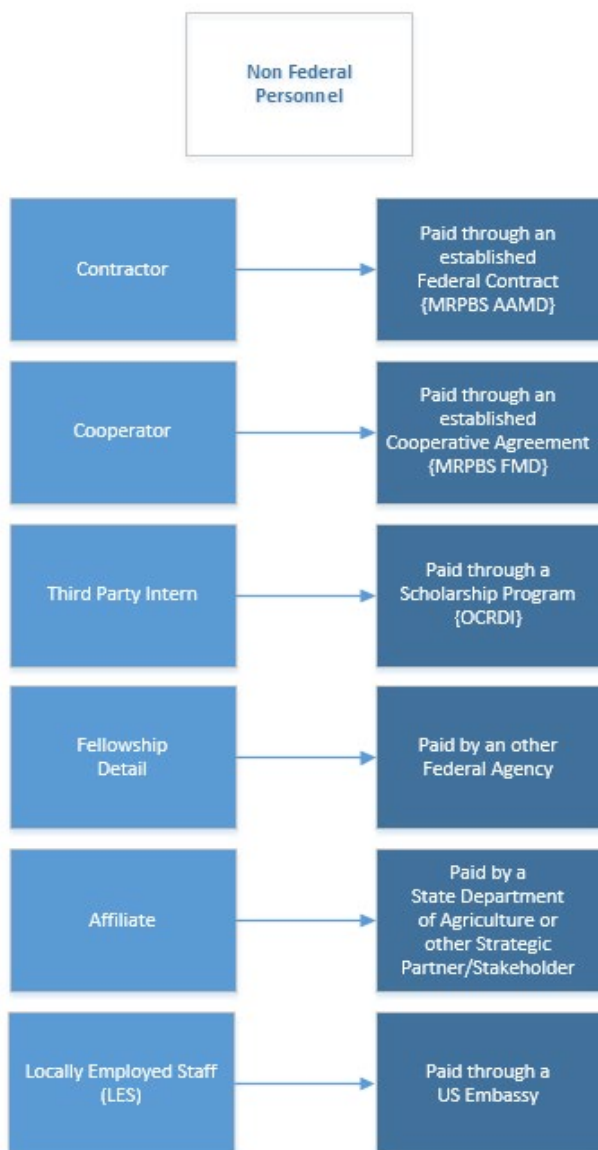


Onboarding Non-Federal Resources

Non-Federal personnel have become so much an integral part of the government workforce; it is often difficult to distinguish between them and Federal employees; it is, however, important to do so. Non-Federal personnel typically work under a defined service contract/agreement whereby they are not subject to the supervision and control usually prevailing in relationships between the government and its employees. The government formalizes {in writing} a commitment with an outside entity for a required service; specifies the details in a work statement which becomes part of the understanding; and reviews, approves, and pays for work products (as applicable), but does not manage individual performance. The outside entity typically dictates its employees' compensation, benefits, and rewards. There are many different types of Non-Federal personnel.

Non-Federal personnel are most typically employed by and paid through the outside entity (contract, cooperative agreement, state Department of Agriculture, embassy, scholarship board, etc.) not through the National Finance Center (NFC) as federal employees are.



CONTRACTOR – A federal contract is a mechanism through which the federal government can purchase products or services. Typical services purchased: information technology, research & development, housekeeping services, maintenance of real property or supplies/equipment, transportation, advisory and assistance services, etc. The principal purpose of a federal contract is to purchase property or services for the direct benefit or use by the US Government.

COOPERATOR – A cooperative agreement is distinct from contracts and thus are not subject to the Federal Acquisition Regulation. This provides agencies greater freedom to craft the terms of an agreement around new endeavors.

THIRD PARTY INTERN – Scholarship programs often provide full tuition and work opportunities to students pursuing degrees in agriculture, food, natural resource sciences, etc. Interns often have an opportunity for conversion when the scholastic requirements have been completed.

FELLOW/DETAIL – Agencies offer detail opportunities to employees from other USDA agencies. While salary & benefits are paid 'home' agency; a dual agency relationship ensures access to equipment, facilities, networks and/or applications.

LOCALLY EMPLOYED STAFF (LES) – provide unique services in support of USDA at more than 270 embassies and consulates worldwide. These Foreign Service Nationals (FSN) provide the institutional knowledge and professional contacts that are integral to representing USDA's interests to other countries. When they require access to USDA applications and networks, establishment of a Non-Federal relationship may be needed.

AFFILIATE – APHIS & AMS maintain strong partnerships with local State Department of Agriculture(s), tribal nation(s), or other strategic partner/stakeholder organizations. These local entities assist USDA by gathering surveillance or investigative data on different plant or animal health issues. When reporting of this data requires access to USDA applications or networks, establishment of a Non-Federal relationship may be needed.

Onboarding Non-Federal Resources

The Agency/Program/Business Unit is **solely responsible** for working with the appropriate points of contact within MRP to establish the mechanism(s) by which they will bring non-federal personnel into their Agency. It is only after the point of entry has been legally established will they begin to work with MRPBS HRD & MTAC on ensuring the identified personnel are ready to be onboarded.

NOTE: If Affiliates (typically State Department of Agriculture employees) require access only to a specific application(s) administered by a specific MRP Agency/Program all the onboarding requirements identified below may not be required. Certain program driven applications do require Affiliates to create their own Level 2 eAuthentication accounts, to provide their own identify verification documentation, and to follow log in procedures developed for that specific application. These Program Administrators should ensure that all processes and procedures are provided and followed.

Access to USDA networks or applications via eAuthentication or a USDA Linc Pass must be requested by a Federal employee on behalf of Non-Federal personnel. For Contractors, this is typically done by the Agency/Program's Contracting Officer's Representative (COR) or Contracting Officer's Technical Representative (COTR) who has been working closely with MRPBS AAMD's Contracting Team. For other types of Non-Federal personnel this is handled by an identified Agency/Program Point of Contact associated with the project or team the person will be working on.

If equipment will be provided to the Non-Federal resource, the Agency/Program should work closely with their Program Inventory Point of Contact to ensure that equipment is available and that either OCIO CEC or MTAC are alerted so it can be properly provisioned and configured.

ONBOARDING RESPONSIBILITIES

The Agency/Program onboarding Non-Federal Personnel may work with two Information Technology (IT) organizations, the Office of the Chief Information Officer (OCIO) - Client Experience Center (CEC) and APHIS Marketing and Regulatory Programs Information Technology (MRP IT or MTAC), to ensure the Non-Federal can log into their computer equipment and access the network(s) and applications. CEC and MTAC partner to deliver and support IT services for AMS and APHIS customers; but they are separate organizations. In many ways, like the rest of AMS and APHIS, MTAC is a customer of CEC. MTAC communicates with CEC via the System Authorization Access Request (SAAR) as they manage the information technology resources for the Program.

- OCIO CEC – APHIS IS Non-Federal Personnel **located domestically**
- OCIO CEC – MRP Non-Federal Personnel **located in non-laboratory** locations
- MTAC – APHIS IS Non-Federal Personnel located overseas
- MTAC – MRP Non-Federal Personnel located in laboratory locations

While MTAC manages the IT set up and equipment requests for any overseas and laboratory services information technology (LSIT) Non-Federal personnel, **ALL** requirements for cellular telephones are handled through CEC.

If Agencies/Programs/Business Units have questions around which group is responsible for which items, they can contact Help@usda.gov for guidance and assistance.

Onboarding Non-Federal Resources

Within the Human Resources Division (HR), the MRP Agency/Program/Business Unit bringing Non-Federal personnel onboard will work with the HR Operations Personnel Security Section (PSS).

Agency/Program Responsibilities - Onboard

- Ensure the mechanism (contract, agreement, scholarship, etc.) is in place. If Non-Federal personnel require access to MRP networks, facilities, applications, equipment; they should not be onboarded until all the HR Personnel Security requirements have been fulfilled.
- Alert HR Personnel Security about an incoming Non-Federal
- Provide HR Personnel Security with a packet of information for each Non-Federal needing onboarding. This list may vary depending on what access the Non-Federal needs:
 - [Information Security Awareness](#) completion certificate or screenshot of certificate
 - Fingerprints obtained at a [Fieldprint Site](#)
 - Electronic Questionnaire for Investigations Processing (eQIP)
 - [OF306](#) – Declaration of Federal Employment – to determine fitness for Federal service
 - HRO1197 – Background investigation Supplement
 - Identify USDA Point of Contact Name
 - Identify USDA Organizational Affiliation (Agency/Program)
 - Scanned Copies of Two (2) Forms of Identification
 - Identification of any persons who are Locally Employed Staff (LES)
 - Statement of Work or Statement of Objective (AMS Tier 2 background only)
 - Fair Credit Authorization Form (AMS Tier 2 background only)

HR Personnel Security will provide the incoming Non-Federal with specific information related to fingerprinting at a Fieldprint site and will send them the eQIP invitation email

- **APHIS IS or APHIS PPQ Locally Employed Staff (LES)** have an additional hurdle as they do not have a Social Security Numbers which is required to determine ‘fitness’ to work for the Federal government and to create NFC Person Model records. The Agency/Program seeking to employ LES should indicate that on the paperwork returned to PSS.
- Request creation of an @usda.gov email address & Enterprise Active Directory (EAD) account for Non-Federal personnel using the [MRP 408](#) Active Directory User Account Provisioning Form. This form should also identify if the Non-Federal personnel are international or domestic AND if they are or are not a part of the APHIS Laboratory Network.
- Request permissions to email distribution groups, shared mailboxes, network share drives and security groups using the [MRP 408](#).
- Create equipment or software installation requests using [Digital Workplace](#) (DWP). Equipment purchase/allocation requests can be submitted at any time. The Agency/Program Office should get the equipment into the hands of MTAC or CEC as quickly as possible to avoid work stoppages. Find additional Digital Workplace information [here](#).
- Work with Program Inventory Point of Contact as appropriate. [IT Equipment Request Form](#)
- Work with MTAC or CEC on pick up or shipping logistics for equipment
- Work with MTAC or CEC on any equipment configuration/connectivity issues

Onboarding Non-Federal Resources

Non-Federal Personnel Responsibilities

- Provide the requested documentation & complete the required tasks in a timely manner
- Alert the Agency/Program/Business Unit POC when all tasks are completed
- Create a personal Level 2 eAuth account **ONLY** if requested to by the Agency/Program

Information Technology (MTAC/CEC) Responsibilities

- Contact the Non-Federal personnel's identified Agency/Program point of contact when the AD account and email configuration are complete
- Configure equipment such as Laptops, iPad, iPhone
- Work with Agency/Program Point of Contact on pick up or shipping logistics for equipment

HR Operations Personnel Security Section Responsibilities

- Create the Non-Federal record in EmpowHR
- Provide information around Fieldprint fingerprinting requirements
- Request a name trace through USDA Agricultural Research Service (ARS) and the Department of Homeland Security (DHS) to determine 'fitness' **for LES**
- Request a pseudo-SSN **for an LES** who has cleared the name trace process & been determined 'fit' to work for the USDA
- Initiate the Non-Federal into eQIP
- Review documentation and alert Agency/Program/Business Unit POC of any issues
- Alert the HR Systems Analysis and Reporting Branch or Tanika Harris (AMS Non-Federals) to send the eAuthentication invitation
- Sponsor/Adjudicate for Linc Pass (*as applicable*)

Agency/Program Points of Contact whether they are formal COR/COTR or simply MRP employees responsible for the project should review all information for accuracy and completeness **prior to** submission to HR Operations Personnel Security. If Linc Passes are required, the Point of Contact must **clearly indicate the location to which the LincPass badge should be shipped for activation.** (*Note: Inaccurate or incomplete location information will result in significant delays in obtaining Linc Pass credentials.*)

Within 5 days of receipt of the complete package, Human Resources will create the EMPL ID for the Non-Federal resources in EmpowHR. **Note:** The time for LES onboarding will start once the complete package is received, the name trace has cleared, and the pseudo-SSN has been obtained.

Onboarding Non-Federal Resources

An EmpowHR action is required if Non-Federal personnel require access to USDA MRP applications or networks via the Virtual Private Network (VPN). It also facilitates the establishment of the Level 2 eAuthentication account and allows for the issuance of a LincPass (if LincPass is required). The established government email address will be populated in EmpowHR and will be used to send all messages related to eAuthentication and LincPass. If no government email address will be established, the Agency/Program Point of Contact should include an alternate personal email address.

Once onboard, Non-Federal personnel are also required to complete all mandatory training assigned via AgLearn. If training courses are not completed, access to USDA MRP networks & applications can be terminated. There may be additional workplace safety requirements that require compliance by Non-Federal personnel.

Agency/Program Responsibilities – Offboarding

When Non-Federal personnel leave or 'roll off the project'; the Agency/Program/Business Unit Point of Contact is responsible for the following:

- Alert HR Personnel Security so the access to USDA applications & networks via eAuthentication & Linc Pass can be terminated
- Ensure the physical Linc Pass card is destroyed appropriately
- Ensure any facility access is terminated and/or site badges are returned
- Notify MTAC and any other information system owners who may have provided the Non-Federal personnel with access to agency/program applications that they can remove this access
- Ensure **ALL** federal equipment is returned in good condition. Non-Federal resources should work with their Agency POC to determine where & how equipment should be returned
- Ensure all material created, received or maintained during an employee's employment or appointee's tenure with the Federal Government that meets the criteria for a [Federal record](#) remains in Federal custody when an employee or appointee departs the Agency
- Request access to departing Non-Federal resources' email or network resources for legitimate business continuity purpose(s)

Similar notification to MTAC or information system owners is required if a resource is switching projects. As with Federal Employees, Non-Federal personnel should have only the appropriate level of access to applications, not more.

Onboarding Non-Federal Resources

Expected Timeframes

Event	Performed By	Expected Timeframe	Comments
1 Email and Active Directory Creation	OCIO CEC	24 - 48 Hours after receipt of the MRP 408	Non Federals who are moving from one USDA Agency to another may take longer
2 Laptop Configuration & Shipping	OCIO CEC	2 Weeks after receipt of equipment from the Program	Programs <u>DO NOT</u> need to wait until the Non Federal's name populates in Active Directory to send equipment configuration requests to CEC
3 iPad and iPhone Configuration & Shipping	OCIO CEC	2 Weeks after receipt of equipment from the Program	Configuration <u>CAN NOT</u> begin until the Non Federal's name appears in Active Directory
3 Network/Shared Drive/Email Group Configuration	OCIO CEC	3-5 Days after receipt of the SAAR from MRP IT	
5 Creation of the Person Model record in NFC	Human Resources	5 days from receipt of the complete package of required documents	LES who need a Name Trace and Pseudo-SSN will take longer
6 eAuthentication (APHIS) Federally Created Account	Human Resources	24 Hours after creation of the Person Model Record in NFC	
7 eAuthentication (AMS) Federally Created Account	Tanika Harris	24 Hours after creation of the Person Model Record in NFC	
8 eAuthentication Personally Created Account	Non Federal Resource	A personal eAuthentication account should be created only if required by the Agency/Program to facilitate access to a specific application	
9 Access to AgLearn		24 Hours after the acceptance of the eAuthentication Invitation	
10 Linc Pass Enrollment Message	Human Resources	Within the first pay period <u>IF</u> there is a Linc Pass Credentialing Center open within the local geographic area	Non Federals may not need Linc Pass
11 Linc Pass Activation Message	Human Resources	7 Days after the Enrollment Appointment <u>UNLESS</u> there are discrepancies that needs to be rectified	Non Federals may not need Linc Pass
12 Access to Program Owned Applications	Program Administrators	Dependent on Program Requirements	Submission of Application specific access request forms may be required

FREQUENTLY ASKED QUESTIONS

1. What if the Non-Federal works or worked for the Federal Government?

Non-Federal resources often work across multiple government agencies either in sequence or simultaneously, leave and return or even move between Federal and Non-Federal statuses. Agency/Program Points of Contact should alert both the Human Resources and Information Technology teams well in advance of the Non-Federal's start date to avoid duplicate accounts being created or access to resources removed or rendered unavailable.

- Non-Federal resource transfers between two Government or USDA Agencies
- Non-Federal resource needs 'Dual Access' to both MRP resources and resources at another USDA Agency
- Federal Employee separates and becomes a Non-Federal Resource
- Non-Federal resource becomes a Federal Employee

2. Do mandatory AgLearn training requirements apply to Non-Federal resources?

Non-Federal AgLearn profiles are created for Non-Federal resources in the same way they are created for Federal employees. When Non-Federal resources need access to the USDA resources (VPN, applications, networks, equipment, facilities) they are required to complete mandatory training courses. These courses are assigned to them via their AgLearn profile and if not completed will result in termination of logical or physical access.

3. Do all Non-Federals need EmpowHR (NFC) or Active Directory (AD) profiles?

No. EmpowHR or Active Directory profiles are established solely on an Agency/Program determination of the work they are expected to complete and level of access (VPN, applications, networks, equipment, facilities) required. If they require building access only, please work with the facility manager at that location. Regardless of any required IT set up, all Non-Federals **must be** fingerprinted and determined 'fit' for Federal Service

4. What happens if the Non-Federal can't access assigned equipment?

To help with Windows/Bitlocker/VPN ID and Password issues:

- Contact person identified in documentation shipped with equipment
- CEC Help Desk 877-873-0783
- [CEC Group Manager Site](#)
- CEC [Contact Options](#)

BitLocker is a specific set of keys unique to your equipment that captures information like the make, model, and internal part serial numbers, and uses it to ensure that your drive hasn't been stolen and inserted into another machine. You'll be asked for this key every time you turn on your equipment. Once this information has been verified, you'll log into your computer using your Linc Pass or Windows ID and Password. If you enter a BitLocker key incorrectly multiple times, your equipment will lock, and you'll need to contact CEC to obtain a recovery key.

Virtual Private Network (VPN) establishes a secure connection between you and the internet. Via the VPN, all your data traffic is routed through an encrypted virtual tunnel. A VPN connection is also secure against external attacks. Any issues with VPN should be directed to CEC.

Windows ID and temporary password will be provided to you when you receive your equipment. You will change your Windows password upon logging in for the first time. This set of credentials is used to log into equipment and networks.

5. How do Non-Federals access government furnished equipment (GFE)?

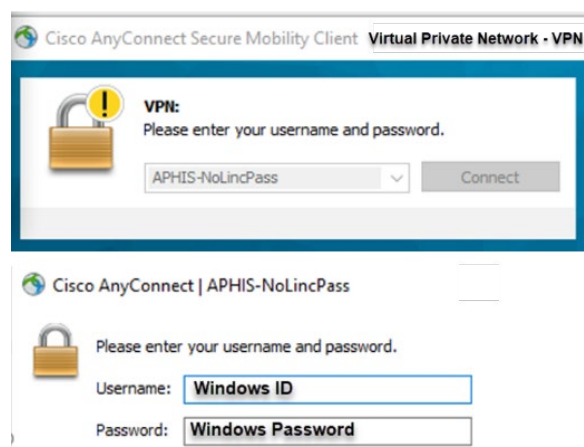
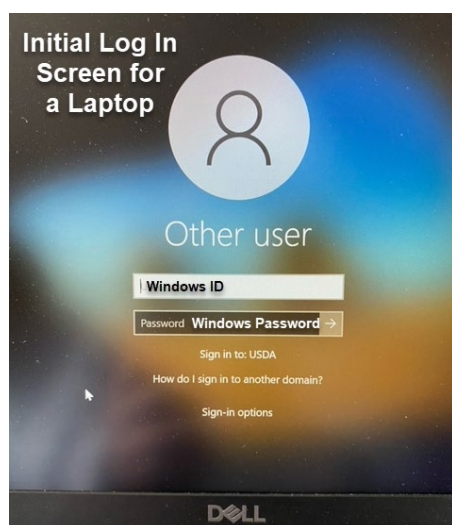
- Turn on the equipment
- Enter the Bitlocker Key provided by CEC
- Enter Windows ID and Password – Typically formatted like this: John.Public
- Access the VPN
 - Select APHIS No Linc Pass or AMS No Linc Pass depending on your Agency
 - Enter Windows ID and Password - Typically formatted like this: John.Public

Note: this is your official name as identified on your HR Person Model records

6. Which ID/Password should a Non-Federal use?

In the first few weeks of engagement, the Non-Federal may be overwhelmed with the number of IDs and Passwords they'll need to keep track of. When the Linc Pass is issued, this will subside as many applications will use an 8-character PIN & single sign on capabilities to authenticate the user.

- Windows ID & Password – used to access equipment & networks including VPN
- eAuthentication ID & Password – used to access applications

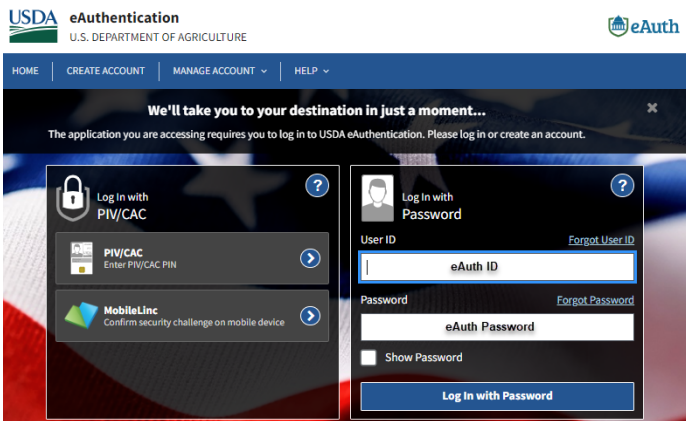


7. What is eAuthentication?

In a nutshell it means “more access with fewer passwords”

USDA eAuthentication(eAuth) is the system used by USDA agencies to enable employee’s secure access to Web applications and services via the Internet. A single eAuth account saves time and reduces the number of passwords needed by providing single sign on to multiple online resources, programs and benefits to view or conduct official business via the Internet with USDA.

New employees use an eAuth ID and Password combination until such time as they receive their Linc Pass. **eAuthentication IDs are typically formatted like this: John.Public**. If a long tenured employee changes Agencies; however, it is possible that when they first were offered eAuthentication, they were allowed to create their own eAuthentication ID like: LuckyDuck1 or #AbelLincoln or any other combination of characters.



This is the eAuth window. This interface appears as the access point for many USDA applications.

1 Non-Federals logging in with their eAuth ID/Password use the right side of the pane

2 Users with a Linc Pass use the left side of the pane

8. What happens if the Non-Federal can't find their eAuthentication Invitation?

The eAuthentication invitation or an eAuthentication recovery message can be sent/resent.

- AMS employees – Tanika.Harris@usda.gov
- APHIS employees – HR.System.Access@usda.gov

9. What happens if the Non-Federal needs a password reset or needs to confirm their eAuthentication ID and the self service options are not working?

The eAuthentication invitation or an eAuthentication recovery message can be sent/resent.

- AMS employees – Tanika.Harris@usda.gov
- APHIS employees – HR.System.Access@usda.gov

10. What is a SAAR and when is it used?

SAAR stands for System Authorization Access Request and they are typically completed and submitted by someone in a supervisory capacity who has the authorization to request IT actions on behalf of others.

11. Who does the Non-Federal contact if they left their Linc Pass at home and need access to equipment or applications for that day?

- CEC can provide the employee temporary log in credentials to access their equipment.
- The APHIS or AMS POCs for eAuthentication can send an eAuth recovery message to the employee allowing them to recover their eAuthentication credentials to access applications

A lost or stolen Linc Pass should be immediately reported to the Agency/Program POC and to HR Personnel Security Staff at lincpass.security@usda.gov

Lost or stolen equipment should be reported immediately to the Agency/Program POC and entered in the [CEC Digital Workplace](#). From the home screen look for the Report Lost or Stolen Equipment icon or type "Lost" in the search tool then follow the scripted prompts. Additionally lost or stolen equipment can be reported to help@usda.gov or by calling MTAC at 1-877-744-2968

12. How do I check the status of a SAAR?

SAAR Each SAAR will have a ticket number (REQ00000XXXXXX) identified in an email message sent from the MRP Service Desk team. Request status can be checked by accessing the [CEC Digital Workplace](#) or by contacting the [Group Manager](#) (for the state in which the employee identified in the ticket) resides.

13. Who does the Supervisor contact when CEC reports that the Active Directory account has been disabled by EEMS or by inactivity?

This is a common scenario if a Non-Federal leaves and returns or if the Federal Contract is terminated. The Agency/Program POC should contact the MTAC Service Desk at help@usda.gov or 877-944-8457 as well as HR.System.Access@usda.gov.

14. Who does the Agency/Program POC alert when CEC reports that the Active Directory account has been disabled due to the Information Security Awareness (ISA) or the PII Fact Sheet not being current?

Non-Federal resources are required to keep up with the ISA refresher training required every 52 weeks. Currently, CEC will not disable the AD user account for ISA training non-completion. Instead, they initiate a "restricted desktop" allowing the Non-Federal access ONLY to AgLearn.

The end-user should also be in contact with their Agency/Program AgLearn POC to ensure the record updated and now reflects completion of the ISA course or the signed PII fact sheet. The "restricted desktop" the end-user experiences will clear in approximately 4 hours.

15. How can the Agency/Program POC confirm the AD account/email are created?

To determine if the AD account and government email have been created for a new or returning Non-Federal resource, the Supervisor can check the Global Address Listing.

Additionally, the Point of Contact identified on the MRP 408 form will receive an email message like the one below acknowledging the existence of the account/email address.

Title: Example: CRQ0000000000 – Non Federal Resource Name

The Active Directory (AD) and email accounts have been created. An email notification was sent via Remedy to the local TSD group email distribution list.

If you have any questions, please contact your local TSD support that is available from the CEC icon at the bottom right hand corner of your desktop.

Thank you,
Access SAAR Group

16. How does the Supervisor order equipment?


Each Program may have their own internal processes for ordering and provisioning equipment for Non-Federal resources who need a Lifecycle replacement (laptops, iPad, iPhone, etc.). Program SOP's should always be followed and Program Inventory POCs should always be contacted first. Once equipment needs have been identified and approved at the Program level, requests can be submitted to CEC via the [Digital Workplace \(DWP\)](#).

Note: Equipment requests should be submitted to CEC as soon as the Agency/Program know *someone* is coming onboard. Doing so allows time to obtain and configure the equipment before the Non-Federal start date

Agency/Program POCs can submit the equipment request as early as 30 days before the new hire will come onboard. You DO NOT need to know the name of the Non-Federal prior to submitting the equipment request. If the location of the Non-Federal is known at the time of submission; please include that information.

Once equipment needs have been identified and approved at the Program level, requests can be submitted to CEC via the [Digital Workplace \(DWP\)](#).

[Home](#) [Details](#) [Unfavorite](#) [Share](#)

**IT Equipment Request**
Request Services, Device Request

Description

Complete this form to request actions (New; Move/Change; Remove/Disconnect) for hardware devices such as workstations, mobile devices, desk phones or monitors.

QTY: 1

Request for: Nancy Bradford

17. Who does the Agency/Program POC notify if the email is not in the GAL?

Email MRP-IT at help@usda.gov for help as there may be:

- A misspelled name
- Creation of an email identifying the employee as John, Roberts instead of Roberts, John
- An email with a Jr or Sr or III designation that is sometimes harder to find
- An email with two last names - Atkins Johnson, Ann may be found identified as Atkinsjohnson, Ann

18. Who does the Supervisor contact with Linc Pass Questions?

The Linc Pass is also known as the US Access Credential or the Personal Identify Verification (PIV) card. This credential is used to control access to federal facilities and information systems at the appropriate security level. There are many staffs that can help:

- Human Resources Personnel Security can answer questions about Linc Pass sponsorship, enrollment, adjudication, printing and reprinting/reissue. They are also a resource for Linc Pass certificate updates and card renewals.
- Facility Staffs can answer questions about building access
- MTAC or CEC can answer questions about access to equipment

Personnel Security Section - LincPass.Cecurity@usda.gov

OCIO Customer Experience Center - [Contact Options](#)

MTAC Service Desk – help@usda.gov

NOTE: The ability to obtain an appointment at a Linc Pass credentialing center has been adversely impacted by the COVID 19 pandemic. Only now are sites beginning to open more fully although they are often still restricting access to only “their” Agency resources. This means that even if there is a site very close to you, you may not be able to get an appointment there. None of the staffs identified above can help with this issue.

Everyone may not need a Linc Pass immediately. For Non-Federals in both AMS and APHIS, the eAuthentication ID and Password may be sufficient and allow for access to the applications used.

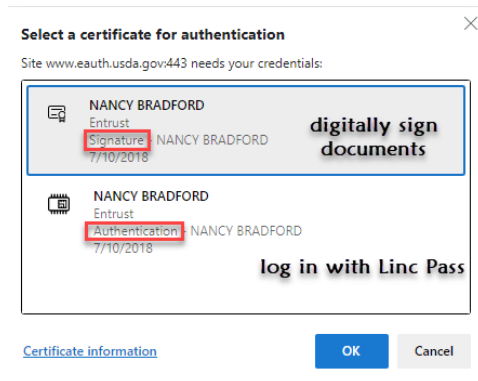
Non-Federals coming into MRP from another USDA Agency – **please hold onto your Linc Pass.**

For Non-Federals facing an upcoming **credential expiration** date, an appointment at a credentialing center may not be possible depending on location. If a Linc Pass expires, a SAAR will need to be submitted requesting that the resource be put into the 30-day exception group until such time as an appointment is available.

Those needing a **certificate update** can now facilitate this at their workstation without a visit to a credentialing center.

Troubleshooting some common Linc Pass issues

The Non-Federal just received/activated their Linc Pass and it “doesn’t work” in their computer



- Ensure that the employee is selecting the AUTHENTICATION certificate and not the SIGNATURE certificate (*see picture*)
- The Active Directory Account is missing attributes and/or the number associated with the Linc Pass isn't populated in the account. Contact MTAC at help@usda.gov for validation and resolution

- Hewlett Packard Computers have a known issue with the new PIV4 cards. The resolution for this is to go to the HP site, download & install the Alcor driver for the machine model and then update activclient to the [newest version](#)
- Non-Federal receives a message indicating their Linc Pass is BLOCKED. This indicates that there are setting issues on the Non-Federal's laptop and they should contact MTAC at help@usda.gov for resolution
- Non-Federal receives a message indicating their Linc Pass is LOCKED. This indicates that the Non-Federal has incorrectly entered their PIN multiple times. The Non-Federal may need to visit a credentialing center to have this resolved

Common Terminology or Forms used in this Process

HRO 1197

Background Investigation Supplement provides HR PSS with information to establish the Non-Federal record in EmpowHR and begin the Linc Pass sponsorship & adjudication processes.

MRP 408

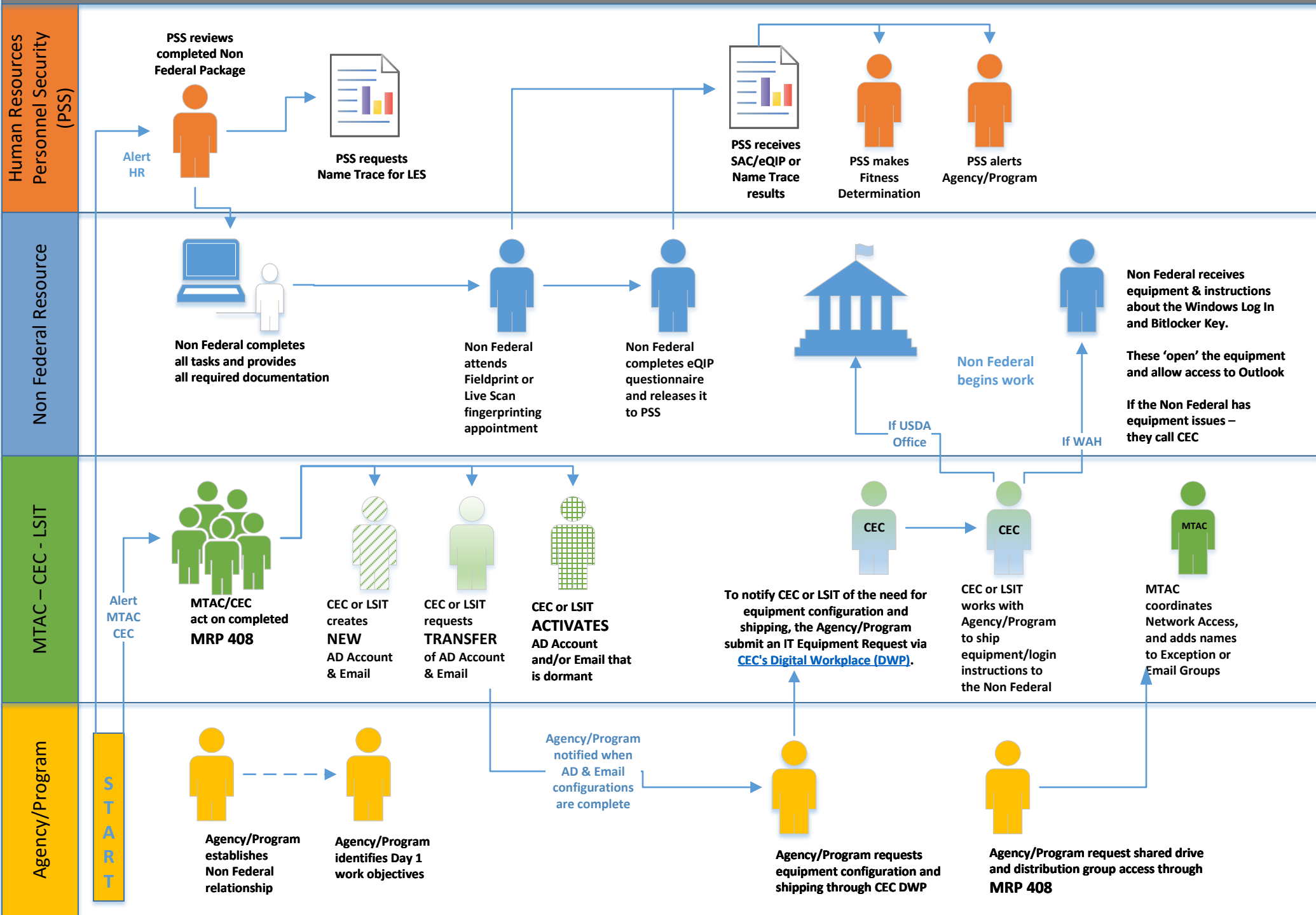
Active Directory User Account Provisioning Request Form provides MTAC and/or CEC with information to establish the Non-Federal record in Active Directory, Government Email Address as well as access to identified networks, applications or email groups .

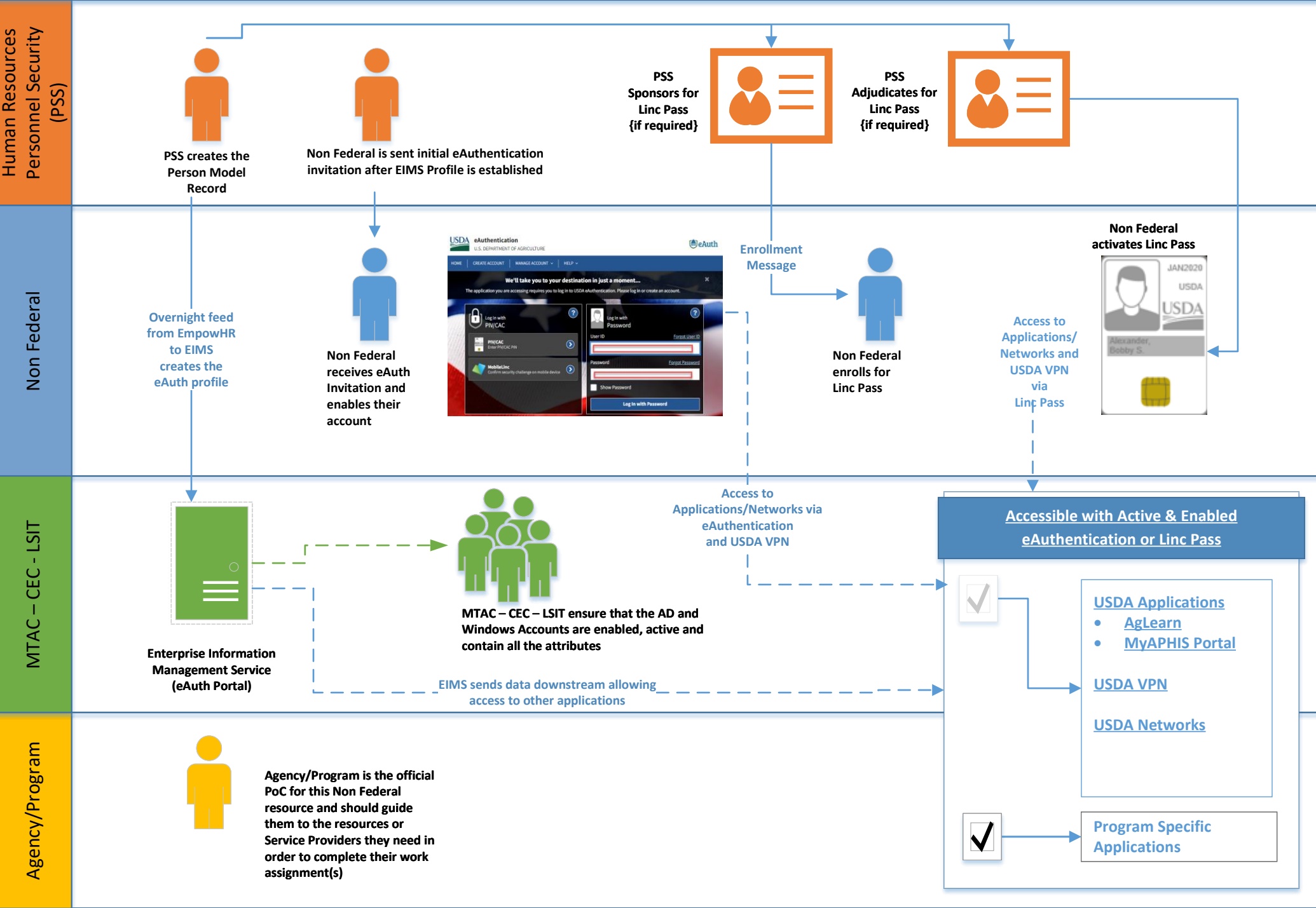
PIV Card – Linc Pass – CAC Card – US Access Credential

For the most part, these names are interchangeable, and all mean the same thing; identification cards that control access to Federally Controlled Facilities and information systems at the appropriate security level.

Site Badge

Site badges are specific to a location, are issued by facility management and are used for building access only.





**UNITED STATES DEPARTMENT OF AGRICULTURE
MARKETING AND REGULATORY PROGRAMS**

**ACTIVE DIRECTORY USER ACCOUNT
PROVISIONING REQUEST FORM**

The information collected will be used to submit a System Authorization Access Request (SAAR) to CEC for the creation of non-privileged active directory (AD) user accounts or transfer of accounts between MRP and other USDA agencies. Five business days advance notice is **required** for all new user account creations/transfers. Supervisors (or their acting/designee) or RMO should email the signed form (as an attachment) with as much information completed to the agent who sent it to you or send to: **Help@USDA.GOV** . This form is for MRP internal use only.

User Contact Information

(All information is required)

1. EMPLOYEE NAME <i>(Last, First, MI)</i>	2. JOB TITLE
3. CITY/STATE	4. AGENCY
5. ORGANIZATION/DIVISION/PROGRAM	6. DEPARTMENT/BRANCH
7. SITE ID	8. OFFICE ID
9. PHONE NUMBER	10. ROOM NUMBER

Type of Action Needed

(One use per form only)

11. ADD NEW USER ACCOUNT AND ACCESS <i>(select only one action)</i> FULL TIME CONTRACTOR INTERN INTERMITTENT	11a. START DATE	11b. END DATE <i>(if intern or intermittent)</i>
12. UPDATE USER ACCOUNT INFORMATION NAME CHANGE PHONE NUMBER SUPERVISOR CHANGE	13. MOVE USER ACCOUNT <i>(including interagency transfers)</i> FROM APHIS/AMS PROGRAM TO APHIS/AMS PROGRAM TRANSFER ACCOUNT FROM APHIS/AMS TO <i>(insert new agency and remove access)</i> TRANSFER ACCOUNT TO APHIS/AMS FROM <i>(insert new agency)</i>	
14. WILL USER NEED AN EMAIL ACCOUNT? YES NO	13a. IS TRANSFER TEMPORARY? YES NO	
	13b. IF YES, WILL USER NEED DUAL AGENCY ACCESS? YES NO	

Account Access Privileges

15. SHARED DRIVES <i>(server/drive/folder)</i>	
16. EMAIL DISTRIBUTION LISTS	
17. SECURITY GROUPS <i>(division or branch)</i>	
18. SHARED MAILBOX <i>(if applicable)</i>	
19. HARDWARE POINT OF CONTACT <i>(if known)</i>	20. HARDWARE POINT OF CONTACT PHONE NUMBER
21. SUPERVISOR NAME <i>(Last, First, MI) (COR if user is a contractor)</i>	22. SUPERVISOR PHONE NUMBER
23. SUPERVISOR SIGNATURE	24. DATE

HRO – 1197 Non-Federal Supplement

Position Information

Agency	Program	Company Name	Company Address		
Point of Contact (POC) First Name	POC Last Name	POC Phone Number	POC E-Mail Address		
Category of Service	Position Title	Start Date	End Date	Duty Station (City)	Duty Station (State)

Access/Background Requirements

USDA eAuthentication (Level 2): Provides employee with a username and password. This username and password provide access to authenticated sites (those that require passwords) that track contracts, programs, and services.

Lincpass: Personal identity verification (PIV) card. Only required if employee needs access to programs where a username and password can't be used. *Sponsorship for a lincpass will not occur until an eQIP is complete by the individual.*

None: The non-federal employee will not have a computer or access to any systems.

Note: Site Badges are not processed by the HR-Personnel Security Section. If you are in need of a Site Badge contact your Individual Security Office.

LEVEL OF BACKGROUND INVESTIGATION REQUIRED:

If you are unaware of the level of BI needed, contact the Classification Specialist

Employee Information

Full Last Name(s)	Full First Name	Full Middle Name (or NMN if none)	Suffix	
Home Street Address	Street Address (Line 2)	City	State	Zip Code
Personal E-mail Address	Phone Number	Government Program Manager's Name:	Government Program Manager's E-mail:	

Required Documents

OF-306 (signed by employee as appointee)

FINGERPRINTS for FBI Background Check

These are to be done at a Fieldprint location; Fieldprint is a company that provides all aspects of the fingerprinting process at more than 1,200 locations nationwide. Follow instructions given by the Personnel Security Department.

Photocopies of 2 Identity Source Documents (provide details of each below)

Ensure documents have not expired and photocopies are legible.

ISA Test Completion Certificate

This can be taken here: <https://deliver.courseavenue.com/Login/usda>

**Photocopy of Government Issued Social Security Card

**This applies to Non-U.S. Citizens.

Send Items to Personnel Security

Send All Documents To: USDA/APHIS/MRPBS/HRD - Personnel Security
Sponsor: