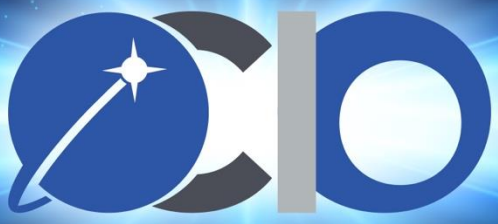
National Aeronautics and Space Administration

Identity and Access Management (IdMAX) Handbook

Office of the Chief Information Officer



September 2022

www.nasa.gov

Revision History

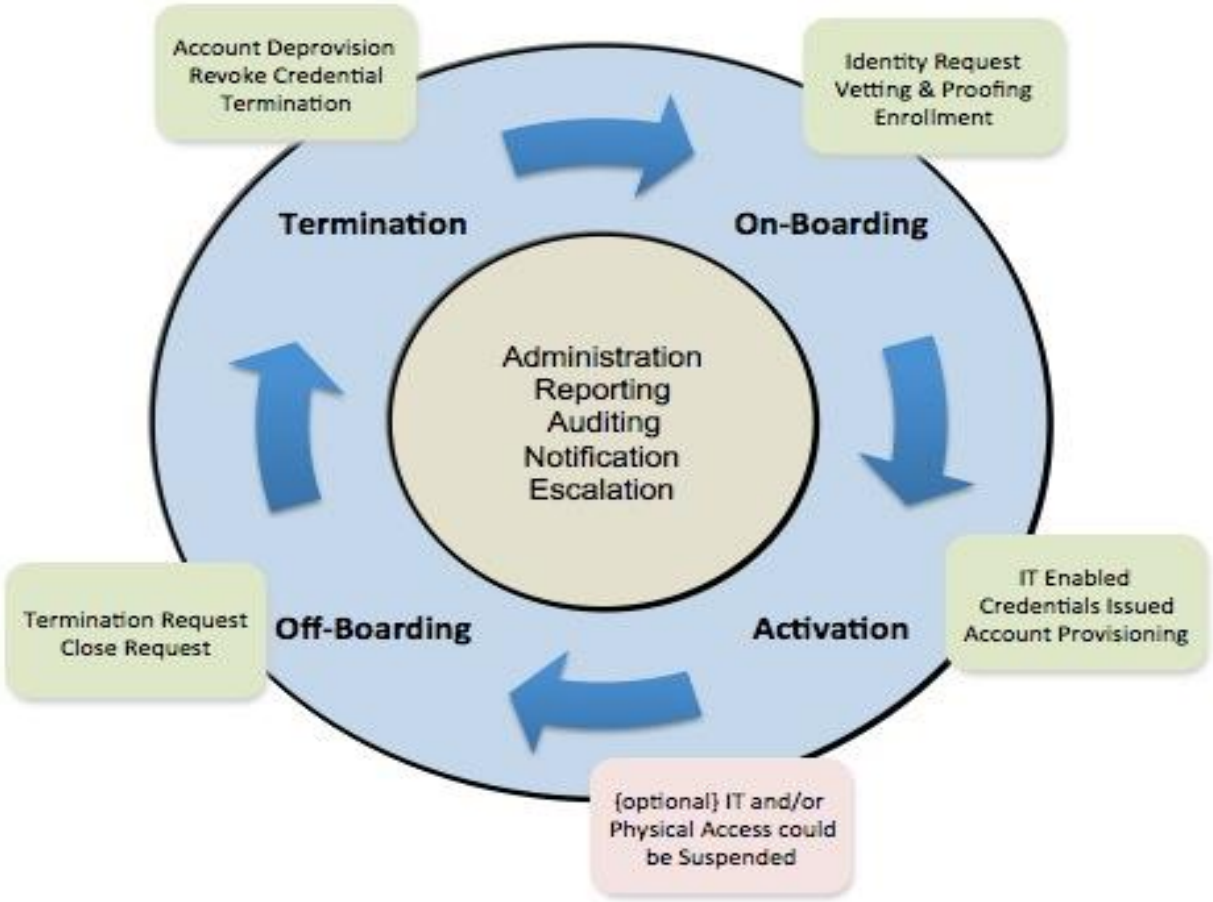
Revision #	Description	Date
18	Adding Document Upload to Agreements & ACP sections	01/09/2017
19	Updated X500, Title of handbook change, ACP & documents, LOR	3/09/2017
20	IVC Workbench, FN Escort Waiver, Record CI Review tool,	5/24/2017
21	Adding Agency Smart Badge Lifecycle, SWB / EOWB / IVC WB, Audit tool,	8/24/2017
22	Including PerSec Security Workbench / Queue Updates	12/14/2017
23	PecSec Roles / Queue Updates	5/17/2018
24	Adding Center Information Security Role / Workbench Lite	6/28/2018
25	Foreign National Visit Workbench	7/9/2018
26	DD254 Updates / Deferred Investigations	9/20/2018
27	Local Print, Foreign Travel Reporting, Resynch Lenel Access, Agreement Rollover	11/14/2018
28	Investigations deferred, Enrollment updates	01/31/2019
29	Remote Proofing, LOC 25 & 45	04/04/2019
30	New Badge Types, Copy PD feature,	10/10/2019
31	Adding Non-NASA Smartcard to the Credential section	7/13/2020
32	Remove FN Check and replaced with Visual Compliance, decommissioned Override IT Security Training Tool	9/17/2020
33	Add Supported Browser Information	3/17/21
34	Adding Suspension Types	8/4/21
35	Adding Submitted BI/Level 2-5 to Investigation table	10/14/21
36	Updated cover page to OCIO, added SAP and EVAMS	12/2/2021
37	Added Cardstock workbench to the Tools section	01/27/2022
38	Updating FAR Clause 1852	09/17/2022

Table of Contents

1. Introduction

PURPOSE

The purpose of this document is to assist the ICAM community in the management of the identity and credential lifecycle using the Identity Management and Access Management eXchange (IdMAX) system. IdMAX tracks a unique person with a trusted relationship with NASA who needs access to NASA assets and is granted access using the centralized system designed for creating, sponsoring, vetting identities, and issuing credentials. It also provides a repository of user account information for NASA employees, contractors, and remote users. As well as allows integration with applications to receive and provide identity and credential information.



ROLES

IdMAX has several roles that provides privileges to specific menu options that allows you to perform your job accordingly. Some restrictions have been applied that limits some role holders to view sensitive information. A list of roles and their descriptions are below.

NOTE: *IdMAX Roles are provisioned via the AGCY0011 ICAM Infrastructure workflow in NAMS.*

Role	Role Description
Identity Requester	NASA civil servant or authorized contractor officiate that provides the initial data about the user and submits an identity request on behalf of the user
Affiliation Sponsor	NASA civil servant who vouches for an individual's need for identity lifecycle management services in order to be authorized access to NASA physical or IT assets.
Investigation Reviewer (IR)	Approves Local Badges and initiates a background investigation if necessary or verifies the current background investigations meet NASA's minimum requirements.
PIV Authorizer	Authorizes the issuance of a NASA PIV Smartcard or a Local Badge to a user who has met all proofing, enrollment and investigation requirements
Enrollment Official	Validates the identity and captures identity information and biometrics
International Visitor Coordinator (IVC)	Reviews the Foreign National request, perform a Foreign National Check to an existing completed background investigation that meets the Agency's reciprocity requirements, and ensure that Export Control requirements are approved before authorizing the Foreign National request
FN Approver - Center Export Control, Agency Export Control, Agency Desk Officer	**Center Export Control**-Validates the export control requirements for Center Premise Equipment (CPE), access to Center facilities, and Center-specific information technology (IT) systems **Agency Export Control**-Validates the export control requirements from an Agency perspective, as well as reviewing and validating the export control approval submitted by the Center **Agency Desk Officer-**Confirms whether the information requested is justifiable in terms of concrete benefits to NASA and for documenting technology transfer considerations, both direct and incidental that corresponds to the foreign national's requested access.
Counterintelligence Officer	Reviews on-boarding Foreign National identities to detect, identify, assess, counter, exploit and/or neutralize adversarial or threats to NASA
Access Control Plan Maintainer	NASA civil servant or authorized contractors who maintains Access Control Plans
Foreign National Escort	NASA civil servant or authorized contractors who maintains Foreign National Visiting Workflows in NAMS & authorized to escort Foreign Nationals.
Secure View Only	An IdMAX User that requires Access to PII information but cannot make changes to the Identity information

Support View Only	An IdMAX User that cannot view PII information or make changes to an Identity record.
Agreement Maintainer	NASA civil servant or authorized contractor who maintains agreement data.
ICAM Help Desk	Help desk personnel that can assist in resetting Launchpad password and assist with PIV-M Exceptions.
Suitability Agent	Supports Civil Servant Investigation records in IdMAX
Postmaster	Ensures that user's mail attributes are in compliance with NASA standards.
Invitational Traveler Coordinator	Collects information for a traveler and submitting the NAMS request for access to the NASA Travel system.
Basic User <no role>	A person who relies on computer systems to conduct duties and business activities. Ability to Invite a Foreign National to Create Their Identity
Special Events Coordinator	Creates events for their center within NVMS & is the NASA Host
Security Adjudicator	Supports & Initiates Investigations, Clearances, SCI and DOE
Special Security Representative	Supports SCI Initializations at the Centers, conduct briefing and debriefing
Center Information Security	Supports Security personnel by initiating suspensions, changing asset availability, or by requesting a credential

ASSUMPTIONS

To use IdMAX the following access privileges are required:

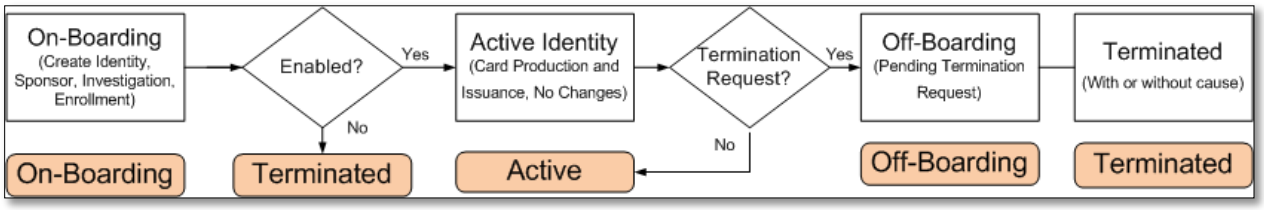
1. Having one of the following authentication credentials:
    a. NASA Smartcard
    b. Agency User ID with RSA Token
2. Access to the NASA network
    a. If you are working remote, access via the CISCO AnyConnect VPN client is sufficient
3. Have a role in IdMAX/NAMS "Identity Requester, Authorizer, Enrollment Official, Investigation Reviewer, IVC, FN Approver, Agency Desk Officer, Agency Export control"
    a. The role is requested via NAMS under the NAMS resource "AGCY0011 Agency ICAM Infrastructure".
4. Log in access to IdMAX/NAMS
    a. The following URL is the access point for IdMAX/NAMS. https://idmax.nasa.gov or https://nams.nasa.gov
    b. From the Launchpad screen, select either authentication options: "Smartcard" or "RSA Token"
    c. If accessing NAMS and have a role you will be required to log in using "Smartcard Only"

2. Identity Management Lifecycle

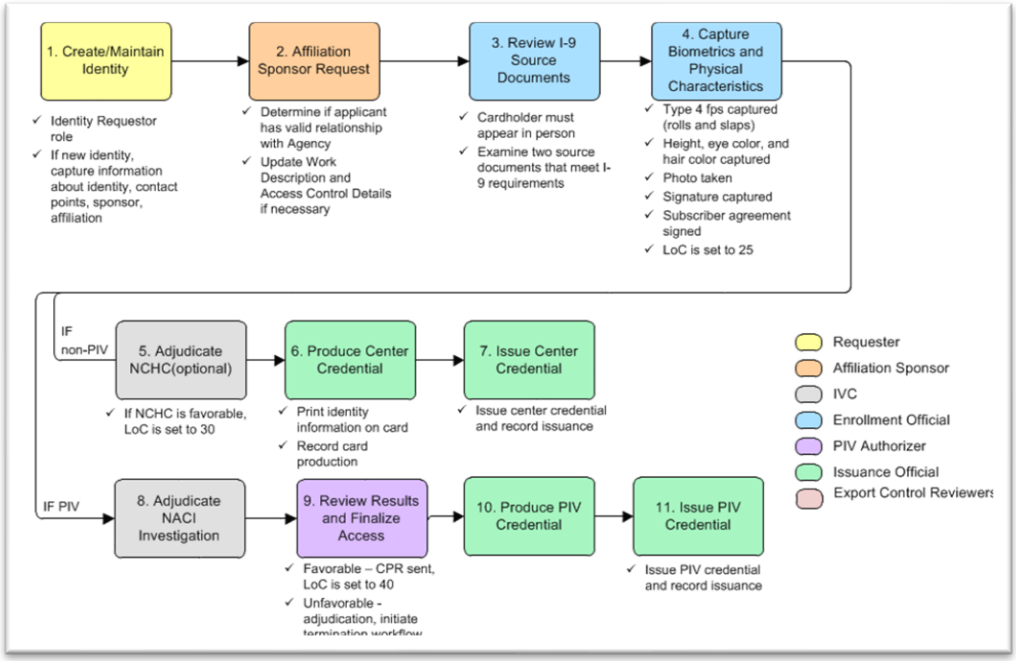
Identity Management refers to the creation, maintenance, and lifecycle management of digital records of people who have a relationship with NASA. It is the process for tracking a unique person with a trusted relationship with NASA who needs access to NASA assets and is granted access via documenting identity assurance related information.

An identity is a set of attribute values by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity-*Federal Identity, Credential, and Access Management Roadmap and implementation Guidance, Version 2.0*

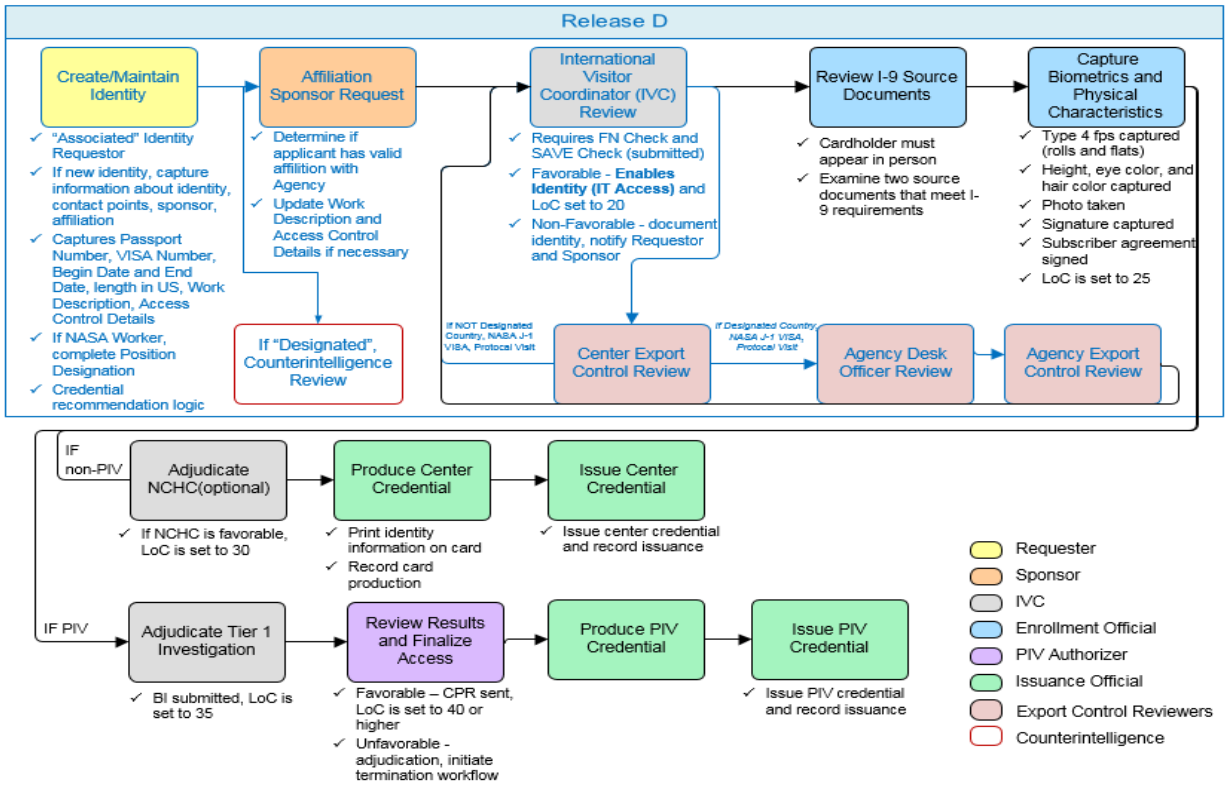
IDENTITY LIFECYCLE



IDENTITY ONBOARDING WORKFLOW



Foreign National Identity Onboarding Workflow



Requester Workbench

A single tool that allows Identity Requesters the ability to create, invite, modify and terminate identities where they are listed as the associated Identity Requester.

Access the Requester Workbench- Role / Associated / Non-Associated

Role

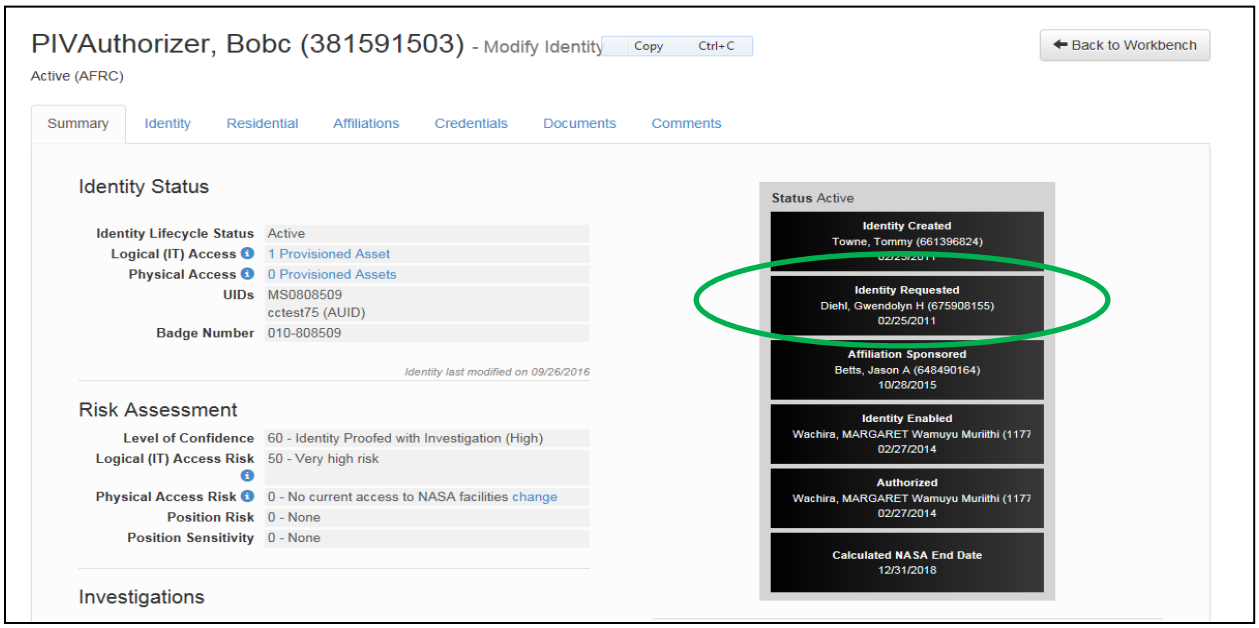
To access the Identity Workbench the user must have the following Agency ICAM Infrastructure role, Identity Requester. You must complete the required SATERN course prior to requesting for a role in NAMS. When your NAMS request has been approved, a link on the IdMAX console page will display the Requester Workbench.

A description of the role and assigned responsibilities are outline in the following table:

Role	Role Description
Identity Requester	• NASA civil servant or authorized contractor officiate that provides the initial data about the user and submits an identity request on behalf of the user.

Specified Identity Requester

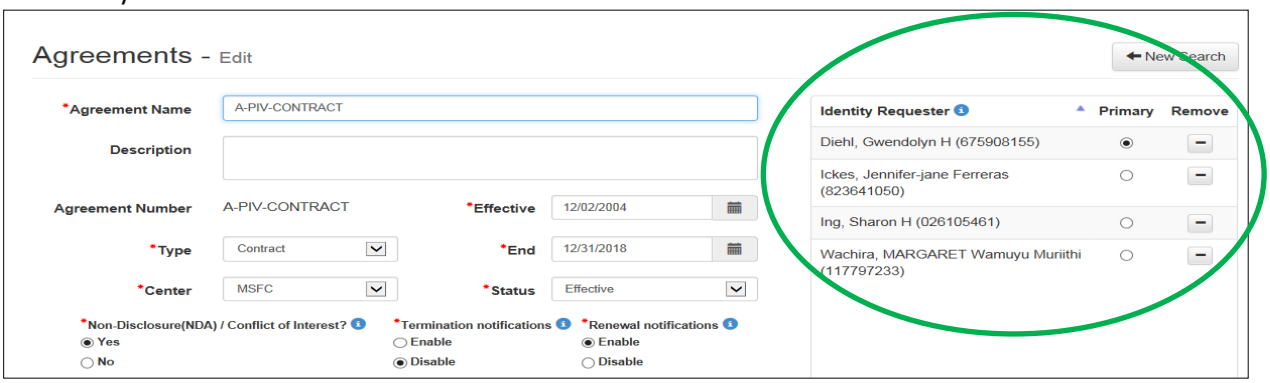
The Specified Identity Requester is the last Identity Requester to Modify / Save the user's record. They are reflected on the timeline and receives all email communications.



Note: If the Specified Identity Requester is Terminated, any Associated Identity Requester can make changes to the identity record and become the Specified Identity Requester.

Associated Identity Requester

To manage identity records, you must be listed as an Identity Requester on an associated Agreement(s). As an associated Identity Requester you will be able to view sensitive data for the identities you are associated to.

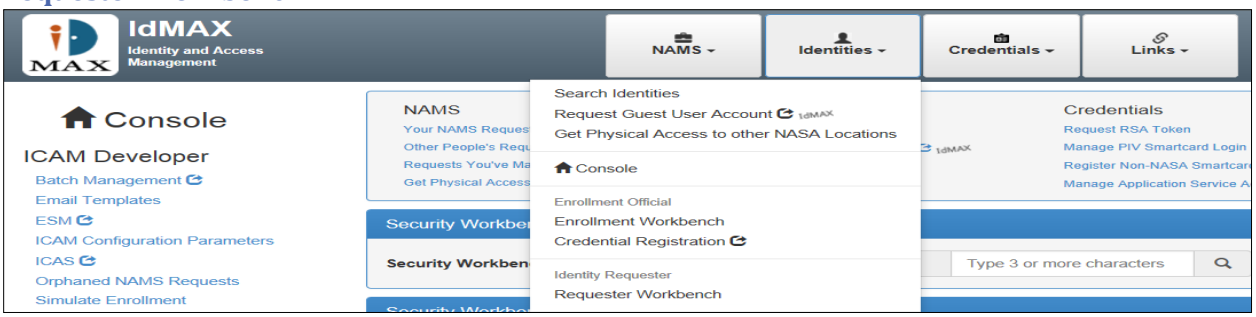


In this example everyone listed as the Identity Requester will be able to manage an identity that is associated to the A-PIV Contract Agreement.

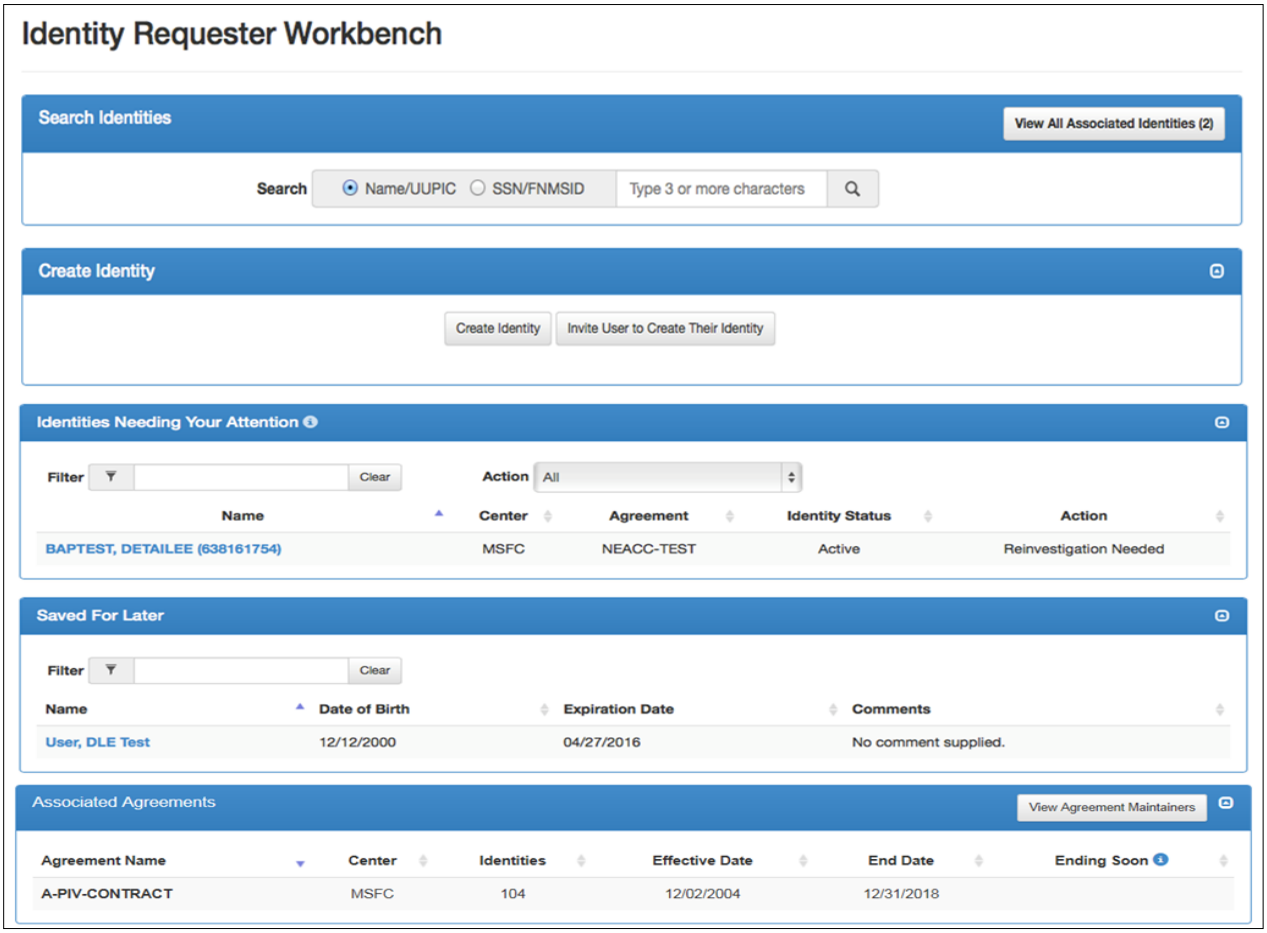
Non-Associated Identity Requester

A Non-Associated Identity Requester has no direct relationship with the identity or their Agreement allowing limited modifications / view to an identity record. You can search for an Identity that you are non-associated with displaying only non-sensitive information about that Identity. As a Non-Associated Identity Requester you have the ability to add a new Affiliation, transitioning the active identity to Associated for the agreements that you are associated with, or Start the Returning User process if the identity is terminated.

Requester Workbench



a. In this example, Requester Workbench is listed under the Identities tab.
b. Click the link to open the Requester Workbench



Search Identities

You have the ability to search for a specific Identity using the Individual Search feature. To begin a Search enter either the persons, First and Last Name, UUPIC, or click advanced to search by SSN, Center, AUID, First Name, Middle, Last Name, Org Code, Agreement, Company, Identity Status, Email, FNMS ID, Citizenship, or Birth Country. Results will display allowing you to select the record you would like to review/modify.

View All Associated Identities

Displays a list of identities that you are associated with. Allows you to make modifications to the user's identity record if needed.

Identities Needing Your Attention

Displays a listing of Identities requiring an Action on your behalf. It allows the Identity record to be opened in a Modify view to assist with Identity Actions: Affiliation Ending Soon, Position Designation Actions, Upcoming Smartcard Renewals, and Foreign National Review Action. The Name of the Identity, Center, Agreement, Identity Status, and Action are displayed.

Saved For Later

Displays a listing of Identity records that you have started but have not been submitted through the create process.

Associated Agreements / View Agreement Maintainers

Displays a listing of Agreements that you are designated as an Identity Requester. The Agreement Name, Center, Effective Date, End Date, and Ending Soon are displayed. Ending Soon will display a flag if the Agreement end date is within 60 days of expiration.

View Agreement Maintainers displays all Agreement Maintainer role holders for your center. This allows for center support on updates to Agreements and who can record the association.

CREATE IDENTITY / INVITE USER TO CREATE THEIR IDENTITY

Create a NASA Identity means to generate a record in the Identity Workflow that establishes a relationship between the applicant and NASA. Prior to creating a NASA Identity you will need to gather information from the applicant, including the applicant's Biographic / personal information, Residential information and Affiliation information, including end date.

If you do not have access to the personal information, use the Invite User Feature. This process allows you, as an Identity Requester to issue an invitation to applicants to allow them to enter their own personal information into the Identity workflow. For each NASA Identity you send an invitation to, you will need to complete two sub-forms: ***Identity*** that includes Legal Name, Position Detail; ***On-boarding Access*** that includes questions regarding physical access (if yes, you will be asked to select a New Credential & Badge Type), logical (IT access) desktop login (NCAD), email access (NOMAD) and Verification documents / Number / Issuing State**.** If a Trusted Identity, a user will complete input tabs that are based on the Trusted Partner Identity Plan (Residential, Identity Information, Naturalization, and Registered Credential).

It is best practice to review Matching Identities prior to Creating a New Identity. The system checks for uniqueness using SSN and Last Name/DOB. If a new Foreign National is created with multiple last name and date of birth matches, an email will be sent to the Center IVC for awareness.

For each NASA Identity you will need to complete sub-forms/Tabs:

Identity Tab

The *Identity* tab allows you to enter the applicant's Identity information. This includes the Legal Name, Birth Information, Citizenship, Proof of Identity, Position Detail and Notification information.

Note: *You should be very careful to enter the applicant's name exactly as it appears on their I-9 documents, otherwise, they will not be allowed to enroll.*
Do not add a suffix, such as Jr., to the applicant's name unless it appears that way on the I-9 documents. It would be helpful to have the applicant's I-9 documents in front of you while you create the NASA identity
If the two I-9 documents do not have matching names, the applicant will not be allowed to enroll, as the enrollment officials are instructed to verify that both I-9 documents show the name exactly the same, and that the name exactly matches what has been entered into the system.
Note: *Changing a Personal Email address:*

- *If the Identity is Active and has a Launchpad account, the user can make the change themselves using id.nasa.gov*
- *If the Identity is On-boarding any Associated Identity Requester can make the change manually using Modify Identity*
- *If the Identity is Active and does not have a Launchpad account, contact the NISC to submit a trouble ticket.*

Residential Tab

The *Residential* tab allows you to enter the applicant's residential information.

Foreign National Tab

The *Foreign National* tab provides the ability to enter the identities documentation information, complete the questionnaire (host, time period, eQIP, protocol visit, escort, gender, work description, export controlled items, facilities, business hours, EAR or ITAR data), view pending approvals for the foreign national, view Provisos that will be added by the FN approver, add NAMS Visiting Center Requests, add Access Control Plans as well as documents on an ACP, and enter any comments that will be viewable in the comments tab.

Documentation (Foreign National)

In this section you have the ability to add to the Foreign National's record with any provided documentation information. Select Add Document button and select the document type from the option. Populate the document number, expiration, country, if it is a visa the visa type, begin and end date, and I-94 end date.

Note: *If the Foreign National does not require a VISA you can select the "No VISA Required" from the drop-down menu option.*

- ***On-boarding Access***-includes questions regarding physical access (if yes, you will be asked to select a New Credential & Badge Type), logical (IT access) desktop login (NCAD), email access (NOMAD) and Verification documents / Number / Issuing State

Affiliations Tab

In this section you can add the Affiliation information associated with the identity. Select the Agreement from the drop-down menu option. Only agreements that you are listed as an Identity Requester will be displayed. If you are unable to locate the specific agreement, for example, the Grant, Contract, or IPA, then you will need to contact the Agreement Maintainer for your Center. You will also need to select the Affiliation Sponsor, Company, Affiliation Start/End date, and whether they are a NASA worker (A person who is working for or "on behalf" of the government and is assigned work to advance the Agency's mission.) if the field is not prepopulated. Keep in mind that

you will need to return to the Affiliation tab once the identity is submitted to fill out the Position Designation questionnaire.

Note: *A 'signed DD254' for an Agreement in ICAM indicates the contract performs national security (Classified) related work. Therefore some personnel may require clearances adjudicated prior to performing official duties.*

NASA Worker	NASA Non-worker
A NASA worker is defined as a person who is working for or on behalf of the government and is assigned work to advance the agency's mission.	A NASA non worker is defined as a person who is invited to interact with the agency and or to utilize its low risk assets.
A position designation is required to ensure appropriate proofing and vetting is completed based on the risk of their work assignment.	Identity proofing is required only to grant the privileges of the low risk asset usage.
	Examples include tenants, or a super computer users which we consider a logical non worker.
	NASA non workers are not required to complete a position designation and will be submitted for low risk identity proofing and vetting.

On-boarding Access Tab

In this section you will be asked to complete a series of questions. Includes questions regarding physical access (if yes, you will be asked to select a New Credential & Badge Type), logical (IT access) desktop login (NCAD), email access (NOMAD) and you have the option to add any Verification documents / Number / Issuing State.

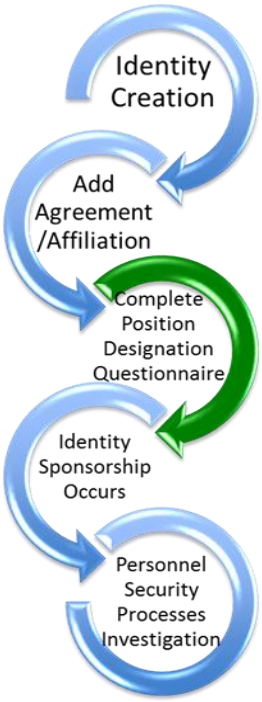
Credential Recommendation

Depending on the answers you selected on the On-boarding access tab, you may be presented with a credential recommendation pop-up. A recommended Credential and Badge Type have automatically been selected for you. If this is not the correct credential or badge type, select a different option from the drop down. When you are satisfied with the selections click the Submit button to process the request.

Position Designation

Identifying Position Designation is necessary to get a proper investigation for the NASA worker based on the risk they pose to the Agency for the work they do. This tool is used to calculate Position Risk and Position Sensitivity during the on-boarding process and through the following lifecycle actions for NASA workers: Re-investigations, Primary Affiliation Changes, and Agreement Rollovers. The Identity Request is NOT submitted to the Sponsor until Position Designation is completed for an On-boarding NASA worker. The Identity Requester will need to understand the applicant's position and related risk prior to creating an Identity Request. The Identity Requester will receive notifications / actions to complete an updated Position Designation for an active identity if a Reinvestigation is upcoming, the

user has a new primary Affiliation either individually or via an Agreement Rollover, or if Security requests a Position Designation. These actions will be available on the Identity Requester Workbench in the Pending Actions section.



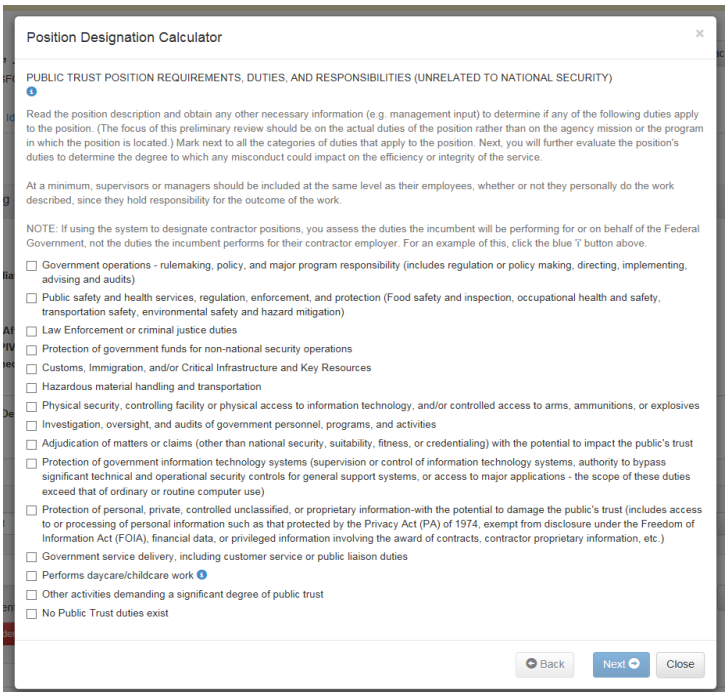
Civil Servant: Position Designation is initially entered and maintained in the HR systems

Contractors: Position Designation is identified through completion of a questionnaire within IdMAX during the Onboarding process and other lifecycle processes. Identifying Position Designation is tied to the workers Affiliation, which is closely associates job duties to the NASA worker

During the onboarding process the Identity requester will complete the Questionnaire that will establish the Position Sensitivity + Risk for the NASA worker and produce recommended investigation results.

The Identity Requester and Sponsor can modify the Position Designation to produce different Position Sensitivity + Risk to result in a different investigation if the one generated is not correct.

The Investigation Reviewer, Authorizer, or IVC role holders can modify the Position Designation from the Security Workbench to produce different Position Sensitivity + Risk to result in a different investigation.

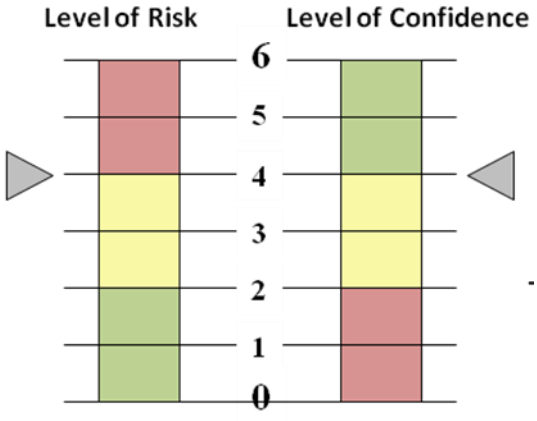


When completing the PD questionnaire, the answers you provide drive Position Risk and Position Sensitivity as well as the recommended investigation for the NASA worker. Once you have completed the Position Designation, the results will be displayed, and the applicant will continue through the Identity Workflow process. If you are not satisfied with the results you have the option to Recalculate the results.

Note: "i" boxes are available if you have any questions.

Position Risk/Sensitivity, Levels of Confidence, Asset Risk, and Trust

ICAM ensures that NASA can identify people to an appropriate Level of Confidence, helping NASA asset owners make risk-based determinations about granting access to NASA physical and/or logical assets. One of the goals of ICAM is to align the confidence NASA has in an individual with the risk associated with their physical and logical access.



Level of Confidence (LoC), which measures: 1) the degree of certainty that a person is who s/he claims to be, 2) a person's fitness for his/her position or access. NASA workers require a minimum of LoC of 40 regardless of work location.

Level of Risk (LoR), which is the degree of potential damage that access to an asset represents. For users of NASA assets and services that are not workers, the LoR of the asset is utilized to determine the proofing and investigation requirements in place of the position risk and sensitivity.

NASA's goal is that the Level of Confidence equals or exceeds the Level of Risk.

Level of Trust (LoT) is the degree certainty that a person's access to an asset is an acceptable risk. The goal is that LoT never be a negative number. When taken a step further, a position LoR can help determine what type of background investigation a person requires.

Level of Assurance (LoA), which is the degree of certainty that a credential presented represents the person who is accessing the asset.

A **Trusted Partner** is an agreement where NASA enters into an identity trust relationship and security posture with another company, federal agency or other entity that allows for stream-lined tracking of identities to provide NASA IT services as defined by an asset provisioning plan.

Trusted Identities is an identity with limited identity data collection and proofing requirement with a predefined access initiation plan due to primary affiliation designation as a Trusted Partner. The user's Level of Confidence is the greater of the Identity Plan's default value or calculated values if individual proofing and vetting is pursued.

Logical Level of Risk

- **-10 - Flagged Identities-** The user is Terminated "With Cause" or Completed, Unfavorable Investigation of any type.

- **-5 - No logical (IT) Access Allowed-** This user is prevented from requesting IT access in NAMS.

- **0 - No current logical (IT) Access** –The user only needs access to NASA Facilities.

- **10 - Very Low Risk - Guest User** - This asset presents a very low risk to the Agency. Examples include SATERN and WebEx.

- **20 - Very Low Risk - Name check w/o Identity Proofing** - This access presents a very low risk to the agency. Examples include basic tools such as SATERN and Webex.

- **25- Low Risk-Enrollment Complete-** This access presents a very low risk to the agency. The user may be granted access to this asset due to the completion of in-person proofing.

- **30 - Very Low Risk - Identity Proofing with National Criminal History Check** - This asset presents a low risk to the agency. Examples include access to their own privacy data, PKI encryption and signing certificates, and Level of Assurance 2 and 3 credentials.

- **35- Low Risk-Investigation Submitted-**This asset presents a low risk to the agency and may be accessed by a user with a submitted investigation. Examples include smartcard protected applications and computers, user access to their own privacy data, and local application system administration and/or elevated privileged on their own workstation.

- **40 - Low Risk - OPM Tier 1** - This asset presents a low risk to the agency. Examples include applications requiring a PIV credential to access smartcard protected applications and computers, user access to their own privacy data, and local application system administration and/or elevated privileges on a single workstation.

- **45- Interim Moderate Risk-** This asset presents a moderate risk to the agency. The user may be granted access to this asset at the time of the submission of their higher investigation. Examples include System Administrators needing NDC access.

- **50 - Moderate Risk - OPM Tier 2** - This asset presents a moderate risk to the agency. The user will need access to sensitive data such as other people's privacy data, SBU data, and ITAR/EAR. Examples include access to ICAM infrastructure with the ability to view user PII, and collaboration tools (SharePoint/Windchill) with ITAR/EAR and SBU projects.

- **55 - Moderate Risk –(SECRET) - OPM Tier 3** - This asset presents a moderate risk to the Agency and to National Security. The user will need access to Secret classified systems. The user will need to have a completed background investigation and clearance before access will be granted. Examples include access to the Secret Internet Protocol Router Network. The user will need user

or privileged level access to NASA CLASSIFIED IT resources such as SiPRNET terminals and infrastructure. Requires a signed DD-254 for contract employees. Note: Should not be selected during on-boarding.

- **60 - High Risk - OPM Tier 4** - This asset presents a high risk to the Agency. The user will need access to systems that the compromise of could cause severe harm to the Agency and/or mission. Examples include identity vetting and credentialing system administrators and users with the capability of producing credentials, Agency Domain Administrators, high impact financial records, procurement systems, and EPACS regional and enterprise administrators. The user will need privileged level access to high risk NASA IT resources such as command and control systems, human flight and safety systems, EPACS regional and application administration, and credential production systems. Note: Should not be selected during on-boarding.

- **70 – Very High Risk – (TOP SECRET) - OPM Tier 5** - This asset presents a very high risk to the Agency and to National Security. The user will need access to Top Secret classified systems. The user will need to have a completed background investigation and clearance before access will be granted. Examples include access to the Joint Worldwide Intelligence Communications System. The user will need user or privileged level access to TOP SECRET NASA IT resources such as JWICS terminals and infrastructure. Requires a signed DD-254 for contract employees. Note: Should not be selected during on-boarding.

Physical Level of Risk

- **-10 - Flagged Identities-** The user is Terminated “With Cause” or Completed, Unfavorable Investigation of any type.
- **-5-No Access Allowed to NASA Facilities** -This user is prevented from requesting Physical access in NAMS.

- **0 - No current access to NASA Facilities** – The user only needs access to NASA's IT Resources. Often called "IT Only".

- **10 - Public Access Only** - This asset has very low risk to the agency. Examples include access roads and "open" events. The user needs the ability to access roads and attend "open" events. Generally non-work affiliations.

- **20 – Open Facilities - Name check w/o Identity Proofing** - This asset presents a low risk to the Agency. Examples include "open" facilities such as cafeterias and gyms.

- **25- Open facilities – Identity Proofing-** This asset presents a low risk to the Agency. Examples include facilities that require card reader access to enter.

- **30 - Unrestricted - Identity Proofing with Criminal History Check** - This asset presents a low risk to the Agency. Examples include facilities that require identification to enter, such as a day care. The user needs access to administrative facilities to achieve work affiliation requirements.

- **35-Controlled Facilities-Investigation Submitted-**This asset presents a low risk to the Agency. Examples include unrestricted access to NASA center perimeters and administrative facilities. Users will normally obtain and utilize a PIV credential to access these assets. This user needs access to NASA controlled facilities. They will need to have an investigation submitted and a smartcard issued before access will be granted.

- **40 - Controlled Facilities - OPM Tier 1** - This asset presents a low risk to the Agency. Examples include unrestricted access to NASA center perimeters and administrative facilities. Users will normally obtain and utilize a PIV credential to access these assets. The user needs access to identified special access facilities. This access normally includes additional approval and training. Please see center procedures for this access.

- **45- Interim Limited Access-** This asset presents a moderate risk to the Agency. The user may be granted access to this asset at the time of the submission of their higher investigation. Users will normally obtain and utilize a PIV credential to access these assets.

- **50 - Limited / NCI Facilities - OPM Tier 2** - This asset presents a moderate risk to the Agency. Examples include NASA critical infrastructure (NCI), data centers and server rooms, SBU/ITAR/EAR storage areas, and electrical infrastructure. This access can include additional approval and training. The user needs access to NASA Classified Facilities. He/she will need to have a completed background investigation and clearance before access will be granted.

- **55 - Limited Facilities w/ National Security (SECRET) OPM Tier 3** - This asset presents a moderate risk to the Agency and National Security. He/she will need to have a completed background investigation and clearance before access will be granted. Examples include SECRET reading rooms and classified storage areas. Note: Should not be selected during on-boarding.

- **60 - Exclusion facilities - OPM Tier 4** - This asset presents a high risk to the Agency. Examples include areas with hazardous materials, weapons, and/or explosives, areas with NASA critical IT infrastructure, areas storing investigation information and materials for producing credentials. The user needs access to areas with hazardous materials, weapons, and/or explosives, areas with NASA critical IT infrastructure, areas storing investigation information and materials for producing credentials. Note: Should not be selected during on-boarding

- **70 - Exclusion facilities w/ National Security (TOP SECRET) OPM Tier 5** - This asset presents a very high risk to the Agency and National Security. Examples include NASA TOP SECRET Classified Facilities. He/she will need to have a completed background investigation and clearance before access will be granted. Examples include Special Access program areas and Sensitive Compartmented Information Facilities. The user needs access to areas with hazardous materials, weapons, and/or explosives, areas with NASA critical IT infrastructure, areas storing

investigation information and materials for producing credentials. Note: Should not be selected during on-boarding.

Copy Position Designation

The ability to copy a Position Designation from a completed identity is available for Associated Identity Requesters, Sponsors, Enrollment Officials, PIV Authorizers, and IVCs. This feature is available for identities that do not have a completed Position Designation and the one completing the PD would like to use an existed completed PD from an identity that is on the same agreement. Note: A PD cannot be copied from a Civil Servant and this feature is not available for Foreign Nationals.

3. Agreement Lifecycle

Agreement Creation and Maintenance

Agreement workflows can be maintained by anyone with the Agreement Maintainer role or who is assigned as the Agreement Identity Requester. Each center is responsible for creating agreements for their center.

Status Management for Agreements:

- **Active-**Fully Available to assign to a user
- **In-Active-**Agreement remains functional but not assigned to a user

Access to Agreement Maintenance Tool- Roles

To access the Agreement Maintenance Tool the user must have the Agreement Maintenance role, be a PIV Authorizer, or an Investigation Reviewer. The Agreement Maintainer is the representative that assists in the management of agreements.

Anyone who is assigned as an Agreement Requester or Agreement Sponsor will be able to access the Agreement for which they are identified as the maintainer. A description of these roles and assigned responsibilities are outline in the following table:

Agreement Maintenance Role	Responsibilities
Agreement Maintenance	• A NASA or contractor official that are granted restrictive access to the Agreement Maintenance tool. The Agreement Maintenance Tool allows them the access to create or make modifications to agreements for their center specific agreement.
PIV Authorizer	• A NASA or contractor official that are granted restrictive access to the Agreement Maintenance tool. The Agreement Maintenance Tool allows them the access to create or make modifications to agreements for their center specific agreement.
Investigation Reviewer	• A NASA or contractor official that are granted restrictive access to the Agreement Maintenance tool. The Agreement

	Maintenance Tool allows them the access to create or make modifications to agreements for their center specific agreement.
Agreement Requester /Identity Requester	• Agreement Requesters must have the Identity Requester role in NAMS and cannot be a terminated employee. Agreement Requesters can be added, removed and designated as primary on a specific agreement. They are responsible for completing the affiliation tab in IdMAX which defines the affiliation the identity has with NASA.
Agreement Sponsor	• A NASA civil servant who vouches for an individual's need for identity lifecycle management services in order to be authorized to access NASA physical or IT assets. They are responsible for managing Foreign Nationals working at Centers and on NASA databases.

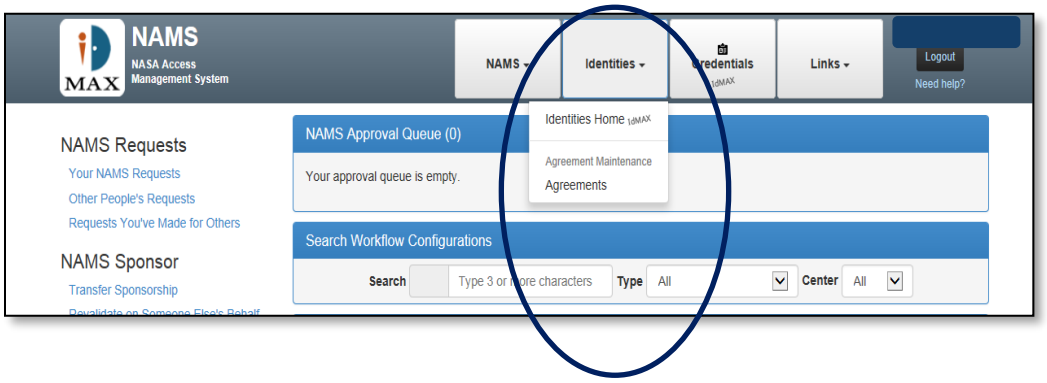
AGREEMENTS TOOL

The *Agreements* Tool is used for the development and modification of agreements. It is a tool that provides flexibility for each asset's unique workflow. To access the Agreements tool, you must have the Agreement Maintenance role, PIV Authorizer role, or Investigation Reviewer role which allows full access to all the features of the Agreement Tool for all agreements. You must complete the required SATERN course prior to requesting for a role in NAMS. When your NAMS request has been approved, a link on the NAMS console page will display the Agreements Tool.

DETAILS

The Agreements tool captures data during the creation/modification of an agreement:

- Basic General Data about the agreement
- Selection of Agreement Requesters
- Selection of Sponsors
- Add Companies associated to the agreement



- In this example, Agreements is listed under the Identities tab.

Creating or Modifying an Agreement

Developing a new agreement ensures that the agreement is available for selection. You will begin by creating a new agreement.

The steps for creating a new agreement are listed in the following table:

Step #	Agreement Steps
1	Identify the agreement that needs to be created
2	Input the Basic Agreement information. Agreement Name, Description, Agreement Number
3	Select the Type of Agreement
4	Select the Center
5	Select the Effective and End Date
6	Select the Status of the Agreement
7	Answer the Non-Disclosure (NDA) Conflict of Interest question
8	Determine and select if you would like for Termination notifications to be sent via email- Requester & Sponsor: 60-day, 30-day, 15-day, 10-day, 5 day, daily
9	Determine and select if you would like for Renewal notification to be sent via email- Sponsor, User, & Badging Office: 90-day, 60-day, 30-day, 15-day, 5 day, daily
10	Identify, search, and select the companies associated with the agreement
11	Identify, search, and select the Agreement Requester(s) for the agreement
12	Identify, search, and select the Sponsor(s) for the agreement
13	Review the information entered on the request form
14	Select the Create Agreement button

NOTE: If you create the agreement with missing information, it will be saved as closed. You can search for the agreement and continue to edit the agreement for completion then or at a later date.

NOTE: If making modifications to an agreement, it is best practice to SAVE the agreement before navigating away from the screen to another tool. For example, if you need to make changes to the agreement name and transfer affiliations, make the change to the agreement name, SAVE the change, then navigate to the transfer affiliation tool. If you move away from the screen without saving, it will not capture any changes that were made.

Agreement Name

Enter the *Agreement Name* also known as the friendly name of the agreement. The agreement name is displayed when a search for the affiliation is made.

Description

The *Description* is displayed when the user searches for an agreement. The words in the field are searched when someone does an agreement search. Add any keywords that your user population would associate with your agreement.

Agreement Number

Agreement Number is a unique number that is assigned to each agreement.

TYPE

Agreement *Types* are expanded to include NASA Employment, Contract, Grant, Memorandum of Understanding (MOU), Space Act, Intergovernmental Personnel Action (IPA), NASA Defense Purchase Request (NDPR), Tenant, Intergovernmental Agreements (IGA), Other, Trusted Partner, and Non-Appropriated Funds Activity (NAFA).

CENTER

The *Center* field is the center for which the agreement is developed and maintained. This field is required to allow the ICAM Cognos Reports to provide accurate information.

EFFECTIVE

The *Effective* date is the date in which the agreement became active.

END

The *End* date is the date in which the agreement will be in-active.

STATUS

Status is the state in which the agreement is in.

NASA FAR CLAUSE 1852 OR EQUIVALENT?

You would answer:
Yes-The NASA FAR Clause 1852.237-72 & -73 (Access to and Release of Sensitive Information) or equivalent s included in this agreement.
No- The NASA FAR Clause 1852.237-72 & -73 (Access to and Release of Sensitive Information) or equivalent is NOT included in this agreement.

TERMINATION NOTIFICATIONS

Termination notifications will go to the Requester and Sponsor for the Agreement. Notifications will be sent on days 60, 30, 15, 10, 5, and daily until completed.
You would answer:
Enable-Termination notification will be sent to the identities
Disable-Termination notification will not be sent to the identities

RENEWAL NOTIFICATIONS

Renewal notifications will go the Sponsor, User, and Badging Office for the Agreement. Notifications will be sent on days 90, 60, 30, 15, 5, and daily until completed.
You would answer:
Enable-Renewal notification will be sent to the identities
Disable-Renewal notification will not be sent to the identities

PIV ELIGIBLE

Agreement Maintainers can identify specific agreements as NOT PIV eligible. This will exclude the users with the Agreement as their Primary Affiliation from the PIV Step Up Batch job.
Yes-Identities are eligible for a PIV credential and will be included in system credential calculations.

No-Identities are NOT eligible for a PIV credential. The system will not generate a PIV credential for identities on this agreement. PIV Ineligibility must be determined based on NPR 1600.4 ineligibility criteria.

Personal Security can overwrite PIV eligibility on any individual on the agreement on the Identities Credential tab.

SIGNED DD254

A DD Form 254 is a Contract Security Classification Specification. The intention of a DD Form 254 is to convey security requirements, classification guidance and provide handling procedures for classified material received and/or generated on a classified contract. The DD Form 254 is a resource for providing security requirements and classification guidance to a contractor. The DD Form 254 is a U.S. publication referenced in the DFAR and applied to contracts involving access to classified information by U.S. contractors. If the contract is with non-US Industry (foreign governments, cleared foreign companies or international organizations) additional guidance is on a case-by-case basis. The Industrial Security Implementing Agreement (to the General Security of Military Information Agreement) is the overarching authority for the bilateral protection of classified information with foreign governments. The Federal Acquisition Regulation (FAR) requires that a DD Form 254, Contract Security Classification Specification, be integrated in each classified contract. The DD Form 254 provides the contractor (or a subcontractor) security requirement and the classification guidance that is necessary to execute a classified contract.

If yes is selected for DD254 additional information will be required to be completed.

- Cage Code: Unique identifier issued by the government to identity commercial and government entities.
- Facility Clearance Level: Administrative determination that, from a national security standpoint, a facility is eligible for access to classified information at the same or lower classification category as the clearance being granted (Confidential, Secret, or Top Secret)
- Facility Security Officer (FSO) Information: Individual in charge of managing security in their organization's facilities.
    - SCI: Sensitive Compartmented Information
    - DOE: Depart of Energy
    - NATO: North Atlantic Treaty Organization

NASA WORKER

If NASA Worker (where the NASA worker is set to Yes), a position designation will need to be completed for associated individual's primary affiliation. If NASA Non-worker (where the NASA worker is set to No), the associated identities will not be required to have a position designation and will be vetted for low risk. Agreements will be defaulted to be NASA Worker or Non-Worker based on the Agreement Type selection, and some agreement types will not all modification of this flag.

NASA Worker	NASA Non-worker
A NASA worker is defined as a person who is working for or on behalf of the government and is assigned work to advance the agency's mission.	A NASA non worker is defined as a person who is invited to interact with the agency and or to utilize its low risk assets.

A position designation is required to ensure appropriate proofing and vetting is completed based on the risk of their work assignment.	Identity proofing is required only to grant the privileges of the low risk asset usage.
	Examples include tenants, or a super computer users which we consider a logical non worker.
	NASA non workers are not required to complete a position designation and will be submitted for low risk identity proofing and vetting.

ID	Definition	Description	NASA Worker Default	PIV Eligible Default
1	Contract	NASA Procurement defines resource support for a person representing another entity or themselves	Worker	Yes
2	Grant	Grants define NASA access to users as hospitality	Non-Worker	Yes
3	MOU	Memorandum of Understanding for Detailees from another US Government Department or Agency	Non-Worker	Yes
4	Space Act	Space Act	Non-Worker	Yes
5	IPA	Intergovernmental Personnel Action associate users with another government entity	Worker	Yes
6	NDPR	NASA Defense Purchase Request Agreement	Non-Worker	Yes
7	NASA Employment	NASA Employment	Worker	Yes
8	Other	Other relationships where NASA provides access to users as hospitality	Non-Worker	No
9	Tenant	Tenant - Physical Access	Non-Worker	No
10	IGA	Inter-Governmental Agreement	Non-Worker	No

11	NAFA	Non appropriated fund activity or entity that is not funded by money appropriated from the general fund of the U.S. Treasury	Non-Worker	No
12	Test Accounts	Designation for Identities that are to support Test requirements.	Non-Worker	No
13	Non-Human	Designation for identities that represent a Non Person Entity with IT Access on behalf of another user/group	Non-Worker	No
14	Trusted Partner	Designates when NASA has an identity trust relationship and security posture with another company, federal agency or other entity	Non-Worker	No
15	Foreign National Visitor	Tracks Foreign National Visitors by supporting NASA entities	Non-Worker	No

MANAGE TRUSTED PARTNER PLANS

Trusted Partner Identity Plan

The Agreement Maintenance tool will record the details of the Trusted Partnership. Trusted Partner Identity Plan will be documented based on coordination with the partner. A custom Invitation user interface requirements will be defined by tab (Residential, Identification, Naturalization) IT Security training may be over-ridden (will use tertiary date for initial override) The default level of confidence will be used for all related Trusted Identities; reflects proofing and vetting done by partner that NASA accepts. Comments and Documents may be used as needed.

Agreement Access Plan

Access Plan will provide a listing of asset with the related NAMS request template for the asset to be auto-initiated at each Trusted Identity's enablement.

- **Add Asset-**Allows selection of Assets
- **Modify Template**-Allows for Configuration of Request Template for and the Enablement Action
    - **Save for Later**- Partial request form that will be submitted as Save for Later status
    - **Auto-Submit**-Complete request form and based on Asset setting in WCT for Auto-Submit vs Auto-Approval
        - Auto-Approval/Provisioning can occur if Asset is configures in WCT by Asset Owners as allowed for Trusted Partnerships
    - **Manual Request**- No request form but available in "White List" for Manual Requests in NAMS for users assigned to the Partnership

- Note: *If NAMS request form is modified, the Request Templates will need to be also modified*

- **Clear Template**-Resets template
- **Remove Asset**- Will submit Close Requests for all Trusted Identities on the related Trusted Partnership

ADD COMPANY

The Company block is where companies can be maintained for a specific agreement. A new company can be added by clicking the +Add Company button. The maintainer can search for a specific company in the Find Company search box and add a company from the retrieved list by clicking on it and the company data will be retrieved and populated on the screen.

If the company that the maintainer wants to add is not listed, a new company can be created by clicking the +Create New Company button. A new company name is required and must be unique. In order to help ensure that company names remain unique, a list of current companies will be displayed as the maintainer is typing in the new company name. The maintainer can select a company from the current list, which will then be inserted in the company block along with the remainder of the company data.

If the company that the maintainer wishes to add is not listed, then complete the new Company Name, add a friendly name and choose a Country and click the Create Company button and the company data will be displayed in the Company block.

The Company block also displays the Company Country, the number of identities that are associated with the company and a button to remove the company.

A Company cannot be removed if there are identities associated with it. When clicking the remove radio button and identities are associated with that company, a screen will pop up stating that the company cannot be removed and will contain a link to the screen that will allow the identities to be transferred to another company.

ADD AGREEMENT REQUESTER

The Agreement Requester block is used to associate an Agreement Requester, who has the Identity Requester role in NAMS, with a specific agreement. An agreement is required to have at least one Agreement Requester, one of which is required to be the primary.

NOTE: Any errors on the agreement will be displayed in a pink ERROR box at the top of the screen when an agreement is retrieved. These errors must be resolved before any changes to the agreement can be saved.

An Agreement Requester can be added to the agreement by clicking the +Add Agreement Requester button and searching for a requester and then add them. If the person searched for does not currently have the Identity Requester role in NAMS an message will be displayed with a button which contains a link to take the user to NAMS to request the role for that person. The person will not be allowed to be added until they have been approved to have the role.

An Agreement Requester can be removed from the agreement if they do not have any identities associated with them. If that person currently has identities associated with them, a message will be displayed to notify the user and will contain a link to transfer the identities to another Agreement Requester.

An Agreement Requester cannot be removed if they are the primary on the agreement. The primary can be moved to another Agreement Requester and then the original primary can be removed, provided there are no identities associated with them.

If an Agreement Requester has been terminated and is still associated with an agreement, a message will appear under the Agreement Requesters name stating the user has been terminated and must be removed. When the maintainer clicks on the remove button to remove the Agreement Requester from the agreement and the Requester still has identities associated with them, a message will be displayed with a link to transfer the identities to another Agreement Requester before the original Requester can be removed. Once the identities have been transferred, the Agreement Requester can be removed.

If an error is displayed when the agreement is retrieved stating that a specific Agreement Requester does not have the Identity Requester role, the maintainer can then request the role in NAMS. Once the Agreement Requester has been approved, the error will not be displayed again.

Add Sponsor

The Sponsor block is used to associate a Sponsor, who has the Sponsor role in NAMS, with a specific agreement. An agreement is required to have at least one Sponsor, one of which is required to be the primary.

NOTE: Any errors on the agreement will be displayed in a pink ERROR box at the top of the screen when an agreement is retrieved. These errors must be resolved before any changes to the agreement can be saved.

A Sponsor can be added to the agreement by clicking the +Add Sponsor button and searching for a Sponsor and then add them. If the person searched for does not currently have the Sponsor role in NAMS an message will be displayed with a button which contains a link to take the user to NAMS to request the role for that person. The person will not be allowed to be added until they have been approved to have the role.

A Sponsor can be removed from the agreement if they do not have any identities associated with them. If that person currently has identities associated with them, a message will be displayed to notify the user and will contain a link to transfer the identities to another Sponsor.

A Sponsor cannot be removed if they are the primary on the agreement. The primary can be moved to another Sponsor and then the original primary can be removed, provided there are no identities associated with them.

If a Sponsor has been terminated and is still associated with an agreement, a message will appear under the Sponsor name stating the user has been terminated and must be removed. When the maintainer clicks on the remove button to remove the Sponsor from the agreement and the Sponsor still has identities associated with them, a message will be displayed with a link to transfer the identities to another Sponsor before the original Sponsor can be removed. Once the identities have been transferred, the Sponsor can be removed.

If an error is displayed when the agreement is retrieved stating that a specific Sponsor does not have the Sponsor role, the maintainer can then request the role in NAMS. Once the Sponsor has been approved, the error will not be displayed again.

Create Agreement

The *Create Agreement* button saves and submits the information that was entered on the agreement. A message will display across the top of the screen indicating the agreement was successfully created.

Cancel

Cancel allows for any information entered to be deleted from the form with no changes saved or submitted.

VIEW AUDITS

View Audits allows you to see the changes made to that specific agreement.

NOTE: The View Audit button listed on the agreement will only display the audit trail for that agreement only.

CLOSING AN AGREEMENT

Verify that an agreement can be closed as long as all affiliations have been transferred to another agreement and the Identity Requester, Sponsor and Company CAN remain on the agreement when closing.

SETTING AN AGREEMENT BACK TO EFFECTIVE

Verify that if all Agreement Requesters, Sponsors and Companies that have previously existed have been removed including the primary, that the agreement cannot be saved as effective, it must be closed at this time or an error will occur stating. The status cannot be set to effective without assigned Identity Requesters, Sponsors and Companies.

UPDATE IDENTITY REQUESTER

The *Update Identity Requester* tool is used when an Agreement Requester is no longer associated with an agreement and needs to be removed and updated with a new Agreement Requester. This will allow you to select the identities that are associated to the old Identity Requester and move them to a new Identity Requester. The Identity Requester must have completed the SATERN training and have the role in NAMS.

NOTE: If the Identity Requester is terminated you will see an error message on the Agreement until an update to the Agreement Requester field is made or if the Agreement Requester selected does not have the Identity Requester role in NAMS.

SEARCH IDENTITY REQUESTER

To begin the update, type the Identity Requesters name in the *Search Identity Requester* block. Select the Identity Requesters name once it is displayed to open the request. The identities that are associated to the Identity requester will be displayed on the screen in alphabetical order. Only engaged, engaging, and separating affiliations are included in the transfer. You can individually select the Identities that need to be transferred to the new Identity Requester or you can select the top box to select all the identities listed.

SEARCH NEW IDENTITY REQUESTER

Once the Identities that will be transferred to the new Identity Requester are selected, begin a Search for the New Identity Requester in the block. Select the new Identity Requesters name once it is displayed. The Identity Requester must have completed the SATERN training and have the role in NAMS.

EMAIL REQUESTER

You have the option to send the new Identity Requester an email letting them know new affiliations have been reassigned to them. Select the box if you would like to inform the new Identity Requester of the change or leave the box unchecked to choose not to send an email to the new Identity Requester.

Update Identity Requester button

If you are satisfied with the changes, select the Update Identity Requester button to process the request. A message will display across the top of the screen indicating the update was successful.

Update Sponsor

The *Update Sponsor* tool is used when an Agreement Sponsor is no longer associated with an agreement and needs to be removed and updated with a new Agreement Sponsor. This will allow you to select the identities that are associated to the old Sponsor and move them to a new Sponsor.

Search Sponsor

To begin the update, type the Sponsors name in the *Search Sponsor* block. Select the Sponsors name once it is displayed to open the request. The identities that are associated to the Sponsor will be displayed on the screen in alphabetical order. You can individually select the Identities that need to be transferred to the new Sponsor or you can select the top box to select all the identities listed.

Search New Sponsor

Once the Identities that will be transferred to the new Sponsor are selected, begin a Search for the new Sponsor in the block. Select the new Sponsor name once it is displayed.

Email Sponsor

You have the option to send the new Sponsor an email letting them know new identities have been reassigned to them. Select the box if you would like to inform the new Sponsor of the change or leave the box unchecked to choose not to send an email to the new Sponsor.

Update Sponsor

If you are satisfied with the changes, select the Update Sponsor button to process the request. A message will display across the top of the screen indicating the update was successful

Companies

The Companies tool is available to make any updates or create new Companies. To begin the update, type the Company name in the *Search Company* block. Select the Company name once it is displayed to open the request. The Company Name, Friendly Name, and Country are fields available for updating. A company can be set to active or inactive by placing a check in the box marked Active. Please note if a company is still being used on an effective agreement it must remain active. Select the *Save* button to submit the changes. A message will display across the top of the screen indicating the update was successful.

Create Company

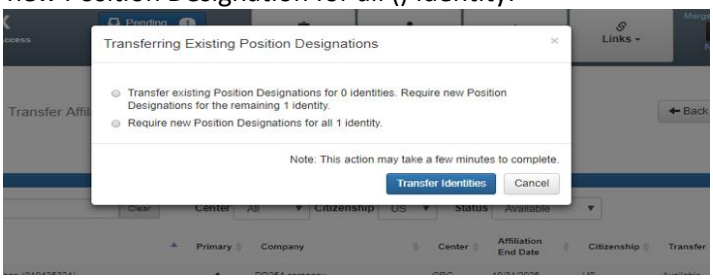
To create a new Company, select the Create Company button located on the Companies tool. Enter the Company Name, Friendly Name, and select the Country. A message will display across the top of the screen indicating the update was successful.

Search Agreements

Search Agreements allows you to search for an Agreement and make any necessary modifications to that Agreement. It also allows you the option to Transfer an affiliation from one agreement to another agreement and the ability to change the end date for an affiliation.

Transfer to New Agreement / Position Designation Connection

The *Transfer to New Agreemen*t tool provides the ability to transfer an affiliation(s) from one agreement to a new agreement. This is done when an identity is no longer associated with the agreement and needs to be transferred to a new agreement. Within the transfer Affiliations to New Agreement, you will be presented between selecting the rollover details and the data update. Transfer existing Position Designations modal has two options related to moving existing PDs: Transfer existing Position Designation for () Identities. Require new Position Designation for the remaining () Identity, or Require new Position Designation for all () Identity.



Change End Date

The *Change End Date* tool provides the ability to update an end date for any affiliations that is associated to the agreement. To begin the update, select the Change End Date button. A list of Identities will be displayed on the screen. Select the identities that require an end date extension. You can individually select the Identities or you can select the top box to select all the identities listed. Enter the new end date in the *Affiliation End* date block. Select the *Change End Date* button to submit the changes.

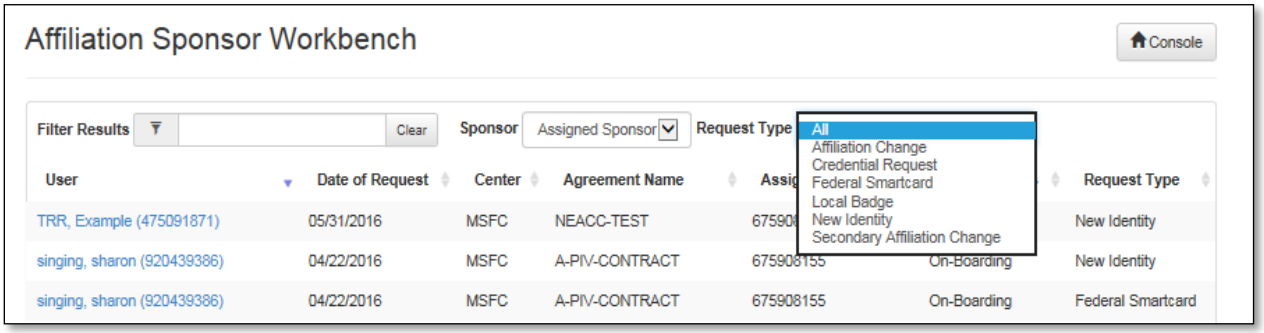
Tips & Tricks Agreements

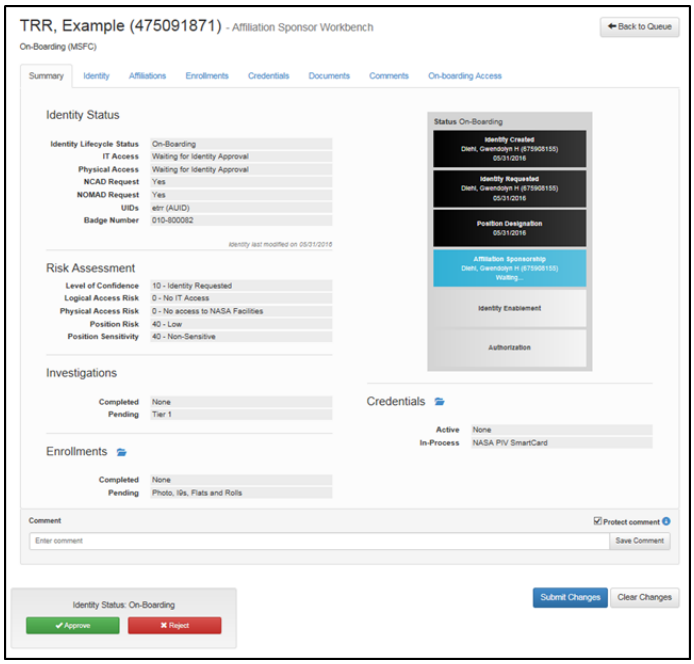
Error Message

Any errors on the agreement will be displayed in a pink ERROR box at the top of the screen when an agreement is retrieved. These errors must be resolved before any changes to the agreement can be saved.

4. Affiliation Sponsor Workbench

The Affiliation Sponsor Workbench is a listing of identities that are requiring approval for on-boarding, affiliation change or some credential requests. It allows you to approve and reject affiliation sponsorship actions.





The affiliation Sponsor form will have a subset of the associated identity data and has the ability to see assigned requests and those Associated by Agreement using the Sponsor filter. The Approve and Reject buttons are located within the identity record. If you reject a request you will be required to enter a justification for the rejection.

5. Authorization

Authorization is the process of ensuring that the person attempting to access an asset has been provisioned to do so. Authentication and Authorization are often thought of as a single process, but it is useful to understand the difference between the two. You may be properly authenticated to a system (you've proven you are who you say you are), but not be authorized to access that system.

6. Investigation Lifecycle

To assure that people have the access they need to further the mission of NASA, without putting NASA assets at risk, they gain knowledge about the person based on investigations and record checks. The identity proofing and background investigations that a person undergoes help determine the risk of the access granted to that person.

Investigation Results are listed as Favorable, Unfavorable, Waived, Reciprocal, and Unclassifiable
Note: Unfavorable does not invoke Immediate Termination as Flagged Identity; will simply negate that investigation from LoC calculation

LoC Recalculation Logic Change if a Submitted Investigation exist:

- If Investigation is Submitted and current LoC is 40 or greater, the LoC will remain
- If Investigation is Submitted and current LoC is less than 40, the LoC is set to 35

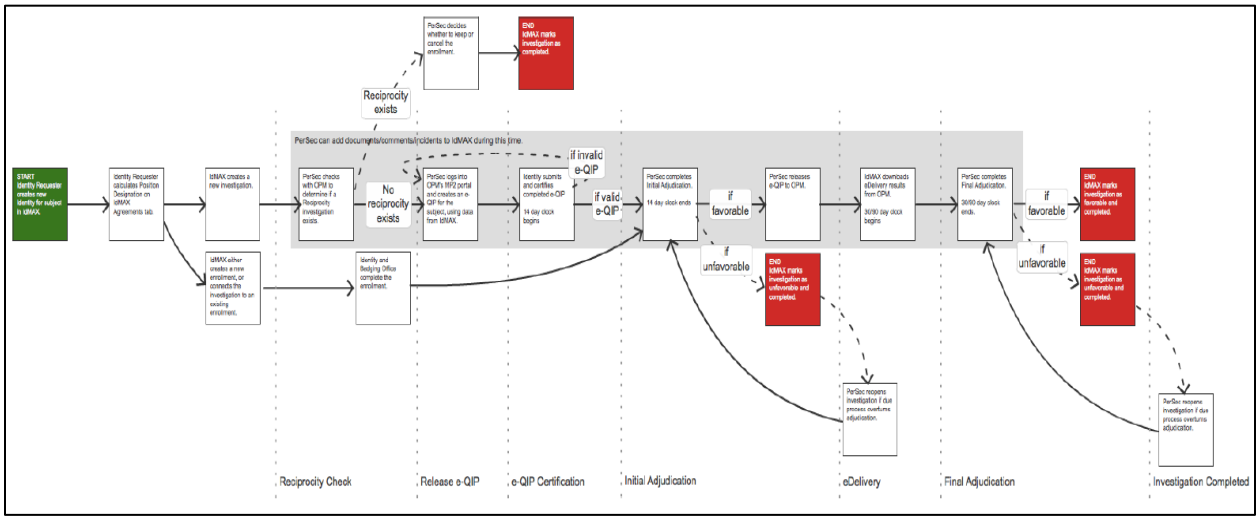
Investigation Types

NCIC	Name, DOB, SSN check via federal or state tools
NCHC	Fingerprint Check via federal or state tools
BI	Investigations
Visual Compliance	Foreign National Screening
SAVE Check	Department of Homeland Security immigration status or naturalized / derived citizenship check

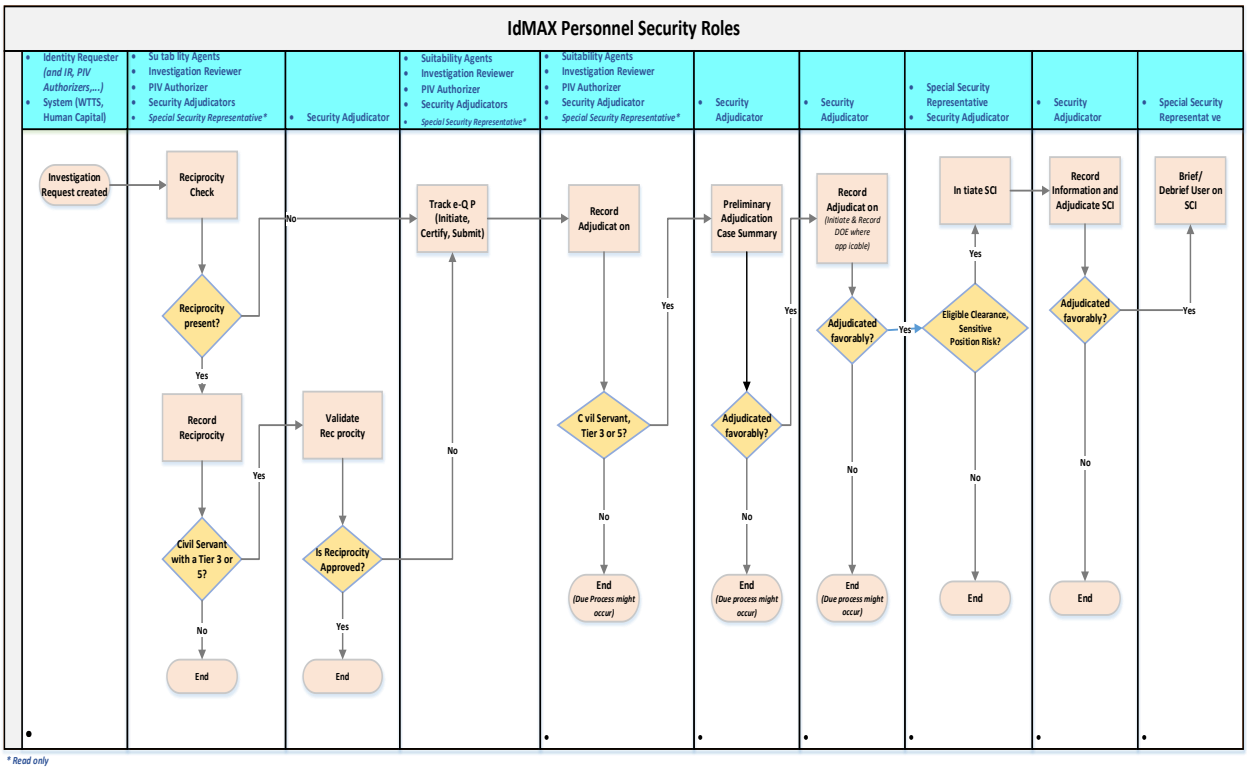
Investigation Statuses

Pending	Investigation has not been submitted; generated by Engine or user
Submitted	Investigation has been submitted to OPM/FBI
Completed	Investigation has been adjudicated
Expired	Investigation is inactive due to expiring
Cancelled	Investigation is cancelled

Investigation Lifecycle



IDMAX PERSONNEL SECURITY ROLES



* Read only

BI TABLE (BACKGROUND INVESTIGATIONS)

id	Description	LOC	Is Active	Validity Period	BI Type Form
0	NAC	20	false	1	(null)
1	NACI	40	true	100	0
2	BI	60	true	5	2
3	PRSC	60	false	1	(null)
4	MBI	50	true	5	2
5	LBI	50	true	5	2
6	ANCI	50	true	5	2
8	NACIC	40	true	10	0
9	PRRC	50	true	5	2
10	SBI	70	true	5	2
11	PRI	60	true	5	2
12	SAC	30	true	1	0
13	SGI	70	true	5	2
14	NACLC	50	true	5	2
16	ANACII	50	false	1	(null)
17	BI-R	60	false	1	(null)
18	CNAC	20	false	1	(null)
19	ENAC	20	false	1	(null)
20	LBI+	50	true	5	2
21	NACLN	50	false	1	(null)
24	PRI+	60	true	5	2
25	PRIR	60	true	5	2
26	PRIS	60	true	5	2
27	PRS	60	true	5	2
28	SBIP	70	true	5	2
29	SBIPR	70	true	5	2
30	SBPR	70	true	5	2
31	SDI	70	true	5	2
32	SSBI	70	true	5	2
33	XNAC	20	false	1	(null)
34	ANACI	55	true	5	2
38	BDI	60	true	5	2
39	BGI	60	true	5	2
40	LDI	50	true	5	2
41	LGI	50	true	5	2
43	NACL6	50	false	1	(null)
52	PPR	70	true	5	2
56	SSBI-PR	70	true	5	2
57	CNACI	40	true	10	0
58	PTSBI	70	true	5	2
59	ANACI-P	50	true	5	2
60	Tier 1	40	true	100	0
61	Tier 2	50	true	5	1
62	Tier 3	55	true	5	2
63	Tier 4	60	true	5	1
64	Tier 5	70	true	5	2
65	Tier 2 R (Reinvestigation)	50	true	5	(null)
66	Tier 3 R (Reinvestigation)	55	true	5	(null)
67	Tier 4 R (Reinvestigation)	60	true	5	(null)
68	Tier 5 R (Reinvestigation)	70	true	5	(null)
69	Tier 1 Substitute	40	true	100	0
70	Tier 3 Substitute	50	true	10	2
71	Tier 2S	50	true	5	1

REINVESTIGATION

The Reinvestigation batch job will run nightly and if it is 60 days from Reinvestigation date for an "Active" BI, user has LoC >40 and is low risk (Position Risk is 40 or below, Position Sensitivity is 40 or below, an email is sent to the Identity Requester to notify them to update the employees Position Designation. Another email will be sent to center security that includes all users within 60 days of a BI reinvestigation or 30 days of an NCIC, NCHC or Visual Compliance.

REINVESTIGATION DEFERRED (TIER 2 OR 4)

Reinvestigation Deferred is the ability to defer a Tier 2 or Tier 4 investigation for a user that has a completed NCHC via FBI or OPM in the last 120 days. This deferment allows the investigation to be valid for another 7 years and will occur only after the e-QIP Certification step. To select Reinvestigation Deferred, click Request New Investigation, select Investigation, the Investigation Type is Tier 2 RD (Reinvestigation Deferred) or Tier 4 RD (Reinvestigation Deferred), select the Investigation Form and then click Request Investigation.

LEVEL OF CONFIDENCE- INVESTIGATION

Level of Confidence (LoC) is NASA's degree of fidelity in a person based on identity proofing (match user to other information via checks and I9 verification) and vetting (investigations).

LoC is recalculated each time an identity is "saved" or "updated" from all IdMAX user interfaces (Security Workbench, Modify Identity/Identity Requester Workbench, Enrollment Workbench) Results sets include: Favorable, Favorable Substitutes (Reciprocal, Waiver, Unclassifiable (NCHC only)), or Unfavorable

What does not impact LoC is an Unfavorable Investigation, Sponsor rejection, Risk change, In-Person Registration, or Position Designation.

INVESTIGATION OR IDENTITY PROOFING EVENTS INCREASE THE LOC:

Identity Created	10
Favorable or Favorable Substitute SAVE	10
Favorable or Favorable Substitute NCIC is recorded	20
Favorable or Favorable Substitute Visual Compliance	20
NASA Civil Servant	20
Enrollment Complete (based on Identity Vetting through I-9 Capture)	25
Favorable or Favorable Substitute NCHC recorded	30
Submitted BI (Support PIV Issuance until BI Investigation Adjudicated)	35
Favorable or Favorable Substitute BI with Investigation Type	Based on BI Type 40 or higher (see BI Type table)
Submitted BI/Level 2-5 AND Completed Tier 1	45

LOC IS ONLY DOWNGRADED DUE TO THE FOLLOWING EVENTS

Termination with Cause	**-10**
Expired Investigations	Recalculated

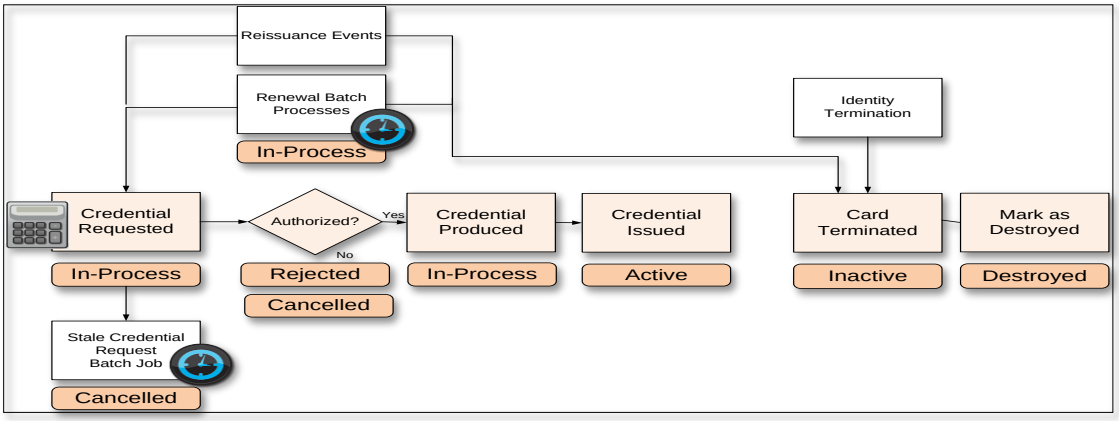
Events that have no impact on Level of Confidence

Sponsor Rejection
Cancellation of Identity Request
Risk and Position Designation Changes

7. Credential Lifecycle

Similar to the Identity Management, Credential Management also has a lifecycle. In this lifecycle the credential is requested via the Identity process by the Identity Requester or Security personnel, then sent for authorization by Security. In order to Authorize a NASA PIV Smartcard, the Authorizer must validate an engaged Affiliation Sponsorship, the user's Level of Confidence (LoC) =35 or greater, and has a Completed, Favorable NCHC within the past 180 days. In order to Authorize an Agency Smart Badge, the Authorizer must validate an engaged Affiliation Sponsorship, the user's Level of Confidence (LoC) =30 or greater and has a current Favorable NCHC within the past 180 days. In order to Authorize a Local Badge (Center Credential) an Authorizer must validate an engaged Affiliation Sponsorship, Completed, Favorable NCIC, NCHC, or BI, and a Level of Confidence (LoC) =20 or greater. Once authorized the credential is issued and integrated in the Credential Systems either with a PIV via CMS, Agency Smart Badge via Agency Smart Badge instance of CMS or a Local Badge via Lenel only. When the user no longer requires a credential the credential is set to Inactive and the Credential is Mark as Destroyed.

Credential Lifecycle



Credential Types

For an employee to be issued a NASA PIV Smartcard, Agency Smart Badge or Local Badge the employee must meet the following criteria:

NASA PIV Smartcard

- Requires LoC = 35 or greater, Sponsorship and Enrollment Complete for Authorization / CPR Submission
- Must have a Completed Favorable or Submitted Background investigation
- Must have current, Favorable NCHC (within past 180 days)
- Must be approved by a PIV Authorizer
- Approval initiates the CPR if Active Identity
- Printed by Vendor and issued at Center

Agency Smart Badge

- Requires LoC = 30 or greater, Sponsorship and Enrollment Complete for Authorization / CPR Submission
- Must have a current, Favorable NCHC (within past 180 days)
- Approved by a PIV Authorizer or System Authorized
- Approval initiates the CPR if Active Identity
- Printed locally

Local Badge

- Requires LoC = 20 or greater, Sponsorship and Enrollment Complete for Authorization
- May be approved by Investigation Reviewer or Authorizer
- Printed from Lenel

Non-NASA Smartcard / Registered Credentials

- A Non-NASA PIV Smartcards registered with NASA

BADGE TYPE

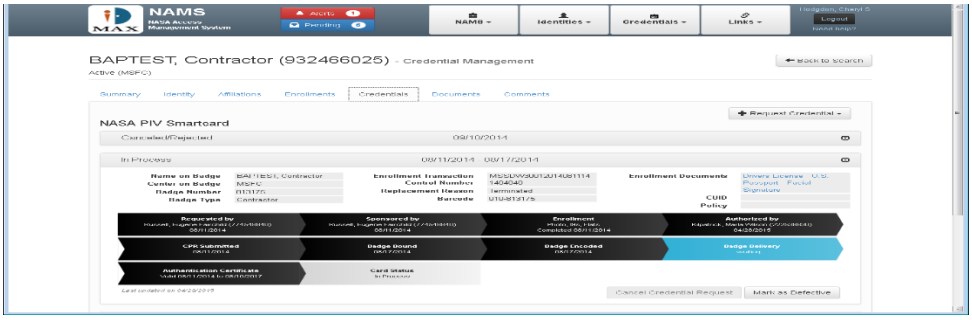
A Credential should be marked with the Badge Type that is associated with the user's affiliation. Provided below is list of the current Badge Types in IdMAX and the options of PIV or ASB. If the badge type that is selected is not correct. You can change it using the Security Workbench > Credential tab > Badge Type.

Badge Type	PIV	ASB
Aerospace Safety Advisory Panel		
Astronaut FN	x	
Bot		x
Civil Servant	x	x
Contractor	x	x
Detailee	x	x
External Customer		x
External Customer- FN	X	x
External Customer- LPR	x	x
FN	x	x
FN (After Hours)		x
FN- Escort	x	x
FN- IPA	x	x
FN- LPR	x	x
FN- Tenant		x
Grantee	x	x
Interim		x
Intern		x
IPA	x	
JPL	x	
NAFA	x	
No Physical Access		
" " FN		
Tenant		x

Credential Status

Credentials can vary in states while going through the lifecycle. The statuses are set to either In-Process, Active, Inactive, Rejected, Canceled, Destroyed. They can also be set to initial, Renewal, Reissuance, Non-Validated.

Your view of the Credential tab



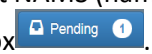
Note: A black chevron indicates a completed action and a blue chevron means an action is pending.

Renewal

A NASA PIV Smartcard is valid for five years from the date of issuance after the five years the employee or Identity Requester can submit a PIV Smartcard Renewal. 60 days prior to a Smartcard expiration date, the employee will receive an email notifying them that their smartcard will expire soon. The instructions in the email guide them through the renewal process. If they do not complete the renewal request, follow up emails will be sent at 30 days, and 15 days prior to the Smartcard expiration date. If they have not responded by 35 days prior to the smartcard expiration date, and email will be sent every day reminding them that their smartcard expires in less than 15 days.

An Agency Smart Badge is valid until the expiration date printed on the badge with an option to renew up to three years from the date of issuance after the three years the Identity Requester can submit a request for a new Agency Smart Badge or determine if a NASA PIV Smartcard is needed.

Submit a Renewal

As an Identity Requester you have permissions to submit a renewal on behalf of a user. To view the employees that are pending renewals, visit NAMS (nams.nasa.gov), in the header you should see a blue box labeled Pending, click the Pending box 

.

To process the request, click the Replace Credential button. From this point it is up to the employee to follow further instructions that are sent to them via email. The instructions should include setting up an appointment with the badging office.

Reissuance

As an Identity Requester or Badging Official you have permissions to submit a PIV Smartcard reissuance if an employee has lost their smartcard, reported the smartcard stolen, the card is damaged, it has been compromised, the card was terminated, or if the employee has recently changed their legal name, citizenship status, work center, or the employee type (from Contractor to Civil Servant or vice versa). If a Civil Servant is requesting a Smartcard reissuance, they must contact their Human Resources (HR) representative and they will make the changes in the Federal Personnel Payroll System (FPPS).

REQUEST A NEW CREDENTIAL

Select the *Request Credential* button located on the top right of the Credential section to begin the request for a new credential. Select one of the following options from the drop-down menu, PIV Smartcard, Agency Smart Badge, Local Badge, or Registered Credential. Once the Credential has been selected a pop up will be displayed that allows you to select the Sponsor and Badge Type. Once the information has been added a chevron will display on the Credential tab indicating the next step in the credential process. You can cancel the request if needed when it is in a Pending Status.

NON-NASA SMARTCARD (CAC / PIV / PIV-I)

Registering a Non-NASA Smartcard will allow NASA to accept and electronically verify credentials issued by other federal agencies, such as CAC, PIV, or PIV-I. Once registration is complete, the user will be allowed to request access to NASA's assets via NAMS. Detailed registration instructions are found in How to Register a Non NASA Smartcard (Credential Registration). There are two types of Non-NASA Smartcard Registrations, In-Person and Remote.

Note: The In-Person Registration is an Enablement event, but it does not drive a Level of Confidence recalculations. A Remote Registration is not an Enablement event.

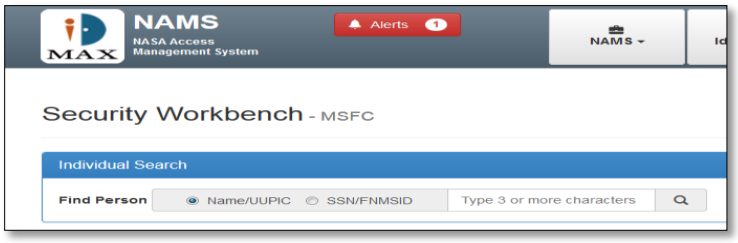
8. Security Workbench

Access to Security Workbench- Roles

To access the Security Workbench the user must have one of the following Agency ICAM Infrastructure roles, PIV Authorizer, Investigation Reviewer, Suitability Agent, and Security Adjudicator. You must complete the required SATERN course prior to requesting for a role in NAMS. When your NAMS request has been approved, a link on the NAMS console page will display the Security Workbench.

A description of these roles and assigned responsibilities are outline in the following table:

Role	Role Description
PIV Authorizer	• Authorizes the issuance of a NASA PIV Smartcard, Agency Smart Badge, or a Local Badge to a user who has met all proofing, enrollment and investigation requirements. Ability to Read Only Partial Clearance Data.
Investigation Reviewer	• Approves Local Badges and initiates a background investigation if necessary, or verifies the current background investigations meet NASA's minimum requirements.
Suitability Agent	• Initiates a background investigation if necessary, or verifies the current background investigations meet NASA's minimum requirements for Civil Servants
Security Adjudicator	• Initiates a background investigation if necessary, or verifies the current background investigations meet NASA's minimum requirements and manages NASA Clearances
Special Security Representative	• Supports SCI Initializations at the Centers, conduct briefing and debriefing



You can search for a specific Identity using the Individual Search feature. To begin a Search enter either the persons, First and Last Name, UUPIC, or click advanced to search by SSN, Center, AUID, First Name, Middle, Last Name, Org Code, Agreement, Company, Identity Status, Email, FNMS ID, Citizenship, or Birth Country. Results will display allowing you to select the record you would like to review/modify.

QUEUES

The Queues provide a list and count of identities in various states in the vetting and proofing process. It provides a capture of pending Investigation actions within the queues at any given time and allows for sortable data to assist with queue management.

Identity Queues	
On-Boarding	Users that have been "requested" but not yet enabled with an Identity Status of On-Boarding. They may be awaiting sponsorship, enrollment or investigations.
Suspended	Users whose Suspend Physical Access and / or Suspend IT Access Flag are currently active
Enrollments Pending	Users with an Enrollment that has a Pending Status.
Flagged	Returning Users that have been "requested" but not yet enabled with an Identity Status of On-Boarding and a Level of Confidence of -10.
Pending Terminations	Users that have a Termination Request submitted by a Requester or by the End Date Auto-Termination program that is awaiting approval.

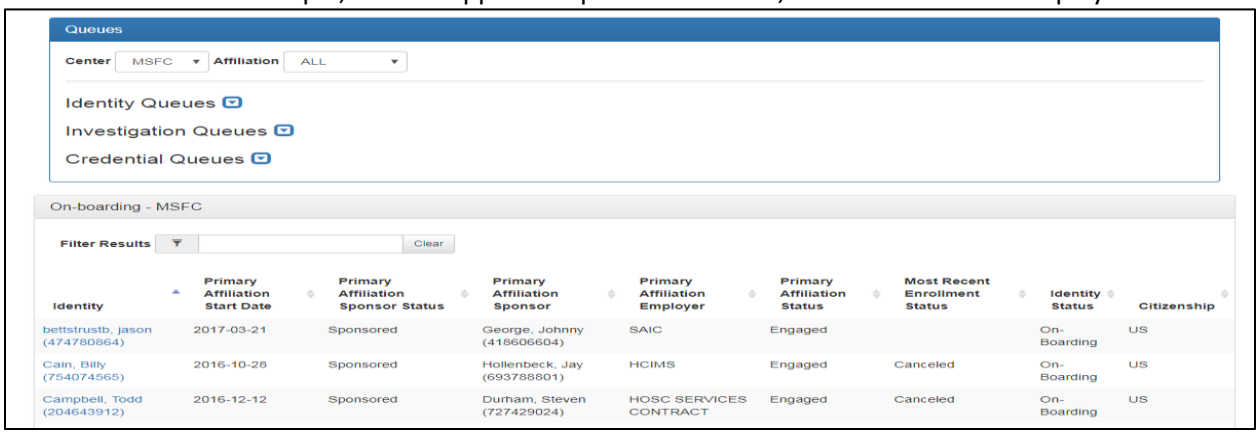
Investigation Queues	
Investigation Actions	
Investigations assigned to you	Includes all Investigations assigned to the logged in individual
Clearance adjudications assigned to you	Lists all Clearance records that are assigned to the logged in user from all Centers
Reinvestigations Pending	Users whose Re-investigation Date for their "primary" investigation (BI) is within the next 60 days
Investigations Needed	Identities with no Pending, Submitted, or Completed investigation
eDelivery Orphaned Results	
eDelivery No Match Results	
NCHCs	
In Process	Users that have a pending NCHC (National Criminal History Check) with no results recorded.
Review Needed	Users that are pending NCHC Reviews
Transmission Errors	User records that

Investigation Queues	
Investigation Actions	
Visual Compliance	
In Process	Users that have a pending Visual Compliance with no results recorded.
NCICs	
In Process	Users that have a pending NCHC (National Crime Information Check) with no results recorded.
Tiers 1, 2,4,	
Reciprocity Check	Pending Investigations awaiting a Reciprocity check
e-QIP Initiation	Users whose Reciprocity checks have been completed and awaiting e-QIP Initiation
e-QIP Certification	Users whose e-QIP Initiation date has been entered and awaiting e-QIP Certification
e-QIP Release	Users with e-QIP Certification date has been entered and pending e-QIP Submission to OPM
Investigation Results Pending	Users whose e-QIP has been submitted pending results
Adjudication	Users whose results has been received and pending Adjudication
Due Process	Users with unfavorable adjudication pursuing Due Process
Older Background Investigation (BI)	
Pending	Users that have a pending or submitted older background Investigation
Clearance Visits	
Needing Review	
Tiers 3, 5	
Reciprocity Check	Pending Investigations awaiting a Reciprocity check
Validate Reciprocity	Lists Clearance records for Civil Servants Tiers 3, 5 where Centers roles enter reciprocity awaiting Security Adjudicator approval
e-QIP Initiation	Users whose Reciprocity checks have been completed and awaiting e-QIP Initiation
e-QIP Certification	Users whose e-QIP Initiation date has been entered and awaiting e-QIP Certification
e-QIP Release	Users with e-QIP Certification date has been entered and pending e-QIP Submission to OPM
Investigation Results Pending	Users whose e-QIP has been submitted pending results
Adjudication	Users whose results has been received and pending Adjudication
Due Process	Users with unfavorable adjudication pursuing Due Process
Clearance Suspension	Records where Centers have requested a Clearance Suspension and awaiting suspension approval
DOE	
Pending	Lists all Clearance records that are assigned to the logged in user from all Centers
SCI	
Pending	Lists all Clearance records with Top Secret Eligible with a Special Sensitive Position Designation result and pending SCIs
Credential Queues	
NASA PIV Smartcards	
Initial Authorizations	Users with an "In Process" PIV Initial Smartcard request that has been sponsored but not authorized.
Investigation Queues	
Reissuance Authorizations	Users with an "In Process" PIV Reissuance Smartcard request that has been sponsored but not authorized.

Renewal Authorizations	Users with an "In Process" PIV Renewal Smartcard request that has been sponsored but not authorized.
Not Delivered	Users with an "In Process" PIV Smartcard request that has been authorized and the related CPR generated but has not been Finalized.
CPR Errors	Users have a PIV Smartcard Request that was authorized but CPR generation errors exist for the request
Agency Smart Badges	
NCHC Review Needed	Users that have a pending NCHC (National Criminal History Check) with no results recorded.
Pending Authorizations	Users with an "In Process" PIV Initial Smart Badge request that has been sponsored but not authorized.
Not Delivered	Users with an "In Process" Smart Badge request that has been authorized and the related CPR generated but has not been Finalized.
CPR Errors	Users have a PIV Smart Badge Request that was authorized but CPR generation errors exist for the request. Failed to submit properly to CMS.
Local Badge	
In Process	Users with an "In Process" Local Badge request that has been sponsored but not authorized.
Non-NASA Smartcards	
Requested	Users who have indicated that they would like to Register a non-NASA Credential

View Pending Request

To view the identities pending in the queue select the queue name. The results will display beneath the queue. You have the option to narrow the search by utilizing the filter option that is available. In this example, the IVC Approvals queue is selected, and the results are displayed.



Summary

The Summary tab provides read only information about the identity. The information includes the Status timeline (on-boarding, active, off-boarding, terminated), Identity Status, Risk Assessment, Investigations, Enrollments, IT Security Training Date, Revalidation Date, and Credentials. As stated, this tab is view only, to make changes to the information that is displayed, you can select the appropriate tab or select the folder icon located next to the section that requires modification.
In this example, the user has a Special Consideration banner indicated at the top of the screen. Any additional actions about the identity will be displayed as such.

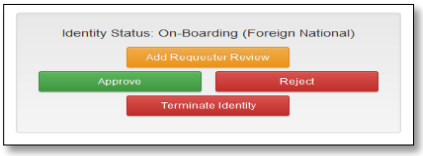
COMMENT

You can add a comment about the identity in the Summary section. Enter the comment in the space provided and click the Save Comment button. The Comment that was entered will now be available in the Comments tab.

ACTIONS

At the bottom of the Summary tab displays a series of Action buttons. The Identity Status (active, on-boarding, suspend, off-boarding, terminated) will determine which action buttons are displayed.

In this example, the Identity is in an on-boarding state and a Foreign National, so you have the ability to Add Requester Review, Approve the request, Reject the request, or terminate the Identity.



IDENTITY TAB

The *Identity* tab provides a read only view of the user's Identity information. This includes the Legal Name, Notification Information, Birth Information, Citizenship, Proof of Identity, Enrollment Photo, and Position Detail. Any information in this section that requires modification should be done by the user's Identity Requester.

RESIDENTIAL TAB

The *Residential* tab displays the identities residential information. This tab is available for modifications.

Note: *If you make changes to this section, select the Submit Changes button before moving away from the tab, failing to Submit Changes will result in the information being cleared automatically.*

FOREIGN NATIONAL TAB

The *Foreign National* tab provides the ability to update or review the identities Documentation information, complete or view the questionnaire, view pending approvals for the foreign national, add Provisos, view NAMS Visiting Center Requests, and add any comments that will be viewable in the comments tab.

Note: *If you make changes to this section, select the Submit Changes button before moving away from the tab, failing to Submit Changes will result in the information being cleared automatically.*

DOCUMENTATION

In this section you can update the Foreign National's record with the provided documentation information. Select the document type from the option and populate the document number, expiration, country, if it is a visa the visa type, begin and end date, and I-94 end date.

Note: *If you make changes to this section, select the Submit Changes button before moving away from the tab, failing to Submit Changes will result in the information being cleared automatically.*

QUESTIONNAIRE

The *questionnaire* section allows additional information to be captured about the Foreign National. The items marked with a red asterisk are required fields.

Questionnaire	
How long has the applicant lived/worked in the US?	Select the length of time the user has been in the US.
Is applicant willing to complete eQIP?	Specify if the user is willing to complete the entire background investigation process which can include completing a SF85, 85P or 86 in the OMB e-QIP system. This is required to receive the Federal PIV Badge credential.
Is this a high level protocol visit?	Specify if this user is completing a protocol visit? If yes, additional approval steps are required.
Is escort required for access to NASA Facilities?	The escort required field designates whether an Escort is required while the user is on-site at NASA facilities. If yes, the Escorts block will appear allowing for the selection of an Escort. Escorts must have the Escort Role and cannot be a terminated employee. Escorts can be added or removed as necessary. Note: The NAMS workflow entitled Foreign National Escort Waiver may be used for a foreign national to be excluded from escort requirements.
Gender	Enter the gender Male / Female of the foreign national
Is the applicant a student?	If the foreign national is a student select yes. Allows for tracking of foreign national students.
Is Guest Wireless needed?	Provide if Guest wireless access will be needed for the foreign national.
Visit Description	Provide a description of the visit that this user will be completing
Export controlled items involved in the programs/projects	Provide a listing of all export-controlled items that this user will have/need access.
Export controlled items which NASA is required to provide to applicant, per Governing Agreement and Contract	Provide a listing of Export Controlled items that NASA is required to provide to the user.
Means of Export or Transfer (include Milestones)	Provide a listing of Export or Transfer that this user will need access.
NASA facilities the applicant will be escorted to.	Provide a listing of the centers that this user will need access.
Applicant will need to work outside of named business hours (6am-6pm)	Provide a list of the users work schedule that is considered outside of named business hours.
Applicant requires access to EAR or ITAR data	Provide a listing of all EAR or ITAR data that this user will have/need access.

Applicant requires access to missile technology data or ITAR detailed design data such as Orion, Shuttle, etc. (Requires Department of State license information)	Provide a listing of all missile technology data or ITAR data this user will have / need access.

Note: *If you make changes to this section, select the Submit Changes button before moving away from the tab, failing to Submit Changes will result in the information being cleared automatically.*

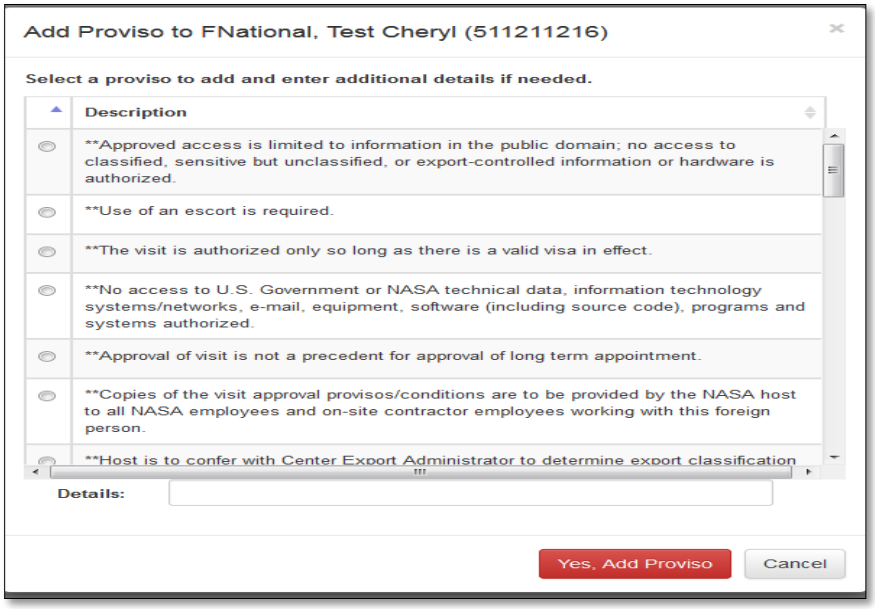
APPROVALS

The Approvals section will display any pending approvals for the Foreign National. This provides a timeline of where the Foreign National is in the approval process.

In this example, the Center Export Control, Agency Desk Officer, and Agency Export Control have approved the request and the approval date is displayed. As you can see the request is pending approval from the IVC.

PROVISOS

In this section you have the ability to add or remove Provisos to the identity record. Select the Add Proviso button to display a list of available Provisos. If additional details is required there is a space provided.



NAMS VISITING CENTER REQUESTS

Any NAMS Visiting Center Request will be displayed in this view only section. To add a visiting center, the user or someone on their behalf can submit a "Get Physical Access to other NASA Locations" Foreign National Visiting Center Access request via the NAMS tool.

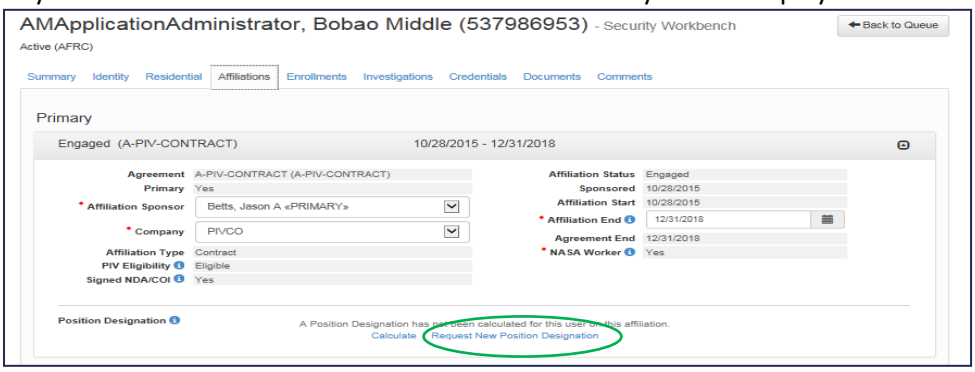
For step-by-step instructions view "The Get Physical Access to Other NASA Locations" job aid found on the ICAM portal:
https://icam.nasa.gov/documents/11201/3208558/Get+Physical+Access+to+Other+NASA+Locations.doc/

or additional information about the process can be found here:

https://icam.nasa.gov/documents/11201/3208558/Foreign+National+Visiting+Center.pdf/

AFFILIATIONS

Any Affiliation information associated with the identity will be displayed in this section.



Reminder: Required Position Designations are triggered by new NASA Worker Primary Affiliation, Security Requesting manually in the Security Workbench, or Reinvestigation Batch Job.

Position Designation Links:

- Recalculate Required-Identity Requester needs to complete PD
- Request New Position Designation-Only available to Security; sets to Recalculate Required and sends an action / email to the Identity Requester

ENROLLMENTS TAB

The *Enrollment* tab allows you the ability to view, request new, cancel, and manage enrollment data for the Identity. Enrollments are displayed (open or closed) on the page in three sections based on the Enrollment status: Pending, Complete, and Cancelled. Enrollments are triggered by Credential or Investigation events.

NEW ENROLLMENTS

When adding a new enrollment, select the *Type* from the drop-down menu option. After selecting the Type you must click the *Submit Changes* button to save the selection. You will notice the *Status* will be updated to Pending & Requested will display the date the new enrollment was initiated.

PENDING ENROLLMENTS

When an enrollment is in a Pending status and is not needed the Cancel Enrollment button will be available. This action will cancel the pending enrollment and will be displayed as a Canceled Enrollment. The following links maybe displayed as an option to the enrollment:

Connect Credentials which allows the identities credential to be selected and added to the record. The options available for that identity will be listed in the pop up.

Connect Investigations which allows the identities investigations to be selected and added to the record. The options available for that identity will be listed in the pop up.

Note: Adding additional enrollments if there is a pending one of a different type already in place, is not allowed.

INVESTIGATIONS TAB

The *Investigations* tab allows specific role holders the ability to track all clearances and investigation cases associated with a NASA Identity.

Investigation Requested: Displays the date the Investigation was initiated.

Reciprocity Check: Recording another Agency's completed Investigation in lieu of NASA conducting a background investigation of their own.

Enrollment: Enrollment Type that is tied to the record

- **Enrollment Replay:** Ability to tie a New NCHC Investigation to a Completed Enrollment
    - Select Connect Enrollment link
    - Select Resubmit to OPM or Resubmit to FBI
        - If FBI, favorable results should Complete the Enrollment and Complete the NCHC
- **Connect Enrollment:** Ability to Change Connected Enrollment
- **Change:** Ability to Modify the current Enrollment tied to the record

e-QIP Initiation: Reciprocity check has been completed and pending e-QIP initiation

e-QIP Certification: e-QIP has been initiated with NP2 Secure Portal

e-QIP Release: e-QIP Certification completed and pending e-QIP Submission to OPM

e-QIP Tracking: Help track Initiation, Certification, Rejection and Submission of an e-QIP in order to have a complete picture of User's Investigation (and for reporting purposes) e-QIP Initiation, e-QIP Certification, e-QIP Release (submission), e-QIP Rejection

e-QIP Rejection Tracking: Prior to the e-QIP Release to OPM, the PerSec Role holder can record any rejection of the e-QIP and the system will track the number of times the e-QIP has been rejected for the user

Investigation Results: Tracking the Investigation results returned from OPM

Adjudication: Favorable and unfavorable recording

Due Process Tracking: Recording Due Process start and end date as well as response

Investigation Documents: Ability to upload investigation support documentation such as e-QIP Signature pages, OF306, COI, CCT, 79A, NF1803…

Investigation Audit Log: A place to perform a quick check on activities around an Investigation record (when, what and who)

Investigation Notes: Can be added to support an Investigation. Notes are protected and can only be seen by SWB roles and only editable by owner

Record Briefing / Debriefing Dates: Record the Clearance Briefing and Debriefing dates

NCIC and NCHC Checks

- **If NCIC Favorable**, the Identity Lifecycle Status is set to "Active", LoC is set to 20 (if less than 20), IT Status is set to "Enabled" / Enablement email is sent to the Requestor and the User (if disabled).
- **If NCIC Unfavorable**, the LoC set to -10, IT Status is set to Disabled, email sent to the Requestor, the related credential request is set to "Rejected" (if applicable), and Immediate Termination is initiated (if user is enabled).
- **If NCHC Favorable**, the Identity Lifecycle Status is set to "Active", LoC is set to 30 (if less than 30), IT Status is set to "Enabled" / Enablement email is sent to the Requestor and the User (if disabled).

- **If NCHC Unfavorable**, the LoC set to -10, email sent to the Requestor, the related credential request is set to "Rejected" (if applicable), and Immediate Termination is initiated (if user is enabled).

Background Investigations (BIs)

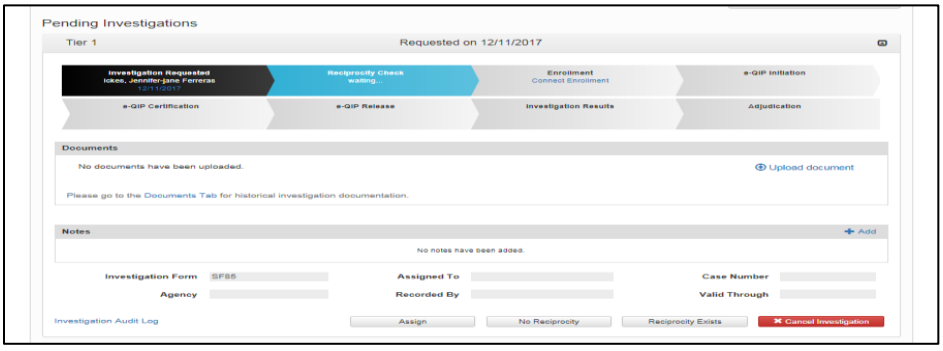
- **If (BI Favorable or Reciprocal) OR (BI Submit and NCHC Favorable)** , the Identity Lifecycle Status is set to "Active", LoC is set to 30, 40 or 50 for the related BI Type (if less than the value), IT Status is set to "Enabled" / Enablement email is sent to the Requestor and the User (if disabled).
- **If BI Unfavorable**, the LoC set to -10, email sent to the Requestor, the related credential request is set to "Rejected" (if applicable), and Immediate Termination is initiated (if user is enabled)

Investigation Types		
NCIC	Name, DOB, SSN check via federal or state tools	LoC = 20
NCHC	Fingerprint Check via federal or state tools	Loc=30
BI	Investigations will be broken out by those that will validate	LoC = 30, 40, 50, and 60
FN Check	Foreign National Check using Visual Compliance	
Investigation Status		
Pending	Investigation has not been submitted; generated by Engine or user	
Submitted	Investigation has been submitted to OPM/FBI	
Completed	Investigation has been adjudicated	
Expired	Investigation is inactive due to expiring	
Cancelled	Investigation is cancelled	

REQUEST NEW INVESTIGATION

When adding a new investigation, select the *Request New Investigation* button located on the top right of the Investigation section. Enter the Investigation *Type, BI Type, Form, Agency, Related Enrollment / Connect Enrollment, Submitted date, Completed date, and Adjudicated date.* The *Results* of the Investigation will be available for selection when the Completed date has been inputted. Select the check box *Reinvestigation is Required* for the identity, if the identity requires a reinvestigation. If the box is left unchecked, then a reinvestigation is not needed for the identity. The *Status* and *Recorded By* field will be populated by the initiator once the information has been submitted. You have the option to *Remove* the investigation from this state if the investigation is not needed.

Once the Investigation has been initiated the timeline will display the next steps for the investigation. In the example below Reciprocity Check > Enrollment (Connect Enrollment) > e-QIP Initiation > e-QIP Certification > e-QIP Release > Investigation Results > Adjudication. The timeline will remain blue until the step is completed.



Other items that are included in the Investigation tab:
Upload document- Ability to upload Investigation support documentation such as e-QIP Signature pages, OF306, COI, CCT, 79A, NF1803

Assign- Ability to assign investigation records to individuals or themselves to work on

Cancel Investigation- Ability to cancel the investigation if the investigation is not needed

Investigation Audit Log-A place to perform a quick check on activities around an Investigation record

Investigation Notes-Investigation notes can be added to support an Investigation. Notes are protected, can only be seen by SWB roles and only editable by owner

CLEARANCE PANEL

The Clearance Panel is available for Identities with Tier 3 and Tier 5 Investigations and provides the ability to capture and track the clearance data. This panel provides audit capabilities allowing traceability to users that view or makes edits to the clearance. Your role determines the amount of clearance data and fields that will be available.
PIV Authorizers / Investigation Reviewers- Read only partial Clearance data for a Civil Servant, Read and write partial Clearance data for a contractor, Record Briefing and Debriefing dates, Request for a Suspension on a Clearance Record, No access to Clearance Documents and Notes.
Special Security Representative- Read only partial Clearance data, No access to Clearance documents and notes
Security Adjudicator (CAF)-Full access to the Clearance Panel except the briefing and debriefing dates, can add Case Summary and Event logs, attach, download or delete documents on Clearance Panel, add, update, or delete notes on Clearance panel, access the Clearance Audit Log.

Sensitive Compartmented Information (SCI) Clearance / Panel

The Initiate SCI button will display when the following two criteria are met:

- User has a Top-Secret Eligible Clearance
- Position Designation results = Special Sensitive

Department Of Energy (DOE) Clearance / Panel

The Initiate DOE button will display when the following criteria are met:

- User has a provisioned Department of Energy NAMS request
- Secret or Top-Secret Eligible Clearance

Other items that are included in the Clearance Panel:

- **Upload document-** Ability to upload Clearance support documentation such as e-QIP Signature pages, OF306, CCT, 79A, NF1803,…
    - Clearance documents accessible to Security Adjudicators
    - SCI documents accessible to Security Adjudicators and Special Security Role
- **Assigned to-** Ability to assign clearance records to individuals or themselves to work on
- **Clearance Audit Log-**A place to perform a quick check on who has viewed or made changes to the clearance record
- **Clearance Notes**-Clearance notes can be added to support a Clearance. Notes are protected, can only be seen by specific role holders and only editable by the owner

CREDENTIALS TAB

REQUEST A NEW CREDENTIAL

Select the *Request Credential* button located on the top right of the Credential section to begin the request for a new credential. Select one of the following options from the drop-down menu, NASA PIV Smartcard, Agency Smart Badge, Local Badge, or Non-NASA Smartcard. Once the Credential has been selected a pop up will be displayed that allows you to select the Sponsor and Badge Type. Once the information has been added a chevron will display on the Credential tab indicating the next step in the credential process. You can cancel the request if needed when it is in a Pending Status.
Note: *Refer to Section 7 of this document for more information on the Credential Lifecycle Management.*

MARK AS DEFECTIVE

If for some reason the badge is not working properly, you can mark the active badge as defective before you Mark as Destroyed.

Conditions:

- For an ACTIVE card, if the Authorize date is less than 30 days from the current date and an Encoded date is displayed, the card can be marked as defective
- For an In-Process card, if the Bound date is displayed the button should be available to mark as defective.

DEACTIVATE

To set an Active credential to Inactive select the *Deactivate* button. Deactivating a credential is not reversible so the credential will no longer be accepted by NASA card readers and cannot be used to log in to NASA systems. Once selected the credential will be set to Inactive.

MARK AS DESTROYED

Once the credential has been set to Deactivate and is now listed as Inactive the *Mark as Destroyed* button is available. Select Mark as Destroyed when the credential has been physically destroyed. This action will provide an update to Lenel.

AUTHORIZE

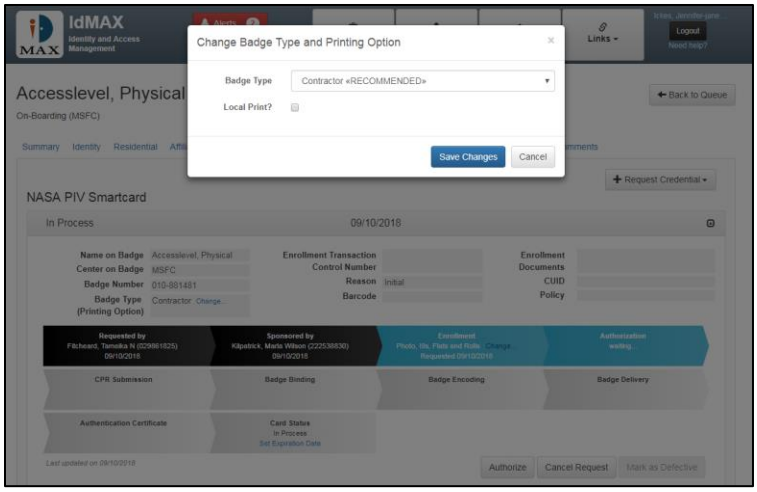
A user who has met all proofing, enrollment, and investigation requirements the Authorize button will processes the NASA PIV Smartcard, Agency Smart Badge, or Local Badge.

LOCAL PRINT

Ability to configure PIV credentials to be locally printed at the center level. By default, the following badge types will be set to Local Print.

- Reissuances
- First, Middle, Last name character count is over 24 (to long)
- Face to Face
- Astronaut-Foreign National (FN)
- Astronaut-US

To add or change the Printing option, select the *Change* link located in the Badge Type section of the In-Process credential request.



Set Expiration Date

By default the expiration date for a credential is set for 60 months after activation if the credential needs to expire prior to the 60 days you can manually set the date by selecting the Set Expiration Date link located in the Card Status block of the In Process timeline.

Documents Tab

The Documents section allow you to add documents that pertain to the identity. All Identity & Credential role holders (Identity Requester, Affiliation Sponsor, Identity Support, Agreement Maintainer, ICAM Support, Authorizer, Investigation Reviewer, IVC, Enrollment Official, Identity Secure View Only, Center Export Control, Agency Export Control, Agency Desk Officer, Counterintelligence Officer, Suitability Agent) have the ability to view Identity Proofing documents in their various tools, and all documents uploaded by the user via the Document Upload web tool. To add a document, select the Add Document button located in the top right corner of the Documents section.

Add a Document

Add the *Document Description*, Select the *Document Type* of the drop-down menu selection. Click the *Add file* button to search for the document. Once added, click the *Upload File* button to add the document to the identity record.

Delete a Document

To remove a document that is listed, select the *Delete* button next to the document that you want removed, a pop up will display verifying that you are sure you want to delete the document. Select *Yes, delete document* button and the document will be removed.

Comments Tab

Any comments that have been added will be displayed in the Comments tab. You will notice that a comments bar is located on each tab but will only be displayed in this section. To add a comment, select the Add Comments button located on the top right corner of the Comments tab. The comments box will highlight blue allowing you to add a comment. Click the Save Comment button to save the changes made.

Note: *If you make changes to this section, select the Submit Changes button before moving away from the tab, failing to Submit Changes will result in the information being cleared automatically.*

9. Suspension Lifecycle

You can create and manage a suspension activity for an identity that is in an active state. The Suspend Identity button is located at the bottom of the Identity record on the Security Workbench.

Note: Users will not receive any system notifications when they are suspended. The groups suspending should coordinate appropriate user communications.

SUSPEND IDENTITY

To initiate a suspend activity, on the Summary tab of the Identity record, select the *Suspend Identity* button. A pop up will display the following:

Suspend Physical Access- Blocks access to all buildings. The user's badge will be denied by all NASA card readers

Suspend Logic (IT) Access- Blocks access to all NASA's NED and NCAD password protected systems. The user will also not be able to log in with their Smartcard and will not be able to access SATERN.

Suspend NCAD Access Only - Blocks access to NASA's NCAD password protected systems, but not NED password protected systems. The user will not have access to their desktop, but will be able to connect to id.nasa.gov, SATERN, etc remotely via the internet.

A list of Suspension Types and Reasons are listed below:

Suspension Type	Reason
IT-NCAD Only	IT Security Non-Compliance
IT-Full	IT Security Non-Compliance
IT- Full Physical	IT Security Non-Compliance
IT-NCAD Only Physical	IT Security Non-Compliance
Physical	IT Security Non-Compliance
IT-Full	Leave of Absence
IT-Full	PSO Action
IT-Full	Unknown
IT-Full	SOC Monitoring
IT-NCAD Only	Rules of Behaviors

Suspension Owner-The user that is initiating the Suspension activity. Click Change to change the owner.

Automatic Reinstate- If yes is selected, you will be required to enter an Automatic Reinstatement Date. If no is selected, you will be required to enter an Automatic Termination Date.

- **Automatic Reinstatement Date -** The account will automatically be reinstated on the date that is entered.

- **Automatic Termination Date -** The account will automatically be terminated on the date that is entered.

Suspension Begin Date- Enter the date in which the suspension will begin. The user will automatically be suspended on this date.

PIV Smartcard being held by Center Security- Check the box if Center Security is in position of the PIV Smartcard.

Suspension Reason-Justification of why the Identity is being suspended. **Note:** When an Identity has been suspended a note will be added to the top of the Identity Record.

Reinstate Suspended User

To Reinstate the Suspended User, on the Summary tab of the Identity record, select the *Edit Suspension* button. A pop up will display the following:

Enter a Reinstatement Reason and Select the *Reinstate This User* button. The Identity is now reinstated, and a new Action button labeled *View Suspension* is available.

Note: Security (Authorizers, IVCs, Enrollment Officials, Investigation Reviewers, and IT Security Personnel can Reinstate a Suspended User.

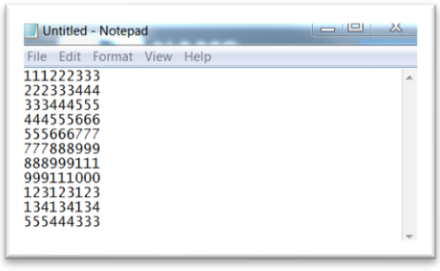
Manage Identity Suspension Tool

This tool is designed to assist the Center Information Security personal with the management of the suspension process. The Manage Identity Suspension Link will be located under the Center Information Security header on your console page. You have the ability to search for the Identity, process or modify a Suspension Request. Refer to the Manage Identity Suspension Tool Job-Aid located on the ICAM portal for detailed instructions on how to use this tool.

Identity Suspension-Bulk

This tool is designed to allow Security personnel to initiate Suspensions for a group of employees. The tool allows you to upload a file that has a simple text file with one user UUPIC per line with a limit of 100 UUPICs. Once submitted the identities will be suspended according to the data that is entered.

An example of user UUPICs per line:



NOTE: Items that are marked with a red asterisk are required fields.

To use the tool, enter the type of Suspension (Physical, IT Access, NCAD Access) the Suspension Owner, Suspension Begin Date, automatic Reinstatement Date, Suspension Reason, Browse for the

file you have created with the uupics, Upload the file, and then select the Submit UUPICs button to process the Suspension.

10. International Visitor Coordinator (IVC) Workbench

To access the IVC the user must have the International Visitor Coordinator Agency ICAM Infrastructure role. You must complete the required SATERN course prior to requesting for a role in NAMS. When your NAMS request has been approved, a link on the NAMS console page will display the IVC Workbench. As an IVC

As an IVC, you also can access various tools within IdMAX. These tools include the Change Agency User ID (AUID), Delete Duplicate Identity, Denied Access Report, Identity Audit Viewer, Identity Suspension-Bulk and Identity Suspension Reinstate-Bulk. Your capabilities include changing an asset availability, suspending an identity, as well as completing immediate termination and submitting termination approvals.

A description of the role and assigned responsibilities are outline in the following table:

Role	Role Description
International Visitor Coordinator	Reviews the Foreign National request, perform a Foreign National Check to an existing completed background investigation that meets the Agency's reciprocity requirements, and ensure that Export Control requirements are approved before authorizing the Foreign National request

QUEUES

The queues provide a list and count of identities in various states in the vetting and proofing process. Queues provide a quick way to identify which items are pending an action.

Queue Name	Description
Annual Review	Foreign Nationals who's last IVC approval is greater than 365 days
Affiliation Changes	Users that have a pending Designated Country Affiliation Change with no results recorded.
Visual Compliance	Users that have a pending Visual Compliance with no results recorded.
All On-Boarding	Requested Foreign National users that are not yet enabled with an Identity Status of On-Boarding. They may be awaiting sponsorship, Visual Compliance, or Foreign National approvals.
Identities On-Boarding	Users that have been "requested" but not yet enabled with an Identity Status of On-Boarding. They may be awaiting sponsorship, enrollment or investigations.
IVC Approvals	Users that have a pending IVC Approval. The Center Export Control, Agency Export Control and Agency Desk Officer approvals have been completed as appropriate.
NCHCs (Temp or Local Badge)	Users that have a pending NCHC (National Criminal History Check) with no results recorded.
Review Needed	
Transmission errors	
NCICs (IT Only)	Users that have a pending NCHC (National Crime Information Check) with no results recorded.
SAVE Checks Pending	User with a Pending SAVE check

Refer to Section 8-Security Workbench in this handbook for details on viewing pending request and information regarding the various tabs.

ACTIONS

At the bottom of the Summary tab displays a series of Action buttons. The Identity Status (active, on-boarding, suspend, off-boarding, terminated) will determine which action buttons are displayed.

In this example, the Identity is in an on-boarding state and a Foreign National so you have the ability to Add Requester Review, Approve the request, Reject the request, or terminate the Identity.

Foreign National Specific Actions

Additional Actions are available in the Security Workbench for Foreign National Identity handling by the International Visit Coordinator. This includes:

On-boarding
Route for Approvals
Add Requester Review
Remove Requester Review
Approve
Reject

Active Identity
Approve (Once other approvals are complete)
Reject
Suspend Identity
Edit Suspension
Terminate Identity
Initiate Off-Cycle Approval
Add Requester Review

Note: The system automatically initiates off-cycle reviews for Affiliation Updates for Designated Country related Foreign Nationals.

11. Termination Lifecycle

As Security personnel or Identity Requeter you can initiate an Immediate Termination without cause for any On-boarding or Active/Suspended Identity using the Terminate Identity action button located in the Security Workbench.

You also have the option to initiate an Immediate Termination with Cause for any On-boarding or Active / Suspended Identity using the Terminate Identity action button located in the Security Workbench.

Identity	Termination Lifecycle Process
Foreign National	Terminate immediately on end date
NASA	Terminate 60 days after end date

Cancel Termination

As Security you can cancel a Termination Request for an Off-Boarding Identity using the Cancel Termination button in the Security Workbench and the identity is updated to an Active status.

Roll-back Terminated User

As Security you can cancel a Termination Request for an Off-Boarding Identity using the Rollback Identity button in the Security Workbench and the identity is set to an Active status.

Future Date

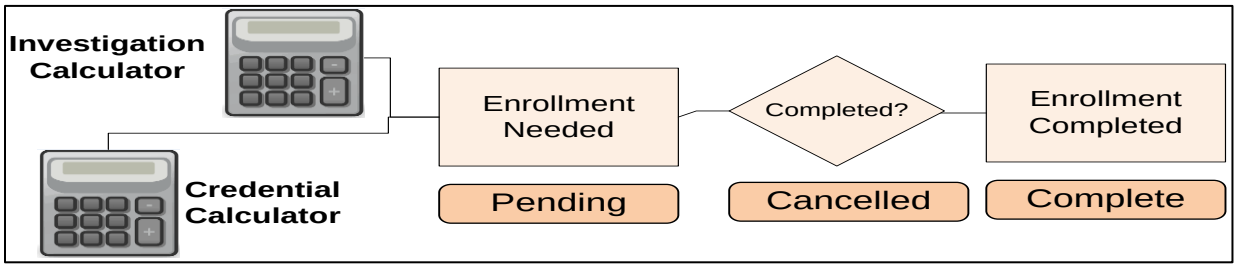
As Security you can approve a future date Termination Request for an Off-Boarding Identity using the Approve Termination button in the Security Workbench and the Identity is set to an Off-Boarding Status.

Approve Termination

As Security you can approve a past dated or current dated Termination Request for an Off-Boarding identity using the Approve Termination button in the Security Workbench and the Identity is updated to a Terminated status.

12. Enrollment Official Workbench

The *Enrollment Official Workbench* allows Enrollment Officials the ability to view, request new, cancel, and manage enrollment data for the Identity. Enrollments are triggered by Credential or Investigation events.

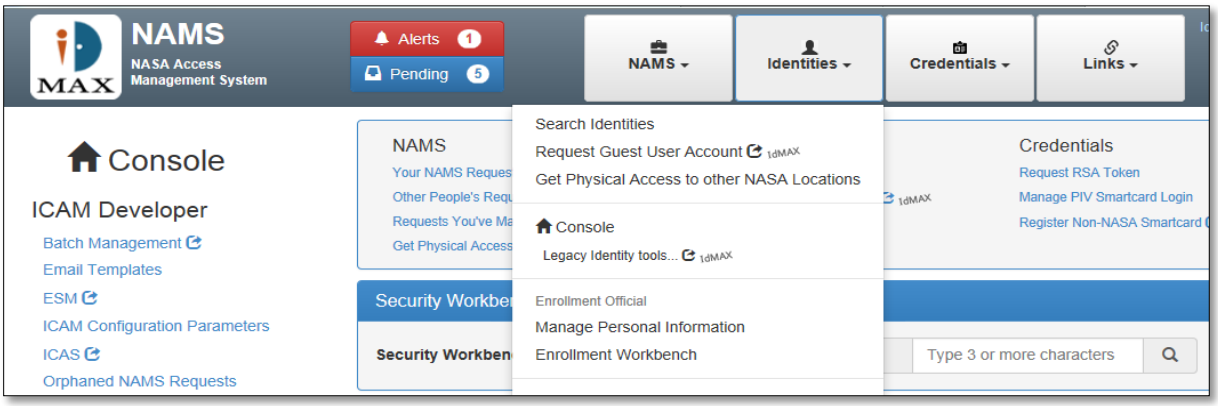


Access to Enrollment Workbench- Roles

To access the Enrollment Workbench the user must have the following Agency ICAM Infrastructure role, Enrollment Official. You must complete the required SATERN course prior to requesting for a role in NAMS. When your NAMS request has been approved, a link on the NAMS console page will display the Enrollment Workbench.

A description of these roles and assigned responsibilities are outline in the following table:

Role	Role Description
Enrollment Official	Validates the identity and captures identity information and biometrics.



a. In this example, Enrollment Workbench is listed under the Identities tab.
b. Click the link to open the Enrollment Workbench

Individual Search

You can search for a specific Identity using the Individual Search feature. To begin a Search enter either the persons, First and Last Name, UUPIC, or click advanced to search by SSN, Center, AUID, First

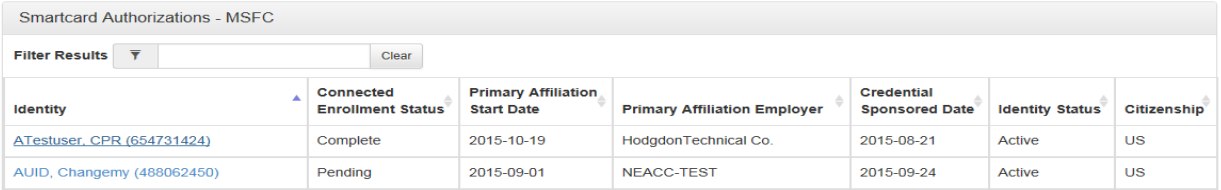
Name, Middle, Last Name, Org Code, Agreement, Company, Identity Status, Email, FNMS ID, Citizenship, or Birth Country. Results will display allowing you to select the record you would like to review.

QUEUES

The *Queues* provide a list and count of identities in various states in the vetting and proofing process. Queues provide a quick way to identify which items are pending an action.

Identity Queues	
Enrollments Pending	Users with an Enrollment that has a Pending Status.
Credential Queues	
NASA PIV Smartcards	
Initial Authorizations	Users with an "In Process" PIV Initial Smartcard request that has been sponsored but not authorized.
Reissuance Authorizations	Users with an "In Process" PIV Reissuance Smartcard request that has been sponsored but not authorized.
Renewal Authorizations	Users with an "In Process" PIV Renewal Smartcard request that has been sponsored but not authorized.
Not Delivered	Users with an "In Process" PIV Smartcard request that has been authorized and the related CPR generated but has not been Finalized.
CPR Errors	Users have a PIV Smartcard Request that was authorized but CPR generation errors exist for the request
Agency Smart Badges	
NCHC Review Needed	Users that have a pending NCHC (National Criminal History Check) with no results recorded.
Pending Authorizations	Users with an "In Process" PIV Initial Smart Badge request that has been sponsored but not authorized.
Not Delivered	Users with an "In Process" Smart Badge request that has been authorized and the related CPR generated but has not been Finalized.
CPR Errors	Users have a PIV Smart Badge Request that was authorized but CPR generation errors exist for the request. Failed to submit properly to CMS.
Local Badge	
In Process	Users with an "In Process" Local Badge request that has been sponsored but not authorized.
Non-NASA Smartcards	
Requested	Users who have indicated that they would like to Register a non-NASA Credential

To view the identities pending in the queue select the queue name. The results will display beneath the queue. You have the option to narrow the search by utilizing the filter option that is available. In this example, the Smartcard Authorizations queue is selected, and the results are displayed.



Identity Information-Tabs

The Summary, Identity, Residential, Affiliations, and Investigations Tabs provides read only information about the identity. The Summary tab includes the Status timeline (on-boarding, active, off-boarding, terminated), Identity Status, Risk Assessment, Investigations, Enrollments, and Credentials. You can select the folder icon located next to the Credentials or Enrollments that is available for modification.

Comment

You can add a comment about the identity in the Summary section. Enter the comment in the space provided and click the Save Comment button. The Comment that was entered will now be available in the Comments tab.

Enrollments Tab

As an Enrollment Official you have the ability to manage Enrollments for an identity.

New Enrollments (Request New Enrollment)

When adding a new enrollment, select the Request Enrollment action button to display the enrollment form. Select the enrollment *Type* from the drop-down menu option. After selecting the Type, you must click the *Submit Changes* button to save the selection. You will notice the *Status* will be updated to Pending & Requested will display the date the new enrollment was initiated.

Modify Enrollments

When an enrollment is in a pending state you will have the option to modify the enrollment *Type* you must click the *Submit Changes* button to save the selection.

Pending Enrollments

When an enrollment is in a Pending status and is not needed the Cancel Enrollment button will be available. This action will cancel the pending enrollment and will be displayed as a Canceled Enrollment.

Expire Enrollment

When an enrollment is in a completed status and is not needed the Expire Enrollment button will be available. This action will cancel the enrollment and will be displayed as Expired. This action will drive the Level of Confidence (LOC).

Unexpire an Enrollment

When an enrollment is in an expired status and is within the 6 months of the Expiration Date the Unexpire Enrollment button will be available. This action will remove the expiration date and change the status to Complete.

External Enrollment

This option provides the ability to mark an enrollment as Complete when a paper enrollment / fingerprint is used. The complete Enrollment button has been added to an Enrollment that is an External Enrollment. This action will change the enrollment status to complete.

Connected Credentials

This option allows a credential to be selected and added to the record. The options available for that identity will be listed in the pop up.

Connected Investigations

This option allows an investigation to be selected and added to the record. The options available for that identity will be listed in the pop up.

Credentials Tab

You can manage Credentials for an identity via the Credential Tab on the Enrollment Workbench.

Request a New Credential

Select the *Request Credential* button located on the top right of the Credential section to begin the request for a new credential. Select one of the following options from the drop-down menu, PIV Smartcard, Local Badge, or Registered Credential. After the Credential has been selected a pop up will be displayed that allows you to select the Sponsor and Badge Type. Once the information has been added a chevron will display on the Credential tab indicating the next step in the credential process.

Cancel an In-Process Credential

When a Credential is in an In-Process status and is not needed the *Cancel Request* button will be available. This action will cancel the pending Credential and will be displayed as a Canceled request.

In-Process Credential

When the status of the Credential is In-Process the *Change* Enrollments link will be available on the timeline. This option allows an Enrollment to be selected and added to the record. The options available for that identity will be listed in the pop up.

Deactivate Credential

To set an Active credential to Inactive select the *Deactivate* button. Deactivating a credential is not reversible so the credential will no longer be accepted by NASA card readers and cannot be used to log in to NASA systems. Once selected the credential will be set to Inactive.

Mark as Defective

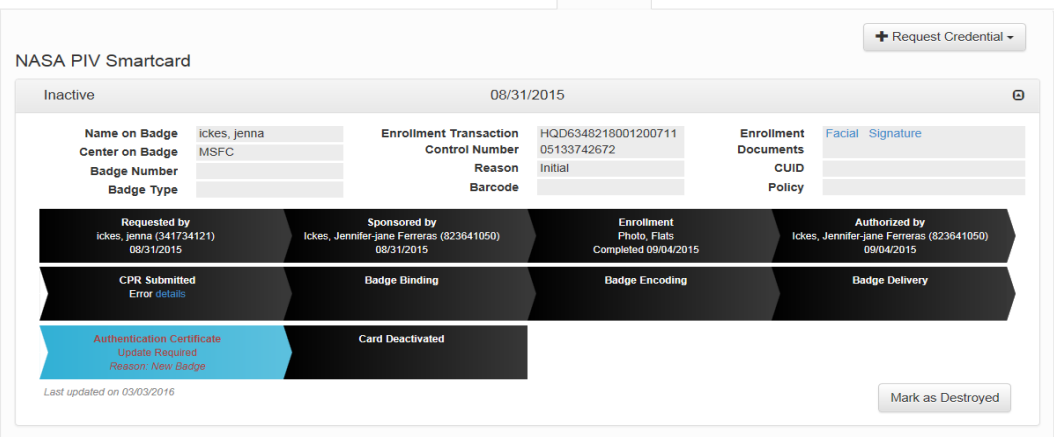
If for some reason the badge is not working properly, you can mark the active badge as defective before you Mark as Destroyed.

Conditions:

- For an ACTIVE card, if the Authorize date is less than 30 days from the current date and an Encoded date is displayed, the card can be marked as defective
- For an In-Process card, if the Bound date is displayed the button should be available to mark as defective.

Mark as Destroyed

Once the credential has been set to Deactivate and is now listed as Inactive the *Mark as Destroyed* button is available. Select Mark as Destroyed when the credential has been physically destroyed. This action will provide an update to Lenel.



SYNCH ACCESS LEVELS

Resynch Lenel Access button is displayed in the Identity Status box of the Identity Summary page when a provisioned physical access level asset is present. Selecting the Synch button will trigger the Synch Lenel Badge Access Levels modal, access levels in Lenel are synched for the user and the synchronized Lenel access levels are written to all badges assigned to the user.

DOCUMENTS TAB

The Documents section allow you to add documents that pertain to the identity. To add a document, select the Add Document button located in the top right corner of the Documents section.

ADD A DOCUMENT

Add the *Document Description*, Select the *Document Type* of the drop-down menu selection. Click the *Add file* button to search for the document. Once added, click the *Upload File* button to add the document to the identity record.

DELETE A DOCUMENT

To remove a document that is listed, select the *Delete* button next to the document that you want removed, a pop up will display verifying that you are sure you want to delete the document. Select *Yes, delete document* button and the document will be removed.

COMMENTS TAB

Any comments that have been added will be displayed in the Comments tab. You will notice that a comments bar is located on each tab but will only be displayed in this section. To add a comment, select the Add Comments button located on the top right corner of the Comments tab. The comments box will highlight blue allowing you to add a comment. Click the Save Comment button to save the changes made.

Note: *If you make changes to this section, select the Submit Changes button before moving away from the tab, failing to Submit Changes will result in the information being cleared automatically.*

Note: Refer to Section 4 of this document for more information on the Credential Lifecycle Management.

13. Foreign National Workbench:

The *Foreign National Workbench* allows Agency Desk Officers, Agency Export Control, and Center Export Control the ability to ensure that the correct data has been entered into the system and that the Foreign National check has been completed.

Access to Foreign National Workbench- Roles

To access the Foreign National Workbench the user must have the following Agency ICAM Infrastructure role, Agency Desk Officer, Agency Export Control, or Center Export Control. You must complete the required SATERN course prior to requesting for a role in NAMS. When your NAMS request has been approved, a link on the NAMS console page will display the Foreign National Workbench.

Note: Refer to the Foreign National Approver Job Aid located on the ICAM portal: https://icam.nasa.gov/documents/11201/3202477/Foreign+National+Approver.pdf/ for step by step instructions on the how to use the Foreign National Workbench.

Access Control Plan (ACP) Tool (ACP Maintainers)

As an ACP Maintainer, you have the ability to create a new Access Control Plan, Update an ACP to include adding assets, remove assets, and de-activate an ACP.

The access control plan is a grouping of NASA assets, both physical and logical, which can be assigned to a person. This assignment allows the person to request access that has been pre-approved by export control authority which greatly expedites the provisioning process. Access control plans are primarily used for foreign national access management.

The ACP is a centralized management of approved access for foreign national management. It is an agency process which allows for centralized auditing, control, and reporting. It also allows fast and accurate reporting of what a foreign national can have access to against what they actually have access to, all within one easy to use system. The ACP replaces any current center processes, specifically the technology transfer control plan, referred to as the TTCP.

The ACP does not automatically grant any access to a person, it only allows the foreign national the opportunity to request access to assets within their ACP and not need additional export control review. The application owners must still approve the request for access as they do for all requests.

An ACP can be assigned to multiple people and a person can have multiple ACPs, dependent on their affiliation requirements with NASA. If a foreign national requests access to an asset outside of their ACP, additional export control approvals must be obtained prior to asset approval.

At this time, the ACP tool is designed for planning and build out of your center ACPs that are appropriate for your missions. With the ICAM modernization final release later in 2016, you will have the capability to then assign the ACP to a person.

To access the ACP tool, visit nams.nasa.gov, search for the ICAM Infrastructure asset and within that asset, request the ACP Maintainer role.

Note: The Access Control Plan at each facility should address all measures and procedures in place to prevent access to controlled technology at that facility. There must be access controls documented for every entry identified on the controlled technology inventory, including EAR 99. The Access Control Plan must demonstrate that the facility has instituted sufficient measures and procedures to assure full compliance with the EAR; however, each facility has some flexibility to prepare its plan based on the particular circumstances at that facility.

Search for existing ACPs

As an ACP Maintainer you have the ability to Search for an existing ACP using the ACP Search screen. You can begin a search via Title, Center, and Status. The results will include ACP Title, Availability (Center Only versus Agency), Description, included NAMS Assets, Center, and Status.

New ACP

As an ACP Maintainer you have the ability to add a new ACP via the ACP Tool. Select the New ACP button and enter the required fields for a new ACP: Title, Status (default is Active), Center (default to user's Center), Designation (default is Designated Only). You have the option to add a description and non-NAMS Access details in the text fields provided.

Modify Existing ACP

As an ACP Maintainer you have the ability to modify an existing ACP via the ACP Search Screen. Select an existing ACP and click the Edit view. You can modify the Title, Description, Non-NAMS Access Details from this view. Save the changes once completed modifying the ACP.

Clone Existing ACP

As an ACP Maintainer you have the ability to Clone an Existing ACP by clicking the Clone button. This allows you to make a copy of an existing ACP that you can modify to meet your criteria.

Add Foreign National to Acp

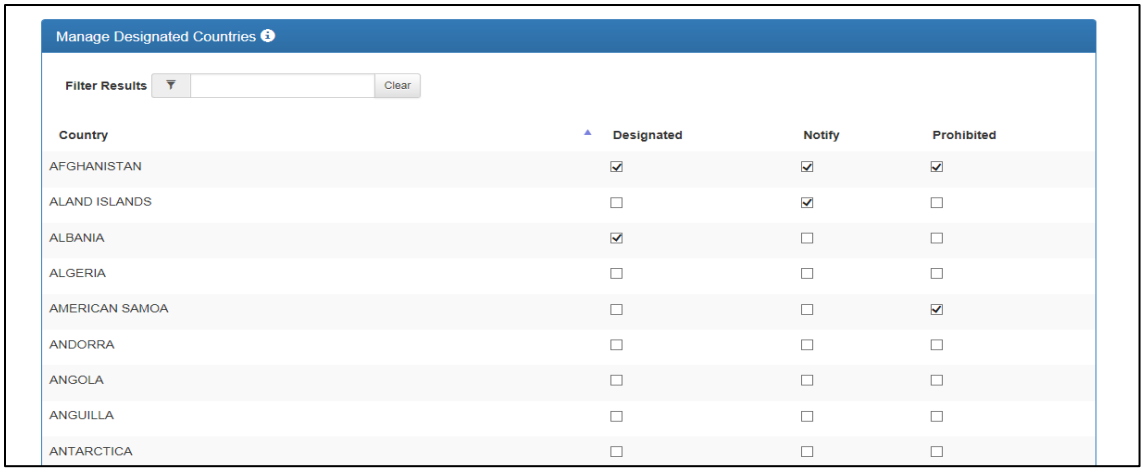
As an ACP Maintainer you have the ability to manage the users listed on the ACP as well as add an ACP relationship to an Agreement by selecting the "Manage Foreign Nationals" button. Here you have the option click the "Add Foreign National" to add a specific user to the ACP or you can click the "Add by Agreement" button to add a specific agreement to the ACP.

Add a Document to an ACP

As an ACP Maintainer you have the ability to manage documents on an Access Control Plan. Documents that are attached to an ACP should be non-sensitive, less than 5 MB, and only .doc, .docx, .xls, .xlsx, .pdf, .jpg, and .jpeg files are allowed. To add or remove a document, search for the ACP via the ACP Maintainer Tool. Select the "Documents" button located on the ACP. Select the Upload Document button to add the document or Remove to delete a document. Once you have uploaded the file the Documents button will indicate that a document has been added to this ACP. You can also view the "How to Add a Document to an ACP" job aid located on the ICAM portal for step-by-step instructions.

Manage Designated Countries (Agency Export control / counterintelligence Officer)

As an Agency Export Control officer you have the ability to maintain NASA's designated country listing for identity proofing and access control workflows within IdMAX. This list of Designated Countries is a compilation of countries with which the United States has no diplomatic relations, countries determined by Department of State to support terrorism, countries under Sanction or Embargo by the United States and countries of Missile Technology Concern. Foreign National visitors to NASA from these countries require approval by the Headquarters International Visit Coordinator. All NASA mail to these countries require the concurrence of the Headquarters Office of External Relations, in accordance with NPR 1450. 10D, NASA Correspondence Management and Communications Standards and Style, Appendix D.



The tool allows you to insert a check mark indicating the country is Designated, Notify, or Prohibited. If the country is left unchecked then it is not considered as a designated country.

Field Name	Definition
Designated	Country has no diplomatic relations with the United States
Notify	Used for Foreign Travel Reporting- if the user travels to this country a notification email will be sent to the Security Adjudicators (CAF)
Prohibited	Used for Foreign Travel Reporting- if the user travels to this country a notification email will be sent to the Security Adjudicators (CAF) and Counterintelligence Officers

Manage Foreign National Proviso (Agency Desk Officer, Export Control)

As an Agency Desk Officer, Agency Export Control, or Center Export Control you have the ability to add a new or maintain an existing Foreign National Proviso. Provisos are standard clauses that impose a qualification, condition or restriction for a Foreign National during their affiliation with NASA.

Add New Proviso

To add a new Proviso, click the ***Add Proviso*** button at the bottom of the current list. A pop up box will be displayed. Add a ***Description*** for the new proviso and set the ***Status*** to either Active or Inactive. When you are satisfied with the information added click the ***Add Proviso*** button to save to create the new proviso.

To modify an existing Proviso, select the edit button located next to the Status of the Proviso. A pop will display allowing you to make the necessary changes.

14. Workbench Lite

The *Workbench Lite* allows Center Information Security role holders the ability to assist with completing Suspensions, Change Asset Availability (if no provisioned assets of that type), and Request a Credential. The Workbench Lite has non-Security View of the identity records.

Access to Workbench Lite- Role

To access the Workbench Lite the user must have the following Agency ICAM Infrastructure role, Center Information Security. You must complete the required SATERN course prior to requesting for a role in NAMS. When your NAMS request has been approved, a link on the NAMS console page will display the Center Information Security / Workbench Lite / Identity Suspension-Bulk / Identity Suspension Reinstate-Bulk.

15. Tools & Tips

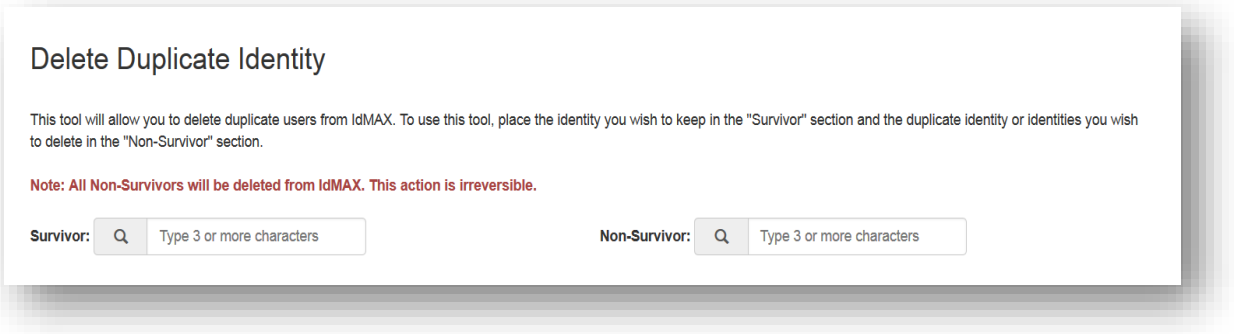
Tool Name	Available To	Description
Maintain Identity Invitations	Identity Requesters	View and modify in-process identity invitations to potential on-boarding identities.
Credential Registration (In-Person)	Security, Enrollment Officials	Capture a non-NASA PIV card for enablement and access at NASA using the Registered Credential
Delete Duplicate Identity	Security	Merge duplicate identity records by identifying survivor and non-survivor UUPIC.
Terminate Employee Bulk	Security	Initiate terminations for a list of UUPICs.
Cardstock Workbench	Cardstock Manager	Allows Cardstock Managers to order cardstock for their center, they can also provide the status of a card.
Change AUID Tool	Security	Allows an ICAM Administrator to change a user's AUID and submits a new CPR.
Identity Suspension Bulk	Security	Initiate Suspension for a list of UUPICs.
Manage Personal Info	Identity Requesters, Security	Modify a user's personal information on their behalf.
Manage Names / Email	Postmasters	Manage Common Names and email related attributes
Manage Civil Servants Investigations	Suitability Agents	Add and modify Investigations for Civil Servants

Manage Civil Servant Sponsors	Suitability Agents, Security	Manage Civil Servant Sponsor designation at center level
Destroy Badges	Security, Enrollment Officials	Destroy a group of badges via selection of Inactive Badges. (Dependent on Lenel 7.0 Upgrade)
NAMS Audit Viewer	Security, Agreement Maintainers, Help Desk Support, Identity Secure View Only	View non-NAMS and non-identity specific audits for Email, Agreements, and Access Control Plans.
ICAV (ICAM Central Audit Viewer)	Security, Identity Secure View Only	View Identity and Credential data audits.
Denied Access Report	Secure Roles	Listing with picture of all uses with LoC = -10.
User Administration	ICAM Developer	Tool utilized by ICAM Developer role holders for operational support. Mirrors data table lay-outs with limited UI validations but updates captured in Audit log. Includes the Sync User Certificate action, which retrieve Certificate from NOCA and syncs the user's ASI in NED and 3 accounts in Active Directory as applicable.
Manage Certificate Toolkit	ICAM Developer	Compilation of JSP Tools used for PIV Credential and Certificate development and operational Support.
Identity Summary Report	Secure Roles	One page view of a single identity for printing needs
Manage Guest Users	All IdMAX users	Ability to create a Guest Identity lite record for defined guest services
Create Invitational Traveler	Invitational Travel Coordinator	Custom method to create a Guest Identity record and NAMS request for a Traveler account in the travel system
Record Counterintelligence Reviews	Counterintelligence Officer	View version of Identity information with the ability to 'Mark as Reviewed' and will capture the CI Officer Name and Date
Active Directory User Maintenance Tool	NCAD Admin	ADUMT (Active Directory User Management Tool) is a restricted tool used to provision and de-provision the AGCY0012 Active Directory Basic Account, AGCY0025 Active Directory Resource Admin Account , AGCY0026 NOMAD Exchange Mailbox assets bypassing the approval workflow. It also can be used to assign and un-assign the AGCY0032 Active Directory Generic Account and AGCY0031 Active Directory Service Account Assets.
Identity Update-Bulk	Security	Ability to modify list of UUPICs with attribute name, attribute value
Manage X500 UID	AAO Security	Ability to Generate X500 UID for identities.

		X500UID (A): User ID carried over from the legacy X.500 systems. This user id is used primarily by IEMP financial systems. The Manage X500 ID tool generates an ID by combining the 2-digit center code with a 9-digit uupic (example – MS123456789), so all X500 IDs generated by the tool have 11 characters. There are also other ways to generate X500 IDs outside the tool – Center Locator files, Center Business Information NAMS Workflow (none currently configured), through direct LDAP browser updates, or ICAM Support using the User Admin Tool.
Manage Identity Suspensions	Center Information Security	Ability to submit suspensions for identities
Building Maintainer	Building Manager	Ability to manage building and rooms within the database.
Bot Enrollment	PIV Authorizer	Ability to complete an enrollment event for a non-human identity (Bot) to meet system needs for credential request (Automate- NCHC – Waived if Primary Affiliation = Non Human)
Foreign National Visitor Workbench	FN Visitor Requester (ASB / PIV card Holders)	Ability to Create / Manage a Foreign National Visitor Request.

Delete Duplicate User (Security Personnel)

The Delete Duplicate user tool is available to Security Personnel that need to delete multiple identity records for the same user in IdMAX. The tool will allow you to select the "Survivor" identity (the record you want to keep) and delete any duplicate identity or identities in the "Non-Survivor" section.
NOTE: All Non-Survivors will be deleted from IdMAX and the action is irreversible



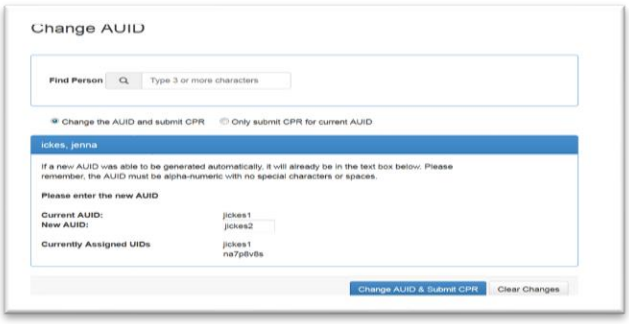
Change AUID (Agency User ID)

The Change AUID tool is intended to be used when an employee has changed their name and would like for their AUID (Agency User ID) to be changed as well.

To use the tool, search for the user that requires an auid change, enter a new auid and select either, “Change the AUID and submit CPR” or “Only submit CPR for current AUID”

- Change the AUID and submit CPR- This process will change the user’s current auid and submits a CPR
- Only submit CPR for current AUID-This process will only submit a CPR

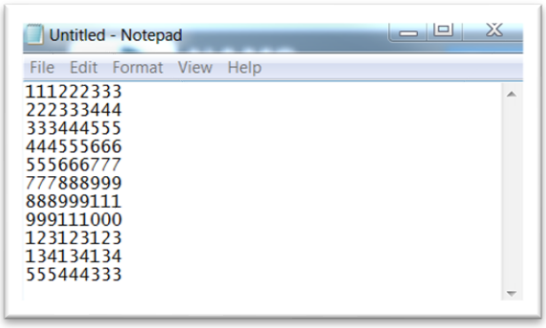
Note: A CPR is required to update the AUID on the badge.



Bulk Employee Termination (Security Personnel)

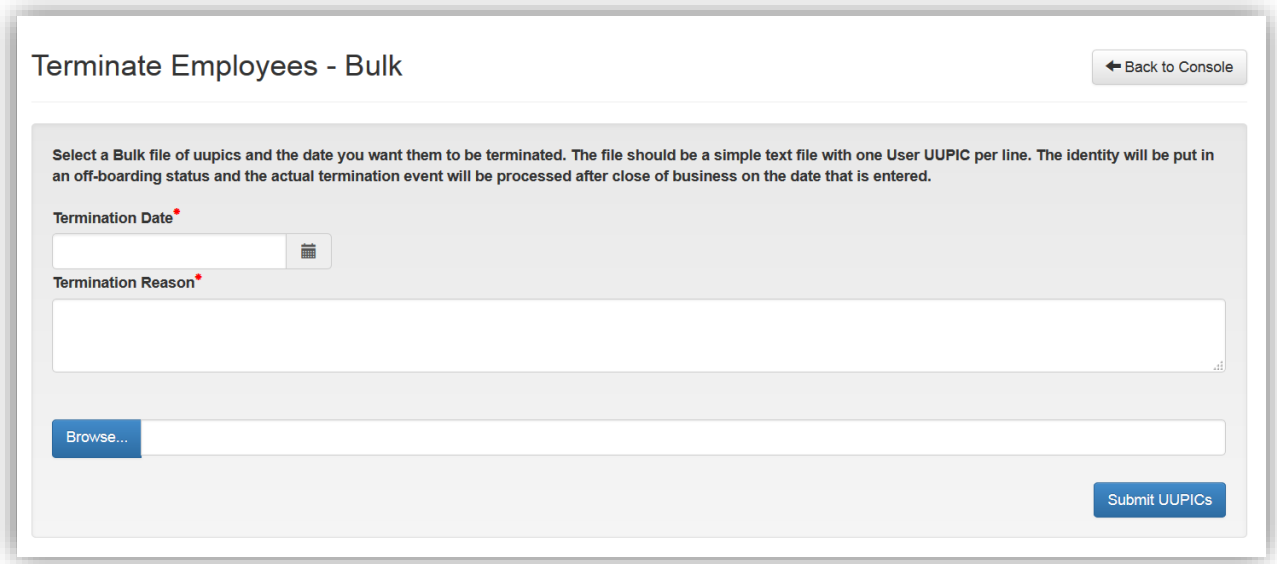
The Bulk Employee Termination tool is available to Security Personnel that need to initiate terminations for a group of employees. The tool allows you to upload a file that has a simple text file with one user UUPIC per line. Once submitted the user will be put in an off-boarding status and the actual termination event will be processed after close of business on the date that is entered.

An example of user UUPICs per line:



NOTE: Items that are marked with a red asterisk are required fields.

To use the tool, enter the Termination Date, Termination Reason, Browse for the file you have created with the uupics, Upload the file, and then select the Submit UUPICs button to process the termination.



View Identity

The View Identity tool (previously known as Identity Status Viewer) is available to all IdMAX role holders from the Search Identities quick link in NAMS. To protect personal information this tool will display either a "Sensitive Version" or a "Non-Sensitive Version".
NOTE: The role that you hold in IdMAX will drive the version you are displayed.

Secure role holders such as, Authorizer, Investigation Reviewer, IVC, Foreign National Approvers, Identity Secure View Only, Enrollment Official, Counterintelligence Officers, Suitability Agent and Identity Requester (Associated Identities/you are listed as the Identity Requester) will see the Sensitive Version. This version will display all tabs in the tool and you will see all sensitive information.

Non-Secure role holders such as, Identity Requester (non-associated Identities/you are not listed as their Identity Requester), Affiliation Sponsor, Identity Support View Only, Agreement Maintainer, ICAM Support/Help Desk role holders will see the Non-Sensitive version. This version will include the Summary, Affiliation, Foreign National, Enrollment, Credential and Documents tabs with some sensitive information retracted.

Non-Identity role holders will see the Non-Sensitive version of their own Identity record only (this includes NAMS Roles, Invitational Traveler Coordinator, Postmaster)

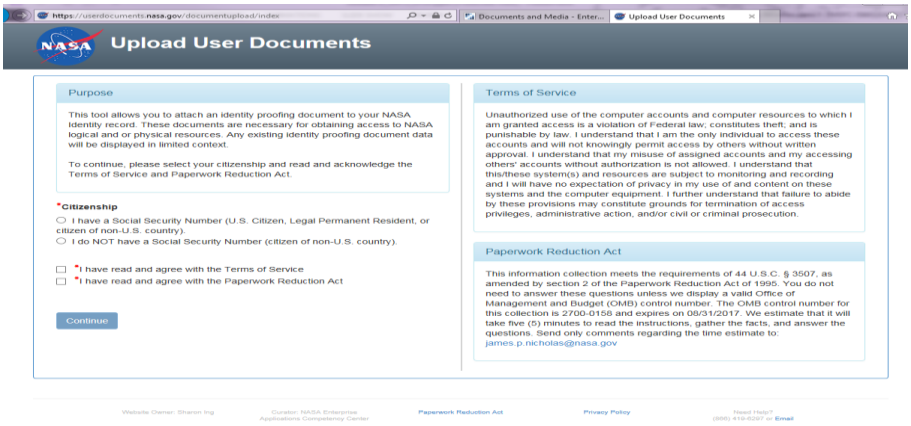
Sensitive Data includes SSN, Birth Information, User's Photo, Enrollment Data, Residential Information, and Sensitive Documents and Comments managed by Personnel Security.

Documents	Handling
Investigation Documents	Sensitive
Access Control Plan	Non-Sensitive
Identity Proofing	Sensitive
FNMS Documents	Sensitive

SAVE Investigations	Sensitive
Other	Non-Sensitive

UPLOAD DOCUMENT TOOL

This tool allows you to attach an identity proofing document to your NASA Identity record. These documents are necessary for obtaining access to NASA logical and or physical resources. Any existing identity proofing document data will be displayed in limited context. The user can access this tool by visiting the website: https://userdocuments.nasa.gov



COUNTERINTELLIGENCE TOOL

The Counterintelligence Officer is required to perform a check on foreign nationals of interest to determine if the foreign national has any affiliation to intelligence services or terrorism. Once this check has been completed the Counterintelligence officer can mark the foreign national's record as reviewed in IdMAX using the link Record Counterintelligence Review. From the link you will search for the foreign national, once you have selected the foreign national and the identity record is displayed you will see the Mark as Reviewed action button on the bottom of the Summary page. You also have the option to Review History. This will allow you to view any previous counterintelligence reviews for this foreign national. The Counterintelligence Review Queue only provides Foreign National identities that have not had any Counterintelligence Reviews recorded in IdMAX. This queue provides you the ability to see the Foreign Nationals that need to be reviewed.

Note: You must have the Counterintelligence Officer role to see the link/tool. If you do not have the role you will need to submit a NAMS request for "Agency ICAM Infrastructure" under "IdMAX ICAM Permissions" select Counterintelligence Officer. SATERN training will be required before requesting the role in NAMS.

NASA GUEST USER ACCOUNT

This tool is designed to assist you in creating and/or managing a Guest User account. Keep in mind that Guest Users typically require limited access to specific, low risk NASA IT services for a specific time period. A Guest Identity record is maintained on the NASA Enterprise Directory, and also details the Services that the Guest User has authorization to access. Any IdMAX user can access the Manage

Guest User workbench by selecting the Manage Guest Users link located under the Identities section of the IdMAX console page. The Guest User will receive notifications with login information upon the creation of the Guest Account by the requestor. There are additional capabilities to resend Guest Account passwords, extending expiration dates, etc. For detailed instructions, refer to the How do I Submit or Manage a Guest User Account Job-Aid located on the ICAM portal.

Note: Guest User accounts must have a password reset every 60 days. Keep in mind that password rules are the same as standard identities.

Note: The Citizenship of a Guest user is not tracked, except for Invitational Traveler guests. An Invitational Traveler's citizenship must be US or LPR for a guest user account to be enabled.

Guest Account Services

Guest.nasa.gov is a web application for use by non-NASA identities that have a need for a NASA Guest Account to access public, low-risk web application capabilities supported by NASA.

Self-registration of a Guest Account is available to users upon providing their Name, Email Address and Citizenship Country. Upon creation of the account, the Guest Account Services interface also allows a Guest to manage his/her password, register a Non-NASA Federal Credential, and modify related Guest attributes. Guest Account management is also supported in IdMAX (idmax.nasa.gov) when an application wants to continue to support only invited Guests by a NASA Requester.

Guest Level of Confidence:

- 0 – Guest Account Initiated
- 5 – Active Self-Registered Guest
- 15 – Active Managed Guest
- 20 – Identity-Proofed Remote

Manage Civil Servant Sponsors Tool

This tool provides the ability to change the centers designated Civil Servant sponsor. Since the WTTS Integration with the Human Capital system creates a civil servant identity in IdMAX and initiates the Credential, including sponsorship both the Identity and Credential are auto-sponsored with the name of the Human Capital Center POC per the Manage Civil Servant Sponsor tool. Since all Civil Servants should have a PIV card, even Renewals and Reissuances for Civil Servants regardless of type are auto sponsored by the system. There is no Identity Requester concept for a NASA civil servant, since the Identity data is sent via Human Capital System integrations, and out of band credential reissuances should be initiated in Enrollment Official Workbench or Security Workbench and the user can complete the enrollment in the same visit since there is no "employment review" requirement for an Identity Requester/Sponsor.

IVC Visitor Workbench

This tool provides the ability for a U.S. citizen or Legal Permeant Resident with an Agency Smart Badge or PIV Smartcard to submit a Foreign National Visiting Request for a Foreign National that is

visiting NASA for less than 30 days within a 365-day calendar. The Foreign National will have not have logical (expect for approved Guest wireless) or physical access and must be escorted. The workbench is located in the Identities section of IdMAX by clicking the Manage Foreign National Visitors link. The queues on the workbench:

Inviting Foreign National to Create Their Identity
This is an invitation process that allows the visitor to enter their own PII and Foreign National data. The Requester will need to know the following information prior to submitting a request:

- Visitor First and Last Name
- Assigned Center
- Notification Email
- Assigned Org code
- Affiliation Sponsor (default to requester)
- Company (default company)
- Affiliation Start Date
- Affiliation End Date

Invited Foreign Nationals (In-Process)
Foreign nationals that are listed in this queue have been invited and but have not completed the invitation request. They will remain in this queue until that have completed the invitation. The actions available from this queue:

- **Resend Passphrase**-Ability to resend the passphrase to the visitor using the notification email
- **Remove Invitation**- Ability to cancel and invitation that is no longer needed

Invited Foreign Nationals
Foreign Nationals that have completed the invitation request and the Requester has not completed the review or the IVC has requested additional information from the Requester.

REVIEW ASSETS FOR EXPORT CONTROL TOOL

This tool provides the ability for Agency and Center Export Control role holders the ability to track the Export Control status of an Asset. The concept is to stream-line ACP development and user approval due to asset detailed analysis being completed/tracked at the Asset Level. The latest Export Control Review status will be displayed in the Workflow Configuration Tool (WCT) / Basic Asset Configuration, NAMS Request for Foreign nationals in the Requirements Table, and in the ACP Tool.

The Export Control Review Status include:

- Approved - Asset is approved for foreign national access without further review by export control
- Prohibited – The asset cannot be accessed by foreign nationals
- Requires Authorization – Foreign nationals may be granted access following review by export control

System Characters / Symbols

To avoid having system characters and symbols when coping text from a Word document to an Identity Record you will have to replace the special characters with standard characters in Word. To do this, try the following steps in Word:

1. Save As
2. Save as type: Plain Text
3. Other encoding: Unicode UTF-8
4. Allow character substitution: checked
5. Close file
6. Reopen file
7. Cut and paste items from file as needed

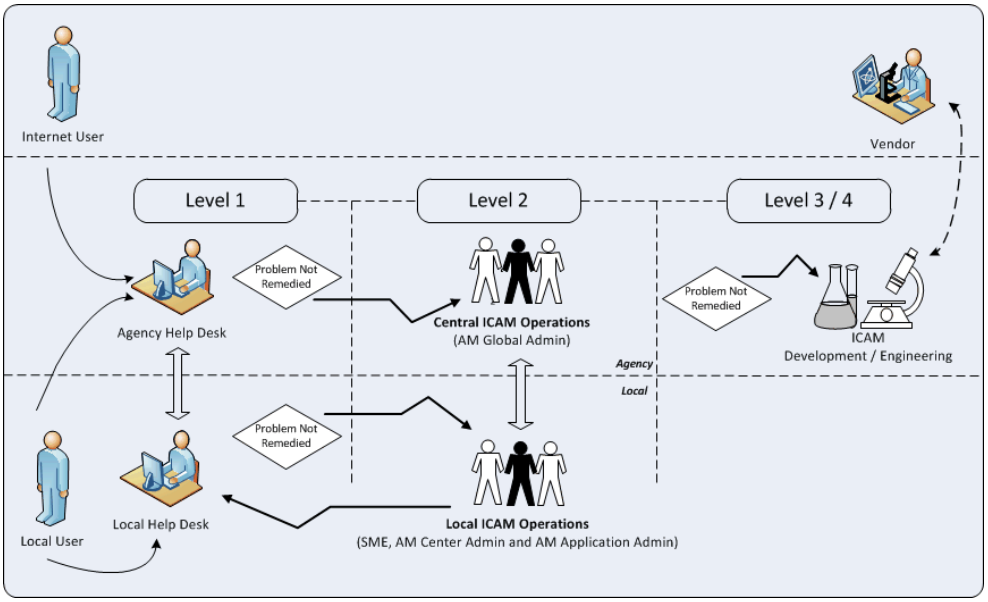
Another option is to use a simple text editor like notepad to store this information, as it does not try to insert special characters into your text.

16. Reports

ICAM utilizes the Cognos / BOBJ tool to provide Reports related to managing or measuring NASA Identity requests and other related processes for the ICAM project, including the Identity Details reports and several statistical reports. You can access these reports by clicking the Links tab within IdMAX and then ICAM Reporting. There is a Help document located with the reports if you have further questions.

17. Support

The ICAM authentication/authorization services are maintained by the AAO ICAM technical support team. For production issues affecting end users, the Center local help desk is the first line of support for ICAM operations (Level-1). Following the Center's assessment, unresolved technical issues should be escalated to the Enterprise Service Desk (ESD) and a Service Request (SR) submitted. Level-2 troubleshooting, and resolution would be conducted in coordination with the ICAM SME and AAO ICAM technical team. The ICAM support model is illustrated in the following diagram.



In regards to Application Integration support, the Center Identity Point of Contact will be the initial contact for Level-2 troubleshooting, see ICAM web portal (https://icam.nasa.gov) for details. If needed, the Identity SME/SETE can submit a Service Request (SR) for assistance from the AAO ICAM technical team.

18. Supported Browsers

Secure NAMS supports the following web browser version for an optimal user experience:

- IE 9 or greater
- Firefox 25 or greater
- Chrome 24 or greater
- Safari (latest version)

Compatibility Mode

Internet Explorer has a feature called Compatibility Mode (or Compatibility View) which allows the browser to display content as it would appear on an earlier version of the browser. For example, IE 9 with Compatibility Mode enabled will render a website as if it was running on IE 7.

Unfortunately, when this feature is turned on, SNAMS will not function properly. Please take the following steps to turn Compatibility Mode off.

Option 1

1. In the **Tools** drop-down menu or the **Tools** command bar, deselect **Compatibility View**. (Note: If you do not see the **Tools** drop-down menu or command bar, right-click on an empty space on the toolbar and select **Menu bar** or **Command bar**.)

Option 2

1. In the **Tools** drop-down menu or the **Tools** command bar, select **Compatibility View Settings**. (Note: If you do not see the **Tools** drop-down menu or command bar, right-click on an empty space on the toolbar and select Menu bar or Command bar.)
2. Ensure that this website is not listed in the **Websites you've added to Compatibility View** text area. If it is listed, remove it.
3. Uncheck the **Display intranet sites in Compatibility View** and **Display all websites in Compatibility View** checkboxes.
4. **Close** the window to save your changes.

Enabling Javascript

In order for SNAMS to function properly, Javascript must be enabled. If Javascript is disabled for your browser, please enabled it by taking the following steps for your particular browser:

Internet Explorer

1. In the **Tools** drop-down menu, select **Internet Options**.
2. Select the **Security** tab. (Please note: Admin-level settings may prevent access to this tab.)
3. Select the **Earth/Internet** icon.
4. Select the **Custom Level** button.
5. Locate **Scripting** near the bottom of the list.
6. Under **Active Scripting**, select **Enable** and then click **OK**.
7. Answer **Yes** to the following confirmation box.
8. Click **OK** to close the **Internet Options** window.
9. Finally, refresh your browser.

Firefox (PC and Mac)

1. In the address bar, type **about:config** and press Enter.
2. Click **I'll be careful, I promise!**
3. In the search bar, search for **javascript.enabled**.
4. Right click the result row named **javascript.enabled** and click **Toggle** to set the value to **true**. Alternatively, double-click the result row to toggle the value to **true**.
5. Finally, refresh your browser.

Safari (PC)

1. Select the **Safari Settings** icon in the menu bar.
2. From the drop-down menu, select **Preferences**.
3. Select the **Security** icon/tab at the top on the window.
4. Check the **Enable JavaScript** checkbox.
5. **Close** the window to save your changes.
6. Finally, refresh your browser.

Safari (Mac)

1. Select the **Safari** menu item from the Apple/System bar at the top of the screen.
2. From the drop-down menu, select **Preferences**.
3. Select the **Security** icon/tab at the top on the window.
4. Check the **Enable JavaScript** checkbox.
5. **Close** the window to save your changes.
6. Finally, refresh your browser.

Chrome (PC)

1. Select the **Customize and control Google Chrome** icon to the right of the address bar.
2. From the drop-down menu, select **Settings**.
3. Click **Show advanced settings**.
4. Under the Privacy heading, select the **Content settings** button.
5. In the JavaScript section, select the **Allow all sites to run JavaScript** radio button and click **Done**.
6. Finally, refresh your browser.

Chrome (Mac)

1. Select the **Chrome** menu item from the Apple/System bar at the top of the screen.
2. From the drop-down menu, select **Preferences**.
3. Click **Show advanced settings**.
4. Under the Privacy heading, select the **Content settings** button.
5. In the JavaScript section, select the **Allow all sites to run JavaScript** radio button and click **Done**.
6. Finally, refresh your browser.

19. Appendix B: Acronyms / Abbreviations / Definitions

Acronyms / Abbreviations	Description
ACO	Agent Configuration Object
ACP	Access Control Plan
AM	Access Manager
Application	Any server-based software running in the NASA environment that is not included as part of the standard desktop /laptop load and • Is recognized that NAS A owns, funds, or maintains, jointly owns or has right of first refusal or information is critical to the mission of operation of NASA • The Application currently provides user based authentication, e.g. userID and password
AUID	Agency User ID
Authentication	The mechanism that IT systems use to securely identify users. Answers the questions: • Who is the user? • Is the user really who he/she claims to be?
AuthN	Authentication
Authorization	The mechanism by which a system determines what level of access a particular authenticated user should have specific resources. Answers the question: • Should this user be allowed to access this resource?
AuthZ	Authorization
BAS	Biometric Application Service
BI	Background Investigation
BioSP	Biometrics Services Platform
BSMB	Business System Management Board
CBACS	Common Badging and Access Control System
CCB	Change Control Board
CI	Counter Intelligence
CIMA	Center for Internal Mobile Application
CMS	Card Management System
COTS	Commercial-off-the-Shelf
CPE	Center Premise Equipment
CPR	Card Personalization Request
CVS	Central Verification System
DAO	Data Access Objects
DN	Distinguished Name
DOB	Date of Birth
EA	Enterprise Architecture
EAR	Export Administration Regulations
EPACS	Enterprise Physical Access Control System
ESB	Enterprise Service Bus
ESID	Enterprise Service & Integration Division

EPM	Enterprise Policy Management
ESD	Enterprise Service Desk
EVAMS	Enterprise Visitor Management System
FBI	Federal Bureau of Investigation
FN	Foreign National
FNMS	Foreign National Management System
FPPS	Federal Personnel Payroll System
HCO	Host Configuration Object
ICAM	Identity, Credential and Access Management
ICAM-M	ICAM Modernization
ICAS	ICAM Audit Viewer
IdMAX	Identity Management and Account eXchange
IT	Information Technology
LIT	Launchpad Integration Tool
LAPOC	Logical Access Point of Contact
LDAP	Lightweight Directory Access Protocol
MSFC	Marshall Space Flight Center
NASA	National Aeronautics and Space Administration
NCAD	NASA Consolidated Active Directory
NDC	NASA Data Center
NEACC	NASA Enterprise Applications Competency Center
NED	NASA Enterprise Directory
PAP	The Policy Administration Point
PDP	The Policy Decision Point
PEP	Policy Enforcement Point
POC	Point of Contact
RMT	Resource Maintenance Tool
SAP	Special Access Program
VPN	Virtual Private Network