



HRCPO Access Request

Document Owner(s)	Document Number Version or Status	Effective Date	Last Update	Procedure Coordinator
HR Connect Security Team	Version 3.1	05/02/2001	11/02/2006	Carl J Turner
Distribution	Author	Creation Date	Security	Approved by:
HR Connect Program Office	Carl J Turner, ISSO	11/02/2006	Public	Renee Wilmot, ISSM

Procedure Description

Fill out the HRCPO Access Request Form to request to the general HRCPO LAN, the Development System, or to change a User's registration profile, change or revoke access to specific networks/databases. The requestor must obtain the appropriate signatures and submitted to Assistant Director for Technical Architecture for implementation 48 hours before requested completion date.

Scope and Purpose:

Communicate and obtain user acknowledgement on appropriate security rules and control access to production networks and databases in order to protect the security of HRCPO data and systems.

Roles:	Responsibilities:
Requester/Requester designee/User	Fill out appropriate request form, obtain all required signatures and submit to Assistant Director for Technical Architecture. Read, sign and submit the Information Systems Security Rules and Privacy Act form if new employee or submitting first time network access request.
User's Manager/COTR	Complete and verify <i>Status of Background Investigation</i> section of the request form. Certify with signature that user has received security instructions for the system/application and approve access.
HR Connect ISSO / HR Connect ISSM	Review information in Status of Background Investigations section of form and approve ALL HRCPO Network Access Requests.
Functional Application Manager/Federal Infrastructure Manager	Approve ALL HRCPO Network Access Requests.
HRCPO NT Administrator	Implement all approved network access requests within 48 hours of receipt, notify requester of action taken and file forms.

Requirements, Warnings and Special Notes

Related Knowledge	Tools, Systems, Materials, Equipment:
N/A	HRCPO Development System User Registration/Change Request Form Information Systems Security Rules and Privacy Act

Warnings and Precautions	Special Notes:
Prevent HR Connect Security Violations	Security documentation must be filled out and submitted for any new HR Connect employee and the employee must read and sign the Information Systems Security Rules and Privacy Act before network access, at any level, can be granted.
	NOTE: The individual's HRCPO Federal manager must approve all initial access & profile modification requests



Steps

	Step: / How To Do:
1	<p>Complete the user information (boxes 1-11).</p> <ol style="list-style-type: none">1.1 Select the access request to HRCPO systems.1.2 Enter the user's social security number.1.3 Enter the user's name.1.4 Enter the user's title. Contractor: Check the block if user is contractor personnel.1.5 Enter the user's mail and email addresses.1.6 Enter the user's organization.1.7 Enter the time of day when the user's normal workday starts and ends. Circle the symbols that represent the user's normal workdays. Note this will determine the individuals access parameters to HRCPO systems.1.8 Enter the user's phone number.1.9 Enter the user's manager's phone number.1.10 Enter the user's Post of Duty (Bureau, HRCPO, DCC, other)1.11 Enter the name of the Office where the user's Post of Duty is located.
2	<p>Complete the Action Requested information (boxes 13-20 excluding box 16).</p> <ol style="list-style-type: none">2.1 If changing a user's name, enter the user's "old" name and "new" name.2.2 Check the appropriate action to be taken relative to the user, i.e. add, delete, modify, etc.2.3 Enter the Requested Date which is the date the user/requester wants the action to be effective.2.4 Leave the Effective Date, which is the date the action actually became effective, blank. (This date is to be entered by the person responsible for establishing system access, i.e. HRCPO NT Administrator. See Step 8.3)2.5 Enter the User ID/Logon name. For new user requests, this code will be entered by the System Administrator. For user profile name changes and user deletes, the requester will enter the users previously assigned system logon code.2.6 In Box 18, indicate the application access requested: HRCPO Generic, PeopleSoft (PS) HRCPO, Rational ClearQuest, Rational ClearCase, Rational ReqPro, HRCPO NT, HRCPO Unix, HRCPO Oracle or Other. Specify the name of the project and the name of the instance, if applicable. Also specify if "other" is circled. Note: Fill out a separate Network Request Form for each application requested.2.7 Select an Access Profile: User/Tester, System Administration, DBA, Other. Specify if "Other" is circled.2.8 Fill in the special instruction field. Contractors must specify contract number and expiration date. <p>Read, sign and date the User's Acknowledgement (box 21).</p>
5	<p>Submit form to user's HRCPO Federal manager to complete Status of Background Investigation section (box 12). User's manager will:</p> <ol style="list-style-type: none">4.1 For new employees, enter the date the background investigation information was submitted or the date the U.S. Secret Service Police check was completed (if the user is not required to submit a SF 86).4.2 For existing/returning employees, enter the date the background investigation was completed or the date initiated, if not completed. Check with the Functional Security Manager (HRCPO ISSO) if necessary for this information.4.3 For contractors, enter the date the background investigation was complete.4.4 Enter the name of the individual entering the background investigation information on the "Verified By" line.4.5 Indicate the "Source" used for verifying the background investigation date.
6	<p>Obtain the User's FEDERAL Manager's signature (box 22).</p> <ol style="list-style-type: none">5.1 Type or print the name of the user's federal manager in this block. Then this block is to be signed and dated by the user's manager, indicating he/she 1) certifies that the user has received the appropriate security instructions and 2) approves the requested action. If contractor personnel, the COTR signature is required.
7	<p>Obtain the signature of the HRCPO ISSO (box 23) and/or HRCPO ISSM (box 24).</p> <ol style="list-style-type: none">6.1 These blocks are to be signed by the Information System Security Officer (ISSO) or Manager (ISSM). Its purpose is to ensure the person responsible for security for the system or application is aware of and concurs with the requested action.
8	<p>Obtain the signature of the Technical Architecture Advisor (box 25).</p> <ol style="list-style-type: none">7.1 This block is to be signed by either the manager responsible for the operation of the computer system or application being accessed, depending on the system or local policies and procedures. For HRCPO, this is the Federal Technical Architecture Advisor. The purpose of this signature is to allow the system/application "owner"



<p>Step: / How To Do: an opportunity to control access to his/her system. Complete Action Taken section (box 16, 25). 8.1 NT System Administrator/Security Officer (HRCPO NT Administrator)-- as the person responsible for performing the requested action (i.e. access paths, privileges, etc.) -- must sign, date and indicate the action taken (i.e. "user added", "user deleted", "access privileges changed", etc.) in box 25. 8.2 NT System Administrator/Security Officer (HRCPO NT Administrator) also fills in the effective date of the action in box 16. 8.3 The NT System Administrator notifies the requester that the network access activity is complete, files a copy of the request form and any attachments in the appropriate location, and returns the original request form to the HR Connect ISSO.</p>

Contact for Help

<p>Common Problems: Failure to submit signed Information Systems Security Rules and Privacy Act statement.</p>	<p>How to Get Help: Obtain form from HRCPO Security.</p>
--	--

Attachments

<p>Document Title(s) and References: HRCPO Access Request Procedure Information Systems Security Rules and Privacy Act</p>	<p>Location or Source: HRCPO, 1750 Pennsylvania Avenue, NW, Suite 1300, Washington DC, 20006. The electronic file can be found on the J:\docs\Information Security drive under Forms- Policies & Procedures.</p>
--	--

Records

Retention Period:	Contributors:	Revision History and Notes:
Indefinitely	Chuck Watson	03/20/01 - converted procedure to HRCPO Network Requests with new attachments; 3/22/01 - added Rational ReqPro to application selections; 04/05/01 - edits made per R. Wilmot. 09/14/01 - converted to one form for all access requests
Responsible: Chuck Watson		
Retention Period:	Contributors:	Revision History and Notes:
Indefinitely	Carl Turner	08/17/06 - Changed to reflect new organization's name HRCPO 11/02/06 - Changed approving official to Renee Wilmot from Ira Hobbs; added ISSM Role
Responsible: Carl Turner		



I _____ agree to the following:

Information Systems Security Rules and Privacy Act
VIOLATION OF THESE RULES MAY RESULT IN DISCIPLINARY ACTION

1. DO NOT ACCESS, RESEARCH, OR CHANGE any account, file, record, or application not required to perform your official duties.
2. If you are asked by another person to access an account or other sensitive or private information, **verify** that the requested access is authorized. You will be held responsible if the access is not authorized. As a general rule, you should not use a computer or terminal in behalf of another person.
3. PROTECT YOUR PASSWORD from disclosure. You are responsible for any computer activity associated with your password. Do not share your password with others or reveal it to anyone, regardless of his/her position in or outside of Treasury. Do not post your password in your work area. Do not use another person's password. Entry codes must be treated with the same care as your password. Everything done with your entry code or password will be recorded as being done by you.
4. CHANGE YOUR PASSWORD if you think someone else knows your password. Immediately notify your supervisor or your Functional Security Coordinator or Security Representative. Change your password at least every 6 months.
5. DO NOT PROGRAM your login or password into automatic script routines or programs.
6. LOG OFF/SIGN OFF if you go to lunch, or break, or anytime you leave your computer or terminal.
7. RETRIEVE ALL sensitive hard copy printouts in a timely manner. A shredder is available for the proper disposal of sensitive hard copy materials.
8. IDENTIFY ALL sensitive applications or data that you will be placing on a system, and any equipment processing sensitive information to your supervisor, so that appropriate security measures can be implemented.
9. DO NOT USE TREASURY COMPUTERS OR SOFTWARE for personal use.
10. DO NOT USE PERSONAL EQUIPMENT OR SOFTWARE for official business without your supervisor's written approval.
11. DO NOT INSTALL OR USE UNAUTHORIZED SOFTWARE on Treasury equipment. Do not use freeware, shareware, or public domain software on Treasury computers, without your supervisor's permission and without scanning for viruses. Comply with local office policy on the use of antiviral software.
12. OBSERVE ALL SOFTWARE LICENSING AGREEMENTS. Do not violate Federal copyright laws.
13. DO NOT MOVE EQUIPMENT or exchange system components without authorization by the appropriate Information Systems function.
14. PROTECT TREASURY COMPUTER EQUIPMENT from hazards such as liquids, food, smoke, staples, paper clips, etc.
15. PROTECT MAGNETIC MEDIA from exposure to electrical currents, extreme temperatures, bending, fluids, smoke, etc. Ensure that magnetic media is secured based on the sensitivity of the information contained, and practice proper labeling procedures. Ensure that magnetic media is secured in locked cabinets. BACK UP critical programs and data, and store in a safe place. Back ups should be performed often to ensure data integrity.
16. DO NOT DISCLOSE THE TELEPHONE NUMBER (S) OR PROCEDURE (S), which permit system access from a remote location.
17. DO NOT USE SSN OR OTHER SENSITIVE INFORMATION for equipment or program test purposes.



18. Vendors should be escorted and monitored while performing system maintenance duties. All vendors should be identified with an appropriate level badge.

19. DO NOT DISCLOSE OR DISCUSS ANY PERSONNEL INFORMATION with unauthorized individuals. The Privacy Act of 1974, 5 USC 552a, prohibits such disclosure. A person making a willful unauthorized disclosure of information covered by this act may be charged with the misdemeanor and subject to a fine of up to \$5,000.

20. PROMPTLY REPORT all security incidents to your supervisor. For example: unauthorized disclosure of information, computer viruses, theft of equipment, software or information, and deliberate alteration or destruction of data or equipment.

Privacy Act Notice

In compliance with the Privacy Act of 1974, the following information is provided: Solicitation of your Social Security number is authorized by Executive Order 9397 of November 22, 1943 and 5 U.S.C.301. The primary purpose of requesting the social security number (SSN) is to properly identify the employee. Many employees have similar names and furnishing of the SSN will enable HR Connect to identify authorized users of the system. The Information will not be disclosed outside the Treasury Department. Disclosure of your SSN and other information is mandatory. Failure to provide the requested information will result in the denial of the requested system access authority.

I agree to these terms.

Print Name

Signature

Date



HRCPO Access or Change Request		1. Access Requested: <input type="checkbox"/> HRCPO Generic (email) <input type="checkbox"/> HRCPO Development <input type="checkbox"/> Detroit Production HR Connect X Other: Training Database	
User Information (See Security & Privacy Statement)			
2. User's SSN		3. User's Name (last, first, middle initial or nickname)	
4. User's Title <input type="checkbox"/> Contractor		5. User's Mail and Email Addresses	6. User's Org.
7. Requested Access Hours: Start: _____ (AM / PM) Stop: _____ (AM / PM) Circle the days you require access: S M T W T F S		8. User's Phone Number	9. Manager's Phone
10. Post of Duty		11. Office	
Status of Background Investigation			
12. New Employees Only <input type="checkbox"/> Initiated Enter Date Initiated: _____ or <input type="checkbox"/> Enter on Duty Date: _____			
Existing/Returning Employee <input type="checkbox"/> Completed Enter Date Completed: _____ or <input type="checkbox"/> Initiated Date Initiated: _____			
Contractors <input type="checkbox"/> Completed Enter Date Completed: _____			
Verified by: (Print Name) _____		Source: <input type="checkbox"/> HRCPO <input type="checkbox"/> Other _____	
Action Requested			
13. Name Change : Old Name		New Name	
A C C E S S	14. <input type="checkbox"/> New user (Check all that apply) <input type="checkbox"/> Request for new password <input type="checkbox"/> Delete user <input type="checkbox"/> Modify user's profile: <input type="checkbox"/> Access to additional databases <input type="checkbox"/> Modify access hours <input type="checkbox"/> Other: _____		15. Request Date
			16. Effective Date
		17. User ID/Logon N/A	
18. Access to what application/s? 1. HRCPO Generic: <input type="checkbox"/> HRCPO Generic <input type="checkbox"/> OHRCPPO Email 2. Development: <input type="checkbox"/> PS HRCPO <input type="checkbox"/> PS Mint <input type="checkbox"/> ClearQuest <input type="checkbox"/> ClearCase <input type="checkbox"/> ReqPro <input type="checkbox"/> HRCPO NT <input type="checkbox"/> HRCPO Oracle <input type="checkbox"/> HRCPO Unix <input checked="" type="checkbox"/> Other Training D.B. Project _____ Database _____ 3. Production (Detroit): <input type="checkbox"/> PS Detroit Production <input type="checkbox"/> Detroit Unix <input type="checkbox"/> PS Detroit User Acceptance Testing <input type="checkbox"/> Other _____			
19. Access Profile: <input checked="" type="checkbox"/> Project Staff <input type="checkbox"/> QA/Tester <input type="checkbox"/> System Administration <input type="checkbox"/> DBA <input type="checkbox"/> Other: _____			
20. Special Instructions (If contractor, specify contract number and expiration date.)			
User's Acknowledgement			
21. I HAVE READ THE INFORMATION SYSTEMS SECURITY RULES AND UNDERSTAND THE SECURITY REQUIREMENTS OF THE INFORMATION SYSTEM AND/OR APPLICATIONS DESCRIBED ON THIS FORM. I UNDERSTAND DISCIPLINARY ACTION, REMOVAL FROM THE HRCPO PRODUCTION SYSTEM, AND/OR CRIMINAL PROSECUTION MAY BE TAKEN BASED ON VIOLATION OF THESE RULES.			
User's Signature _____		Date _____	
Authorization			
22. User's Federal Manager - I certify that this applicant has received security instructions for the system and/or applications indicated, and I approve his/her access to these systems and/or applications. The applicant's FEDERAL manager must sign this request.		Print and sign name	Date
23. HRC Information System Security Officer (ISSO)			Date
24. HRC Information System Security Manager (ISSM)			Date
25. HRC Technical Architecture Manager			Date
Action Taken			
26. System Administrator/Security Officer (HR Connect HRCPO NT Administrator)			Date