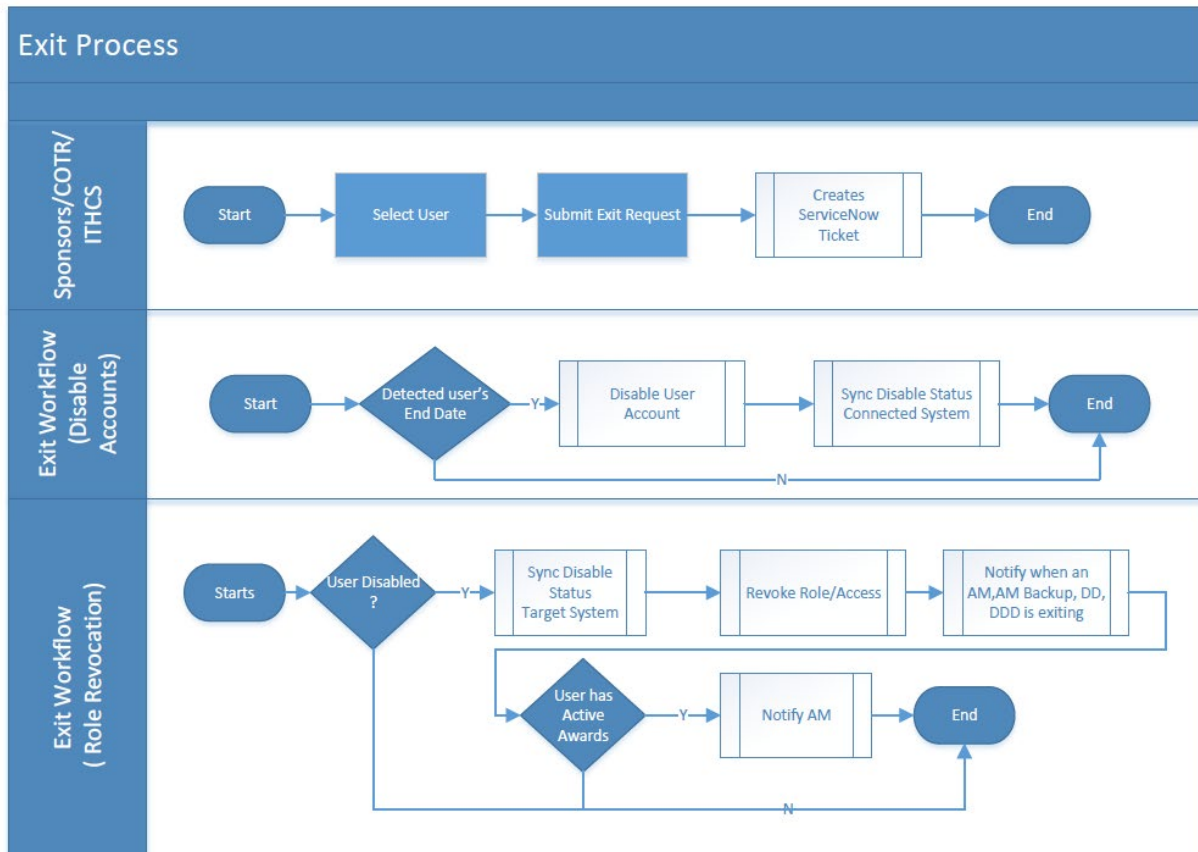
5.1.6 NSF Identity Deactivation

At NSF, identity deactivation is initiated by one of the following processes.

- Exit Process
- Contract Renewal Certification Process
- User Inactivity

5.1.6.1 NSF Exit Process

The NSF standard process for identity deactivation uses a customized Exit Process for Employees and Contractors. Administrative Managers make use of Employee Exit Process to exit Employees while CORs make use of Contractor Exit Process to deactivate contractor by specifying the end date.





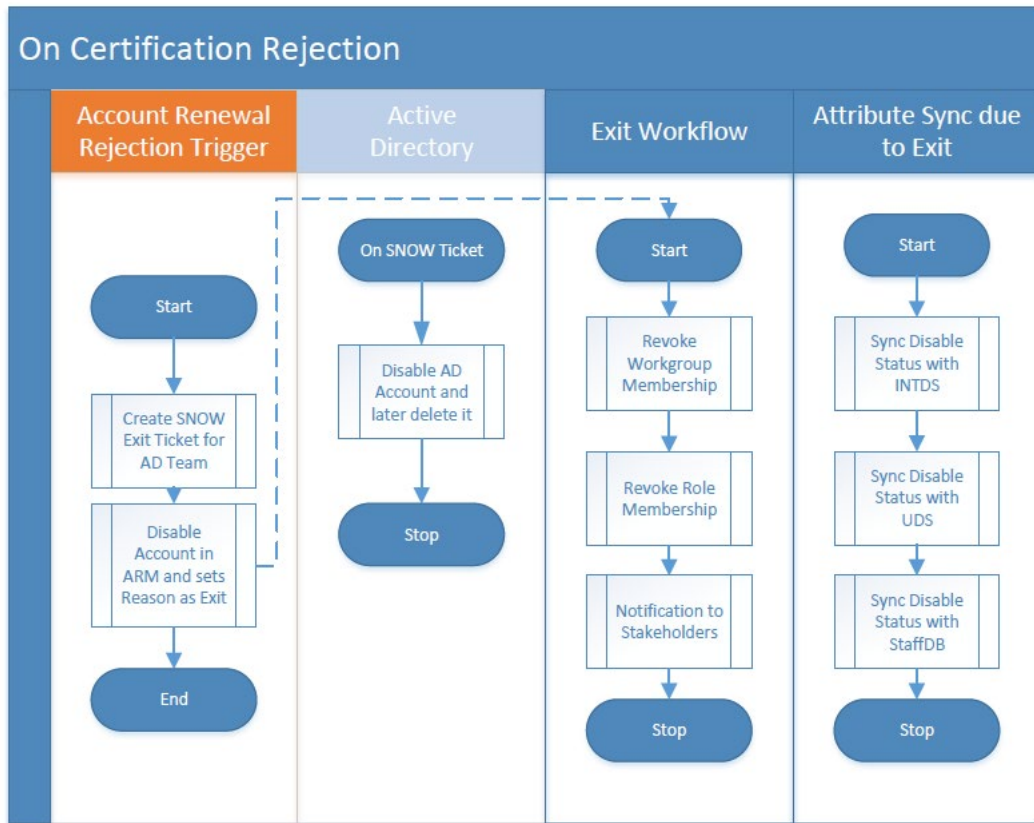
- The Sponsor/COR/ITHCS initiates the Exit Process using customized Identity platform
- The IAM platform creates tickets to disable user identity in Active Directory and disables the identity in all the target systems on the end-date set during the exit process
- The IAM platform detects the disabling event and triggers the Exit Workflow business process. The Exit Workflow performs the following:
 - Synchronizes identity status with various datastores,
 - Revokes all roles associated with the user,
 - Ensures a notification is sent to authorities when the exiting user has any critical roles, and
 - Sends a notification to Primary and Backup Admin Managers to complete any reassignment to support Grants management processes.

Certain roles are considered critical in a division to support its operations (like Primary and Backup Admin Manager). When a user with a critical role is leaving NSF, the system notifies responsible authorities about the exit so supervisors/managers can reassign the role to a designated user. The following table lists the critical role and the notification sent to responsible authorities.

Critical Role	Notification Recipients (Role Organization)
Primary Admin Manager	Backup Admin Manager, Division Director, Deputy Division Director
Backup Admin Manager	Primary Admin Manager
Division Director	Primary and Backup Admin Manager
Deputy Division Director	Primary and Backup Admin Manager

5.1.6.2 NSF Contractor Renewal

NSF uses quarterly contract renewal processes to renew/revoke contractor user accounts to make sure the accounts are still needed to support or to remove accounts no longer needed. The following flow diagram highlights the user deactivation and clean up as soon as a user's identity is revoked during the certification process.



- A service ticket is created to disable/delete account and assigned to the AD Administrator
- ARM system disables the account in the IAM platform
- IAM synchronizes the user status with integrated databases, applications, and directory servers.
- The IAM system notifies Administrative users about automated access revocation for the exited user.

5.1.6.3 Deactivation due to inactivity

NSF Active Directory detects when the user is inactive for 30 consecutive days and marks the identity as Disabled with the reason stated as 'Due to Inactivity'. The IAM platform detects the user's status change due to inactivity and triggers workflow to deactivate users account in all integrated target systems.

5.2 Access Management Services

5.2.1 NSF Entitlement or Role Management

A role defines the user's job responsibility and includes the granular privileges of what a user can do within an application/system. NSF uses Role-based access control (RBAC) in combination with the division attribute to define roles and to restrict the user capabilities within the boundary of the given division. Each Role definition contains entitlement/permission that will also be provided to the application to perform authorization check.



The system implements restricted access control within the NSF Account and Role Manager (ARM) to support specific role visibility (Scope) to their owners (example – Divisional Administrative Manager(s)). Only users with the respective ownership will be able to request, assign, unassign and approve the roles for their division. The system does not allow users making a self-request.

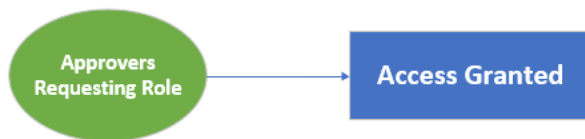
5.2.2 NSF Role Provisioning Workflow

NSF Account and Role Manager (ARM) supports multiple provisioning workflows depending on how the role is defined.

- Role can be requested and approved by the same user (implicit approval)
- Role can be requested by a user but approved by the role owner (defined within the role)

Scenario 1: Roles requested by approvers

In this scenario, the requestor of the role is also the approver (commonly used pattern):



Scenario 2: Role requested by users and approved by role owner



Scenario 3: Role requested by users requires review and approval

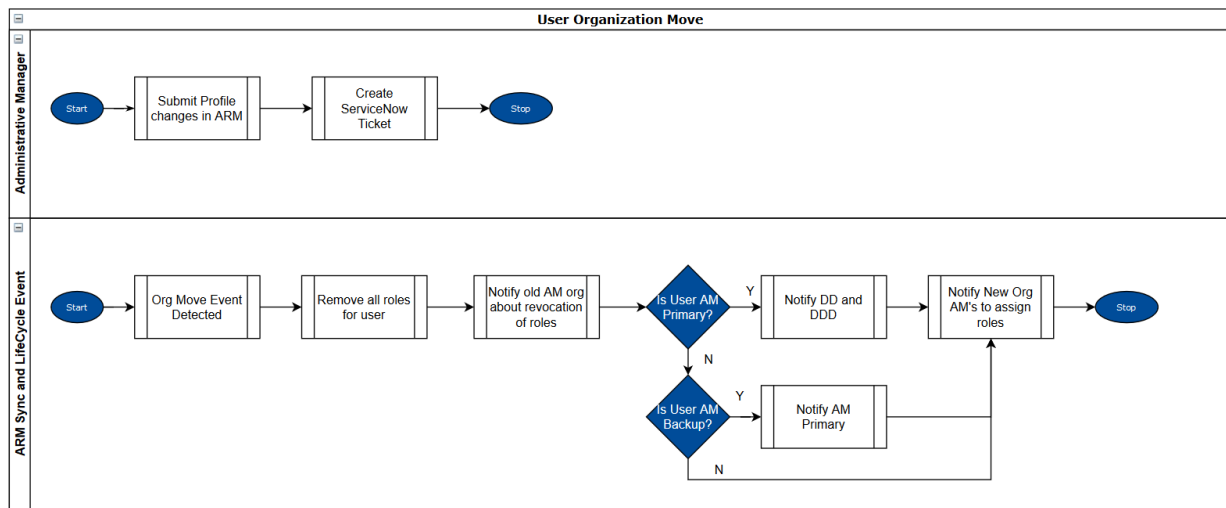




5.2.3 NSF Organization Move Workflow

Users are granted access to perform a privileged activity on an application for a given organization. This organization can be the user's home organization or any organization for which the user is authorized to perform the privileged action. When a user moves out of the organization, the NSF Account and Role Manager (ARM) immediately revokes the access granted to that organization or any functional organization. User should obtain the needed access for the newly joined organization by making a request to the Administrative Manager of the new division.

The following functional flow diagram depicts the organization change flow within NSF Account and Role Manager (ARM) system.



5.2.4 NSF Role Re-Certification

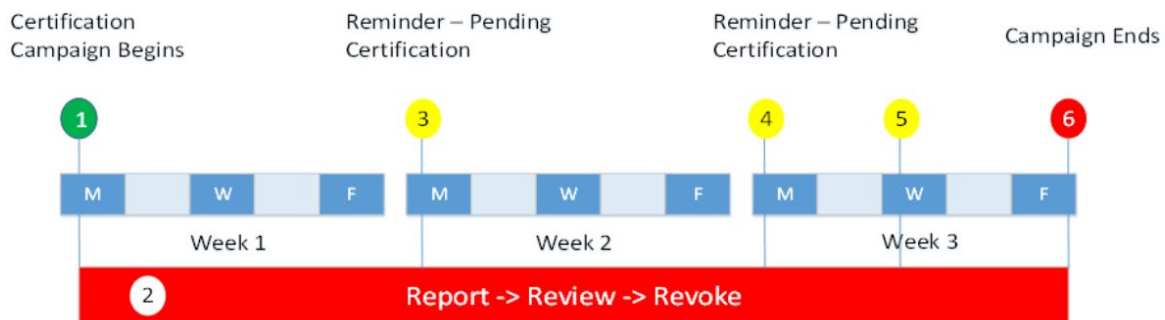
NSF's Administrative Managers (AMs) and Certifying Officials must conduct an annual review of their organizations user role data (access privileges) to ensure each individual in their organization possesses the correct level of access to NSF systems based on their current job roles and responsibilities. It is a three-week process wherein uncertified user's roles get revoked by end of the campaign.

The role re-certification campaign is automated in NSF ARM. The ARM system generates an email to notify Administrative Managers and/or Certifying Official that it is time to begin the annual Role Certification Process. The notification also provides the instructions on how to complete the access review for the individual roles assigned to them.

ANNUAL RECERTIFICATION OF ROLES



Campaign Process

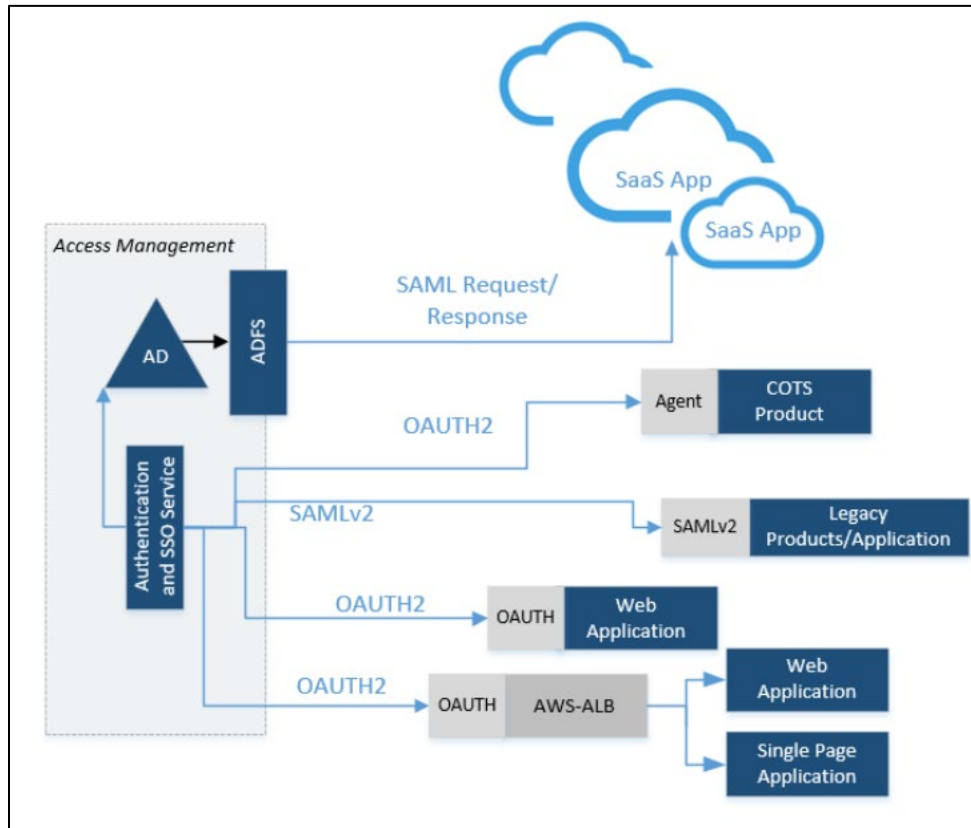


5.2.5 NSF Authentication Internal User

NSF supports different flavors of authentication solution to authenticate internal users. All applications hosted within the internal network, hosted in the cloud or Software as a Service (SAAS) application should authenticate the user using the issued NSF credential. Users log into NSF internal network using the PIV card, and when working remotely use Virtual Private Network (VPN) to access the internal network using PIV card. Internal users not in the network but who want to access the application hosted in cloud are required to authenticate using the Multi Factor Authentication using PIV or hard/soft token.

Active Directory Federation Service (ADFS) is used for performing federated login using the issued NSF credential to sign-in into the trusted SAAS application available in the cloud.

The following diagram depicts how access manager and ADFS integrates with applications of various architectures to authenticate users and allows them to sign-in to the application.



Access Manager integrates with a directory server and with the domain controller to support seamless authentication that prompts users for their user-id/password credential. Users must authenticate their machine using an NSF PIV Card (Smart Card).

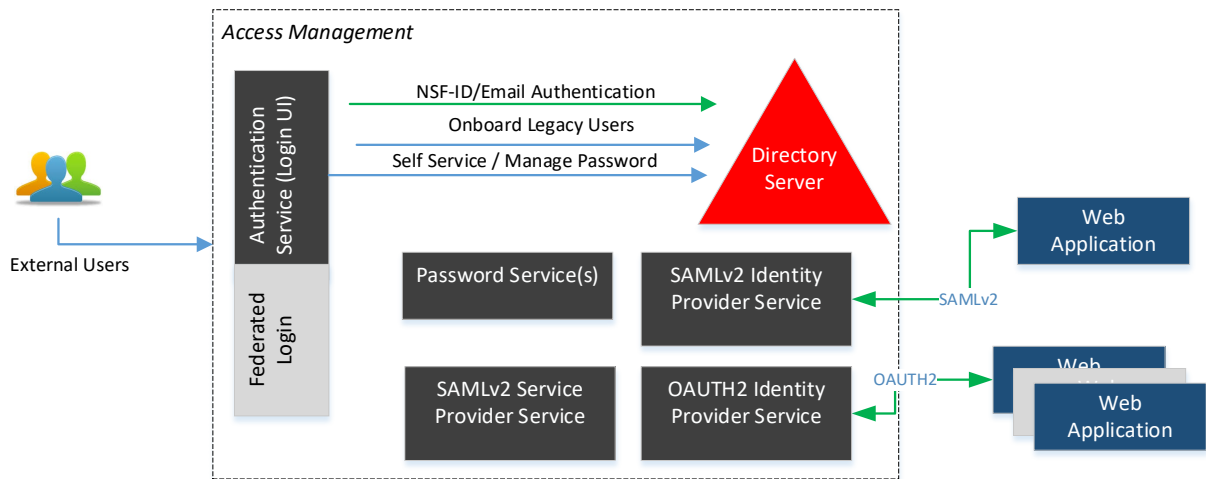
Applications hosted behind the Application Load Balancer (ALB), utilize the OAUTH2 protocol for Single Sign-On. Amazon Web Services (AWS) ALB configuration defines the application path requiring authentication before it can be accessed. When a user tries to access the resources, they get redirected to the access manager to complete the authentication. SaaS application and COTS Product supports authentication using SAMLv2. NSF uses both ADFS and the Access Manager as the IDP Provider to support SSO for SaaS and COTS Product.

Application containers like WebLogic integrate with the Policy Agent to enforce authentication before users can access any protected pages. The Policy Agent serves as the OAUTH2 client between the Access Manager and the application and ensures full transparency in implementing authentication for internal users.



5.2.6 NSF Authentication for External User

All external users access the Research.gov site using credentials issued during the self-registration process or use the federated system for sign-in. The following diagram depicts the high-level logical architecture of external user authentication and single sign on (SSO) integration with the various external services.



Each external application is configured to enforce user authentication using the centralized access management. The applications architectures are configured to support either SAMLv2-based authentication or OAuth2-based authentication using the centralized access management system.

Any user accessing an application's protected link gets redirected to the access manager for authentication. Once authenticated, the system redirects the user to the application endpoint with either SAMLv2 assertion or the OAuth2 authorization grant code. The application consumes the authenticated user identity (attributes) by means of the SAMLv2 assertion payload or using the OAuth2 UserInfo endpoint.

Access Management for external users makes use of several core functionalities to support authentication such as SAMLv2 identity provider and OAuth2 Identity Provider for integrated applications. Access Management is configured to be a SAMLv2 service provider to consume the authentication assertion from the Federation participants.

The Research.gov authentication service has been enhanced to include Login.gov Identity Provider. Login.gov provider enforces all external users to use Multi Factor Authentication (MFA).

Authentication Service: The Authentication Service provides the user interface (UI) to external users so users can choose how to authenticate to the external site (research.gov). The UI provides the user an option to authenticate using the NSF ID/Email or Federation Identity Providers (InCommon and Login.gov). Authentication services enforce password policies such as password expiration interval, account lockout and auto unlock, and notifies users when they need to change their password due to expiration.



Password Policies: The password policy for external users is “Password entered should contain at least one numeric, one alphabetic character and have a length between 6 and 20 characters.” The password policy is configured in the directory and immediately applies to users as soon as they create or change password in the system.

Password Policy	Configured Value
Enforce password history	N/A
Maximum password age	N/A
Minimum password age	1 day
Minimum password length	6 characters
Maximum password length	20 characters
Password must meet complexity requirements	Enabled
Minimum Numeric Numbers	1
Minimum Alphabets	1

Account Lockout: The Account Lockout feature enhances the security of the user’s password and denies system access to individuals who use continuous attempts to guess the password. Account Lockout is part of the external user password policy. The following configuration is added to the password policy to enable account lockout.

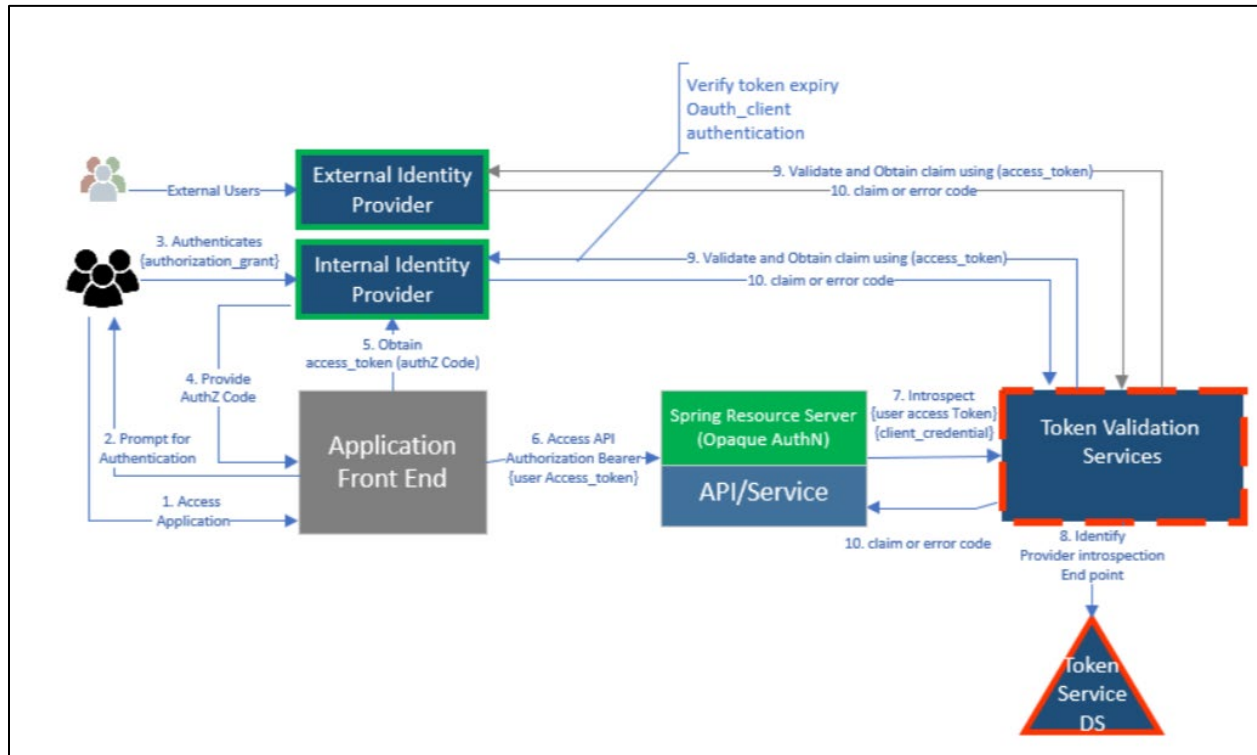
Password Policy	Configured Value
Maximum Failure (Locks user account when x amount of invalid attempt is made)	5
Automatically unlocks the account after 15 minutes.	900 Secs (15 minutes)

Security: The Access Management application is configured to use Secured Cookies, and all authentications use the HTTPS protocol.

Service Authentication

API Services are protected using the OAUTH Protocol. This means that any consumer service or Web Application that requires access to the API, should provide the OAUTH **access token**. API Services **SHOULD** validate the access token against the OAUTH Provider designated end point called **introspect end point** to check the validity. As per OAUTH Specification, introspect end point either provides active=false for invalid/expired token or it generates JSON response containing the token information back to the services. These steps are executed by the API Services underlying security framework.

Each API is required to be configured with the introspect end point for token validation and each API is provided with a unique client-id and secret which **SHOULD** be used to authenticate itself to the OAUTH Identity Provider. Following picture depicts the various components required for API authentication. Token validation service is an optional service available for API's to validate the token against internal and external OAUTH provider. This component is used by common API's which provides services to both internal and external users.





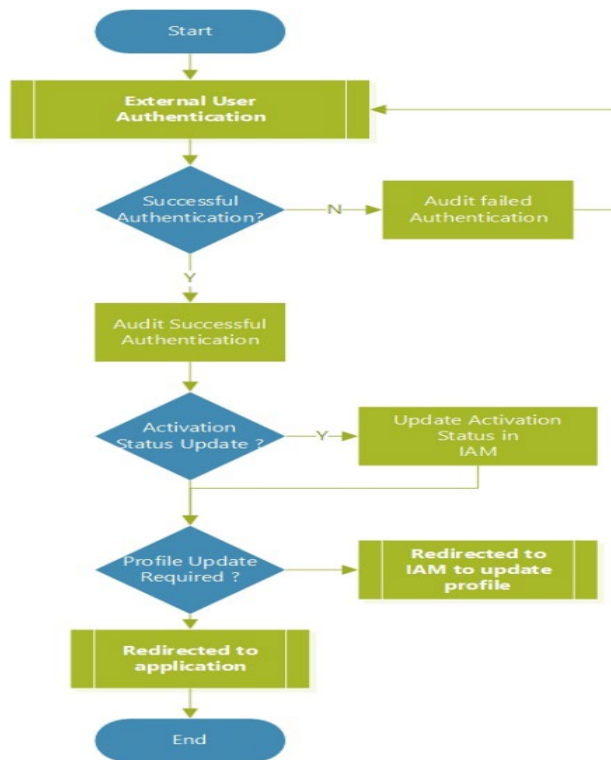
5.2.6.1 Post Authentication Process

The post authentication process executes three major activities to decide the user's landing destination:

- Captures Audit Log in database for success/failure authentication: this function creates an audit log to records who authenticated into the application and records the success or failure of the authentication.
- Sends the User Activation Status to the IAM platform: This notifies the application over API that a newly registered user has successfully authenticated and should be marked as activated within the system.

Checks and Enforces User On-boarding:

- Legacy User (users who are not currently in the Account Management system) are enforced to onboard.





5.2.6.2 Session Management

Access Management enforces session management for each user. The user must reauthenticate when the session timeout is reached. The system establishes control over the user session by configuring various key features such as session timeout, idle timeout, and OAUTH Token expiry interval.

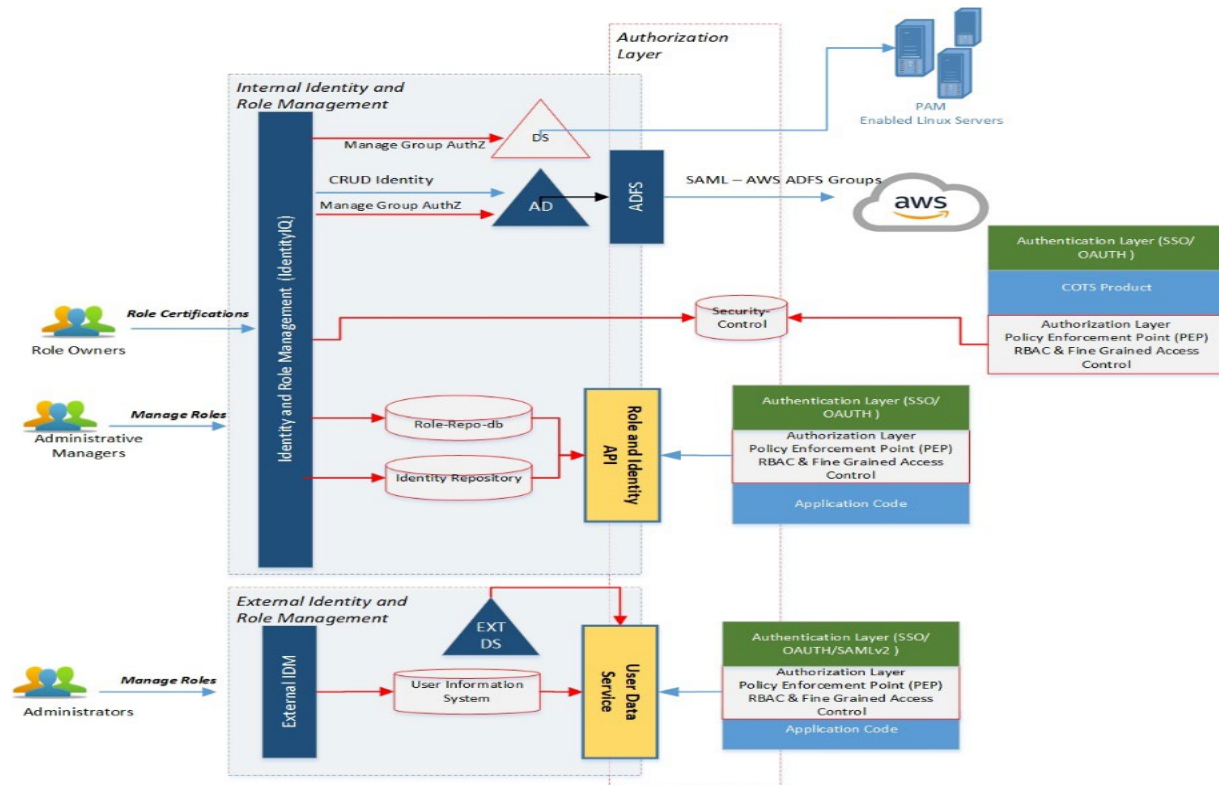
The following table describes the system behavior when the user's session expires or when the OAUTH token expires when using the OAUTH2 Protocol.

Event	Action	Behavior
When Idle Timeout Occurs	When user clicks on any application link	User is redirected to the Login Page.
When Session Timeout Occurs	When user clicks on any application link	User is redirected to the Login Page.
When OAUTH Token Expires	When user accesses OAUTH protected web route	User is redirected to Access Management to get the new access token. If session happens to be terminated, the user will be prompted for authentication. Note: refresh token is not applicable for OAUTH implicit grant flow.
When OAUTH Token Expires	When user accesses OAUTH protected API	System returns forbidden message. Caller should provide the valid access token.
Global Logout	When user clicks on Logout link in any Application	User's session is invalidated from Access Management Server, any access to application will redirect the user to the login page.



5.2.7 Authorization

NSF maintains a dedicated and separate system to manage user authorization for internal and external users. The following section highlights how authorization is defined and enforced for applications and infrastructure systems.



5.2.7.1 Authorization for internal users

The application architecture and design dictates how authorization is evaluated for a given authenticated user. The NSF IAM platform is a centralized role and life-cycle management system for internal users. The IAM platform defines business and IT roles for applications and infrastructure systems. Each Role contains one or more entitlements that grants users rights to access or perform specific functionality within the application.

5.2.7.2 Role Repository and Identity API

Any role assigned to the user using the IDM platform gets written to the persistent layer in a database, the Role Repository DB. The role repository DB serves as the authoritative source where any given application can check for user authorization using an API. The role repository also serves as a data endpoint for auditing and reporting.

5.2.7.3 Web based Application

All web-based applications use centralized access management to enforce authentication. Upon successful authentication, the web application receives the authenticated user's identity and attributes. The



application uses the authenticated user-id to retrieve the user's roles and permissions from the role repository using the API. Retrieved roles and permissions get mapped to the security framework as per the application design.

The application displays only authorized content, navigation menu items and control blocks to the user based on the user's permissions. When a user tries to access content or functions requiring authorization, the system evaluates whether the user within the valid session possesses the specific ROLE or PERMISSION. The required authorization check evaluates if the user will be granted access to the requested resources, otherwise an access denied message is displayed.

5.2.7.4 AUTHORIZATION Control on COTS Products

Commercial off-the shelf (COTS) products come with a built-in Access Control module. Commercial Off the Shelf (COTS) products require that the user profile is provisioned into the specific database table with the security role. COTS products get integrated with the IAM platform. Roles are defined in IAM and mapped to each COTS System's Security Role. When a role containing a COTS product entitlement is assigned, the IAM system provisions the user profile and entitlement into the security control (security table) as defined by the product.

The COTS product evaluates the user authorization whenever the user signs into a system and adjusts the access to the capabilities.

5.2.7.5 Access Control for AWS

The AWS Console and Resources utilize AWS ICAM Role to control access. The AWS ICAM Role is managed through the centralized IAM platform. Each AWS ICAM Role is mapped to an IT Role within the IAM system and assigned to the Active Directory AWS Group as an entitlement. To access the AWS Resource or Console, the user gets the Role assignment by going through the role request process. When a role request is approved, the user assigned with the AWS Role is provisioned to the corresponding Active Directory Group.

The authorization flow for AWS resources requires users to sign-in into AWS using the NSF ADFS services. ADFS generates the SAML Assertion to sign-in into the AWS and along with SAML Assertion it also embeds the AWS Role available to the user. The AWS SAML endpoint intercepts the roles received in the SAML response and allows the user to execute operations as defined in the AWS role.

5.2.7.6 Authorization for Server Access

Servers get configured to use the Privileged Account Management (PAM) module to authenticate a user against the configured user directory. Authorization control to servers uses the Directory Server Group. The server LDAP/PAM module evaluates user authorization to ensure only authorized users can login into the server.

At the IAM tier, each Server entitlement is defined using the Directory Server Group and mapped to the IT Role. Users can only obtain server access by requesting the corresponding IT Role through the proper approval process.

5.2.7.7 Authorization for Database Access

Oracle Databases are integrated with the Directory Server for user authentication and authorization. The directory server is centrally managed using the ARM platform for the user's account life cycle synchronization. The LDAP Group is defined per database per environment to enforce authorization. Users request access through the defined approval process and are granted access to the given database through group membership.



Sybase databases are configured to use both Sybase groups and roles to define fine grained access control. The ARM platform defines Sybase database roles for each environment along with the respective approval process. A given Sybase Role definition includes membership to various Sybase database groups and upon provisioning, each user is given the fine-grained access to the given Sybase database within the specified environment.

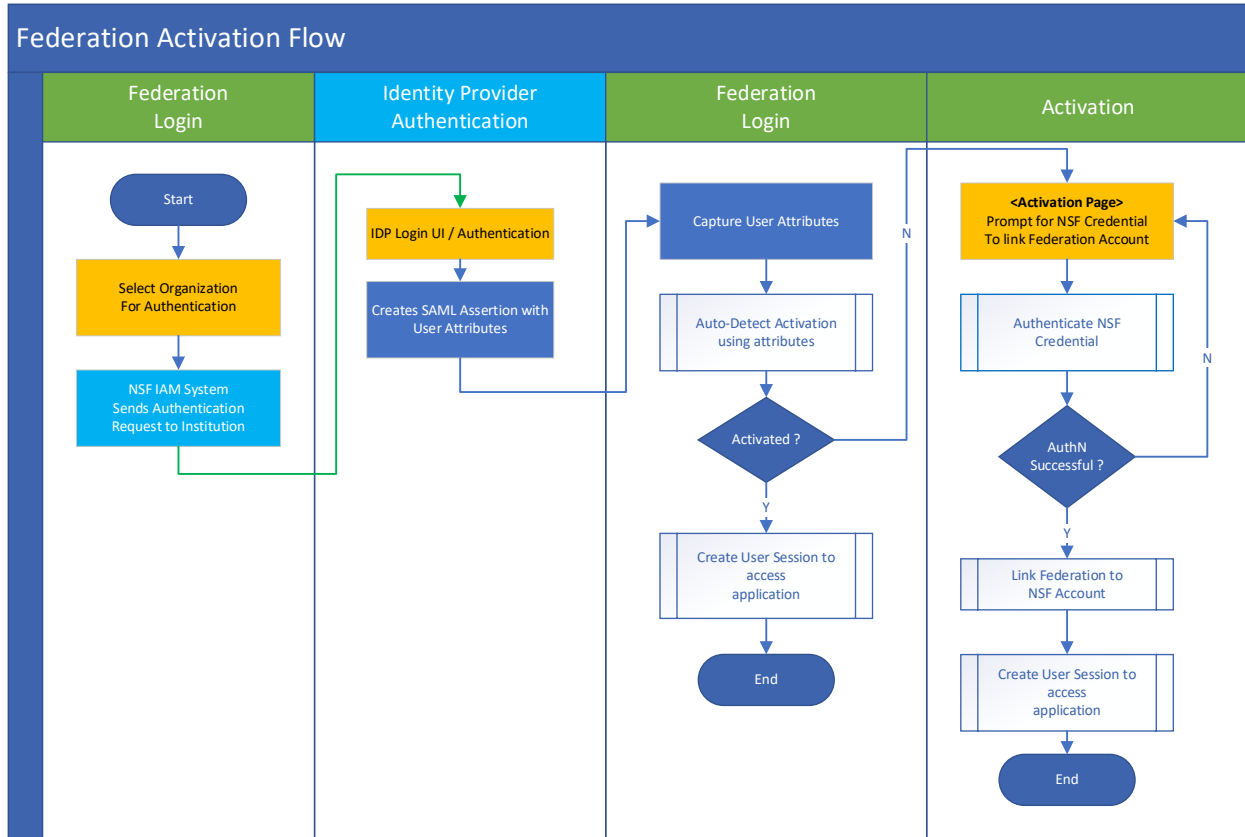
PostgreSQL databases are configured to use groups to define fine grained access control. The ARM platform defines Postgres roles for each environment along with the respective approval process. A given Postgres Role definition includes membership to specific Postgres instance upon provisioning, each user is given the fine-grained access to the given instance within the specified environment.

5.3 Federation

Research.gov is a web-based system that provides grants management functionalities for the external research community. The IAM platform provides federation service to members of the external community in order to access the Research.gov application.

5.3.1 Federation Integration

The NSF Identity and Access Management platform trusts the Universities and Institutions as Identity Providers when they are members of the InCommon Federation network. All trusted Identity Providers with whom NSF integrates are listed on the Research.gov login screen. An external user can choose their Institution from the login screen and use their Institution issued credential to sign-in. The following diagram depicts the flow of Federation Login and account Linking/Activation.



- **Login Request:** The External User Login User Interface allows the user to sign-in using NSF ID/Email Address or using the Institution issued credential. The user selects their University using a drop-down list to initiate a Service Provider (SP) Initiated Secured Assertion Markup Language (SAML) Authentication Request.
- **Login Response:** The Identity Provider accepts the SAML request due to the mutual trust established through the InCommon Federation participation. Users get redirected to the Institution login Screen. Upon successful authentication, the SAML response with required attributes gets sent to the NSF Access Management platform.
- **Account Mapping:** All Federation users logging into the NSF External Grants system get mapped to an account in the directory Server with their unique NSF ID.
 1. The SAML attributes are checked against the Directory Server to the unique NSF ID mapping. If the mapping is found the user will be identified with the NSF ID in the application session.
 2. When the user mapping is not identified then the user will be redirected to an account linking/activation page. This page allows user to link/activate their federation account by providing their NSF issued credentials. Once successfully linked/activated the user will be redirected to the application with the NSF ID in the session.



5.3.2 Attribute Exchange by Identity Providers

The Identity Provider (Universities and Institution) releases basic attributes about the user to the NSF's Access Management system. The SAML Assertion receives those attributes that help access management to identify the user.

5.3.1 Authorizing Federation User for NSF business applications

All Federation users must activate/link their federation account to an NSF issued credential. External users can obtain an NSF account through self-registration and go through the role request process to get authorization to perform operations permitted by the underlying role. If the federation account is not authenticated/linked the users will be able to consume information that does not require any authorization.

5.3.2 Research.gov Federation Policy Alignment

NSF established the trust relationship with InCommon Federation by participating both as an Identity Provider and as a Service Provider. NSF does onboard the InCommon trusted Identity Providers (IDP) into the system when an implicit request is made to the NSF help desk.

5.4 Digital Identity Risk Management

Digital Identity Risk Management is incorporated at all levels in ICAM. This is especially true for internal authenticated services, but it also extends to external authenticated services. NSF provides public-facing digital services that require ICAM application on Research.gov. The security applied to Research.gov for the public-facing services is covered in Section 5.3: Federation. NSF does not provide any digital services on NSF.gov requiring any ICAM provisions.

6 GOVERNANCE

As a small, single-mission agency, NSF utilizes existing governance structures for ICAM governance. Governance falls under the purview the Chief Information Officer and OIRM/DIS. Changes to NSF ICAM policies, systems improvement, and enhancement obtain approval from ERB (Enterprise Review Board) and the DIS Change Control Board (CCB).

6.1 Auditing & Reporting

NSF has an Account Monitoring function within the IT Security Policy and Planning team. The account monitoring process includes validation of account creation, monitoring of separations comparing records from Federal Personnel /Payroll System (FPPS) to ensure prompt account removal actions, and escalation for outstanding actions.

The Account Monitoring function is audited annually as part of the FISMA and Financial Statement Audit. There is also an audit log review process within the same team that verifies privileged account creation and access permissions for essential servers and databases. Again, this is audited annually.

6.2 Redress

The Account Monitoring team produces routine reports on onboarding and separation. As well, escalation emails are produced when discrepancies between policy requirements and activities are detected.



6.3 Recovery

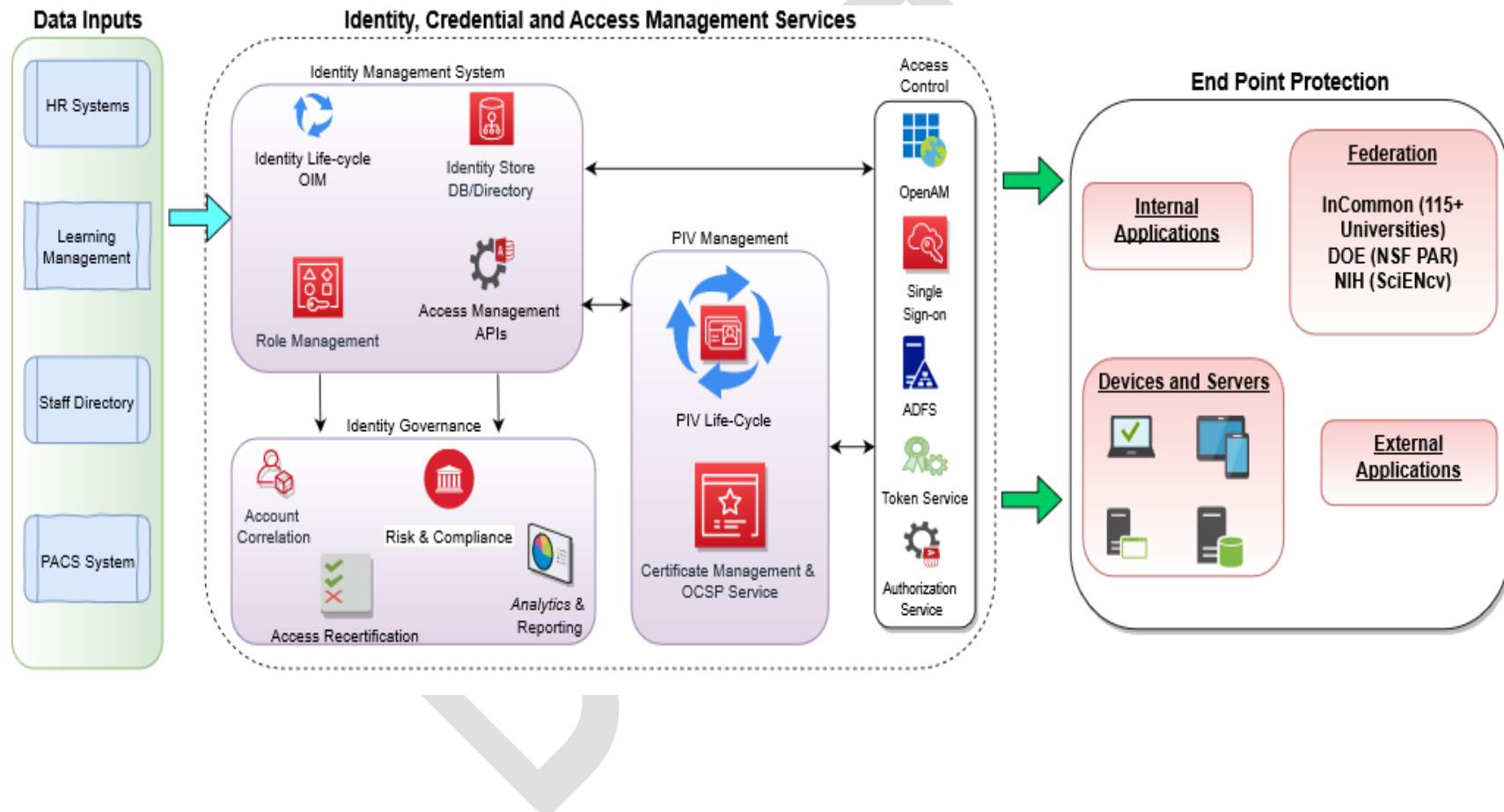
The NSF Computer Security Incident Response and Recovery Procedure outlines the steps for computer security/privacy incident response and recovery at NSF, and would apply to any issue involving ICAM and related capabilities. This Procedure covers all phases of the incident response lifecycle:

- Preparation
- Detection/Analysis
- Containment, Eradication and Recovery
- Post Incident Activities (Lessons Learned)

The procedure also documents the tools and resources for incident response and handling. Roles and responsibilities and a list of teams involved in responding to a security and/or privacy incident are also included.



7 TECHNOLOGY SOLUTION ROADMAP





APPENDIX 1: FEDERAL POLICIES

The following table lists the most pertinent federal policies relating to Identity, Credential, and Access Management (ICAM) and referenced in NSF ICAM development and deployment.

Title	Description
M-05-24 : Implementation of Homeland Security Presidential Directive 12 (HSPD-12) Policy for a Common Identification Standard for Federal Employees and Contractors	This memorandum provides implementing instructions for HSPD-12 and FIPS 201.
HSPD-12 : Homeland Security Presidential 12: Policy for a Common Identification Standard for Federal Employees and Contractors	HSPD-12 calls for a mandatory, government-wide standard for secure and reliable forms of identification (ID) issued by the Federal Government to its employees and employees of federal contractors for access to federally-controlled facilities and networks.
The Privacy Act of 1974	This Act protects certain Federal Government records pertaining to individuals. In particular, the Act covers systems of records an agency maintains and retrieves by an individual's name or other personal identifier (e.g., Social Security Number [SSN]).
Final Credentialing Standards	Formally titled <i>Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12</i> , this memorandum provides final government-wide credentialing standards to be used by all federal departments and agencies in determining whether to issue or revoke Personal Identity Verification (PIV) cards to their employees and contractor personnel, including non-United States citizens.
Executive Order 13681 : Improving the Security of Consumer Financial Transactions	This executive order requires agencies to strengthen the security of consumer data and encourage the adoption of enhanced safeguards nationwide in a manner that protects privacy and confidentiality while maintaining an efficient and innovative financial system.
M-16-04 : Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government	The CSIP directs a series of actions to improve capabilities for identifying and detecting vulnerabilities and threats, enhance protections of government assets and information, and further develop robust response and recovery capabilities to ensure readiness and resilience when incidents inevitably occur.
M-19-17 : Enabling Mission Delivery through Improved Identity, Credential, and Access Management	This memorandum sets forth the Federal Government's Identity, Credential, and Access Management (ICAM) policy.



APPENDIX 2: STANDARDS, GUIDANCE, AND REFERENCES

The following tables lists the standards, guidance, and references recommended by the federal government, and applied in part or in whole during the NSF ICAM development and deployment.

Title	Description
SP 800-53-4 : Security and Privacy Controls for Federal Information Systems and Organizations	This document provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations, assets, individuals, other organizations, and the Nation from a diverse set of threats.
SP 800-63-3 : Digital Identity Guidelines	These technical guidelines supersede NIST SP 800-63-2. Agencies use these guidelines as part of the risk assessment and implementation of their digital service(s). These guidelines provide mitigations for an authentication error's negative impacts by separating the individual elements of identity assurance into discrete, component parts. For non-federated systems, agencies will select two components, referred to as Identity Assurance Level (IAL) and Authenticator Assurance Level (AAL). For federated systems, agencies will select a third component, Federation Assurance Level (FAL).
SP 800-73-4 : Interfaces for Personal Identity Verification	This document specifies the PIV data model, command interface, client application programming interface (API), and references to transitional interface specifications.
SP 800-76-2 : Biometric Data Specification for Personal Identity Verification	This document contains technical specifications for biometric data mandated in [FIPS]. These specifications reflect the design goals of interoperability and performance of the PIV card. This specification addresses image acquisition to support the background check, fingerprint template creation, retention, and authentication. The biometric data specification in this document is the mandatory format for biometric data carried in the PIV Data Model (Appendix A of SP 800-73-1). Biometric data used only outside the PIV Data Model is not within the scope of this standard.
SP 800-79-2 : Guidelines for the Accreditation of Personal Identity Verification Card Issuers	This document provides guidelines for accrediting the reliability of issuers of PIV cards that are established to collect, store, and disseminate personal identity credentials and issue smart cards, based on the standards published in response to HSPD-12.



Title	Description
SP 800-87 : Codes for Identification of Federal and Federally-Assisted Organizations	This document provides the organizational codes for federal agencies to establish the Federal Agency Smart Credential Number (FASC-N) that is required to be included in the FIPS 201 Card Holder Unique Identifier. SP 800-87 is a companion document to FIPS 201.
SP 800-122 : Guide for Protecting the Confidentiality of Personally Identifiable Information (PII)	The document assists federal agencies in protecting the confidentiality of a specific category of data commonly known as Personally Identifiable Information (PII). This document provides practical, context-based guidance for identifying PII and determining what level of protection is appropriate for each instance of PII. The document also suggests safeguards that may offer appropriate levels of protection for PII and provides recommendations for developing response plans for breaches involving PII.
SP 800-157 : Guidelines for Derived PIV Credentials	This document provides technical guidelines for the implementation of standards-based, secure, reliable, interoperable public key infrastructure (PKI) based identity credentials that are issued by federal departments and agencies to individuals who possess and prove control over a valid PIV Card.
SP 800-162 : Guide to Attribute Based Access Control (ABAC) Definition and Considerations	This document provides federal agencies with a definition of attribute-based access control (ABAC). ABAC is a logical access control methodology where authorization to perform a set of operations is determined by evaluating attributes associated with the subject, object, requested operations, and, in some cases, environment conditions against policy, rules, or relationships that describe the allowable operations for a given set of attributes.
FIPS 201-2 : Personal Identity Verification (PIV) of Federal Employees and Contractors	This document specifies the architecture and technical requirements for a common identification standard for federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to federally controlled government facilities and electronic access to government information systems.



Title	Description
Technical Implementation Guidance Smart Card Enabled Physical Access Control Systems	<p>This guidance defines specifications and standards required to enable agencies to procure and implement hardware and software for PACS, such that these systems will: operate with the Federal Agency Smart Credential (FASC), such as NIST-standards-based PIV cards; facilitate cross-agency, federal enterprise interoperability; and allow existing legacy PACS to operate with FASC-compatible card readers until the time comes for its upgrade.</p>
References	
Electronic Signatures in Global and National (ESIGN) Commerce Act of 2000	<p>This Act was intended to facilitate the use of electronic records and signatures in interstate and foreign commerce by ensuring the validity and legal effect of contracts entered into electronically.</p>
E-Government Act of 2002	<p>This Act is intended to enhance the management and promotion of electronic Federal Government services and processes by establishing a Federal CIO within the Office of Management and Budget (OMB) and by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to government information and services, and for other purposes.</p>
Government Paperwork Elimination Act of 1998 (GPEA)	<p>GPEA requires federal agencies, by October 21, 2003, to allow individuals or entities that deal with the agencies the option to submit information or transact with the agency electronically, when practicable, and to maintain records electronically, when practicable. This Act specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form. This Act also encourages Federal Government use of a range of electronic signature alternatives.</p>
E.O.13467 : Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information	<p>This executive order was established to ensure an efficient, practical, reciprocal, and aligned system for investigating and determining suitability for Federal Government employment, contractor employee fitness, and eligibility for access to classified information.</p>



Title	Description
NIEM	The National Information Exchange Model (NIEM) is a partnership of the Department of Justice (DOJ) and the Department of Homeland Security (DHS). It is designed to develop, disseminate and support enterprise-wide information exchange standards and processes that can enable jurisdictions to effectively share critical information in emergency situations, as well as support the day-to-day operations of agencies throughout the Nation.