UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

MANUAL FOR COMPLETING AN ELECTRONIC OPM 1665

FEBRUARY 2012

Revision History

Revision Number	Revision Date	Description
1.0	February 2012	Initial Release
1.1	March 1, 2012	Revision due to form change; update glossary
1.2	March 22, 2012	Revision due to form modification
1.3	April 4, 2012	Revise options for LAN and Mainframe User Accounts
1.4	May 30, 2012	Update information regarding Submission Options
2.0	October 1, 2013	Updated to reflect changes in version 2.0

PRIOR TO INTIATING A REQUEST:

Please verify the email address for the applicant/employee prior to submitting the request. If an incorrect email address is entered the applicant/employee will not receive the invitation to access the system and the request must be deleted and recreated.

CONTENTS

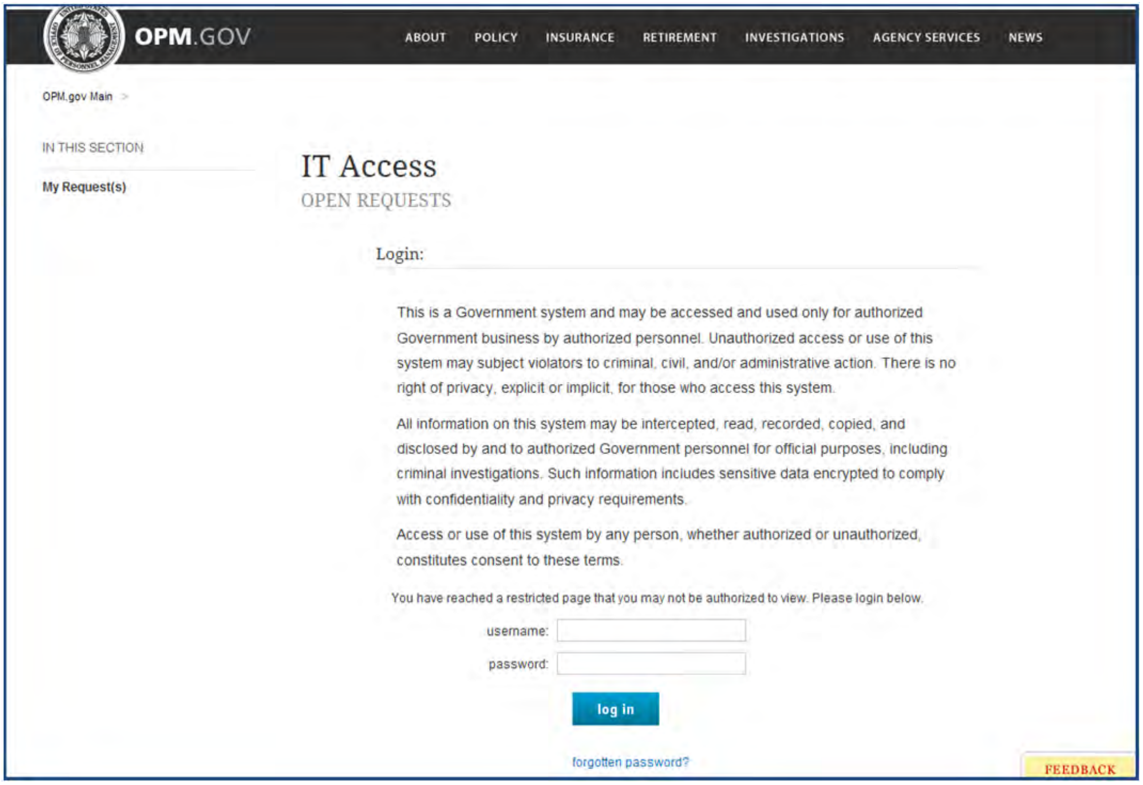
USER MANUAL FOR THE e-1665, IT ACCESS REQUEST FORM

The electronic OPM Form 1665 (e-1665) **must be completed** for the following reasons:

- A new employee who needs access to an OPM system.
- An existing employee who needs new access to an OPM system.
- An existing employee has a significant change to their duties (e.g. transfer, promotion, new manager, new title).
- A contract employee begins work under a new contract. Includes detail assignments.
- Every five (5) years authorized users of OPM IT systems need to refresh their IT Access Request Form

An e-1665 Form **does not** need to be completed for changes to existing system access, for example an employee has PIPS access but needs details of their existing access changed. Changes to existing access may be submitted via email to fisaccesscontrol@opm.gov.

The form has been converted to an electronic format and can be found at **http://www.opm.gov/ITAccess/Requests/Index.aspx**



IT Access

OPEN REQUESTS

Login:

This is a Government system and may be accessed and used only for authorized Government business by authorized personnel. Unauthorized access or use of this system may subject violators to criminal, civil, and/or administrative action. There is no right of privacy, explicit or implicit, for those who access this system.

All information on this system may be intercepted, read, recorded, copied, and disclosed by and to authorized Government personnel for official purposes, including criminal investigations. Such information includes sensitive data encrypted to comply with confidentiality and privacy requirements.

Access or use of this system by any person, whether authorized or unauthorized, constitutes consent to these terms.

You have reached a restricted page that you may not be authorized to view. Please login below.

username:

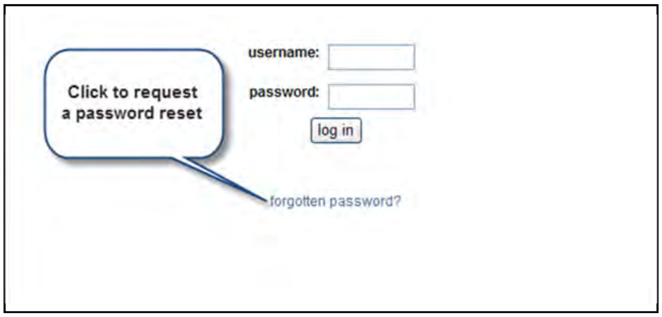
password:

ACCESSING THE SYSTEM: USERNAME AND PASSWORD

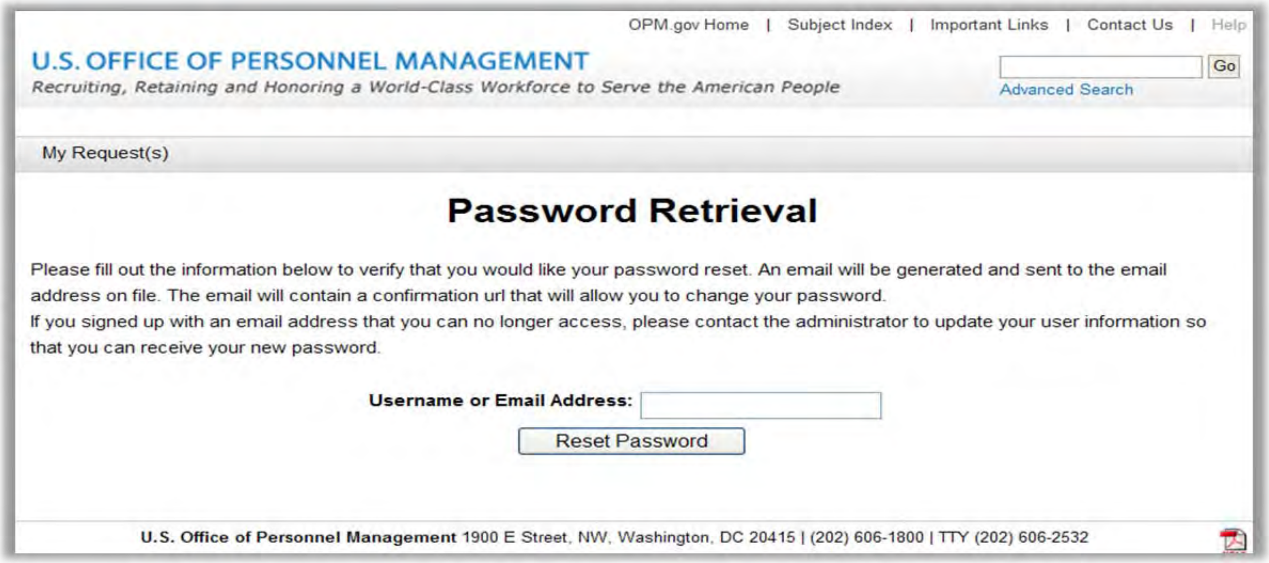
When you are invited into the e-1665 system you will be provided a Username and temporary password. You will be required automatically to change your password upon use. The rules for creating a password are the password must be 8 characters in length and contain 3 of the following: uppercase, lowercase, numeric and/or special character

Once you have established your password you access the system by entering your username, password and then clicking on the log in button.

If you have forgotten your password, click on the **forgotten password?** link as indicated below:



The following page will allow you to enter your username or email address. After entering the information, click on the Reset Password button. A new password will be emailed to your @opm.gov address.


OPM.gov Home | Subject Index | Important Links | Contact Us | Help
U.S. OFFICE OF PERSONNEL MANAGEMENT
Recruiting, Retaining and Honoring a World-Class Workforce to Serve the American People
Go
Advanced Search
My Request(s)

Password Retrieval

Please fill out the information below to verify that you would like your password reset. An email will be generated and sent to the email address on file. The email will contain a confirmation url that will allow you to change your password.
If you signed up with an email address that you can no longer access, please contact the administrator to update your user information so that you can receive your new password.

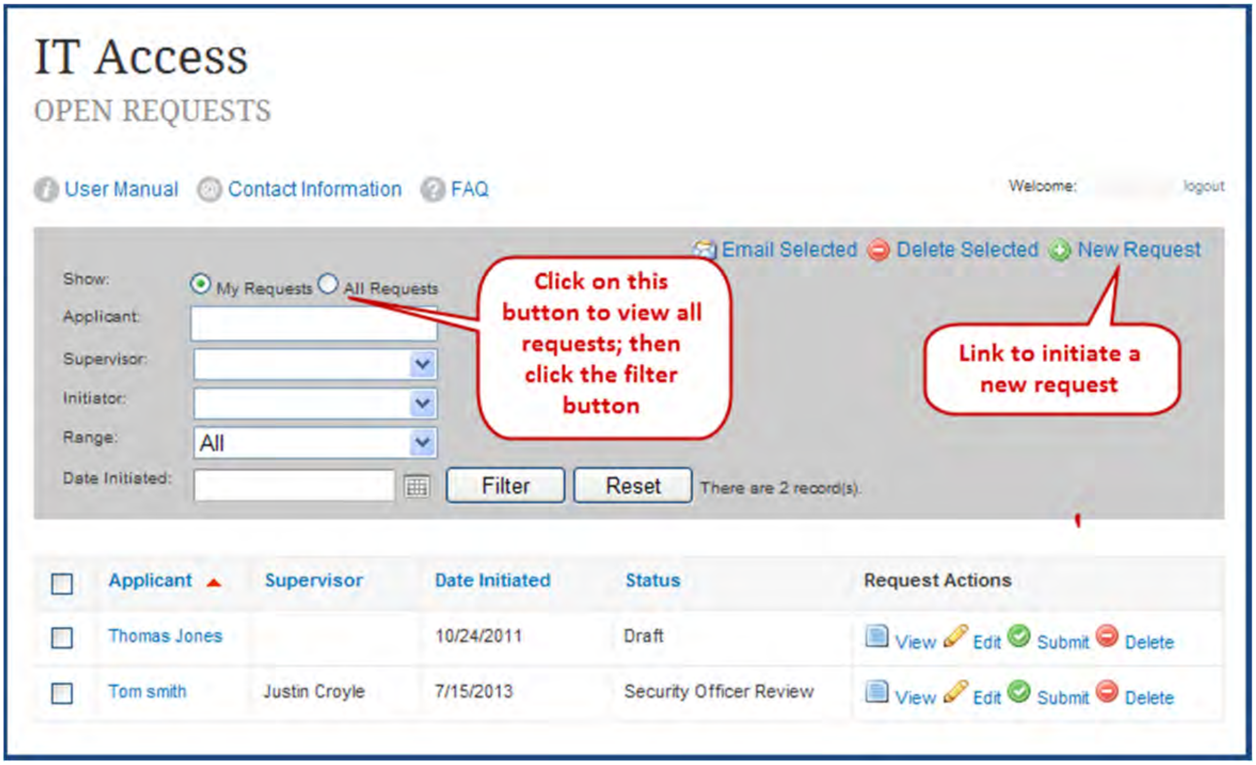
Username or Email Address:

Reset Password

U.S. Office of Personnel Management 1900 E Street, NW, Washington, DC 20415 | (202) 606-1800 | TTY (202) 606-2532

You will receive a temporary password, allowing you to reset the password when you access the system the next time.

The first screen you will see after accessing the system is the following:



IT Access

OPEN REQUESTS

User Manual
Contact Information
FAQ
Welcome:
logout
Email Selected
Delete Selected
New Request
Click on this button to view all requests; then click the filter button
Link to initiate a new request
Filter
Reset

Show: ● My Requests ○ All Requests

Applicant:

Supervisor:

Initiator:

Range: All

Date Initiated:

There are 2 record(s).

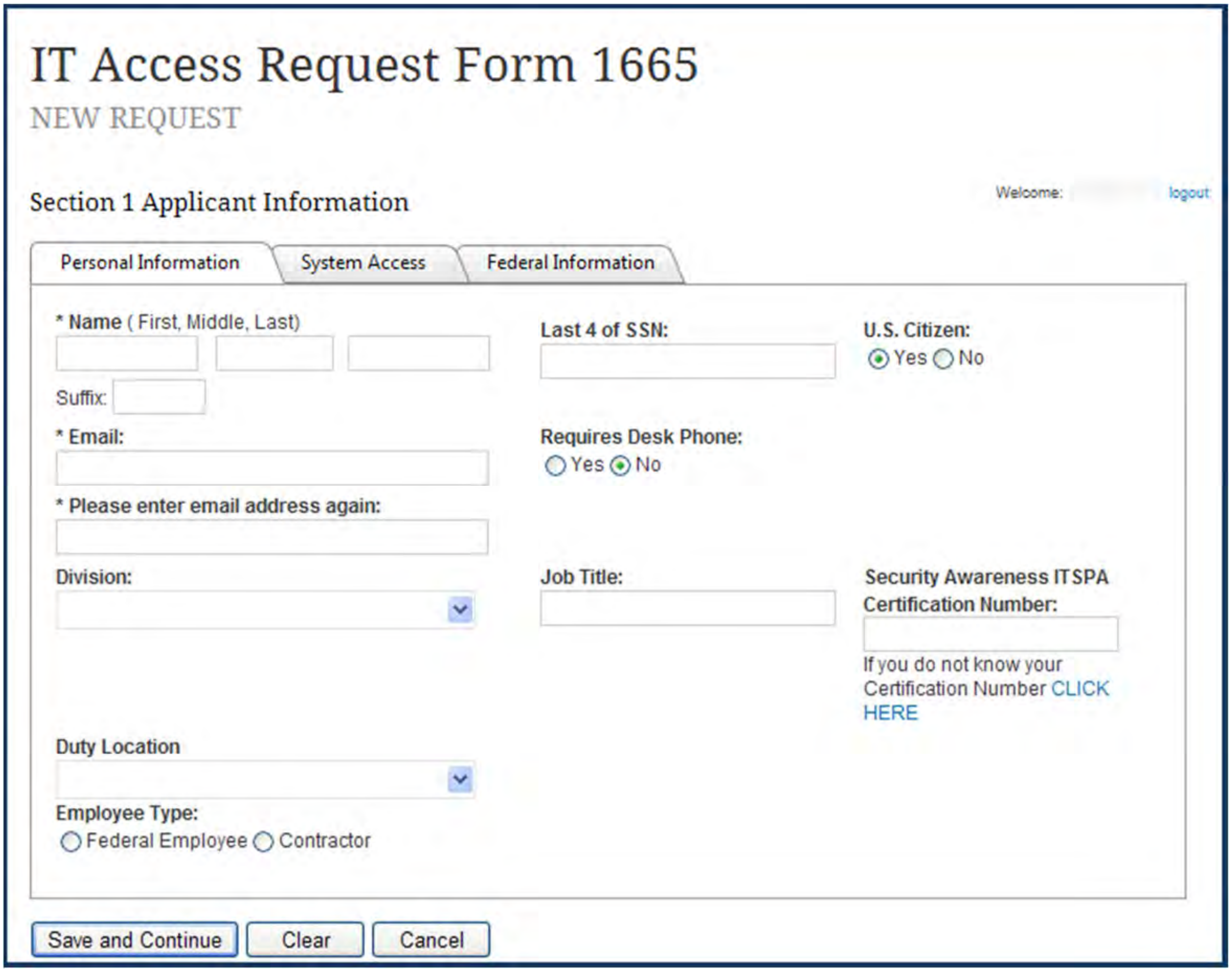
□	Applicant ▲	Supervisor	Date Initiated	Status	Request Actions
□	Thomas Jones		10/24/2011	Draft	View Edit Submit Delete
□	Tom smith	Justin Croyle	7/15/2013	Security Officer Review	View Edit Submit Delete

From this screen you will be able to perform all of the functions necessary to initiate a request for access to FIS systems. Requests that are currently in process and their status would be listed on this screen and can be filtered to reflect their current status. By clicking on the All Requests radio button and selecting Filter you will be able to see the status of requests in your direct line of administration. Requests can also be searched with various criteria, such as Applicant's name, Supervisor's name, who Initiated the request , range (requests initiated for a period of days), or the exact date initiated.

Additionally, to the right of the RESET button is the current number of requests in process. Directly below the Open Requests title are three links that provide shortcuts to an electronic version of the User Manual, Contact Information for assistance in using this application and a Frequently Asked Question (FAQ) section.

STEP 1: INITIATING A REQUEST

After clicking on the New Request link you will see the following screen:



IT Access Request Form 1665

NEW REQUEST

Section 1 Applicant Information

Welcome: [redacted] logout

* Name (First, Middle, Last)

Suffix:

* Email:

* Please enter email address again:

Division:

Duty Location

Employee Type:
○ Federal Employee ○ Contractor

Last 4 of SSN:

Requires Desk Phone:
○ Yes ● No

Job Title:

U.S. Citizen:
● Yes ○ No

Security Awareness ITSPA Certification Number:

If you do not know your Certification Number CLICK HERE

The Personal Information tab is the first of three tabs that need to be completed in order to submit the form. The other two tabs are the System Access and Federal Information tabs.

NOTE: Field blocks with an asterisk are required to be completed for initiation of a request.

PERSONAL INFORMATION TAB

NAME: Enter the first name, middle initial and last name of the individual. There is also a box directly below this line to enter a suffix (such as Jr., Sr., II)

LAST 4 OF SSN: Enter the last 4 digits of the Social Security Number

U.S. CITIZENSHIP: Click on the correct radio button to reflect the individual's citizenship status

EMAIL: Enter the email address of the individual. This will be used to send a message to the individual informing them that a request for access has been initiated and provide the link, username and temporary password for access.

> ***NOTE***: Please verify the email address for the applicant/employee prior to submitting the request. If an incorrect email address is entered the applicant/employee will not receive the invitation to access the system and the request must be deleted and recreated.

REQUIRES DESK PHONE: This option is limited to individuals located at the Theodore Roosevelt Building location in Washington, D.C. Other locations should continue to request phone service/instruments continue following the procedure currently established.

DIVISION: Click on the drop down arrow to the right of the box and select the office to which the individual is/will be assigned.

JOB TITLE: Enter the individual's job title

SECURITY AWARENESS ITSPA Certification Number: This is the certificate number received at the end of the Information Security Awareness Training (https://opmsecurity.golearnportal.org **).** If the applicant does not know their Certificate Number, they can select the phrase "CLICK HERE" below the field. This link will bring up the OPM IT Security & Privacy Awareness Training site and allow the applicant to look up their certificate number. ***NOTE: A new employee must complete the training and receive a certificate number as soon as possible. The e-1665 cannot be processed without this information.***

DUTY LOCATION: Click on the drop down arrow to the right of the box and select one of following duty locations:

Other – To be used if the individual's work location is not included in the preset listing; please specify the work location in the box that pops up to the right of this option

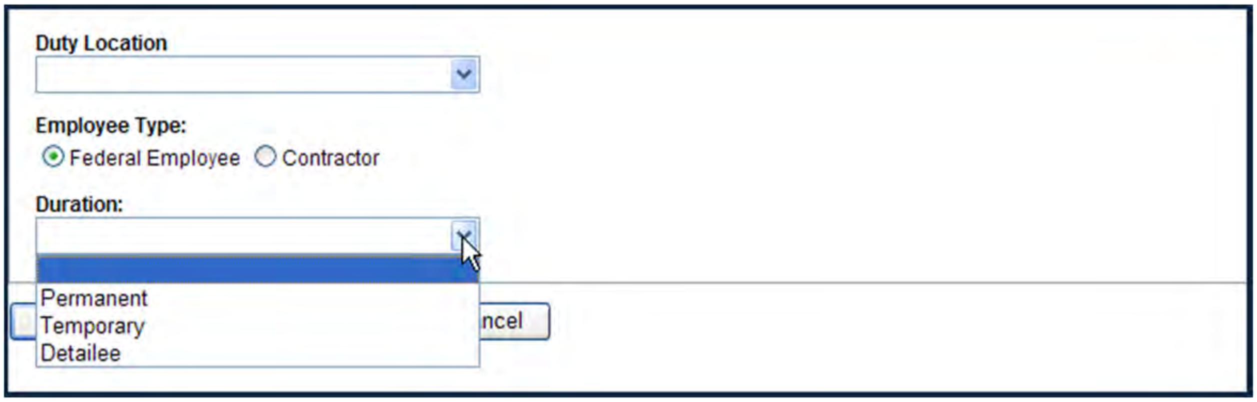
1900 E Street, NW – After selecting this option, enter the Room Number in the box that pops up to the right of this option

Macon, GA – no additional information is required for this option

Boyers/Pittsburgh – After selecting this option, enter the specifics pertaining to the work location in the box that pops up to the right of this option

Region/Field Office – After selecting this option, enter the appropriate distribution list information pertaining to the specific office in the box that pops up to the right of this option

EMPLOYEE TYPE: Select the appropriate radio button indicating whether this is a Federal Employee or Contractor employee



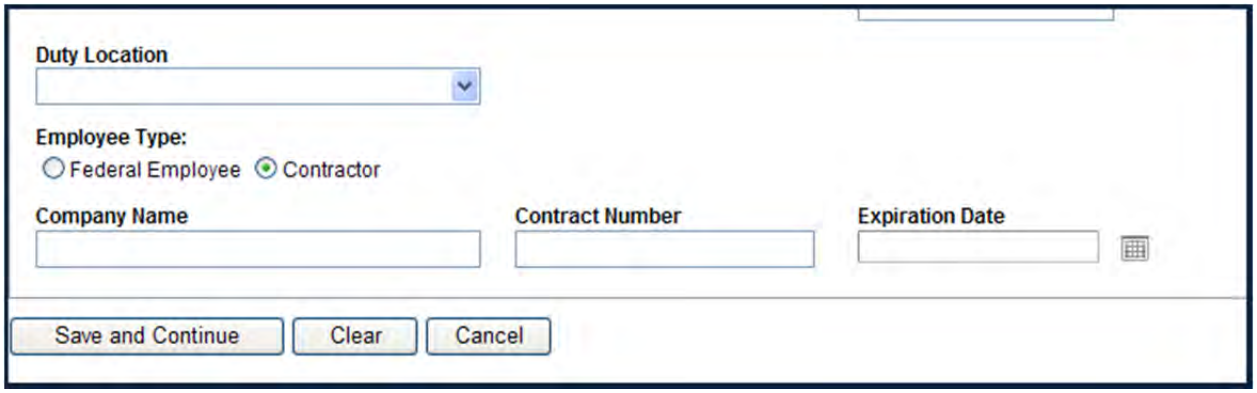
Duty Location

Employee Type:

● Federal Employee ○ Contractor

Duration:

Federal Employee – When selected a Duration box pops up below this option; click on the drop down arrow to the right of the box and select the appropriate option (Permanent, Temporary, or Detailee)



Employee Type:
○ Federal Employee ● Contractor

Contractor – When selected three boxes pop up below this option:

Company Name – Enter the name of the contracting group

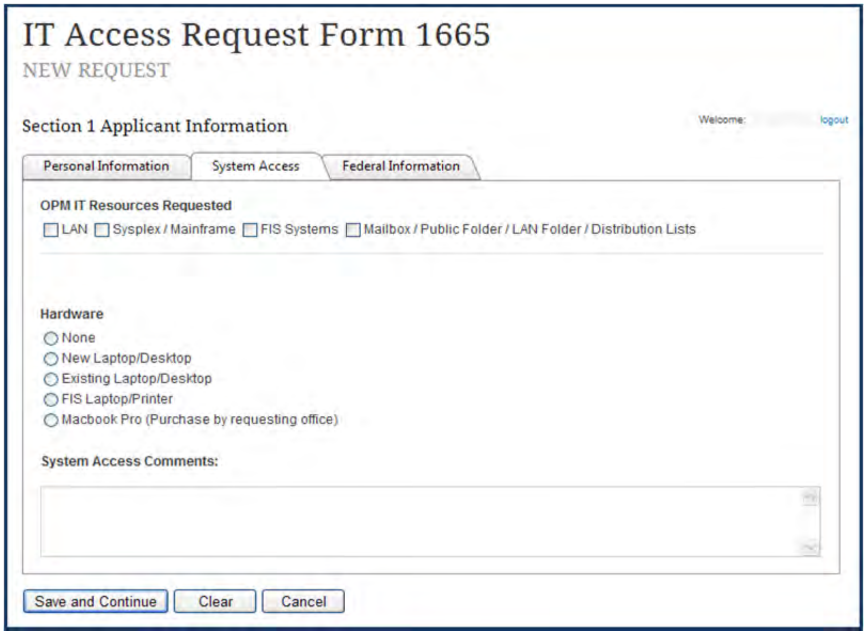
Contract Number – Enter the contract number

Expiration Date – There is a calendar icon to the right of this block; click the icon and select the date the contract expires using the arrow keys at the top of the calendar to move to the appropriate month/year and then select the exact day of the expiration of the contract (NOTE: for an advanced scrolling in the calendar, the double arrows at the top advance/regress the calendar one year)

When you have completed entering all information on this tab, click on the Save and Continue button. This will advance you to the next tab in the form.

SYSTEM ACCESS TAB

This tab will allow you to select various services need to ensure the Applicant can perform their work. Multiple types of access can be requested from this tab, including LAN access, PIPS access, special mailing list and distribution lists, access to shared folders.



IT Access Request Form 1665
NEW REQUEST

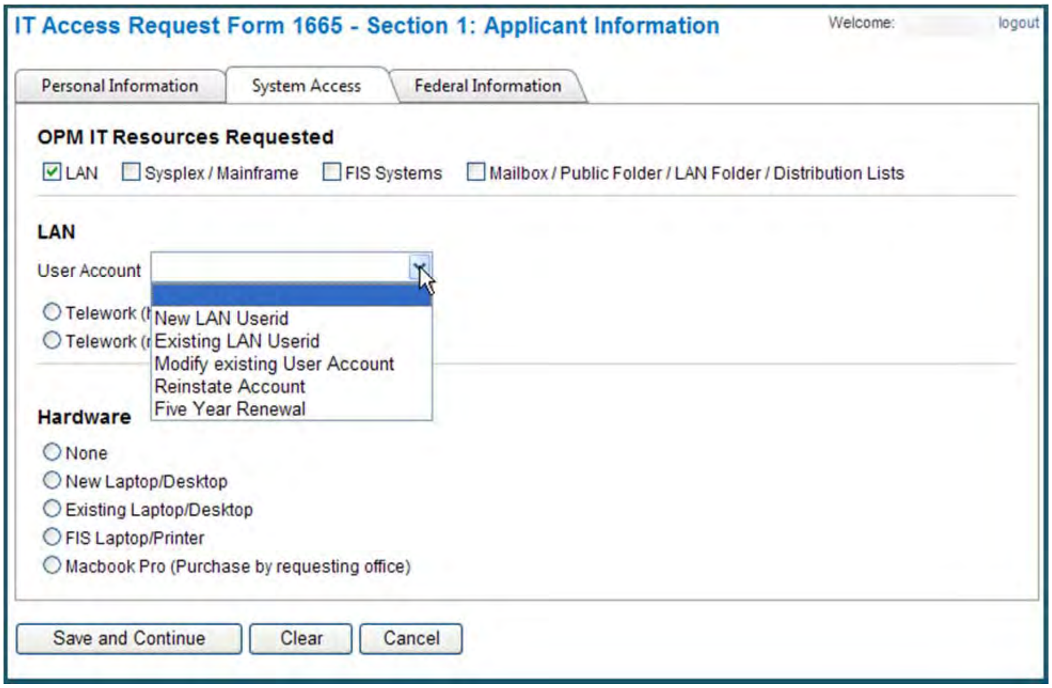
Section 1 Applicant Information

OPM IT Resources Requested
□ LAN □ Sysplex / Mainframe □ FIS Systems □ Mailbox / Public Folder / LAN Folder / Distribution Lists

Hardware
○ None
○ New Laptop/Desktop
○ Existing Laptop/Desktop
○ FIS Laptop/Printer
○ Macbook Pro (Purchase by requesting office)

System Access Comments:

OPM IT RESOURCES REQUESTED: Click on the box next to the service required; multiple boxes may be selected. Options will appear for each box checked; details below:



IT Access Request Form 1665 - Section 1: Applicant Information

OPM IT Resources Requested
☑ LAN □ Sysplex / Mainframe □ FIS Systems □ Mailbox / Public Folder / LAN Folder / Distribution Lists

LAN
User Account

Hardware
○ None
○ New Laptop/Desktop
○ Existing Laptop/Desktop
○ FIS Laptop/Printer
○ Macbook Pro (Purchase by requesting office)

LAN: The following blocks need to be completed

USER ACCOUNT: Click on the drop down arrow to the right of the box and select the appropriate item:

New LAN Userid – Select if the user is not currently in the system. After selecting this option you will be required to enter the start date for the new employee. Click on the calendar to the right of the field and select the date the employee will on board with the agency.

Existing LAN Userid – Select if the user is currently in the system; enter the current UserID in the box that appears to the right of this option

Modify existing User Account – Select if the user is currently in the system and needs modification to their current account; enter the current UserID in the box that appears to the right of this option

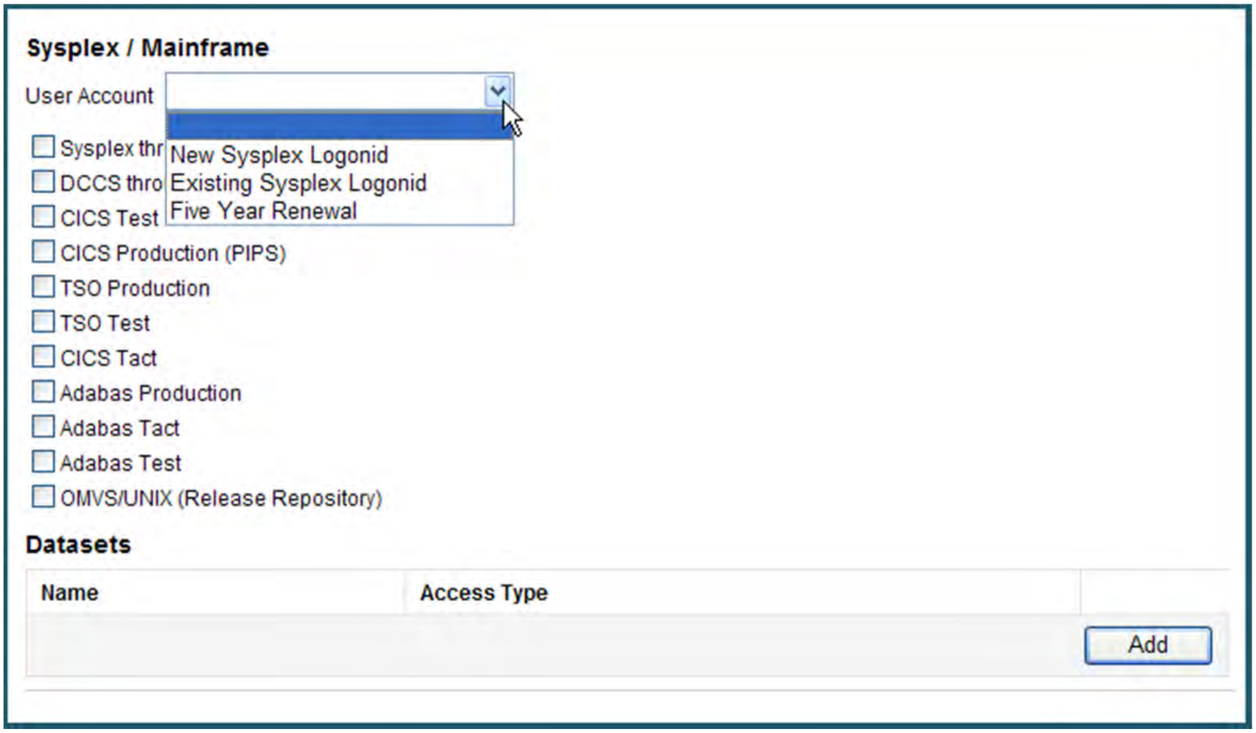
Reinstate Account – Select if the user has been deleted/removed from the system and needs to be restored; enter the UserID for the previous account in the box that appears to the right of this option

Five Year Renewal – Select this option when submitting a request in order to comply with the policy requiring submission of an OPM 1665 every five years to continue access on OPM systems

Below this option are two radio buttons pertaining to Telework (internal OPM employees only; contractor employees should continue to follow established company procedures):

Telework (has PIV card) – Select this option if the Applicant will be teleworking and has completed and been issued a current PIV card

Telework (no PIV card) – Select this option if the Applicant will be teleworking and has not completed the PIV card process; enter the reason why the Applicant does not have a PIV card in the box that appears immediately below this option



Sysplex / Mainframe

User Account

□ Sysplex thr
□ DCCS thro
□ CICS Test
□ CICS Production (PIPS)
□ TSO Production
□ TSO Test
□ CICS Tact
□ Adabas Production
□ Adabas Tact
□ Adabas Test
□ OMVS/UNIX (Release Repository)

Datasets

Name	Access Type

SYSPLEX/MAINFRAME: Select the type of User Account and select the required systems

USER ACCOUNT: Click on the drop down arrow to the right of the box and select the appropriate type of Logon ID needed:

New Sysplex Logonid – Select this option if the Applicant is requesting access for the first time

Existing Sysplex Logonid – Select this option is the Applicant has been provided access to the system and needs modification to their existing access or reinstatement to the system

Five Year Renewal – Select this option when submitting a request in order to comply with the policy requiring submission of an OPM 1665 every five years to continue access on OPM systems

Sysplex through Citrix – Provides access to the OPM VPN

DCCS through Citrix – Provides access to the Document Case Control System (DCCS); if selected enter the Organization Code (identifies the section or office and displays the current location of the case or document (screen shot of this selection is provided below)

DCCS Org Code: Enter the Org Code for DCCS in this box

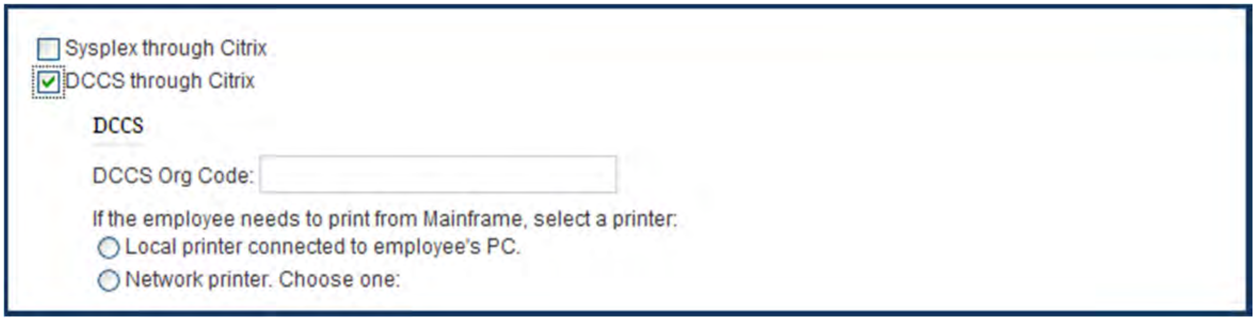
Printer: If the print function for DCCS is needed, select the type of printer that will be used

Local printer connected to employee's PC – Click on radio button to select

Network Printer. Choose one: Click on the appropriate radio button from the options that pop up below this item

Create Y printer – Click on radio button to select

Assign existing network printer – Click on radio button and enter the P Number of the existing printer in the box that appears below this option



□ Sysplex through Citrix

☑ DCCS through Citrix

DCCS

DCCS Org Code:

If the employee needs to print from Mainframe, select a printer:

○ Local printer connected to employee's PC.

○ Network printer. Choose one:

PIPS Test (CICSIQ – DEV/UAT/Training) – Provides access to the PIPS test system through the CICS view

PIPS Production (CICSIP – Production CICS) – Provides access to the PIPS live system through the CICS view

TSO (Time Sharing Option) Production – Provides access to PIPS production through the TSO view

TSO Test – Provides access to PIPS test through the TSO view

TSO CPRO (Operators) - Computer Room Operators; this item is only requested by CDO

Adabas Production – This role is not applicable to FIS

Adabas Tact – This role is not applicable to FIS

Adabas Test – This role is not applicable to FIS

PIPS Development (CICSSIT) – Developers only

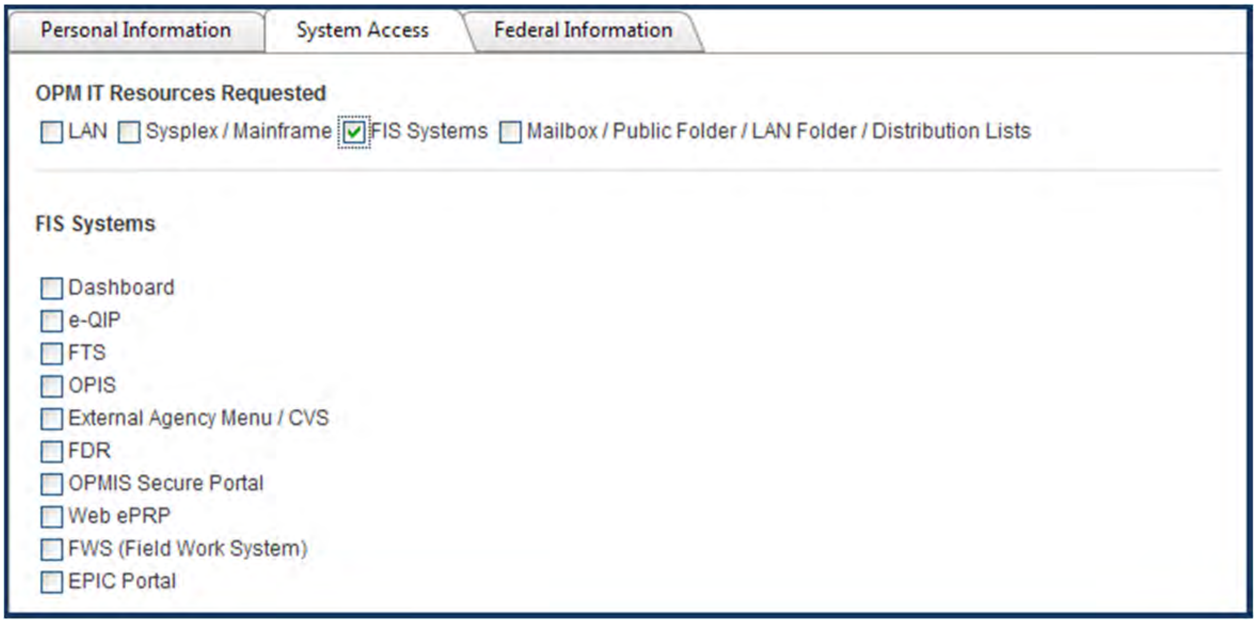
PIPS EPIC SIT (CICSEPIC) – Developers only

DATASETS: Where necessary, enter the Name and Access Type (if required) for any Sysplex/Mainframe system selected – i.e. for OMVS/UNIX type in the following which provides access to RACF groups not listed in the standard options included, such as access to CIRS enter /opm/WTC/data/cirsiph. If additional lines are needed, click the Add button to the right this data block. After entering the name of the dataset, select the Access Type needed:

Read – Allows the user to view the information contained in the dataset

Update – Allows the user to update existing content in the dataset

Alter – Allows the user to modify, delete or add information to the dataset



OPM IT Resources Requested

□ LAN □ Sysplex / Mainframe ☑ FIS Systems □ Mailbox / Public Folder / LAN Folder / Distribution Lists

FIS Systems

□ Dashboard
□ e-QIP
□ FTS
□ OPIS
□ External Agency Menu / CVS
□ FDR
□ OPMIS Secure Portal
□ Web ePRP
□ FWS (Field Work System)
□ EPIC Portal

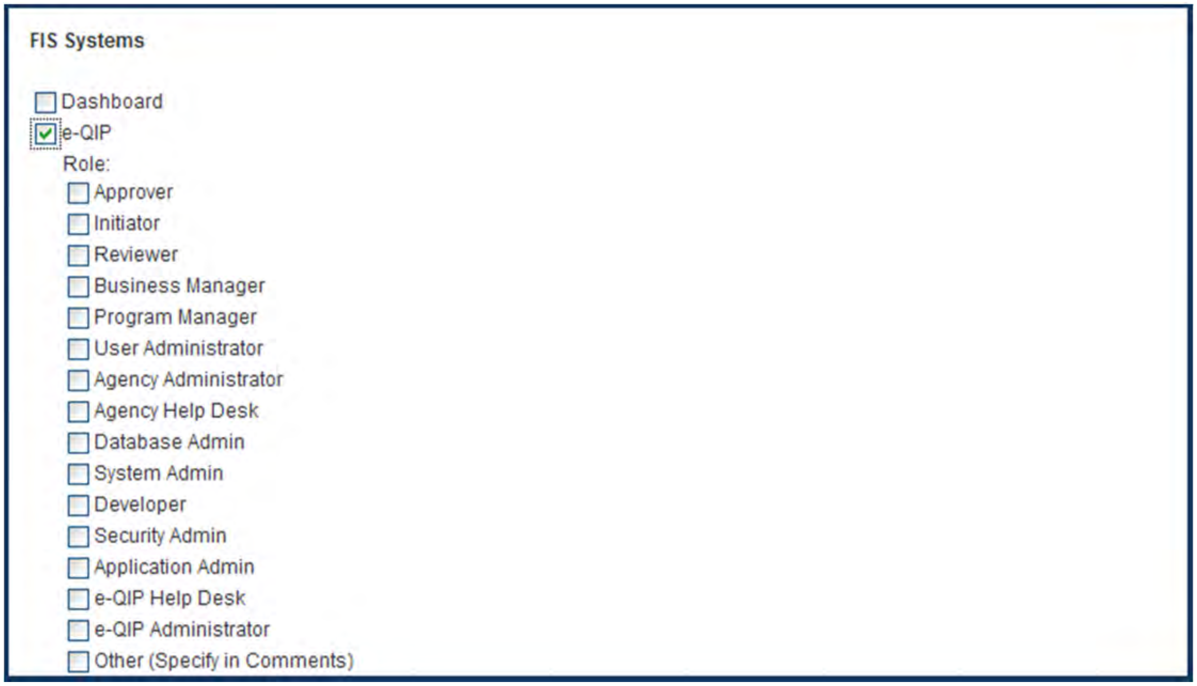
FIS SYSTEMS: Select the systems required by clicking on the box next to the system name

DASHBOARD – Provides access to the FIS Dashboard Management Reporting System. If selected, a drop down field for the Role and Dataset will appear; click on the drop down arrow to the left of the Role field and select the appropriate role type. The dataset field can be left blank. Roles that can be assigned are:

> **User** – This role provides basic access to the Dashboard to execute predefined reports in the appropriate library
>
> **Power User** – This role provides access to the Managed Report Environment (MR); can execute canned reports, shares reports, creates, edits and saves ad hoc reports with Power Painter, Report Assist, and/or Graph Assist using predetermined datasets
>
> **MR Administrator** – This role creates system domains, groups, roles and users; manages user access to reporting domains; creates reports for end users; tests reports submitted by Report Developers and Analysts to ensure information and data are presented in compliance with agency reporting rules and guidelines; creates HTML (web) launch pages; creates and access metadata for data sources; creates reporting objects for managed reporting and Dashboard users; schedules and distributes reports; and customizes user environments
>
> **Library Only User** – This role is accessible to MR users; from this option content stored in the Report library can be viewed
>
> **Developer** – This role has access to the MR to develop reports using Developer Studio; creates, edits and saves reports and reporting objects; submits reports to the MR Administrator for testing and publishing in the appropriate MR environment

Other (Specify in Comments) - This option is provided for all systems in case there is a special circumstance or new role developed and there is a delay in updating the form to provide the new option.

e-QIP (Electronic Questionnaires for Investigations Processing) – Provides access to the FIS e-QIP program for users who need to initiate; review and approve e-QIP requests. If selected, a drop down field for the Role and Dataset will appear; click on the drop down arrow to the left of the Role field and select the appropriate role type. Select the role from the drop down list, as indicated below. If a user needs additional roles, please enter the additional roles in the Dataset box.



FIS Systems

□ Dashboard
☑ e-QIP
Role:
□ Approver
□ Initiator
□ Reviewer
□ Business Manager
□ Program Manager
□ User Administrator
□ Agency Administrator
□ Agency Help Desk
□ Database Admin
□ System Admin
□ Developer
□ Security Admin
□ Application Admin
□ e-QIP Help Desk
□ e-QIP Administrator
□ Other (Specify in Comments)

Approver – A role within the e-QIP system responsible for reviewing Applicant/employee data, approving/rejecting answer(s), entering comments for rejected answer(s), and submitting form(s) to the Investigations Service Providers (ISP) or next higher agency. An approver must be a Federal Employee; contractors cannot be provided this role.

Initiator - A role assigned to an external OPM Federal employee/contractor who can initiate an Applicant/employee, select the form(s) to be completed by the Applicant, completes the Agency Usage Block (AUB), contacts the Applicant/ employee to instruction on how to complete the investigation form(s) using e-QIP, request a reset of Golden Questions, and cancel/un-cancel requests.

Reviewer – A role within the e-QIP system responsible for reviewing Applicant data, accepting/rejecting Applicant/employee answer(s), entering comments for rejected answer(s), and attaching documents.

Business Manager - An Agency User who is capable of generating statistical reports containing requested data within the e-QIP system.

Program Manager – A role within the e-QIP system responsible for performing supervisory tasks including viewing the status of work for the agency, assigning/un-assigning requests, approving/rejecting Golden Question resets, and canceling requests.

User Administrator – A role available in the e-QIP system responsible for managing users who have been provided access and responsibility within their e-QIP compartment.

Agency Administrator - This role within e-QIP (Electronic Questionnaire for Investigative Processing) responsible for managing groups within their own Agency, and Agency attributes and forms.

Agency Help Desk - This is a role within e-QIP that has the ability to check a request or user status, and reset Golden Questions without the concurrence of a second person.

Database Administrator – an internal OPM role assigned to an individual with responsibility for administering the e-QIP database

System Administrator – an internal OPM role assigned to an individual with responsibility for monitoring system hardware and software

Developer – An internal OPM role assigned to an individual with responsibility of programming and maintaining the system application, hardware and database.

Security Administrator – An internal OPM role assigned to an individual with the responsibility of ensuring that all mandated security requirements are being satisfied and followed.

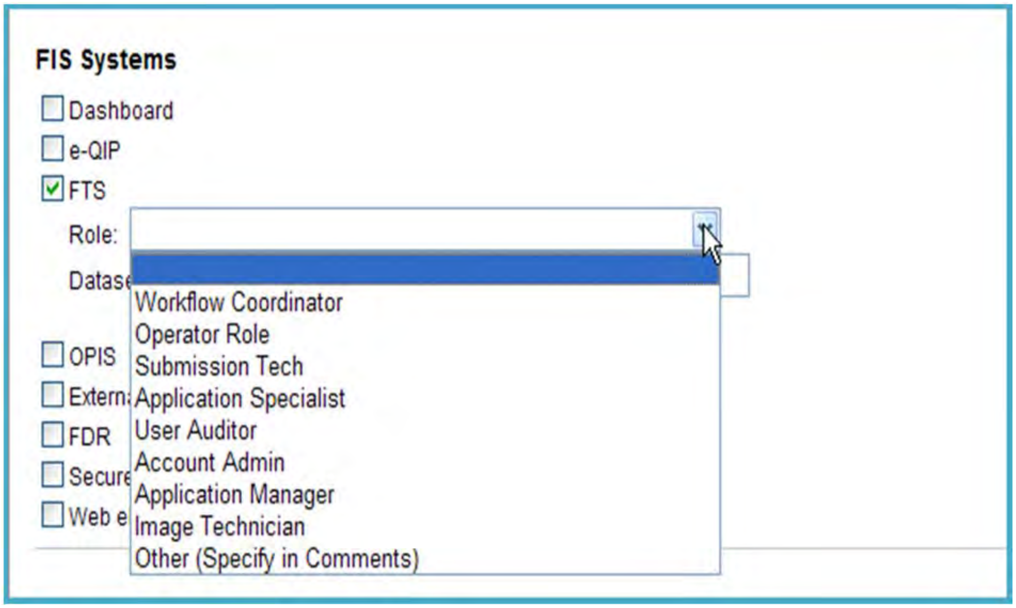
Application Administrator – An internal OPM role assigned to an individual with the responsibility of ensuring this system is available and can process casework.

e-QIP Help Desk – An internal OPM role assigned to an individual with the responsibility of assisting customer agencies with case processing issues using view-only access to the system.

e-QIP Administrator – An internal OPM role assigned to an individual with the responsibility of overseeing the business authorization, building and validation of the system.

Other (Specify in Comments) - This option is provided for all systems in case there is a special circumstance or new role developed and there is a delay in updating the form to provide the new option.

FTS (Fingerprint Transaction System) – Provides access to the automated system used to route fingerprints between an agency, OPM and the Federal Bureau of Investigation (FBI).



FIS Systems

□ Dashboard
□ e-QIP
☑ FTS
Role:
Datas
□ OPIS
□ Extern
□ FDR
□ Secure
□ Web e

Workflow Coordinator – A role within the FTS system that can view, scan, search and see the status of Submission Event List and Submission Event Search; Failed Admission Totals and Failed Admission Search; PIPS Event List; Overdue Submission Totals and Overdue Submission Details; FBI Error Totals and FBI Error Detail; Scan Event List and Scan Event Search; in addition to the functionality of a User Auditor (below).

Operator Role – A role within the FTS system that provides the ability to do the following functions: Case Number Search; Submission Search, Pips File Search.

Submission Tech – A role within the FTS system that provides the following functions: Manual Reprint Processing, Submission Deletion.

Application Specialist - A role within the FTS system that can retrieve and resend FBI Data by case number; retrieve PIPS file data by filename in text format; and can change a case number within certain restrictions.

User Auditor – A role within the FTS system that provides basic access, including the ability to view Processing Totals, State Count, and Current Scanner Status.

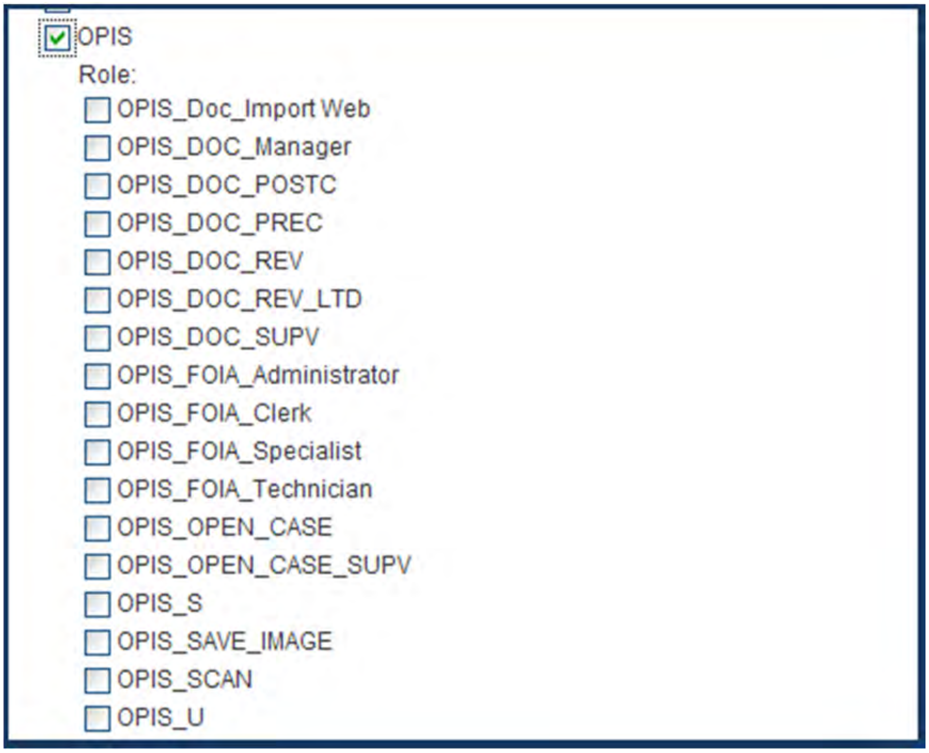
Account Admin – A role within the FTS system that can View, Delete, Enable/Disable, Change Password, and Add New User Accounts; can create new user roles (FIS personnel), and create a user name/password for external users who access the system via dial-up or VPN.

Application Manager - A role within the FTS system that Manages Quartz Jobs/Applications; this is strictly for administration uses, allowing turn on/off functionality behind the scenes.

Image Technician – A role within the FTS system that validates the Card Image and verifies the fingerprint card scanned successfully.

Other (Specify in Comments) - This option is provided for all systems in case there is a special circumstance or new role developed and there is a delay in updating the form to provide the new option.

OPIS (OPM Imaging System) – Provides access to the FIS Imaging System.   If selected, a drop down field for the Role and Dataset will appear; click on the drop down arrow to the left of the Role field and select the appropriate role type.   The dataset field is used to list multiple access levels since the Role field only allows listing of one item.



☑ OPIS

Role:

□ OPIS_Doc_Import Web

□ OPIS_DOC_Manager

□ OPIS_DOC_POSTC

□ OPIS_DOC_PREC

□ OPIS_DOC_REV

□ OPIS_DOC_REV_LTD

□ OPIS_DOC_SUPV

□ OPIS_FOIA_Administrator

□ OPIS_FOIA_Clerk

□ OPIS_FOIA_Specialist

□ OPIS_FOIA_Technician

□ OPIS_OPEN_CASE

□ OPIS_OPEN_CASE_SUPV

□ OPIS_S

□ OPIS_SAVE_IMAGE

□ OPIS_SCAN

□ OPIS_U

OPIS Doc Import Web *– Not yet in production.*

OPIS Doc Manager - Users have the ability to search where all documents reside in Stellent as well as be able to view the Agency Delivery DIF

OPIS Doc PostC – A role within the OPIS system that provides users access to Stellent and the ability to search and retrieve ALL case document images in 'Closed' case only.

OPIS Doc PreC – A role within the OPIS system that provides users the ability to prepare case documents, Oliver, Scan, Re-scan and QA.

OPIS Doc Supv – This role within the OPIS system provides users the ability to prepare case documents, Scan, Re-scan, QA, delete from Captiva and POSTC (if in this group), search and retrieve ALL documents before and after committal to the Stellent database. This role is provided to individuals who need the ability to perform all functions (except for FOI/P).

FOIA/P User – This role is assigned to an individual with OPIS access that provides special limited access to the Freedom of Information/Privacy Act personnel and select individuals based upon their job requirement

OPIS FOIA Administrator – OPIS Redact Users

OPIS FOIA Clerk – OPIS Redact Users (View & Redact Access)

OPIS FOIA Specialist – OPIS FOIA Supervisors

OPIS FOIA Technician - OPIS FOIA Users

OPIS Open Case – This role within the OPIS system provides users the ability to see images for cases that are currently in process.

OPIS Open Case Supv – Ability to modify and delete images in Open Case through EDA

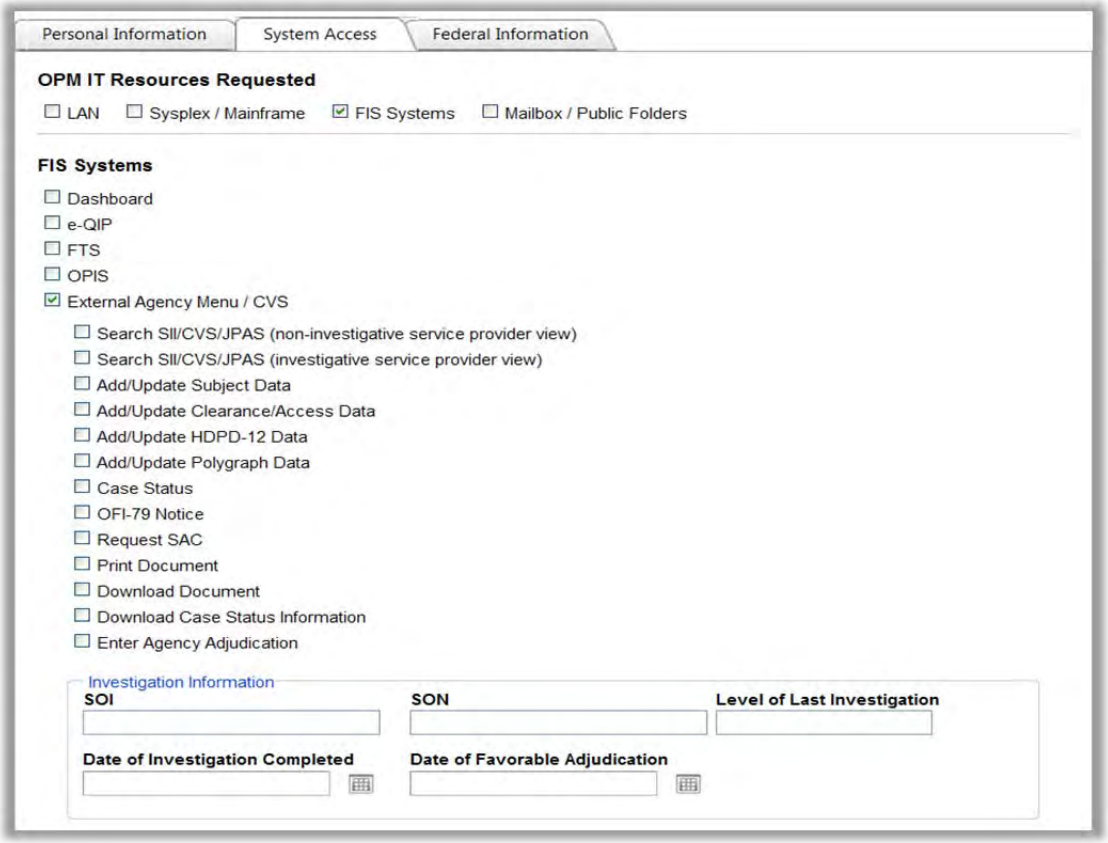
OPIS S – OPIS Application Systems Group

OPIS Save Image – This group was going to be used for EDA 3.6, but never implemented

OPIS Scan – OPIS Captiva Users (Scan, Re-scan and Index Access)

OPIS U – Needed for all OPIS Users

External Agency Menu/CVS –External Federal Agency Users only. This option provides access to the PIPS system through either the OPM Secure Portal or VPN Stand-Alone for external federal agency employees/contractors. Click on each item to provide appropriate access by selecting the box in front of the option. Additionally, when selecting the first or second option to Search SII/CVS/JPAS, chose only one; the PIPS system will not allow both options to be selected for a user.



OPM IT Resources Requested

□ LAN □ Sysplex / Mainframe ☑ FIS Systems □ Mailbox / Public Folders

FIS Systems

□ Dashboard
□ e-QIP
□ FTS
□ OPIS
☑ External Agency Menu / CVS

- □ Search SII/CVS/JPAS (non-investigative service provider view)
- □ Search SII/CVS/JPAS (investigative service provider view)
- □ Add/Update Subject Data
- □ Add/Update Clearance/Access Data
- □ Add/Update HDPD-12 Data
- □ Add/Update Polygraph Data
- □ Case Status
- □ OFI-79 Notice
- □ Request SAC
- □ Print Document
- □ Download Document
- □ Download Case Status Information
- □ Enter Agency Adjudication

Investigation Information

SOI	**SON**	**Level of Last Investigation**
Date of Investigation Completed	**Date of Favorable Adjudication**	

Search SII/CVS/JPAS - A role within the PIPS for non-OPM Federal Agency employees/ contractors. The CVS contains information on security clearances, investigations, suitability and fitness determinations. HSPD-12 , PIV credentials, and polygraph data. A search of CVS performs a simultaneous search of the SII, CVS and JPAS systems. There are two options for this function:

Non-Investigative Service Provider View – select if OPM conducts your investigations

Investigative Service Provider View – only allowed to agencies who are set up in PIPS as an investigative agency

Add/Update Subject Data - This function allows external OPM federal agencies the ability to add a Subject record to the system. Subjects should only be added to CVS to support the reporting of clearances, investigative data, HSPD-12 credentials and polygraphs in accordance with reciprocity policies. Updates to Subject records are required to be entered by the FIS Agency Systems and Liaison at (724) 794-5612 x 4600.

Add/Update Clearance/Access Data - This function allows external OPM federal agencies the ability to submit clearance records to the Central Verification System (CVS).

It allows the user to add new clearance information and update existing clearances in order to maintain the accuracy of the CVS.

Add/Update HDPD-12 Data - This function allows external OPM federal agencies the ability to post and modify reciprocal Homeland Security Personnel Directive-12 (HSPD-12) determinations to the CVS.

Add/Update Polygraph Data - This function allows external OPM federal agencies the ability to report full scope and counterintelligence polygraph data. Agencies can also modify their polygraph data contained in the CVS.

Case Status - Authorized agency officials can obtain the overall status of a case. Detailed information about the case is located on the "Case Assignments Tracking Screen" (CATS), such as the status and result of each item in the case. Users can only view case information on those cases attributed to the Security Office Identifier (SOI) of the User ID.

OFI-79 Notice - This option is used in conjunction with providing access to external Federal Agencies. Federal Investigative Service Providers (ISPs) use this function to report their investigations electronically to OPM's SII as required by Executive Order 10450. ISPs can conduct a CVS search through this function and request OPM files.

Request SAC (Special Agreement Checks)- This function provides for direct request and initiation of SAC. A written agreement is required between the agency and OPM.

Print Document - This function enables agency SOIs to print from their PIPS Terminal. Agencies can print: OPM Investigation Scheduled Notices, Advance Fingerprint Reports, Advance NAC Reports, and/or Case Closing Transmittals with results of investigations. A special terminal and agreement with OPM must be in place to request this function.

Download Document – This function enables agency SOIs to download various OPM documents: OPM Investigation Scheduled Notices, Advance Fingerprint Reports, Advance NAC Reports, and/or Case Closing Transmittals with results of investigations. The Download function transmits the information in a .txt file to the SOI. A special terminal and agreement with OPM must be in place to request this function.

Download Case Status Information - Agencies with automated tracking systems of their own, and request a large volume of OPM cases, may arrange for OPM to transmit status information for download by the agency. A special terminal and agreement with OPM must be in place to request this function.

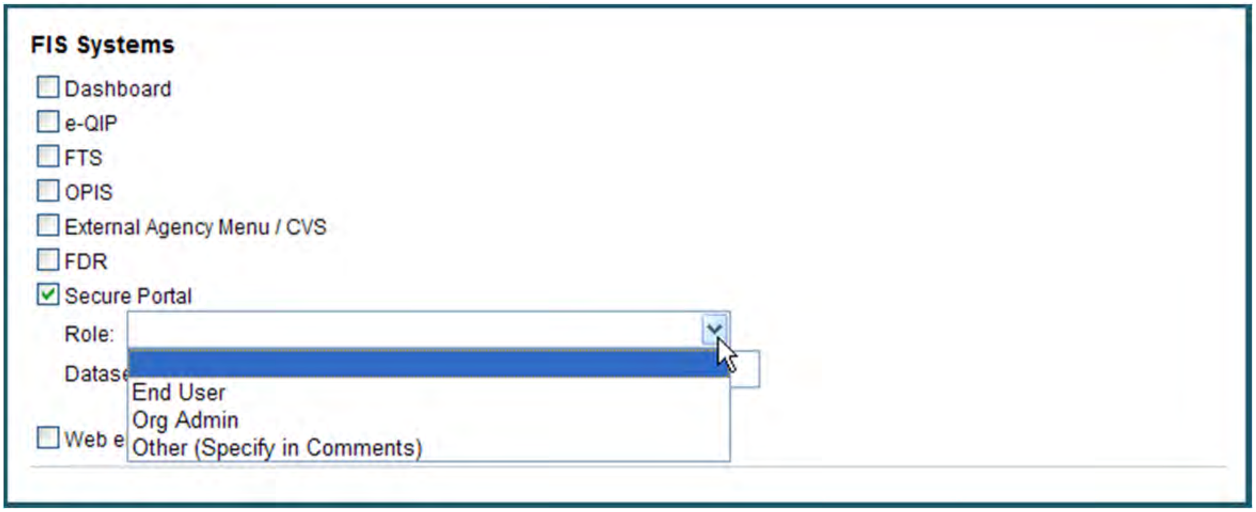
Enter Agency Adjudication - This function enables OPM customers to report the adjudicative action taken on an OPM investigation. Investigative Service Providers (ISPs) can report adjudicative actions on their cases through this function.

***NOTE*: If the agency user requires the ability to Print and/or Download Documents/Case Status Information, VPN access is necessary; these functions are not available through the Secure Portal at this time.**

Investigative Information Section below the External Agency User – Enter the agency's SOI (Security Office Identifier) in the appropriate box; Enter the SON (Submitting Office Number) in the appropriate box, if necessary; Level of Last Investigation – Enter the Applicant's level for which the last investigation was submitted; Date of Investigation Completed – Enter the date that last investigation was completed; Date of Favorable Adjudication – Enter the date on which the submitting agency adjudicated the last investigation. **NOTE:** Dates can be selected by clicking on the calendar icon to the right of each item's box.

FDR (FIS Document Repository) – Provides access to the FIS Document Repository which contains releases executed when an applicant completes an investigative request.

OPMIS Secure Portal – Provides access to the OPM Secure Portal. The Secure Portal contains the link for Agency Users to PIPS, e-QIP and has the link for Agencies to upload CVS information. Additionally, the Secure Portal contains a library of reference information for OPM/FIS and Agency personnel, a secure mail system, and provides a private library location for each user.



FIS Systems

☐ Dashboard
☐ e-QIP
☐ FTS
☐ OPIS
☐ External Agency Menu / CVS
☐ FDR
☑ Secure Portal

Role:

Datas

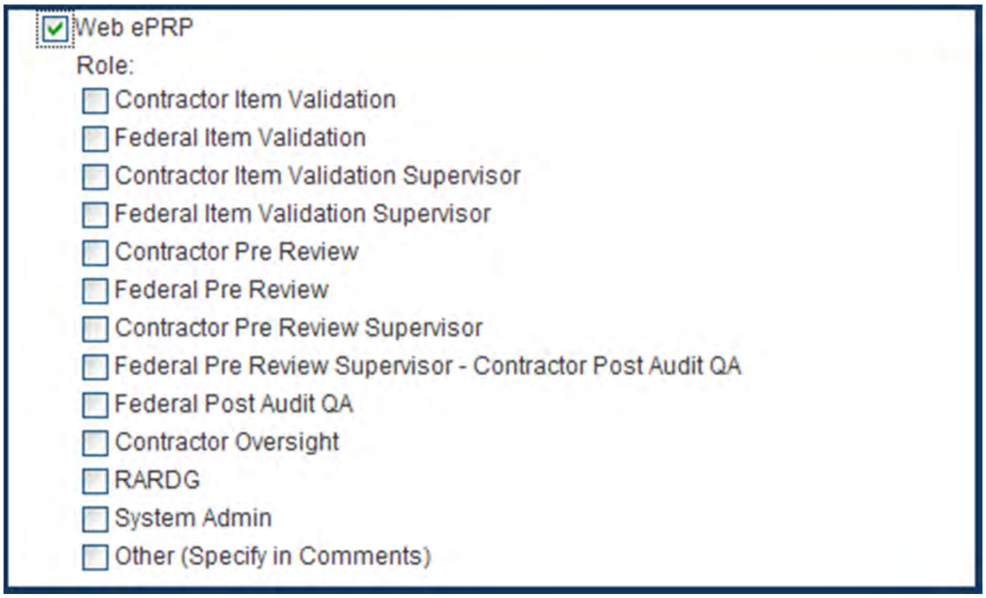
☐ Web e

End User - A role associated with the OPM Secure Portal that provides access to various functions in the system and provides access to Agency Users to e-QIP and PIPS.

Org Administrator - A role associated with the OPM Secure Portal that is provided to internal FIS individuals with administrator responsibilities.

Other (Specify in Comments) - This option is provided for all systems in case there is a special circumstance or new role developed and there is a delay in updating the form to provide the new option.

Web ePRP – This is a web-based electronic Pre-Review Program. Special procedures are required for access to this system, which is used by specific personnel in conjunction with PIPS. After selecting this option, click on the role to select the appropriate function.



☑ Web ePRP

Role:

☐ Contractor Item Validation
☐ Federal Item Validation
☐ Contractor Item Validation Supervisor
☐ Federal Item Validation Supervisor
☐ Contractor Pre Review
☐ Federal Pre Review
☐ Contractor Pre Review Supervisor
☐ Federal Pre Review Supervisor - Contractor Post Audit QA
☐ Federal Post Audit QA
☐ Contractor Oversight
☐ RARDG
☐ System Admin
☐ Other (Specify in Comments)

Contractor Item Validation - A role assigned to an individual with Web ePRP access. This role provides Validation and Pre-Review basic access.

Federal Item Validation Special – A role assigned to an individual with Web ePRP access. This role has not been defined yet.

Contractor Item Validation Supervisor - A role assigned to an individual with Web ePRP access. This role provides Item Validation Supervisor and Pre-Review Supervisor users access to the basic and supervisor functions.

Federal Item Validation Supervisor – A role assigned to an individual with Web ePRP access. This role has not been defined yet.

Contractor Pre Review – A role assigned to an individual with Web ePRP access. This role provides addition access for Post Audit user actions.

Federal Pre Review – A role assigned to an individual with Web ePRP access. This role has not been defined yet.

Contractor Pre Review Supervisor – A role assigned to an individual with Web ePRP access. Not yet defined.

Federal Pre Review Supervisor – Contractor Post Audit QA - A role assigned to an individual with Web ePRP access. This role has not been defined yet.

Federal Post Audit QA – A role assigned to an individual with Web ePRP access. This role has not been defined yet.

Contractor Oversight - A role assigned to an individual with Web ePRP access. Contractor Oversight users have Basic, Supervisor, and Post Audit roles.

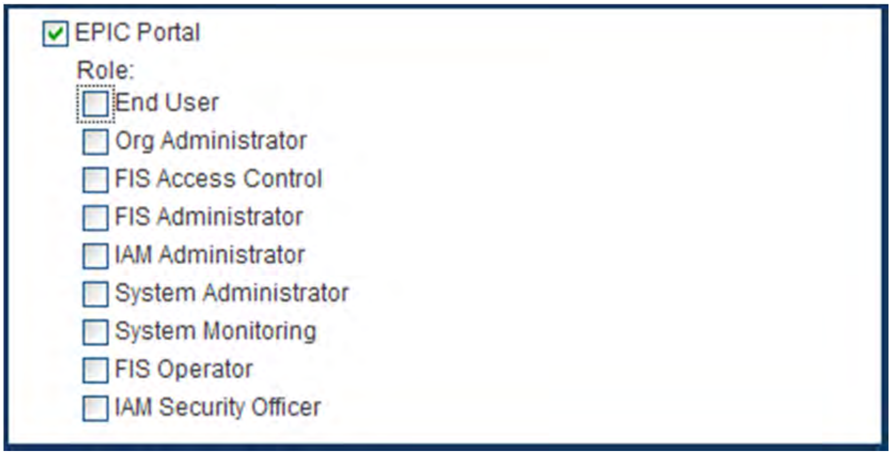
RARDG – Records Access and Research & Development Group

System Administrators - System Administrator Access for maintenance for the system.

Other (Specify in Comments) - This option is provided for all systems in case there is a special circumstance or new role developed and there is a delay in updating the form to provide the new option.

FWS (Field Work System) – The application used by field personnel to record investigative results from interviews, record checks and other information developed during background investigations.

EPIC (e-QIP, PIPS, Imaging and CVS) Portal – OPM's transitional application to integrate current proprietary systems creating a single, standardized and intuitive interface. This system will eventually combine PIPS, e-QIP, FTS, FWS, OPIS, CVS, the OPMIS Secure Portal and the Dashboard Management Reporting System.



☑ EPIC Portal

Role:

□ End User
□ Org Administrator
□ FIS Access Control
□ FIS Administrator
□ IAM Administrator
□ System Administrator
□ System Monitoring
□ FIS Operator
□ IAM Security Officer

End User – Provides basic access to the EPIC Portal to perform daily functions

Org Administrator – To be determined

FIS Access Control – Access provided to members of the Access Control team

FIS Administrator – To be determined

IAM Administrator – Access provided to EPIC Portal database administrators

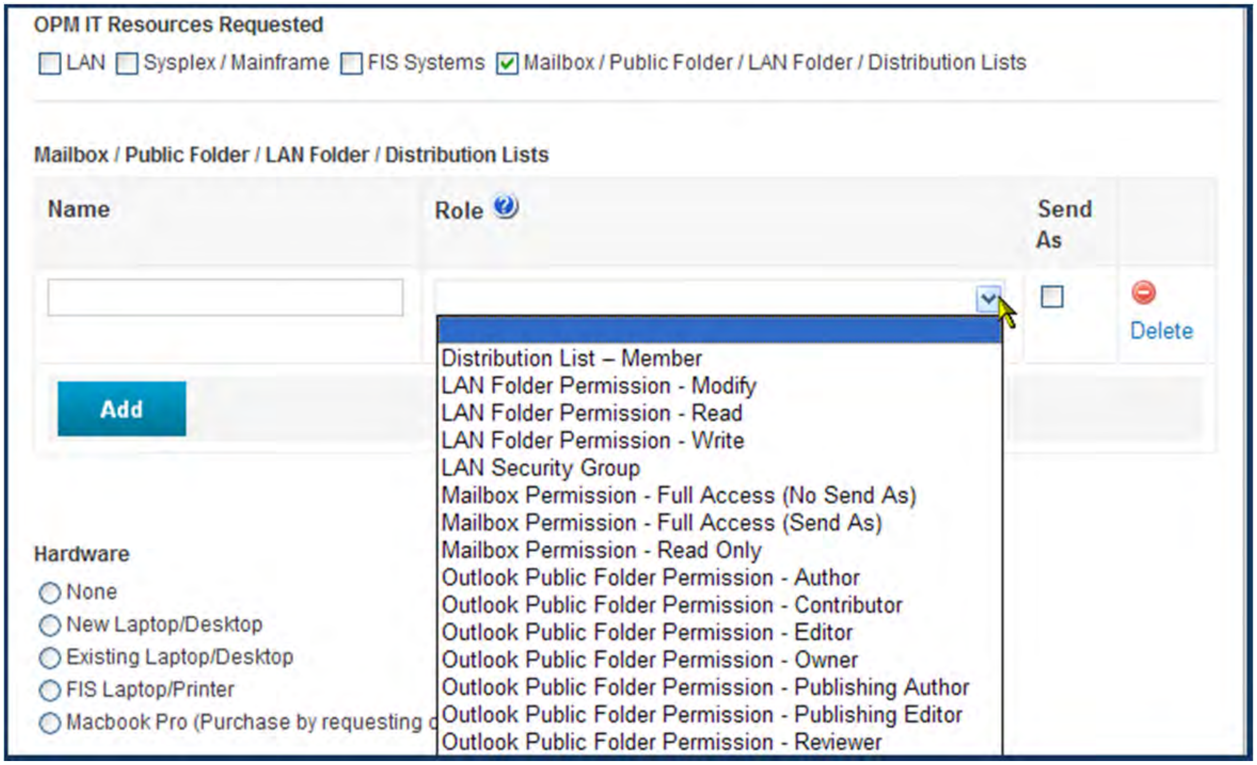
System Administrator – Access provided to Network Management/DCSS personnel responsible for system patches, configuration and installation of hardware/software

System Monitoring – Access provided to Network Management personnel responsible for operation mobility and security

FIS Operator – Access provided to Computer Room personnel responsible for monitoring batch processes, batch printing and password resets for locked accounts only

IAM Security Officer – Access to be provided to the application DSO

MAILBOXES/PUBLIC FOLDER/LAN FOLDER/Distribution Lists: This is the area where any mailbox(es), public folder(s), LAN folders and/or Distribution Lists should be listed which would be necessary for the Applicant to perform at full capacity. To add click on the Add button in the left hand area under Name.



OPM IT Resources Requested

□ LAN □ Sysplex / Mainframe □ FIS Systems ☑ Mailbox / Public Folder / LAN Folder / Distribution Lists

Mailbox / Public Folder / LAN Folder / Distribution Lists

Name	Role	Send As	
		□	Delete

Distribution List – Member
LAN Folder Permission - Modify
LAN Folder Permission - Read
LAN Folder Permission - Write
LAN Security Group
Mailbox Permission - Full Access (No Send As)
Mailbox Permission - Full Access (Send As)
Mailbox Permission - Read Only
Outlook Public Folder Permission - Author
Outlook Public Folder Permission - Contributor
Outlook Public Folder Permission - Editor
Outlook Public Folder Permission - Owner
Outlook Public Folder Permission - Publishing Author
Outlook Public Folder Permission - Publishing Editor
Outlook Public Folder Permission - Reviewer

Hardware

○ None
○ New Laptop/Desktop
○ Existing Laptop/Desktop
○ FIS Laptop/Printer
○ Macbook Pro (Purchase by requesting d

Enter the name of the mailbox, public folder or LAN folder, and the role to be assigned. Definitions of the Role options can be found in the Glossary.

If the individual needs to be able to send from a shared mailbox as a user, click on the **Send As** box.

If a row has been added that is unnecessary, you have the option to delete the request by clicking on the delete button.

The roles for this section are:

Distribution List – Member: This access includes the user as a member that will receive e-mail messages sent to a Distribution List

LAN Folder Permission – Modify: This access allows the user to modify the folder, including deleting subfolders and files, and permissions related to all other lower-level permissions (read and execute, list, write and read). **(NOTE: This is the highest level of permission and does allow for the deletion of files and folders.)**

LAN Folder Permission – Read: This access allows the user to view the files and subfolders in the folder and view other information related to the folder such as ownership, permissions, and file attributes

LAN Folder Permission – Write: This access allows the user to create new contents in the folder, such as subfolders and files; change the folder attributes and view the folder ownership and permissions related to the folder

LAN Security Group:

Mailbox Permission – Full Access (No Send As): This access allows the user to perform standard functions associated with a mailbox, including send, forward, delete and copy messages

Mailbox Permission – Full Access (Send As): This access allows the user to perform all standard functions associated with a mailbox, including send, forward, delete and copy messages

Mailbox Permission – Read Only: This access allows the user to read items in the mailbox, but not modify, add or delete items

Outlook Public Folder Permission – Author: This access allows the user to view all details regarding the folder, create items, edit and delete items they created

Outlook Public Folder Permission – Editor: This access allows the user to view all details regarding the folder, create, modify and delete all items.

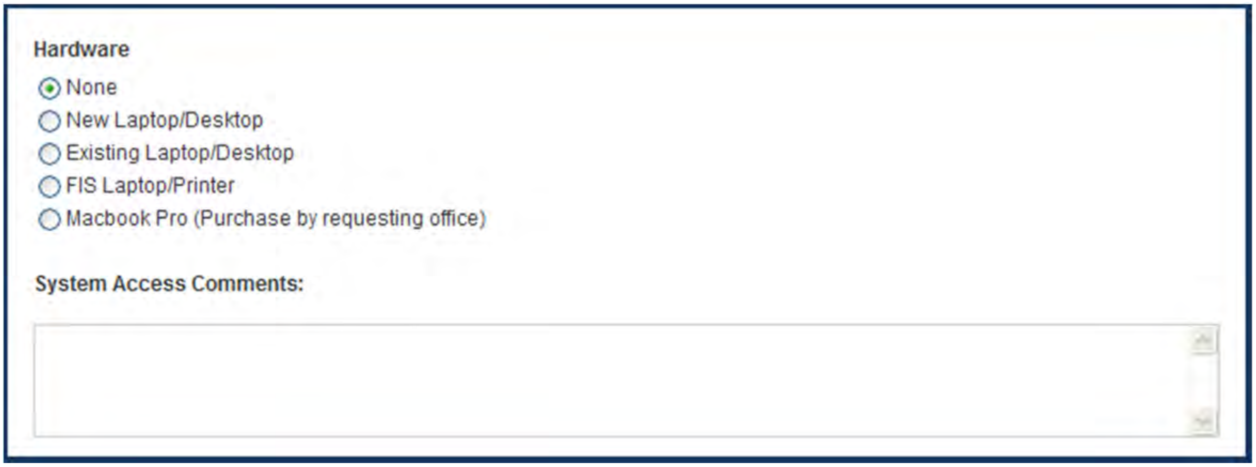
Outlook Public Folder Permission – Owner: This access establishes the user as an owner of the folder with all permissions to access, including create, modify and delete items

Outlook Public Folder Permission – Publishing Author: This access allows the user to view all details regarding the folder, create items and sub-folders, edit and delete items they created

Outlook Public Folder Permission – Publishing Editor: This access allows the user to view all details regarding the folder, and to create, edit, deleted all items, and create sub-folders

Outlook Public Folder Permission – Reviewer: This access allows the user to view the folder and all details associated with the folder

HARDWARE (Internal OPM employee only): Click on the appropriate radio button to select what equipment the individual identified in the request will require.

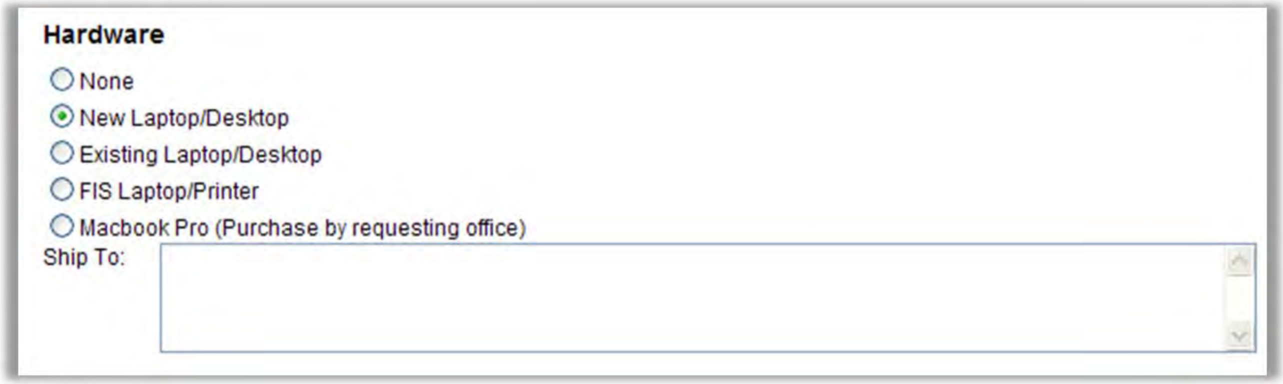


Hardware

● None
○ New Laptop/Desktop
○ Existing Laptop/Desktop
○ FIS Laptop/Printer
○ Macbook Pro (Purchase by requesting office)

System Access Comments:

After selecting any option except None, a Ship To: box will appear. Enter the mailing address to which the equipment should be shipped.



Hardware

○ None
● New Laptop/Desktop
○ Existing Laptop/Desktop
○ FIS Laptop/Printer
○ Macbook Pro (Purchase by requesting office)

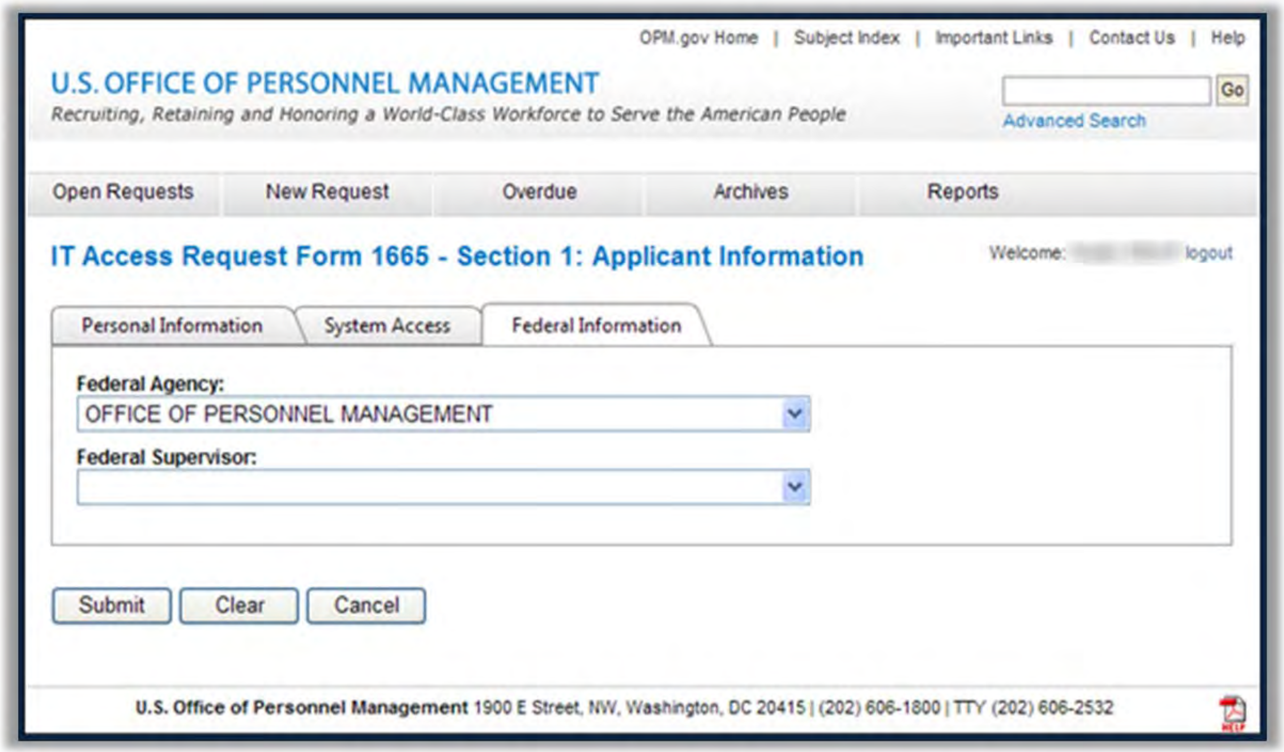
Ship To:

At the bottom of the page is a block called System Access Comments: . Record any special instructions to Facility Access Control or the Help Desk which will clarify this request for access.

When this tab is complete, click on the Save and Continue button at the bottom of the page.

FEDERAL INFORMATION TAB

From this tab the Initiator will select the Federal Agency and the Supervisor that will be approving the access request.


OPM.gov Home | Subject Index | Important Links | Contact Us | Help
U.S. OFFICE OF PERSONNEL MANAGEMENT
Recruiting, Retaining and Honoring a World-Class Workforce to Serve the American People
Go
Advanced Search
Open Requests
New Request
Overdue
Archives
Reports
Personal Information
System Access
Federal Information
Submit
Clear
Cancel

IT Access Request Form 1665 - Section 1: Applicant Information

Welcome: [redacted] logout

Federal Agency: OFFICE OF PERSONNEL MANAGEMENT

Federal Supervisor:

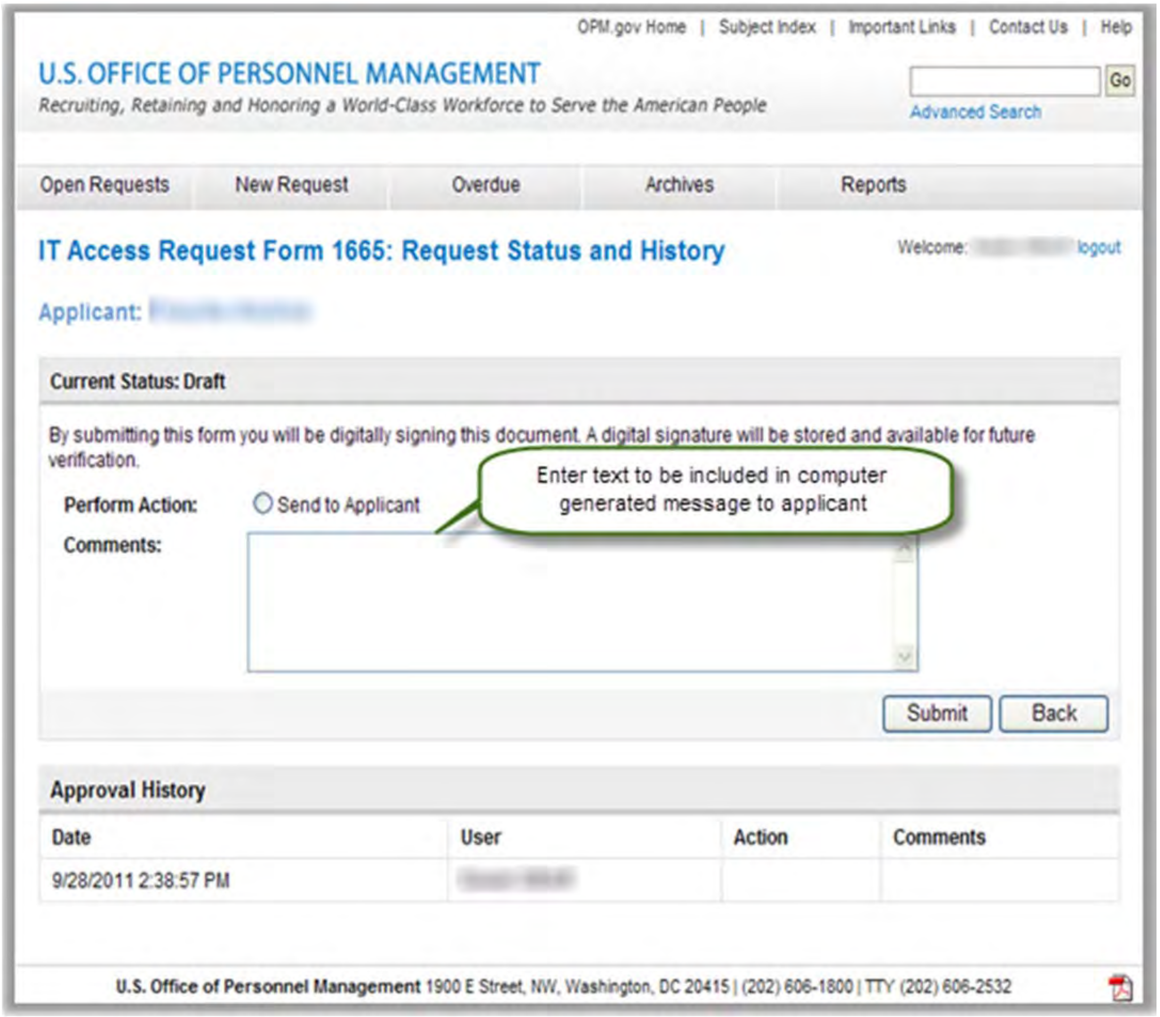
U.S. Office of Personnel Management 1900 E Street, NW, Washington, DC 20415 | (202) 606-1800 | TTY (202) 606-2532

FEDERAL AGENCY: Click on the arrow to the right of the box and scroll down to the agency to which the person being submitted for access belongs.

FEDERAL SUPERVISOR: Click on the arrow to the right of the box and select the appropriate name from the list of federal Supervisors. The list reflects the names of individuals in direct line of supervision for the person being submitted. Please select the name of the first-line Supervisor for the individual or one of their designated authorizers.

When this has been completed, click on the submit button.

After clicking the submit button, the system will display the screen below:


OPM.gov Home | Subject Index | Important Links | Contact Us | Help
U.S. OFFICE OF PERSONNEL MANAGEMENT
Recruiting, Retaining and Honoring a World-Class Workforce to Serve the American People
Go
Advanced Search
Open Requests
New Request
Overdue
Archives
Reports
Submit
Back

IT Access Request Form 1665: Request Status and History

Welcome: [redacted] logout

Applicant: [redacted]

Current Status: Draft

By submitting this form you will be digitally signing this document. A digital signature will be stored and available for future verification.

Perform Action: ○ Send to Applicant

Comments:

Enter text to be included in computer generated message to applicant

Approval History

Date	User	Action	Comments
9/28/2011 2:38:57 PM	[redacted]		

U.S. Office of Personnel Management 1900 E Street, NW, Washington, DC 20415 | (202) 606-1800 | TTY (202) 606-2532

Perform Action: Click on the radio button **Send to Applicant**

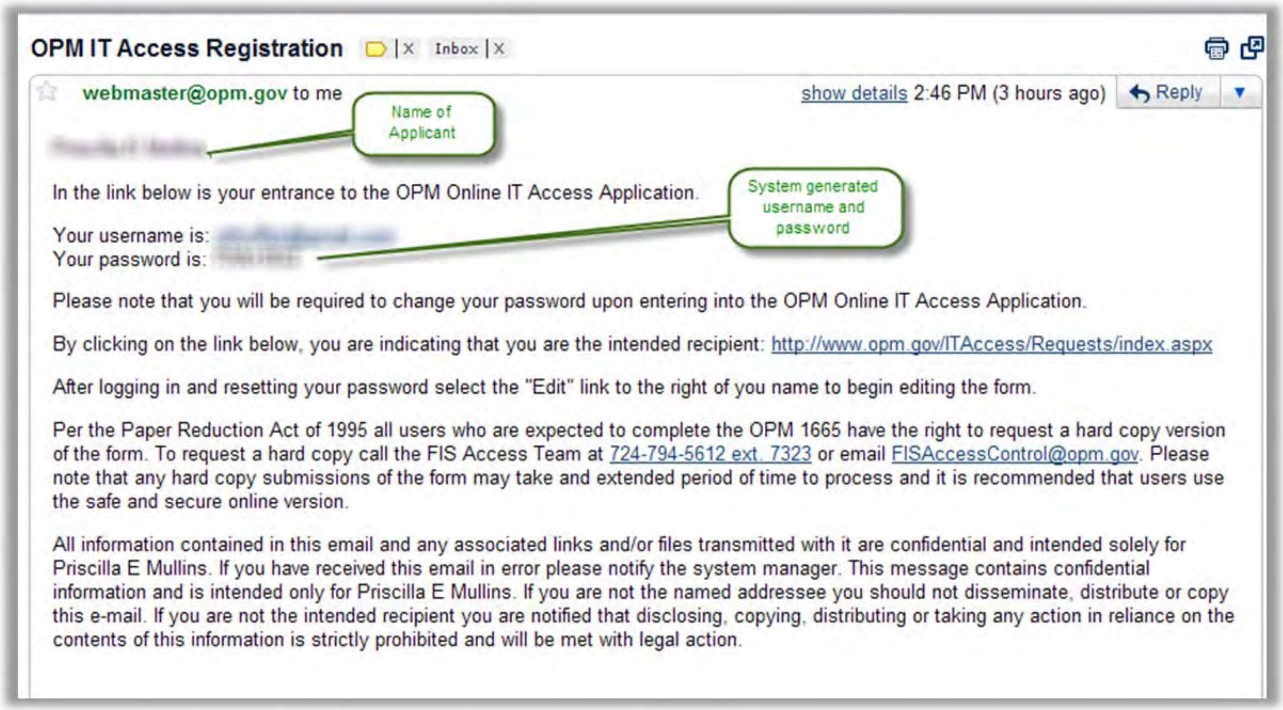
Comments: Enter any special text or instructions that need to be included in a computer generated message that will be sent to the Applicant’s email address included in the Personal Information tab.

Click the Submit button to finalize the request. The Back button will allow you to return to the request and alter information on the application if selected before the Submit button.

When reviewing the status of the request, all **Approval History** will be listed by date.

STEP 2: APPLICANT REVIEW AND PROCESSING

Below is a sample of the message a user receives. The name of the Applicant as entered into the request will be listed as the introduction to the email. The system will generate a username and password for the individual to access the system. As indicated, the message includes an active link for the individual to click to access the system and process the form. Information on how to obtain a hard copy of the form is included to comply with the Paper Reduction Act of 1995, as well as a disclaimer in the last paragraph.


OPM IT Access Registration
Inbox
webmaster@opm.gov to me
show details 2:46 PM (3 hours ago)
Reply
Name of Applicant
System generated username and password

[redacted]

In the link below is your entrance to the OPM Online IT Access Application.

Your username is: [redacted]
Your password is: [redacted]

Please note that you will be required to change your password upon entering into the OPM Online IT Access Application.

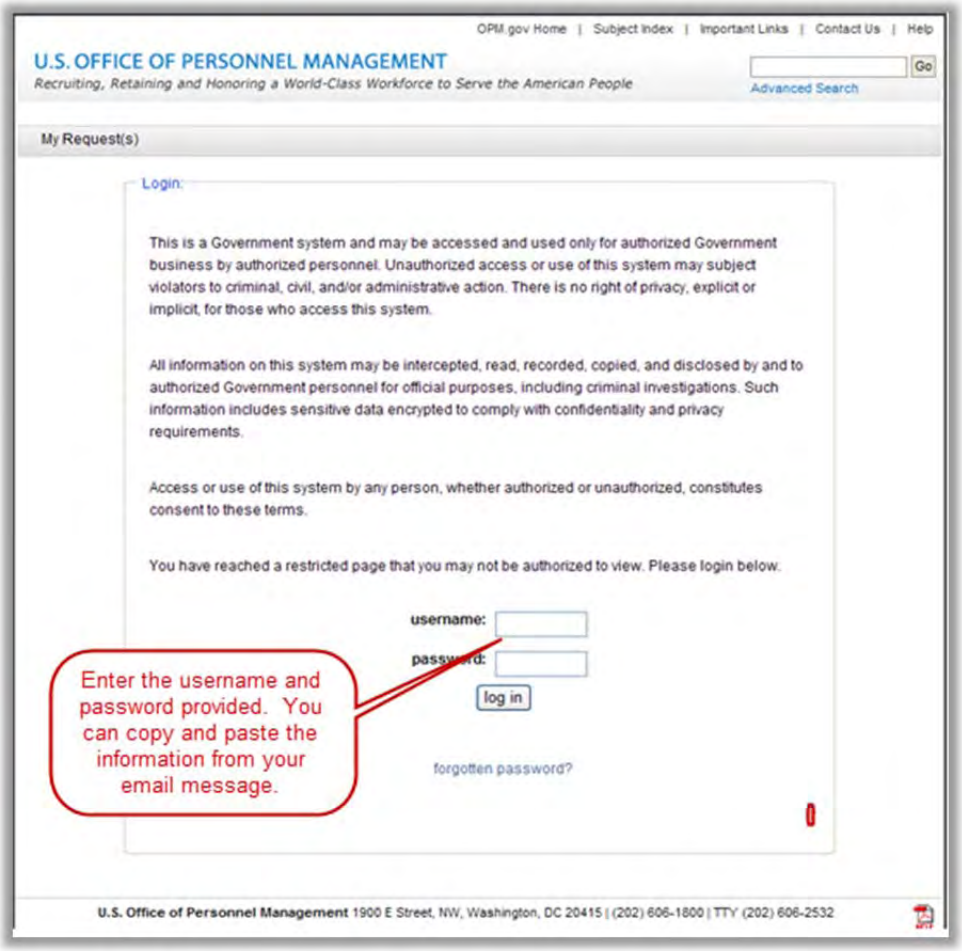
By clicking on the link below, you are indicating that you are the intended recipient: http://www.opm.gov/ITAccess/Requests/index.aspx

After logging in and resetting your password select the "Edit" link to the right of you name to begin editing the form.

Per the Paper Reduction Act of 1995 all users who are expected to complete the OPM 1665 have the right to request a hard copy version of the form. To request a hard copy call the FIS Access Team at 724-794-5612 ext. 7323 or email FISAccessControl@opm.gov. Please note that any hard copy submissions of the form may take and extended period of time to process and it is recommended that users use the safe and secure online version.

All information contained in this email and any associated links and/or files transmitted with it are confidential and intended solely for Priscilla E Mullins. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for Priscilla E Mullins. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited and will be met with legal action.

After clicking on the link provided in the email message, the user will receive the screen below. Type in OR copy and paste the username and password from the email message, then click the **log in** button below the password.


OPM.gov Home | Subject Index | Important Links | Contact Us | Help
U.S. OFFICE OF PERSONNEL MANAGEMENT
Recruiting, Retaining and Honoring a World-Class Workforce to Serve the American People
Go
Advanced Search
My Request(s)
Login:

This is a Government system and may be accessed and used only for authorized Government business by authorized personnel. Unauthorized access or use of this system may subject violators to criminal, civil, and/or administrative action. There is no right of privacy, explicit or implicit, for those who access this system.

All information on this system may be intercepted, read, recorded, copied, and disclosed by and to authorized Government personnel for official purposes, including criminal investigations. Such information includes sensitive data encrypted to comply with confidentiality and privacy requirements.

Access or use of this system by any person, whether authorized or unauthorized, constitutes consent to these terms.

You have reached a restricted page that you may not be authorized to view. Please login below.

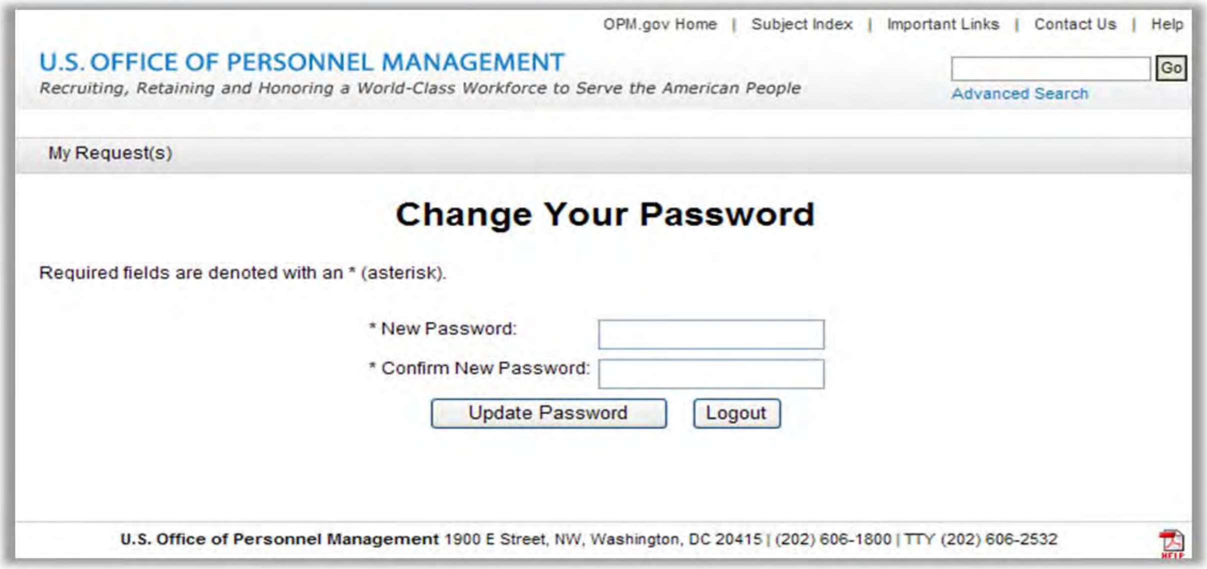
username:

password:

Enter the username and password provided. You can copy and paste the information from your email message.

U.S. Office of Personnel Management 1900 E Street, NW, Washington, DC 20415 | (202) 606-1800 | TTY (202) 606-2532

The system will then require the Applicant to create a new password. This password will be required to contain an uppercase and lowercase alpha, numeric, symbol and be eight characters in length.


OPM.gov Home | Subject Index | Important Links | Contact Us | Help
U.S. OFFICE OF PERSONNEL MANAGEMENT
Recruiting, Retaining and Honoring a World-Class Workforce to Serve the American People
Go
Advanced Search
My Request(s)

Change Your Password

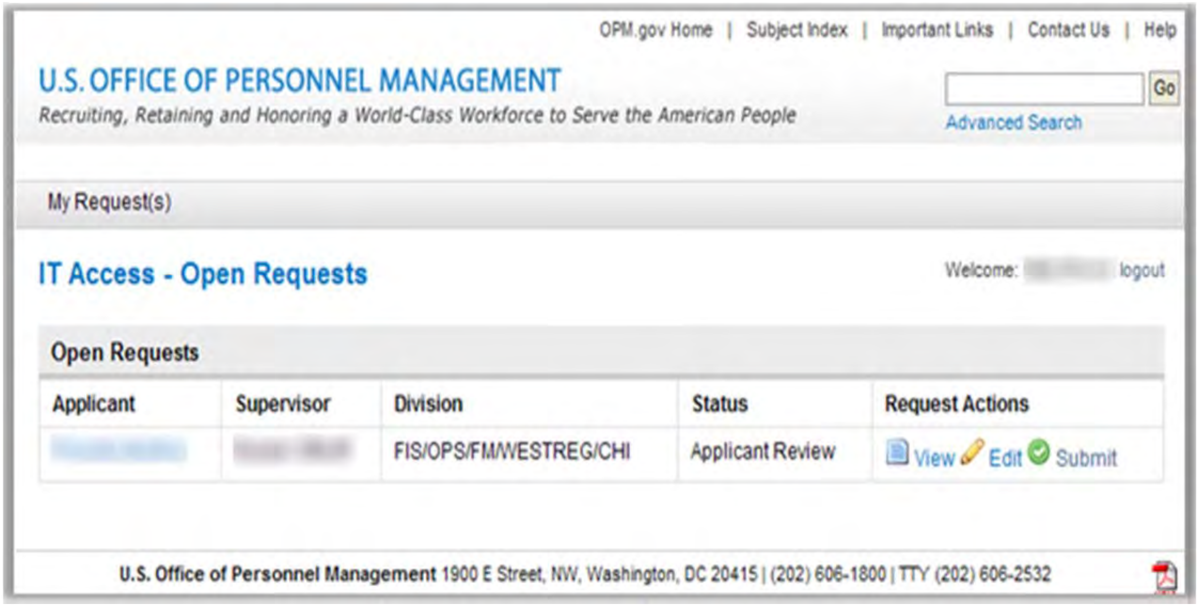
Required fields are denoted with an * (asterisk).

* New Password:

* Confirm New Password:

U.S. Office of Personnel Management 1900 E Street, NW, Washington, DC 20415 | (202) 606-1800 | TTY (202) 606-2532

After successfully changing the password, the Applicant will see the screen below:


OPM.gov Home | Subject Index | Important Links | Contact Us | Help
Go
Advanced Search
My Request(s)
logout

U.S. OFFICE OF PERSONNEL MANAGEMENT

Recruiting, Retaining and Honoring a World-Class Workforce to Serve the American People

IT Access - Open Requests

Welcome: [redacted]

Open Requests

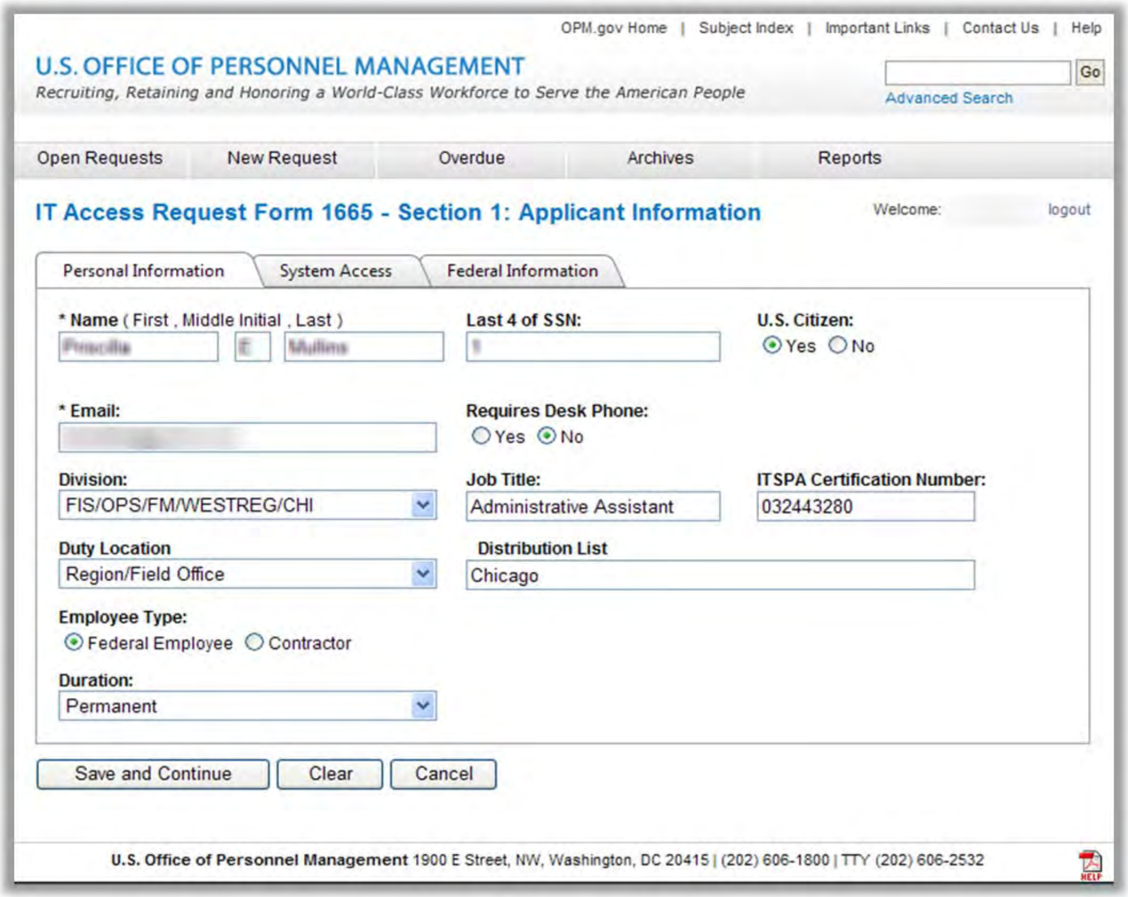
Applicant	Supervisor	Division	Status	Request Actions
[redacted]	[redacted]	FIS/OPS/FM/WESTREG/CHI	Applicant Review	View Edit Submit

U.S. Office of Personnel Management 1900 E Street, NW, Washington, DC 20415 | (202) 606-1800 | TTY (202) 606-2532

Click on the **Edit** link under the Request Actions section which will take the Applicant to the request created by the Initiator.

Personal Information**:** The system will then display the **PERSONAL INFORMATION** tab for the Applicant. The Applicant should review all of the information on this screen to ensure the information is accurate and complete. After reviewing this screen, the Applicant should click the **Save and Continue** button if any changes were made.

System Access**:** The Applicant will be able to view only the **SYSTEM ACCESS** tab. Changes can only be made by the Initiator or Supervisor.


OPM.gov Home | Subject Index | Important Links | Contact Us | Help
U.S. OFFICE OF PERSONNEL MANAGEMENT
Recruiting, Retaining and Honoring a World-Class Workforce to Serve the American People
Go
Advanced Search
Open Requests
New Request
Overdue
Archives
Reports
Welcome: [redacted]
logout
Personal Information
System Access
Federal Information
Save and Continue
Clear
Cancel
U.S. Office of Personnel Management 1900 E Street, NW, Washington, DC 20415 | (202) 606-1800 | TTY (202) 606-2532

IT Access Request Form 1665 - Section 1: Applicant Information

* Name (First , Middle Initial , Last): [redacted] [redacted] [redacted]

Last 4 of SSN: [redacted]

U.S. Citizen: ● Yes ○ No

* Email: [redacted]

Requires Desk Phone: ○ Yes ● No

Division: FIS/OPS/FM/WESTREG/CHI

Job Title: Administrative Assistant

ITSPA Certification Number: 032443280

Duty Location: Region/Field Office

Distribution List: Chicago

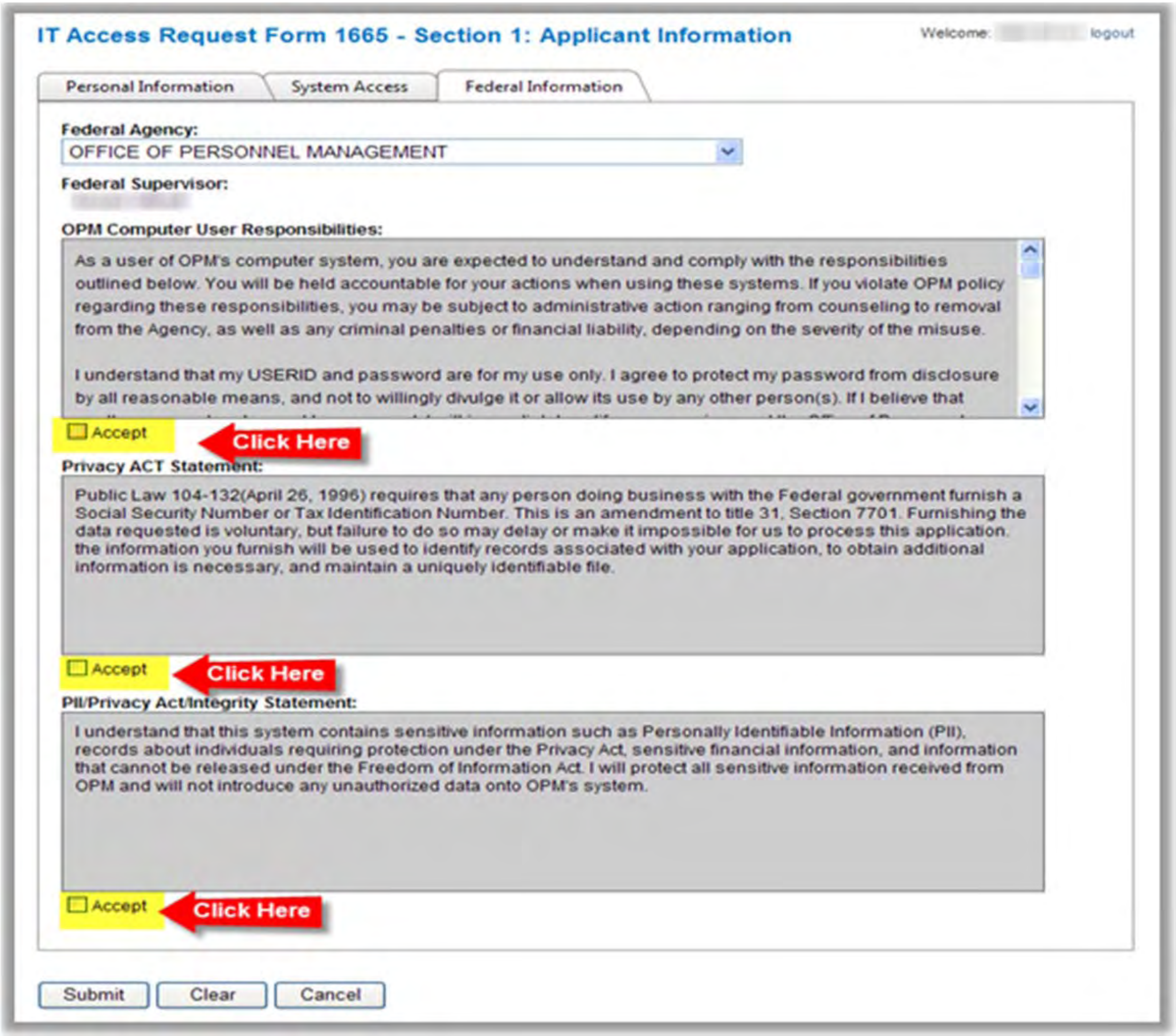
Employee Type: ● Federal Employee ○ Contractor

Duration: Permanent

***Federal Information*:** This is the screen that includes all of the signature requirements. There are three sections that require action by the Applicant: OPM Computer User Responsibilities, Privacy Act Statement and PII/Privacy Act/Integrity Statement. The Applicant should read the paragraphs and then click on the **Accept** box for each section.

> *Contractor Personnel*: When this form is being completed for a contractor employee there will be an additional section that needs to be accepted in order for the form to be complete. The Federal Bureau of Investigation Form (H-1 CJISD-ITS-DOC-08140-5.0, Appendix H) has been included on the e-1665.

***NOTE*:** *For exact phrasing of the paragraphs, see Appendix A*



IT Access Request Form 1665 - Section 1: Applicant Information

Welcome: [redacted] logout

Federal Agency: OFFICE OF PERSONNEL MANAGEMENT

Federal Supervisor: [redacted]

OPM Computer User Responsibilities:

As a user of OPM's computer system, you are expected to understand and comply with the responsibilities outlined below. You will be held accountable for your actions when using these systems. If you violate OPM policy regarding these responsibilities, you may be subject to administrative action ranging from counseling to removal from the Agency, as well as any criminal penalties or financial liability, depending on the severity of the misuse.

I understand that my USERID and password are for my use only. I agree to protect my password from disclosure by all reasonable means, and not to willingly divulge it or allow its use by any other person(s). If I believe that

□ Accept

Privacy ACT Statement:

Public Law 104-132(April 26, 1996) requires that any person doing business with the Federal government furnish a Social Security Number or Tax Identification Number. This is an amendment to title 31, Section 7701. Furnishing the data requested is voluntary, but failure to do so may delay or make it impossible for us to process this application. the information you furnish will be used to identify records associated with your application, to obtain additional information is necessary, and maintain a uniquely identifiable file.

□ Accept

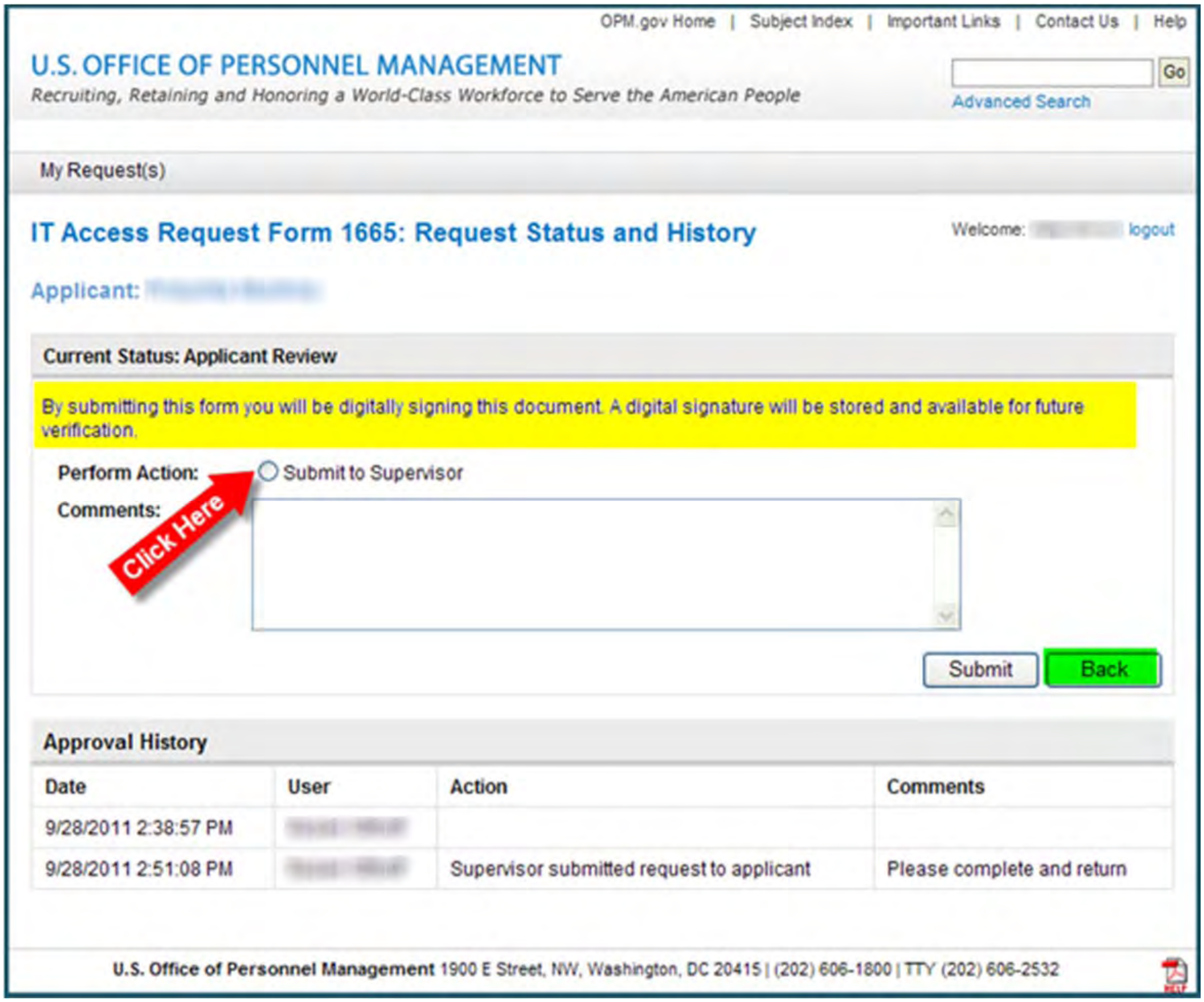
PII/Privacy Act/Integrity Statement:

I understand that this system contains sensitive information such as Personally Identifiable Information (PII), records about individuals requiring protection under the Privacy Act, sensitive financial information, and information that cannot be released under the Freedom of Information Act. I will protect all sensitive information received from OPM and will not introduce any unauthorized data onto OPM's system.

□ Accept

After completing all action on this tab, click the **Submit** button.

The system will then reflect the following screen:


OPM.gov Home | Subject Index | Important Links | Contact Us | Help
Go
Advanced Search
My Request(s)
logout
Click Here
Submit
Back

U.S. OFFICE OF PERSONNEL MANAGEMENT

Recruiting, Retaining and Honoring a World-Class Workforce to Serve the American People

IT Access Request Form 1665: Request Status and History

Welcome: [redacted]

Applicant: [redacted]

Current Status: Applicant Review

By submitting this form you will be digitally signing this document. A digital signature will be stored and available for future verification.

Perform Action: ○ Submit to Supervisor

Comments:

Approval History

Date	User	Action	Comments
9/28/2011 2:38:57 PM	[redacted]		
9/28/2011 2:51:08 PM	[redacted]	Supervisor submitted request to applicant	Please complete and return

U.S. Office of Personnel Management 1900 E Street, NW, Washington, DC 20415 | (202) 606-1800 | TTY (202) 606-2532

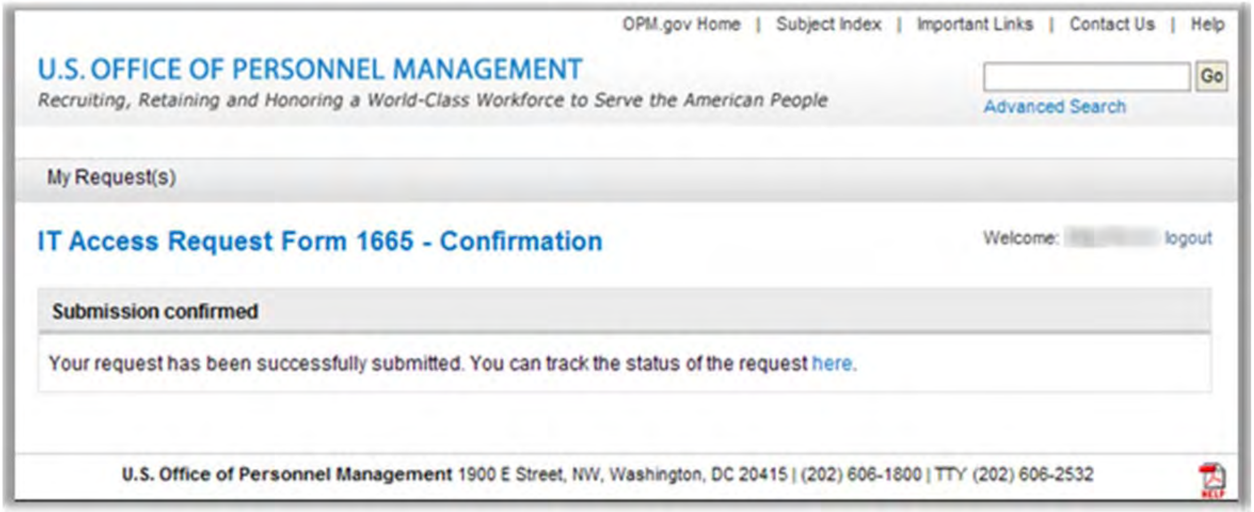
To forward the completed request to a Supervisor the Applicant clicks the **Submit to Supervisor** radio button and then may enter any comment or additional information for the Supervisor in the **Comment** box and click the **Submit** button.

***NOTE*: WHEN YOU CLICK ON THE SUBMIT TO SUPERVISOR RADIO BUTTON AND THEN THE SUBMIT BUTTON, YOU ARE DIGITALLY SIGNING THIS REQUEST.**

The **Back** button (highlighted in green) allows the Applicant to go back to the tabs in order to update or modify information prior to submitting the request.

The Approval History reflects all current information pertaining to this request.

Once the request has been submitted to the Supervisor, the Applicant can go back into the system to view the status of their request, as reflected in the screenshot below:


OPM.gov Home | Subject Index | Important Links | Contact Us | Help
U.S. OFFICE OF PERSONNEL MANAGEMENT
Recruiting, Retaining and Honoring a World-Class Workforce to Serve the American People
Go
Advanced Search
My Request(s)
Welcome: [redacted] logout

IT Access Request Form 1665 - Confirmation

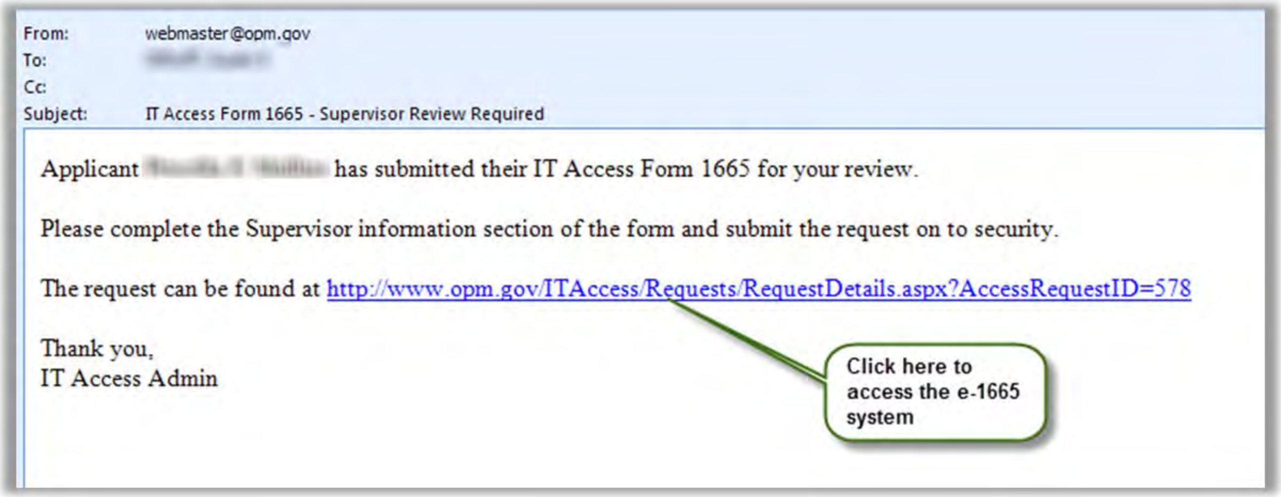
Submission confirmed

Your request has been successfully submitted. You can track the status of the request here.

U.S. Office of Personnel Management 1900 E Street, NW, Washington, DC 20415 | (202) 606-1800 | TTY (202) 606-2532

STEP 3: REVIEW BY SUPERVISOR

After the Applicant has completed the request for access and submitted the form to their Supervisor, the Supervisor will receive a system generated email message (sample below):



From: webmaster@opm.gov
To: [redacted]
Cc:
Subject: IT Access Form 1665 - Supervisor Review Required

Applicant [redacted] has submitted their IT Access Form 1665 for your review.

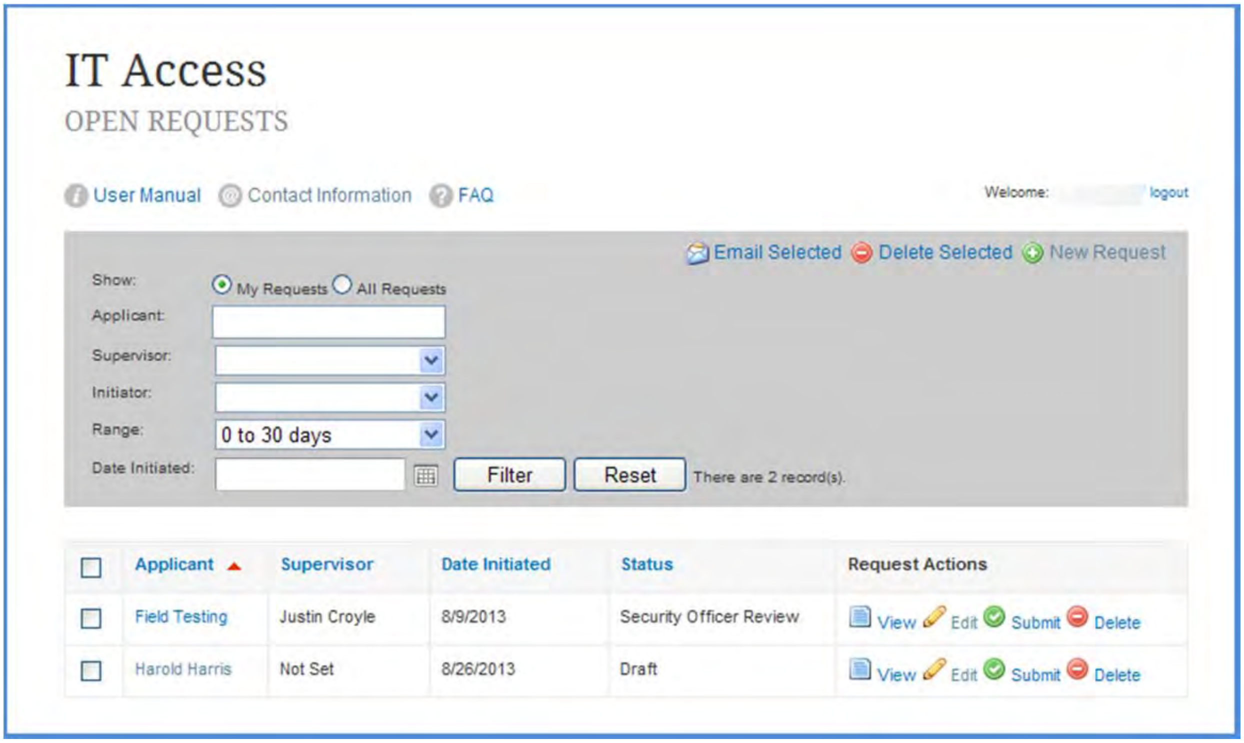
Please complete the Supervisor information section of the form and submit the request on to security.

The request can be found at http://www.opm.gov/ITAccess/Requests/RequestDetails.aspx?AccessRequestID=578

Thank you,
IT Access Admin

Click here to access the e-1665 system

The Supervisor will then click on the link provided in the e-mail message to access the e-1665 system. After entering the username and password, the following screen will display any requests currently active and assigned to the Supervisor:



IT Access
OPEN REQUESTS

Show: ● My Requests ○ All Requests
Applicant:
Supervisor:
Initiator:
Range: 0 to 30 days
Date Initiated:

There are 2 record(s).

□	Applicant ▲	Supervisor	Date Initiated	Status	Request Actions
□	Field Testing	Justin Croyle	8/9/2013	Security Officer Review	View Edit Submit Delete
□	Harold Harris	Not Set	8/26/2013	Draft	View Edit Submit Delete

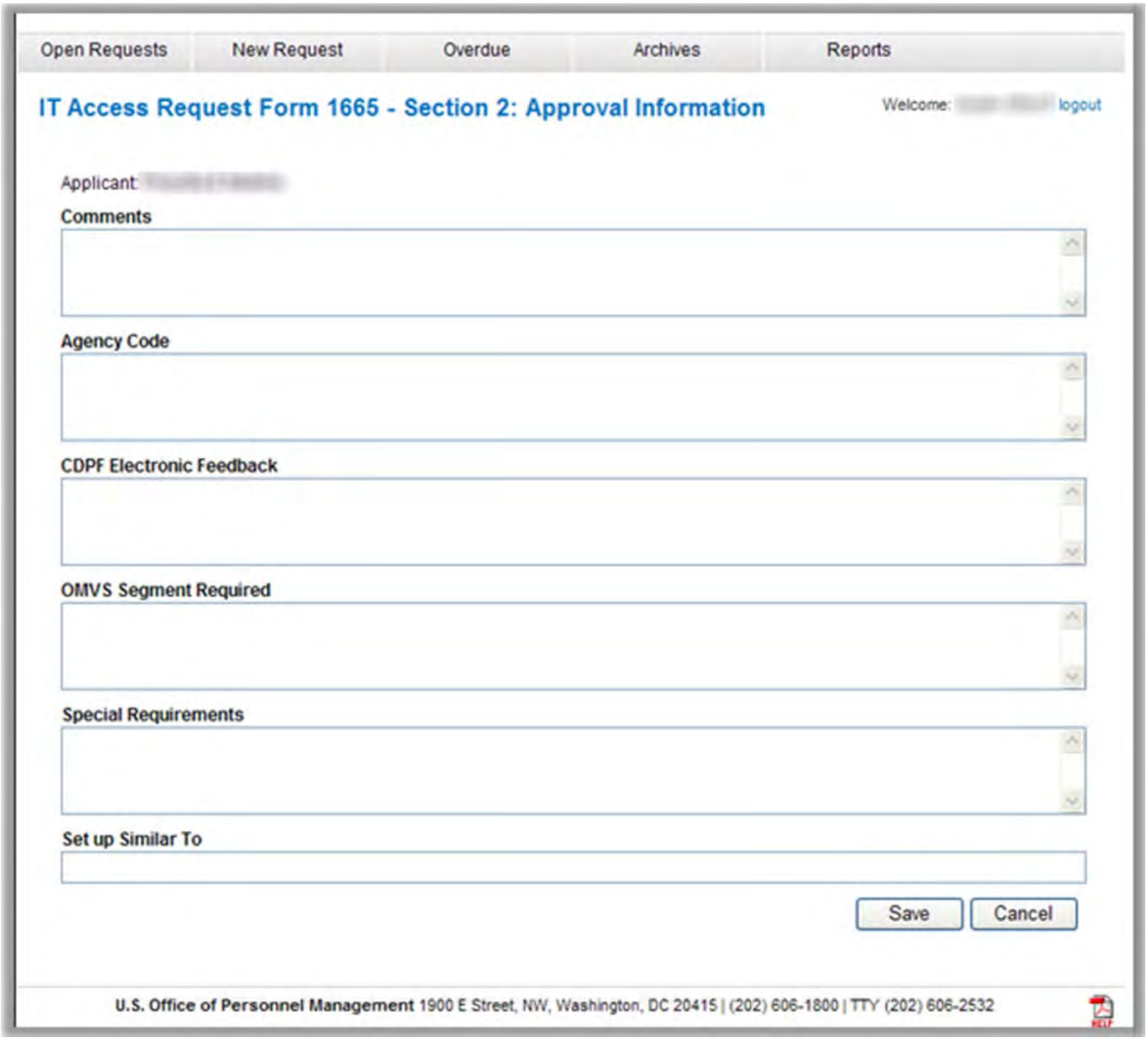
The status of each Applicant's request will be reflected on the screen.

Applicant Review – the request has been initiated and submitted to the Applicant for processing

Draft – the request is still in the initiation process and needs to be completed and submitted to the Applicant or deleted from the system if not necessary

Federal Supervisor Review – the request has been initiated, processed by the Applicant and returned to the Supervisor for final processing and sumission to the DSO

Click on the **Edit** button for the Applicant's request with a status of Federal Supervisor Review. The system will then present the screen below which will allow the Supervisor to enter additional information pertaining to the request selected:



IT Access Request Form 1665 - Section 2: Approval Information

Welcome: [redacted]

Applicant: [redacted]

Comments

Agency Code

CDPF Electronic Feedback

OMVS Segment Required

Special Requirements

Set up Similar To

U.S. Office of Personnel Management 1900 E Street, NW, Washington, DC 20415 | (202) 606-1800 | TTY (202) 606-2532

Comments: Enter any special information for access which has not been included previously on the form.

Agency Code: This option does not pertain to FIS; please leave blank.

CDPF Electronic Feedback: This option does not pertain to FIS; please leave blank.

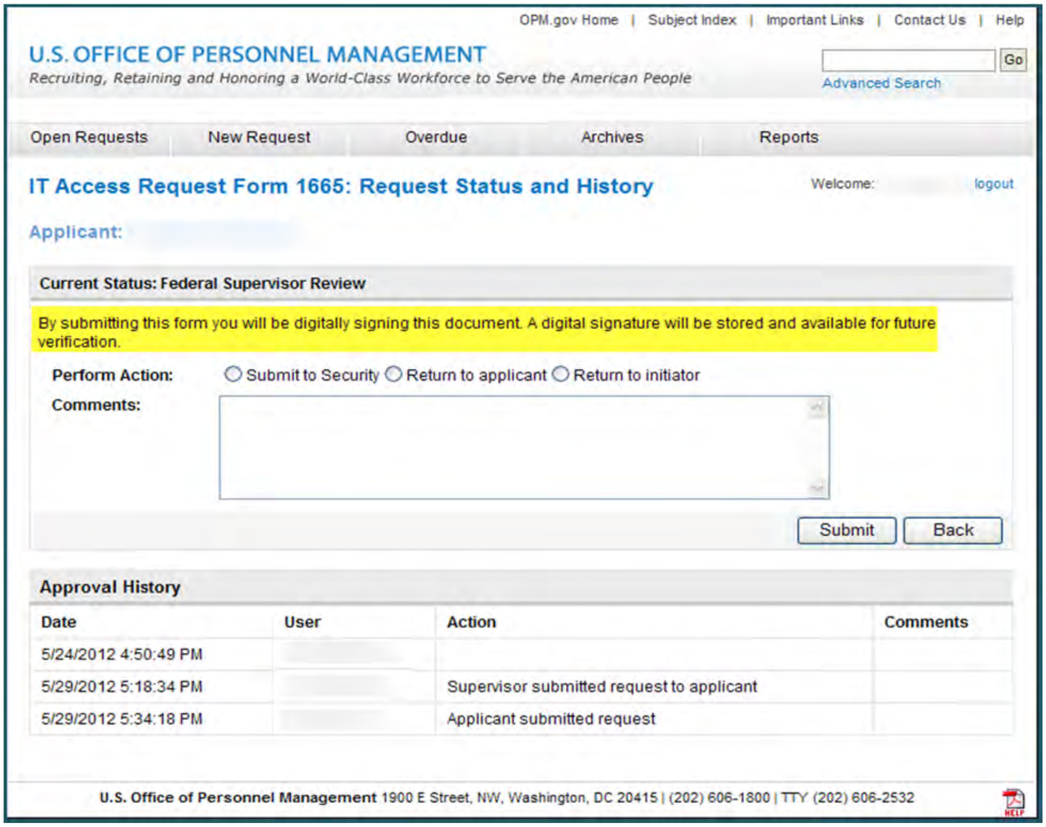
OMVS Segment Required: To access and retrieve Excel Case Information Reports (CIRS) online enter the following information in this section: /opm/WTC/data/cirsiph.

Special Requirements: If there are special applications or portions of applications that need to be added for an applicant, please enter the information in this block.

Set Up Similar To: This field should be disregarded.

Once this information has been completed, click on the **Save** button to proceed to the next action. The next screen is the digital signature section.

PLEASE NOTE: **WHEN YOU CLICK ON THE SUBMIT TO SECURITY RADIO BUTTON AND THEN THE SUBMIT BUTTON, YOU ARE DIGITALLY SIGNING THIS REQUEST.**


OPM.gov Home | Subject Index | Important Links | Contact Us | Help
U.S. OFFICE OF PERSONNEL MANAGEMENT
Recruiting, Retaining and Honoring a World-Class Workforce to Serve the American People
Go
Advanced Search
Open Requests
New Request
Overdue
Archives
Reports

IT Access Request Form 1665: Request Status and History

Welcome: [redacted] logout

Applicant: [redacted]

Current Status: Federal Supervisor Review

By submitting this form you will be digitally signing this document. A digital signature will be stored and available for future verification.

Perform Action: ○ Submit to Security ○ Return to applicant ○ Return to initiator

Comments:

Submit Back

Approval History

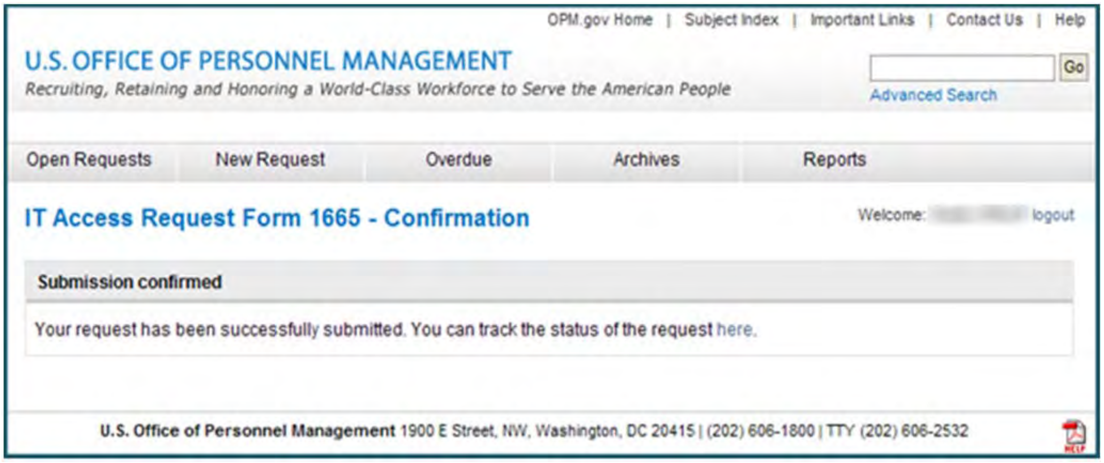
Date	User	Action	Comments
5/24/2012 4:50:49 PM	[redacted]		
5/29/2012 5:18:34 PM	[redacted]	Supervisor submitted request to applicant	
5/29/2012 5:34:18 PM	[redacted]	Applicant submitted request	

U.S. Office of Personnel Management 1900 E Street, NW, Washington, DC 20415 | (202) 606-1800 | TTY (202) 606-2532

There are three options for processing this request:

- Submit to Security: This action will forward the request to a DSO for processing
- Return to Applicant: This action will return the request to an applicant for additional processing before forwarding for completion
- Return to initiator: This action will return the request to the individual that initiated the request, allowing the initiator the ability to modify the information on all tabs inside the form

If this request for access is complete and ready for further action, click on the **Submit to Security** radio button, enter any instruction/information in the **Comment** area and then click the **Submit** button. The system will reflect that the form has been submitted successful and provide a link to track the status of the request.


OPM.gov Home | Subject Index | Important Links | Contact Us | Help
U.S. OFFICE OF PERSONNEL MANAGEMENT
Recruiting, Retaining and Honoring a World-Class Workforce to Serve the American People
Go
Advanced Search
Open Requests
New Request
Overdue
Archives
Reports
Welcome: [redacted] logout

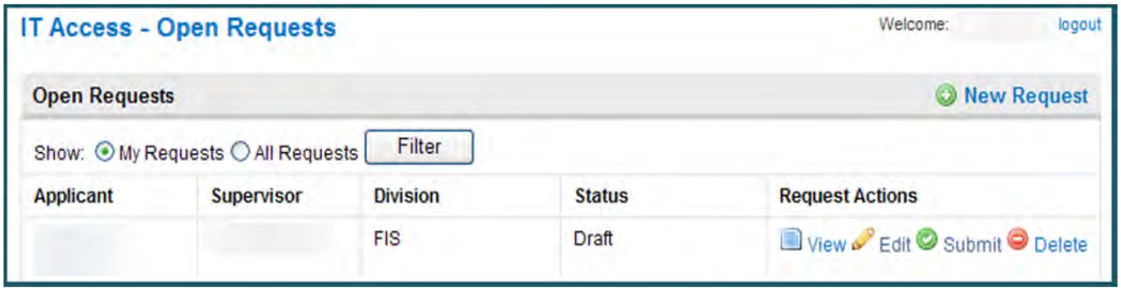
IT Access Request Form 1665 - Confirmation

Submission confirmed

Your request has been successfully submitted. You can track the status of the request here.

U.S. Office of Personnel Management 1900 E Street, NW, Washington, DC 20415 | (202) 606-1800 | TTY (202) 606-2532

If this request needs to be returned to the applicant or the initiator (see screen on prior page), click on the correct option, enter any information /instructions in the Comment area and then click the Submit button. By viewing your open requests section of the application, you will be able to see the status of the request (the status below reflects that the form was returned to the initiator).

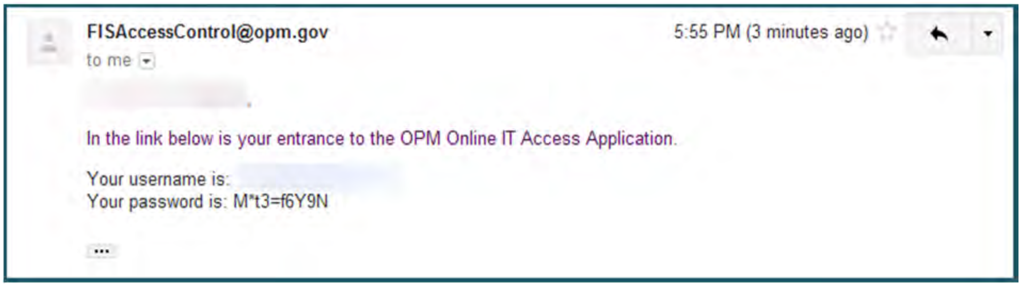

Welcome: [redacted] logout
New Request
Show: ● My Requests ○ All Requests
Filter

IT Access - Open Requests

Open Requests

Applicant	Supervisor	Division	Status	Request Actions
[redacted]	[redacted]	FIS	Draft	View Edit Submit Delete

If the form had been returned to the applicant, the applicant would receive a message generated by the system in the following format:



FISAccessControl@opm.gov
to me

5:55 PM (3 minutes ago)

[redacted]

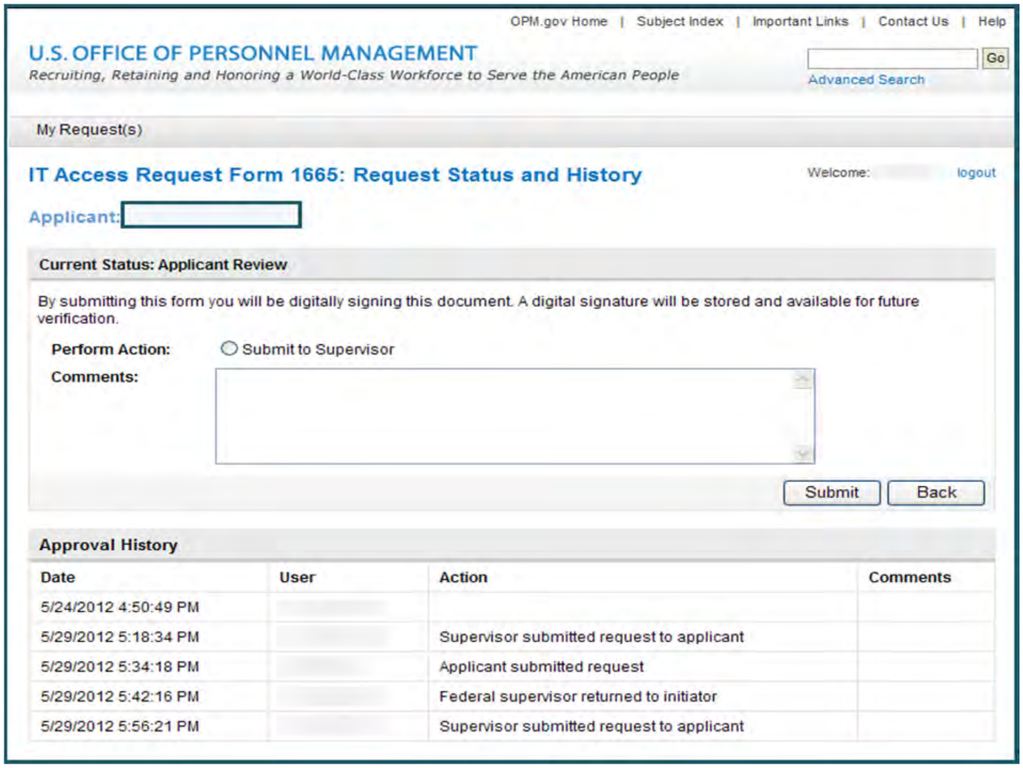
In the link below is your entrance to the OPM Online IT Access Application.

Your username is: [redacted]
Your password is: M*t3=f6Y9N

...

The system would automatically generate a new password for the user instead of maintaining the password the applicant would have previously created.

The screenshot below reflects the Approval History that is generated for each approval or rejection pertaining to a particular request.



OPM.gov Home | Subject Index | Important Links | Contact Us | Help
U.S. OFFICE OF PERSONNEL MANAGEMENT
Recruiting, Retaining and Honoring a World-Class Workforce to Serve the American People
Go
Advanced Search
My Request(s)

IT Access Request Form 1665: Request Status and History

Welcome: [redacted] logout

Applicant: [redacted]

Current Status: Applicant Review

By submitting this form you will be digitally signing this document. A digital signature will be stored and available for future verification.

Perform Action: ○ Submit to Supervisor

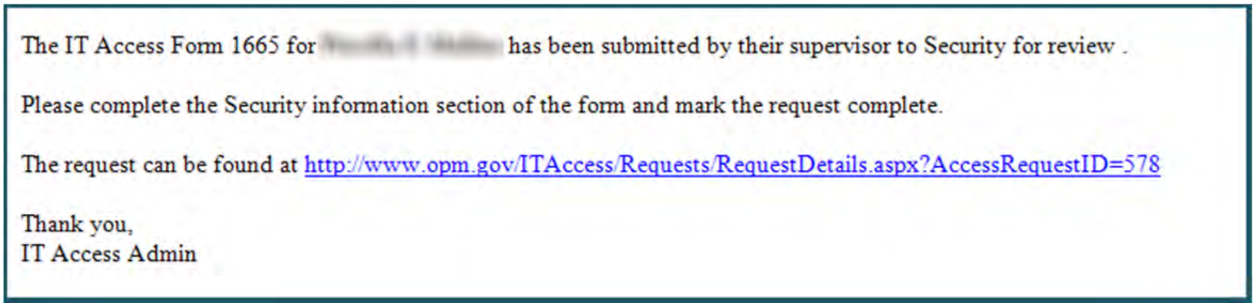
Comments:

Approval History

Date	User	Action	Comments
5/24/2012 4:50:49 PM	[redacted]		
5/29/2012 5:18:34 PM	[redacted]	Supervisor submitted request to applicant	
5/29/2012 5:34:18 PM	[redacted]	Applicant submitted request	
5/29/2012 5:42:16 PM	[redacted]	Federal supervisor returned to initiator	
5/29/2012 5:56:21 PM	[redacted]	Supervisor submitted request to applicant	

STEP 4: REVIEW BY SECURITY

After the Supervisor has reviewed and approved the request, a computer-generated e-mail message will be sent to the Security Team with the following information. The blurred area will indicate the name of the Applicant ready for processing.



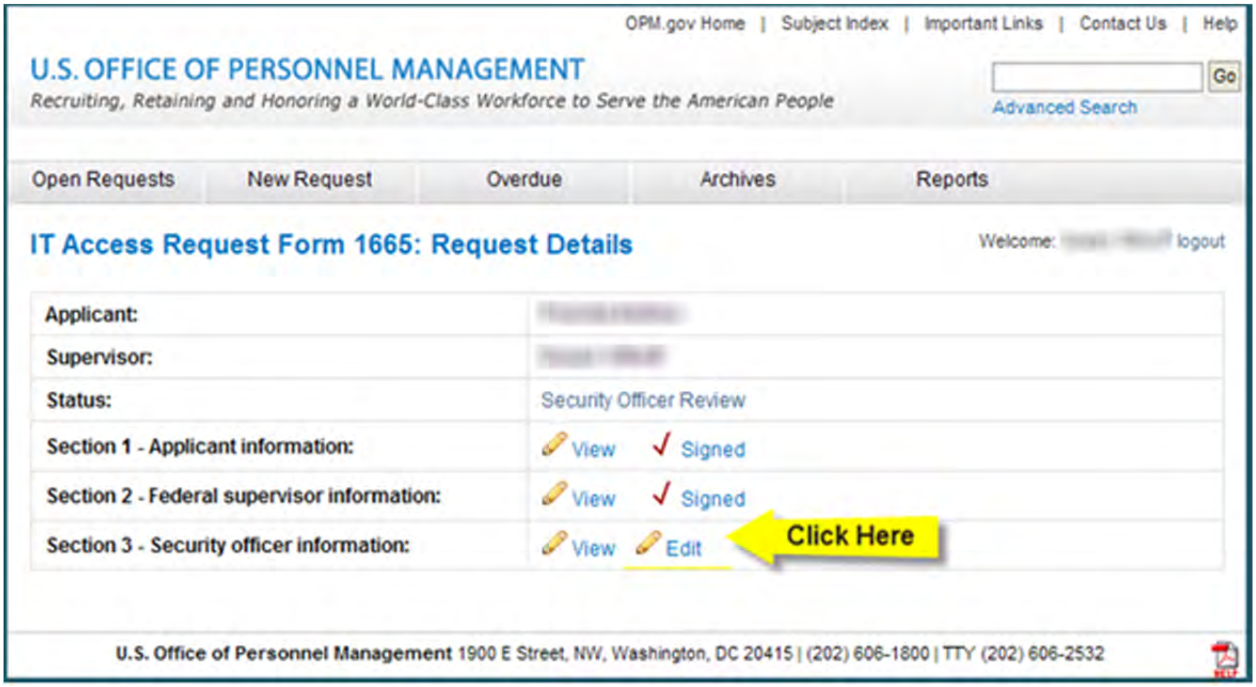
The IT Access Form 1665 for [redacted] has been submitted by their supervisor to Security for review .

Please complete the Security information section of the form and mark the request complete.

The request can be found at http://www.opm.gov/ITAccess/Requests/RequestDetails.aspx?AccessRequestID=578

Thank you,
IT Access Admin

Upon clicking the link provided in the e-mail message and entering the username and password used for entering the system, Security will see the following screen. Click on the **Edit** button for Section 3.



OPM.gov Home | Subject Index | Important Links | Contact Us | Help
U.S. OFFICE OF PERSONNEL MANAGEMENT
Recruiting, Retaining and Honoring a World-Class Workforce to Serve the American People
Go
Advanced Search
Open Requests
New Request
Overdue
Archives
Reports

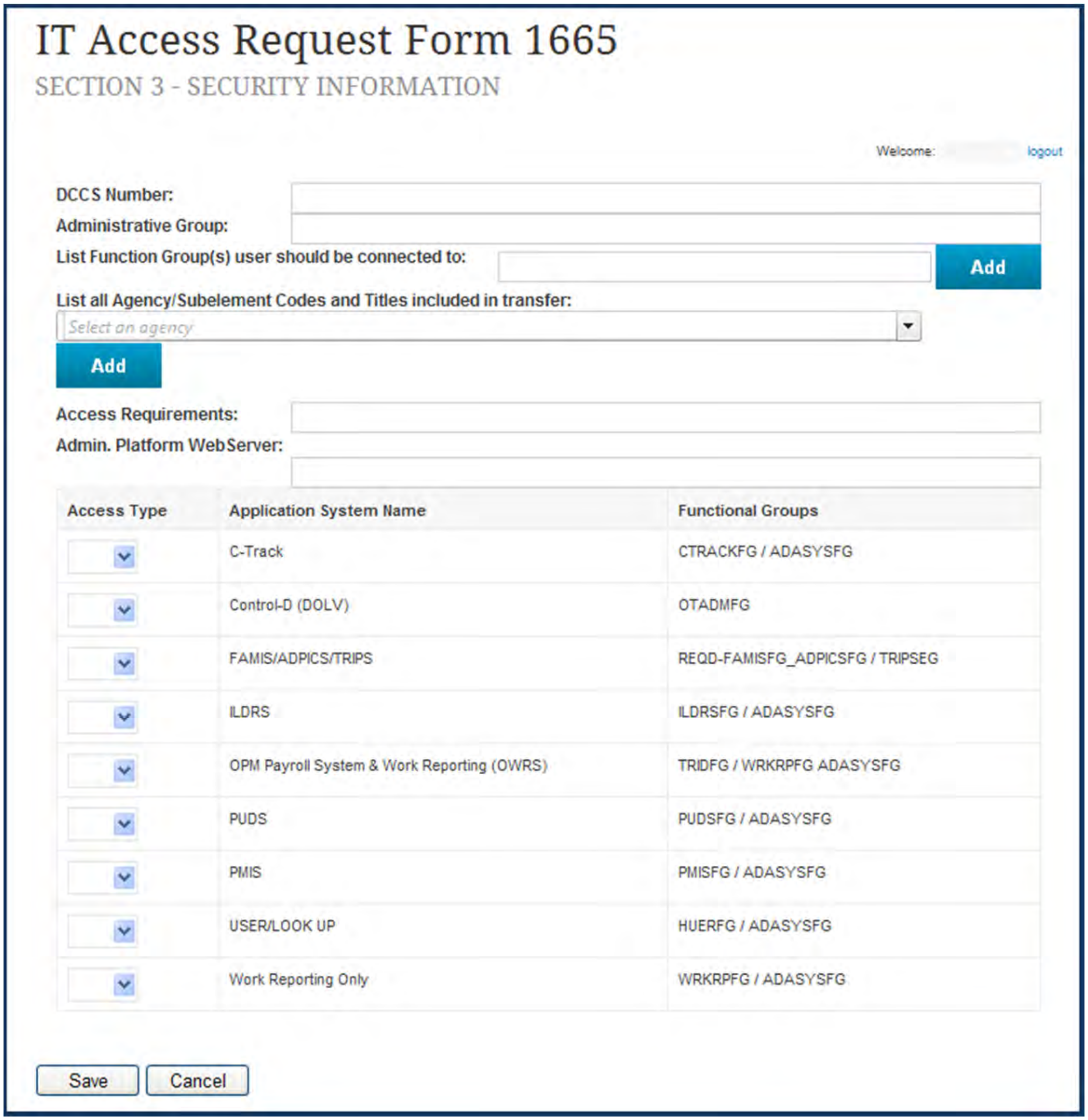
IT Access Request Form 1665: Request Details

Welcome: [redacted] logout

Applicant:	[redacted]
Supervisor:	[redacted]
Status:	Security Officer Review
Section 1 - Applicant information:	View ✓ Signed
Section 2 - Federal supervisor information:	View ✓ Signed
Section 3 - Security officer information:	View Edit

Click Here

U.S. Office of Personnel Management 1900 E Street, NW, Washington, DC 20415 | (202) 606-1800 | TTY (202) 606-2532



IT Access Request Form 1665

SECTION 3 - SECURITY INFORMATION

Welcome: logout

DCCS Number:

Administrative Group:

List Function Group(s) user should be connected to: Add

List all Agency/Subelement Codes and Titles included in transfer:

Select an agency

Add

Access Requirements:

Admin. Platform WebServer:

Access Type	Application System Name	Functional Groups
	C-Track	CTRACKFG / ADASYSFG
	Control-D (DOLV)	OTADMFG
	FAMIS/ADPICS/TRIPS	REQD-FAMISFG_ADPICSFG / TRIPSEG
	ILDRS	ILDRSFG / ADASYSFG
	OPM Payroll System & Work Reporting (OWRS)	TRIDFG / WRKRPFG ADASYSFG
	PUDS	PUDSFG / ADASYSFG
	PMIS	PMISFG / ADASYSFG
	USER/LOOK UP	HUERFG / ADASYSFG
	Work Reporting Only	WRKRPFG / ADASYSFG

Save Cancel

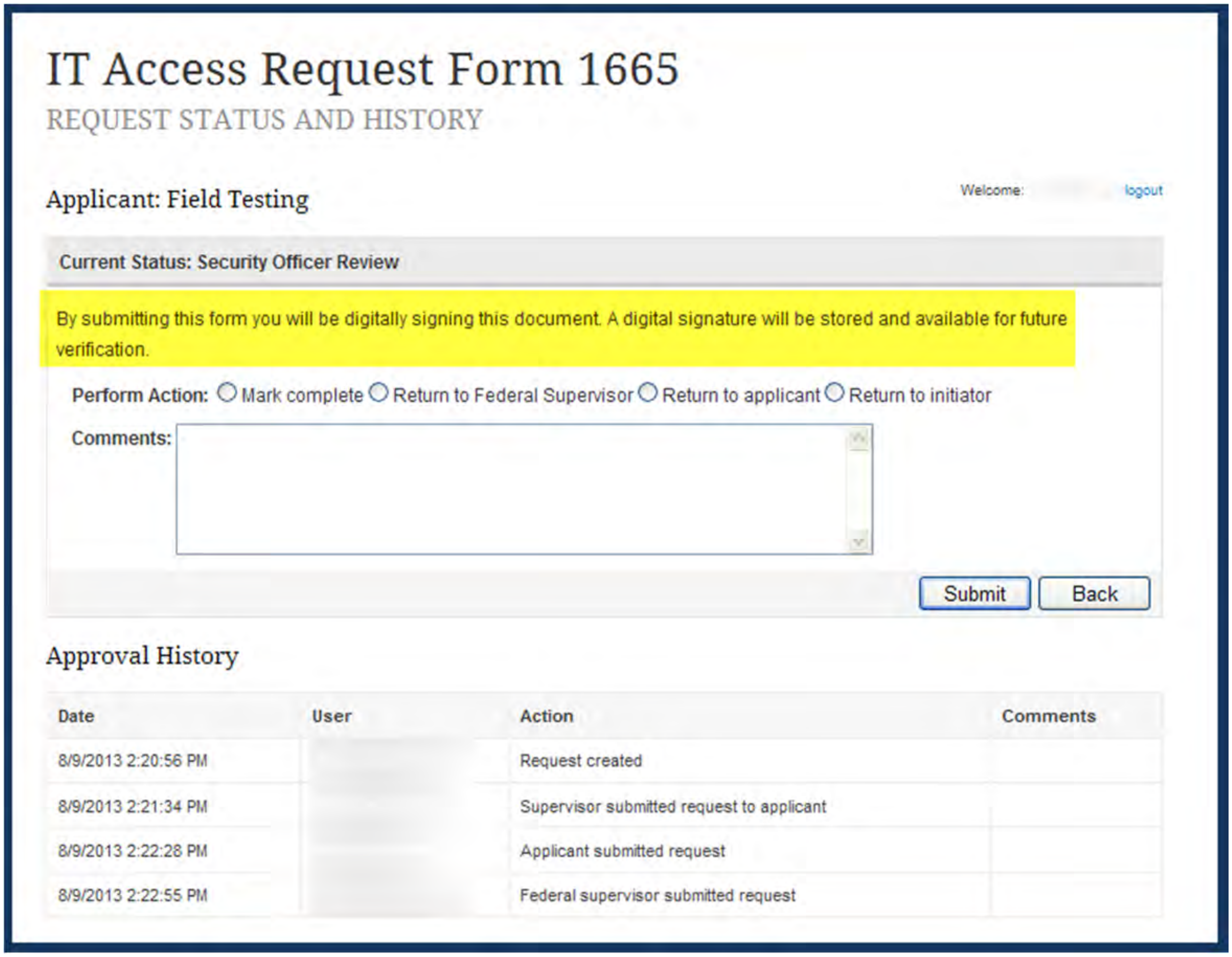
This screen can be modified by Security to request access as required. None of the systems above are relevant to FIS processes/procedures. Click on the **Save** button to continue processing the request.

The next screen is the digital signature section. **PLEASE NOTE: WHEN YOU CLICK ON THE SUBMIT TO SECURITY RADIO BUTTON AND THEN THE SUBMIT BUTTON, YOU ARE DIGITALLY SIGNING THIS REQUEST.**

There are four options for processing this request:

- Mark complete: This action will accept all information and digital signatures on the request and create a PDF image of all access requested.
- Return to Federal Supervisor: This action will return the request to the Federal Supervisor for additional processing or correction. Please include any instruction for the Federal Supervisor in the Comment box on actions which need to be addressed in order to complete the request.
- Return to applicant: This action will return the request to an applicant for additional processing before forwarding for completion
- Return to initiator: This action will return the request to the individual that initiated the request, allowing the initiator the ability to modify the information on all tabs inside the form

After selecting the **Perform Action** option, enter any instruction/information in the **Comment** area and click on the **Submit** button.



IT Access Request Form 1665

REQUEST STATUS AND HISTORY

Applicant: Field Testing

Welcome: [redacted] logout

Current Status: Security Officer Review

By submitting this form you will be digitally signing this document. A digital signature will be stored and available for future verification.

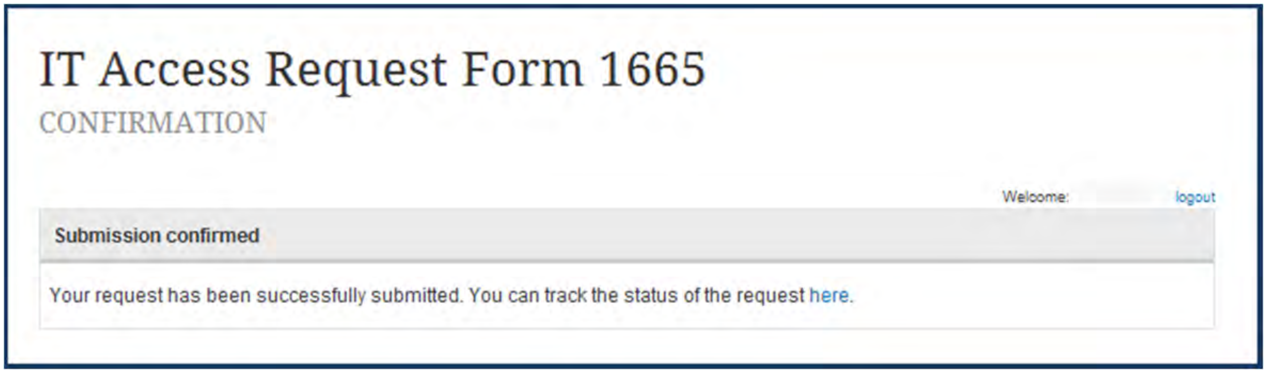
Perform Action: ○ Mark complete ○ Return to Federal Supervisor ○ Return to applicant ○ Return to initiator

Comments:

Approval History

Date	User	Action	Comments
8/9/2013 2:20:56 PM	[redacted]	Request created	
8/9/2013 2:21:34 PM	[redacted]	Supervisor submitted request to applicant	
8/9/2013 2:22:28 PM	[redacted]	Applicant submitted request	
8/9/2013 2:22:55 PM	[redacted]	Federal supervisor submitted request	

If the option to Mark Complete was selected, the system will next reflect the following screen and provide a link to view the tracking status of the request. If an alternate option to return to either the applicant or the intiator was selected, the system will reflect the appropriate status and provide a link to track the status.



IT Access Request Form 1665

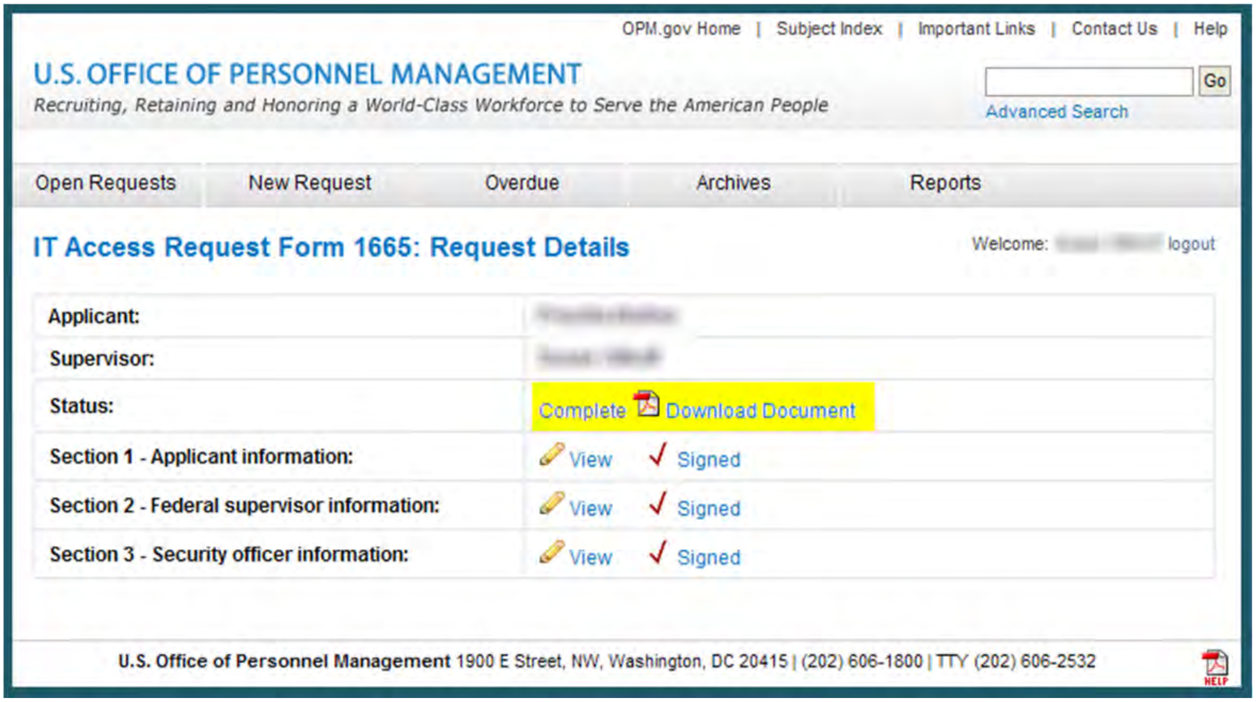
CONFIRMATION

Welcome: [redacted] logout

Submission confirmed

Your request has been successfully submitted. You can track the status of the request here.

Once the request is completed by Security, the system will display the screenshot below reflecting the tracking status of the request. Clicking on the **Download Document** link will bring up the PDF image of the request with all of the access information submitted.



OPM.gov Home | Subject Index | Important Links | Contact Us | Help
U.S. OFFICE OF PERSONNEL MANAGEMENT
Recruiting, Retaining and Honoring a World-Class Workforce to Serve the American People
Go
Advanced Search
Open Requests
New Request
Overdue
Archives
Reports

IT Access Request Form 1665: Request Details

Welcome: [redacted] logout

Applicant:	[redacted]
Supervisor:	[redacted]
Status:	Complete Download Document
Section 1 - Applicant information:	View ✓ Signed
Section 2 - Federal supervisor information:	View ✓ Signed
Section 3 - Security officer information:	View ✓ Signed

U.S. Office of Personnel Management 1900 E Street, NW, Washington, DC 20415 | (202) 606-1800 | TTY (202) 606-2532

APPENDIX A

The following policies are the signature blocks that an applicant electronically signs before they submit a request for access to their supervisor. All Federal and Contractor applicants/personnel are required to accept the first three policies to complete the submission process. Additionally, all Contractor applicants/personnel are required to accept the fourth policy in this appendix as part of their submission for access.

COMPUTER USER POLICY

As a user of OPM's computer system, you are expected to understand and comply with the responsibilities outlined below. You will be held accountable for your actions when using these systems. If you violate OPM policy regarding these responsibilities, you may be subject to administrative action ranging from counseling to removal from the Agency, as well as any criminal penalties or financial liability, depending on the severity of the misuse.

I understand that my USERID and password are for my use only. I agree to protect my password from disclosure by all reasonable means, and not to willingly divulge it or allow its use by any other person(s). If I believe that another person has learned by password, I will immediately notify my supervisor and the Office of Personnel Management. I will not attempt to access my own record in PIPS/CVS for any purpose, including testing/training situations. I understand that unauthorized access of investigative files or information is prohibited by law, and punishable by a fine of not more than $5,000 (5 U.S.C. 552a). I understand that use of government computers for private or personal use is prohibited by law and may result in administrative action or criminal prosecution (18 U.S.C 641; Executive Order 11222). I understand that my use of government equipment, including computer systems, must comply with the policies specified in the OPM Policy on the Use of Government Office Equipment. The policy is available on THEO, OPM's Intranet. I have read, understand my responsibilities, and will comply with the OPM Computer User Responsibilities, which is attached to this document and can also be found on THEO (OPM Intranet).

Privacy While Using Government Equipment - You do not have the right to privacy while using any Government equipment, including Internet or email services. Furthermore, your use of Government office equipment, for whatever purpose, is not secure, private, or anonymous. While using Government office equipment, your use may be monitored or recorded.

Protection of Software, Data and Hardware - You are not allowed to introduce any unauthorized software and data (including software and data protected by copyright, trademark, privacy laws, or other proprietary data or material with other intellectual property rights beyond fair use), hardware or telecommunication devices or modify any configurations. You are not allowed to interconnect to other computer systems or networks without the authorization of OPM's Chief Information Officer. Access to the Internet via the OPM network is authorized. In addition, you will protect all sensitive information residing in OPM computer systems, preventing unauthorized access, use, modification, disclosure or destruction of that information. This includes records about individuals requiring protection under the Privacy Act, sensitive financial information and information that cannot be released under the Freedom of Information Act. Disclosure of sensitive information, trade secrets and intellectual property to unauthorized individuals is also prohibited.

Service Restoration - The availability of the computer system is a matter of importance to you. You are responsible for assisting in any way that you can for restoring service in the even that the computer systems become non-functional. Priority is given to restoring the general support systems and the applications supporting OPM's mission essential functions as defined in the Agency's Continuity of Operations Plan (COOP).

System Privileges - You are given access to the computer systems based on a need to perform specific work at OPM. You are expected to work within the confines of the access allowed and are not to attempt to access systems or applications for which access is not authorized.

Telecommuting - The OPM Human Resources Handbook, Chapter 368, Telecommuting, contains the policy and procedures for authorizing telecommuting. In general, immediate supervisors approve, on a case-by-case basis, employee requests to telecommute. Telecommuters who access OPM's general support systems must adhere to all IT security policy and procedures that would apply if the individual was accessing OPM's systems in the office. Dial-in access for telecommuters or other users whose job functions may require it is authorized by the Chief, Network Management Group.

Use of Passwords - You will create and use passwords as specified in the IT Security Policy. You must keep your passwords confidential and not share them with anyone. Individual applications may have more stringent password requirements than the general policy requirements.

I have been afforded the opportunity to read the CVS User Manual to include the Security section regarding the use of this system. I have read the above and understand the responsibilities inherent with being issued a PIPS/CVS USERID. Upon request, I may receive a copy of this signed statement.

PII POLICY STATEMENT

I understand that this system contains sensitive information such as Personally Identifiable Information (PII), records about individuals requiring protection under the Privacy Act, sensitive financial information, and information that cannot be released under the Freedom of Information Act. I will protect all sensitive information received from OPM and will not introduce any unauthorized data onto OPM's system.

PRIVACY POLICY STATEMENT

Public Law 104-132(April 26, 1996) requires that any person doing business with the Federal government furnish a Social Security Number or Tax Identification Number. This is an amendment to title 31, Section 7701. Furnishing the data requested is voluntary, but failure to do so may delay or make it impossible for us to process this application. the information you furnish will be used to identify records associated with your application, to obtain additional information is necessary, and maintain a uniquely identifiable file.

SECURITY ADDENDUM POLICY (AKA CJIS SECURITY FORM)

H-1 CJISD-ITS-DOC-08140-5.0
APPENDIX H SECURITY ADDENDUM

The following pages contain the legal authority, purpose, and genesis of the Criminal Justice Information Services Security Addendum (H2-H4); the Security Addendum itself (H5-H6); and the Security Addendum Certification page (H7). FEDERAL BUREAU OF INVESTIGATION CRIMINAL JUSTICE INFORMATION SERVICES SECURITY ADDENDUM Legal Authority for and Purpose and Genesis of the Security Addendum Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency. In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows: 1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534. We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The security addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems. The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes. Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read: § 20.33 Dissemination of criminal history record information. a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available: 1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies. 2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and 3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee). This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements. A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI. FEDERAL BUREAU OF INVESTIGATION CRIMINAL JUSTICE INFORMATION SERVICES SECURITY ADDENDUM The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information." The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB). This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security. The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency. 1.00 Definitions 1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum. 1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency. 2.00 Responsibilities of the Contracting Government Agency. 2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. 3.00 Responsibilities of the Contractor. 3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB). 4.00 Security Violations. 4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor. 4.02 Security violations can justify termination of the appended agreement. 4.03 Upon notification, the FBI reserves the right to: a. Investigate or decline to investigate any report of unauthorized use; b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CJA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA. 5.00 Audit 5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum. 6.00 Scope and Authority 6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI. 6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations. 6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor. 6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI. 6.05 All notices and correspondence shall be forwarded by First Class mail to: Assistant Director Criminal Justice Information Services Division, FBI 1000 Custer Hollow Road Clarksburg, West Virginia 26306 FEDERAL BUREAU OF INVESTIGATION CRIMINAL JUSTICE INFORMATION SERVICES SECURITY ADDENDUM CERTIFICATION I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions. I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

APPENDIX B

Glossary

To jump to a location press and hold the “Ctrl” while clicking on a letter below.

A – B – C – D – E – F – G – H – I – J – K – L – M – N – O – P – Q – R – S – T – U – V – W – X – Y – Z

A

Access Administrator – The access administrator controls access and what type of access a user has to for a file or folder.

Account Admin – A role within the FTS system that manages FTS User Accounts and RADIUS Dialup Accounts.

Adabas Production – Not yet defined

Adabas Tact – Not yet defined.

Adabas Test – Not yet defined.

Add/Update Clearance/Access Data - This function allows external OPM federal agencies the ability to submit clearance records to the Central Verification System (CVS). It allows the user to add new clearance information and update existing clearances in order to maintain the accuracy of the CVS.

Add/Update HDPD-12 Data - This function allows external OPM federal agencies the ability to post and modify reciprocal Homeland Security Personnel Directive-12 (HSPD-12) determinations to the CVS.

Add/Update Polygraph Data - This function allows external OPM federal agencies the ability to report full scope and counterintelligence polygraph data. Agencies can also modify their polygraph data contained in the CVS.

Add/Update Subject Data - This function allows external OPM federal agencies the ability to add a Subject record to the system. Subjects should only be added to CVS to support the reporting of clearances, investigative data, HSPD-12 credentials and polygraphs in accordance with reciprocity policies. Updates to Subject records are required to be entered by the FIS Agency Systems and Liaison at (724) 794-5612 x 4600.

Agency Administrator - This role within e-QIP (Electronic Questionnaire for Investigative Processing) responsible for managing groups within their own Agency, and Agency attributes and forms.

Agency Help Desk - This is a role withing e-QIP that has the ability to check a request or user status, and reset Golden Questions without the concurrence of a second person.

Agency User – An external OPM federal employee or contractor who has been provided access to PIPS (Personnel Investigations Processing System). This type of access is requested by using an INV 70-B (US OPM FIS Request for PIPS/CVS User ID/Access) form. This access allows external agency personnel/contractors to access Agency case status, search the SII/CVS/JPAS menu, OFI-79 notices, Request a SAC investigation, supply Agency Adjudication, view Case Status Information and Add/Update Subject Data, Clearance/Access Data, Polygraph Data and HSPD-12 data.

Application Developer - An individual who is tasked with identifying and defining customer requirements, developing and test the software application based on the requirements, and coordinate the deployment of the the application with the customer. This role usually receives access to the test are of OPM systems.

Application Specialist - A role/function associated with the FTS system

Application Tester - A function which allows the user to test a new system/application or modifications to an existing system/application as necessary on a system which mirrors the live environment.

Approver – A role within the e-QIP system responsible for reviewing Applicant/employee data, approving/rejecting answer(s), entering comments for rejected answer(s), and submitting form(s) to the Investigations Service Providers (ISP) or next higher agency. An approver must be a Federal Employee; contractors cannot be provided this role

Assign Existing network printer – Information that needs to be provided when requesting access to the DCCS through Citrix option on the SYSTEM ACCESS TAB. If a network printer is selected, this is one of the options to allow for mapping of printwork.

Author – Provides the ability to create, read, modify and delete items and/or files you create.

B

Business Manager - An Agency User who is capable of generating statistical reports containing requested data within the e-QIP system.

C

Case Status - Authorized agency officials can obtain the overall status of a case. Detailed information about the case is located on the "Case Assignments Tracking Screen" (CATS), such as the status and result of each item in the case. Users can only view case information on those cases attributed to the Security Office Identifier (SOI) of the User ID.

Central Verification System (CVS) – The system designated as the primary tool for facilitating reciprocity decisions as required by Executive Orders, regulations and policies. The CVS contains information on security clearance, suitability, fitness and HSPD-12 Personal Verification credentialing determinations. This information is provided by agency sources, OPM legacy systems and a bridge to the Department of Defense Joint Personnel Adjudication System.

CICS Production - Provides access to the PIPS live system through the CICS view

CICS Tact – This role is not applicable to FIS

CICS Test - Provides access to the PIPS test system through the CICS view

Computer Operator - Are the contractors that oversee the Batch process and printing 24/7 in the OPM Computer Room. They also provide a mini helpdesk and divert calls to FAC or back to the operator. They also reset passwords on PIPS and transfer calls to FAC when needed. They use the OPS menu on PIPS.

Contract Investigator - Operate with the FIDI menu. They are hired to gather all the requested information from the 1665. Through this menu they can transmit PC reports/ schedule/reschedule and add items. Through PIPS they can send and receive a message. They have instructions to update items, modify reports, and display investigations. There is also an administration menu in FIDI that enables the contractor to do time keeping payroll reports to managers, request documents, and download maintenance changes to PIPS-R.

Contractor Item Validation - A role assigned to an individual with Web ePRP access. This role provides Validation and Pre-Review basic access.

Contractor Item Validation Supervisor - A role assigned to an individual with Web ePRP access. This role provides Item Validation Supervisor and Pre-Review Supervisor users access to the basic and supervisor functions.

Contractor Oversight - A role assigned to an individual with Web ePRP access. Contractor Oversight users have Basic, Supervisor, and Post Audit roles.

Contractor Post Audit QA - A role assigned to an individual with Web ePRP access. Post Audit users have their own set of roles, in addition to the Basic and Supervisor roles of only the Pre-Review subset.

Contractor Pre Review – A role assigned to an individual with Web ePRP access. This role provides addition access for Post Audit user actions.

Contractor Pre Review Supervisor – A role assigned to an individual with Web ePRP access. Not yet defined.

Contributor - Create items and files only. The contents of the folder do not appear.

Custom - Perform activities defined by the folder owner.

D

Database Administrator - A database administrator (DBA) is responsible for the performance, integrity and security of a database. Additional role requirements are likely to include planning, development and troubleshooting. The database approach incorporates the following principles: • data remains consistent across the database; • data is clearly defined;

• Users access data concurrently, in a form that suits their needs;

• There is provision for data security and recovery control (all data is retrievable in an emergency).

DBA roles are increasingly identified by the databases and processes they administer and the capabilities of the database management system (DBMS) in use. (PIPS)

Dataset – Specific access needed within the system.

Date of Favorable Adjudication - When was the investigation Adjudicated?

Date of investigation completed - When was the date of the investigation?

DCCS Org Code – Not yet defined.

DCCS through Citrix – Not yet defined.

Developer - Access to Managed Reporting Environment Develops reports using Developer Studio; creates, edits, & saves reports & reporting objects; Submits reports to MRE Administrator for testing and publishing in the appropriate MRE environment.

Download Case Status Information - Agencies with automated tracking systems of their own, and wo request a large volume of OPM cases, may arrange for OPM to transmit status information for download by the agency. A special terminal and agreement with OPM must be in place to request this function.

Download Document – This function enables agency SOIs to download various OPM documents: OPM Investigation Scheduled Notices, Advance Fingerprint Reports, Advance NAC Reports, and/or Case Closing Transmittals with results of investigations. The Download function transmits the information in a .txt file to the SOI. A special terminal and agreement with OPM must be in place to request this function.

E

Editor - Create, read, modify, and delete all items and files.

End User - They will be using the portal as a regular user with no administrative responsibilities.

Enter Agency Adjudication - This function enables OPM customers to report the adjudicative action taken on an OPM investigation. Investigative Service Providers (ISPs) can report adjudicative actions on their cases through this function.

Electronic Questionnaires for Personnel Investigations (e-QIP) – The web-based automated system that has been developed for the US Office of Personnel Management, Federal Investigative Services, to provide a means to facilitate the processing of standard forms for suitability and security investigations.

e-QIP Doc Reviewer – A role within the OPIS system that allows users to Search, View, Modify Doc Types, Delete, Repository Transfer and Print in e-QIP Doc Review repository.

e-QIP Doc Supervisor – A role assigned to an individual with OPIS access that allows the ability to perform all functions, except for FOI/P.

Existing LAN user ID - Currently an Existing Employee with network Credentials.

Existing Sysplex user ID - Currently has PIPS login ID.

F

Field Document Repository (FDR) - The FDR is the system that maintains electronic images of releases, certifications and authorizations that are part of the investigation paperwork created when an individual completes their e-QIP form.

Federal Item Validation Special – A role assigned to an individual with Web ePRP access. This role has not been defined yet.

Federal Item Validation Supervisor – A role assigned to an individual with Web ePRP access. This role has not been defined yet.

Federal Post Audit QA – A role assigned to an individual with Web ePRP access. This role has not been defined yet.

Federal Pre Review – A role assigned to an individual with Web ePRP access. This role has not been defined yet.

Federal Pre Review Supervisor – A role assigned to an individual with Web ePRP access. This role has not been defined yet.

FIS Agent – Federal Investigative Agents are OPM federal employees that perform background investigations for suitability and security purposes.

FIS Systems – Computer systems owned by FIS - Dashboard, OPIS, e-PRP, CVS, e-QIP, FTS, PIPS, FWS, and EPIC

FOIA/P User – A role assigned to an individual with OPIS access that provides special limited access to the Freedom of Information/Privacy Act personnel and select individuals based upon their job requirement

FTS - Fingerprint transaction system.

Full Access - Create, read, modify, and delete all items and files, and create subfolders.

H

Hardware – Equipment provided to a user, including but not limited to a laptop, desktop, printer, scanner, cell phone, GPS unit.

Homeland Security Presidential Directive -12 (HSPD-12) – A Presidential Directive dated 27 Aug 2004 with the subject title of "Policies for a Common Identification Standard for Federal Employees and Contractors". The HSPD-12 directs the implementation of a new standardized badging process designed to enhance security, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees, contractors (and contractor employees) through use of a Personal Identification Verification (PIV) card.

I

Image Technician - Scan Event List, Scan Event Search, Image/Barcode Verify.

Initiator - A role assigned to an external OPM Federal employee/contractor who can initiate an Applicant/employee, select the form(s) to be completed by the Applicant, completes the Agency Usage Block (AUB), contacts the Applicant/employee to instruction on how to complete the investigation form(s) using e-QIP, request a reset of Golden Questions, and cancel/un-cancel requests.

IP (Internet Protocol) Number of existing printer – The printer address indentified as a numeric location on the LAN with the following template: xxx.xxx.xxx.xxx (such as 124.124.124.124. The numeric composition of each section is either 2 or 3 digits in length.

Item Review - Item Review is the main path for items that are validated through PIPS.

Item Validation - Item Validation is the main path for items that cannot be validated through PIPS.

J

Joint Personnel Adjudication System (JPAS) – The DoD database for information pertaining to DoD personnel that provides real-time information regarding clearance, access and investigative status to authorized DoD personnel and other interfacing organizations.

L

LAN - Local Area Network.

Level of last investigation - What was the clearance level of the last investigation?

Library only user - Accesses Dashboard to execute predefined reports in the appropriate library.

Local Printer – Printer that is attached to their work computer

M

Mailbox/Public Folders – Outlook mail box for users to share – outlook public folders folders that user can access from outlook

Manager - A manager is a person who oversees employees or departments in the field or support operation for OPM business. They use the manager's menu in PIPS. They have access to see both what the investigators or support staff is doing and they also have access for employee oversight.

Modify LAN user ID - Permission change for existing LAN account.

MR Administrator - Creates system domains, groups, roles and users. Manages user access to reporting domains. Creates reports for end users. Tests reports submitted by Report

Developers and Analysts to ensure that information and data are presented in compliance with agency reporting rules and guidelines.

N

Network Printer – (LAN Printer) printer shared among other users

New LAN user ID – Requesting New LAN Account needing account to logon to the network

New Laptop/Desktop – Hardware equipment to do your every day job

New Sysplex user ID - Needs new pips login ID.

None - You have no permission. You can't open the folder.

O

OFI-79 Notice - This option is used in conjuction with providing access to external Federal Agencies. Federal Investigative Service Providers (ISPs) use this function to report their investigations electronically to OPM’s SII as required by Executive Order 10450. ISPs can conduct a CVS search through this function and request OPM files.

OMVS/UNIX - Release repository access.

Open Case – A role within the OPIS system that provides users the ability to see images for cases that are currently in process.

Operator Role – A role within the FTS system that provides the ability to do the following functions: Case Number Search; Submission Search, Pips File Search.

OPIS - OPM PIPS Imaging System.

OPIS All Doc Search – Not yet in production.

OPIS Doc Import Web – Not yet in production.

OPIS Doc Post Commit – A role within the OPIS system that provides users access to Stellent and the ability to search and retrieve ALL case document images in 'Closed' case only.

OPIS Doc Pre Commit – A role within the OPIS system that provides users the ability to prepare case documents, Oliver, Scan, Re-scan and QA.

OPIS Doc Supervisor – A role within the OPIS system that provides users the ability to prepare case documents, Scan, Re-scan, QA, delete from Captiva and POSTC (if in this group), search and retrieve ALL documents before and after committal to the Stellent database. This role is provided to individuals who need the ability to perform all functions (except for FOI/P).

OPIS Report Delivery Clerk – Not in production.

OPIS Report Delivery Supervisor - Not in production.

Org Administrator - They will be responsible for maintaining the users in the portal within their organization.

Owner - Create, read, modify, and delete all items and files, and create subfolders.

P

PII (Personally Identifiable Information) – Information that can be used to discern or trace a person's identity, and alone or combined with other information can be used to compromise the integrity of records relating to a person by permitting unauthorized access to or unauthorized disclosure of records. An example of a breach of PII would not necessarily be disclosure of a person's name, but when that name is linked with other identifying data, such as the person's social security number, date of birth or mother's maiden name, it would constitute a breach of PII.

PIPS (Personal Investigative Processing System) - The core system used for processing all background investigations by OPM-FIS. PIPS also houses the Security/Suitability Investigations Index.

PIV Card - The Personal Identity Verification card used by the federal government to complies with HSPD-12 requirements to provide a government-wide credential that contains information about the individual. The PIV card contains an integrated circuit chip that stores 64 kb of data, including four PKI digital certificates; two interoperable fingerprint templates; a digital photo; and a Cardholder Unique Identifier (CHUID) including the organization affiliation, agency affiliation, department affiliation and expiration date.

Power User - Creates and accesses metadata for data sources. Creates Reporting Objects for Managed Reporting and Dashboard users. Schedules and distributes reports. Customizes user environments.

Print Document - This function enables agency SOIs to print from their PIPS Terminal. Agencies can print: OPM Investigation Scheduled Notices, Advance Fingerprint Reports, Advance NAC Reports, and/or Case Closing Transmittals with results of investigations. A special terminal and agreement with OPM must be in place to request this function.

Program Manager – A role within the e-QIP system responsible for performing supervisory tasks including viewing the status of work for the agency, assigning/un-assigning requests, approving/rejecting Golden Question resets, and canceling requests.

Publishing Author - Create and read items and files, create subfolders, and modify and delete items and files you create.

Publishing Editor - Create, read, modify, and delete all items and files, and create subfolders.

R

RARDG – Records Access and Research & Development Group

Read - Only have the ability to read Documents/Messages in the Folder/Mailbox.

Record Specialist - Use the FIDR menu for their work collecting information in Law Checks mainly through the court houses. The FIDR also allows them to transmit PC Reports through PIPS R. They can assign items/update items, Display CATS/Case papers, request documents and send messages through the PIPS mail secure system.

Reinstate LAN user ID - If the applicant is a returning user, please enter their former LAN ID in this area

Request SAC (Special Agreement Checks)- This function provides for direct request and initiation of SAC. A written agreement is required between the agency and OPM.

Reviewer – A role within the e-QIP system responsible for reviewing Applicant data, accepting/rejecting Applicant/employee answer(s), entering comments for rejected answer(s), and attaching documents.

Reviewer - Read items and files only.

Role - The duty that the user will be performing.

S

Search SII/CVS/JPAS - A role within the PIPS for non-OPM Federal Agency employees/ contractors. The CVS contains information on security clearances, investigations, suitability and fitness determinations. HSPD-12 , PIV credentials, and polygraph data. A search of CVS performs a simultaneous search of the SII, CVS and JPAS systems. There are two options for this function:

Non-Investigative Service Provider View – select if OPM conducts your investigations

Investigative Service Provider View – only allowed to agencies who are set up in PIPS as an investigative agency

Secure Portal (aka OPM Security Portal – OPMIS) - A web-based platform that establishes a secure, encrypted environment that is used for the exchange of controlled unclassified information, including Sensitive But Unclassified Information (SBU) such as Privacy Act information and Personally Identifiable Information (PII). This application provides encrypted secure messaging and file sharing capability to OPM-FIS and its customers as well as a user friend interface into e-QIP and PIPS.

Security Office Personnel – An external Federal Agency user with full duties at an OPM authorized SOI.

Send As – When requesting that an applicant be provided access to a shared mailbox this option allows the applicant the to send mail with the mailbox name listed in the from: section of the message.

SII (Security/Suitability Investigations Index) – A repository of over 11 million background investigation records of Federal employees, military personnel and contractors that is maintained for a minimum of 16 years. SII data is not available to the SON; only the SOI can obtain a SII search.

SOI (Security Office Identifier) – A four-character alphanumeric code assigned to non-OPM Federal Agency Security Offices. The SOI is responsible for receiving completed investigation reports from OPM-FIS, controlling the agency’s cases and making the suitability and security determinations on subjects of investigation. The SOI designates security office employees who may contact OPM-FIS to obtain detailed case information after answering questions posed by the Telephone Liaison group in order to confirm the identity of the individual calling prior to the release of information. The security office is also responsible for completing a variety of investigative forms. To obtain a SOI a PIPS 12 Form (obtained from OPM-FIS Telephone Liaison at 724-794-5228) must be completed.

SON (Submitting Office Number) - A four-character alphanumeric code assigned to each non-OPM Federal Agency that requests investigations to OPM. The SON identified the office that initiates the investigation. To obtain a SON the agency must complete a PIPS 12 Form (obtained from OPM-FIS Telephone Liaison at 724-794-5228).

Special – Fed Items in e-PRP

Submission Tech – A role within the FTS system that provides the following functions: Manual Reprint Processing, Submission Deletion.

Support (Data Entry/Review) - PIPS Account.

Suitability Adjudicator – An external Federal Agency user with suitability adjudication duties whose physical location may differ from that of the SOI.

Sysplex through Citrix - Needs PIPS via Citrix for telework reasons.

System Administrators - System Administrator Access for maintenance for the system.

T

Telework - OPM allows employees to work from alternate worksites as part of their regular tour of duty through the OPM Telework program. Locations may include the employee’s home, satellite telecommuting centers or other approved sites away from the office. If the applicant will be working from a Telework location as an option of their employment, select one of the Telework options: Telework (has a PIV card) or Telework (no PIV card). If the second option is selected, enter a reason the applicant does not have a PIV card in the appropriate box below this option.

TSO Production - A portion of the PIPS system that allows access to the RACF production database.

TSO Test – The test area of PIPS associated with RACF Quality Assurance.

U

User - Access to MRE Executes canned reports Shares reports Creates, edits & saves ad hoc reports with Power Painter, Report Assist, and/or Graph Assist using pre-determined data sets.

User Account – When associated with the LAN access on the SYSTEM ACCESS TAB, four options are available for selection: New LAN Userid, Existing LAN Userid, Modify existing User Account, and Reinstate Account. The first option is used if the applicant is new to the OPM LAN system; if the user has or previously had an account enter that User ID in the block for that option.

User Account - Needs pips account login ID.

User Administrator – A role available in the e-QIP system responsible for managing users who have been provided access and responsibility within their e-QIP compartment.

User Auditor – A role available in the FTS system that provides the ability to search users in the system.

W

Web ePRP (electronic Pre-Review Process) – A web-based process that provides the review of investigative materials received ensuring relevant information is available for use in the full investigation process.

Workflow Coordinator – A role within the FTS system responsible for the following options: Submission Event List, Submission Event Search, Failed Admission Totals, Failed Admission Search, PIPS Event List, Overdue Submission Totals, and FBI Error Totals.