

## Workforce Analytics Reporting System Access Request

Document Owner(s)	Document Number Version or Status	Effective Date	Last Update	Procedure Coordinator
OCIO Security Team	Version 1.5	07/26/2011	01/08/2010	Carl J Turner
Distribution	Author	Creation Date	Security	Approved by:
DO/OCIO	Carl J Turner, ISSO	01/28/2008	Public	Renee Wilmot, ISSM

### Procedure Description

Fill out the Workforce Analytics Reporting System (WA RS) Access Request Form to request access to the WADEV 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 the Security Team 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 Treasury data and systems.

Roles:	Responsibilities:
Requester/Requester designee/User	Fill out request form, obtain all required signatures and submit to OCIO CyberSecurity/ Security Team. 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.
OCIO ISSO / ISSM	Review information in Status of Background Investigations section of form and approve ALL Network Access Requests.
NT Administrator	Implement approved network access requests within 48 hours of receipt, notify requester of action taken and return forms to WA RS Security Officer (ISSO).

### Requirements, Warnings and Special Notes

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

Warnings and Precautions	Special Notes:
Prevent DO/OCIO Security Violations	<p>Security documentation must be filled out and submitted for any new 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.</p> <p style="color: red; font-weight: bold;">NOTE: The individual's Federal manager must approve all initial access profile modification requests</p>

## Steps

Step: / How To Do:
<p><b>1</b> Complete the <b>User Information</b> (boxes 1-11).</p> <p>1.1 a- Select the access needed to the WA RS system. b. Internal Roles assigned to WA RS staff only.</p> <p>1.2 Enter the user's last 4 digits of their social security number.</p> <p>1.3 Enter the user's name.</p> <p>1.4 Enter the user's title. <b>Contractor/Intern:</b> Check the appropriate block if contractor personnel or Intern.</p> <p>1.5 Enter the user's mail and email addresses.</p> <p>1.6 Enter the user's organization.</p> <p>1.7 Workforce Analytics System is available 24 hours a day except when maintenance is announced.</p> <p>1.8 Enter the user's phone number.</p> <p>1.9 Enter the user's manager's phone number.</p> <p>1.10 Enter the user's Agency or Bureau (BPD, US MINT, HUD, FINCEN, ATF, USSS, etc.)</p> <p>1.11 Enter the name of the Office where the user's Post of Duty is located.</p>
<p><b>2</b> Complete the <b>Action Requested</b> information (boxes 12-18 excluding boxes 15 &amp; 16).</p> <p>2.12 If changing a user's name, enter the user's "old" name and "new" name.</p> <p>2.13 Check the appropriate action to be taken relative to the user, i.e. add, delete, modify, etc.</p> <p>2.14 Enter the Requested Date which is the date the user/requester wants the action to be effective.</p> <p>2.15 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. WA NT Administrator. See Step 8.3)</p> <p>2.16 The User ID/Logon name will be entered here. 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.</p> <p>2.17 Fill in the special instruction field. Contractors must specify contract number and expiration date.</p> <p>2.18 Read, sign and date the User's Acknowledgement (box 18).</p>
<p><b>3</b> Submit form to user's Federal manager to complete Status of Background Investigation section (box 19):</p> <p>3.19 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). 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 (ISSO) if necessary for this information. For contractors, enter the date the background investigation was complete. Enter the name of the individual entering the background investigation information on the "Verified By" line. Indicate the "Source" used for verifying the background investigation date.</p> <p style="text-align: center;"><b>User's FEDERAL Manager must sign in the signature area (box 20).</b></p> <p>3.20 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.</p>
<p><b>4</b> Submit Request form to WA RS ISSO/ISSM via one of the processes below:</p> <p>a. <b>IRS requests ONLY:</b> Scan completed form into PDF format, encrypt file in a password protected WinZIP file and email to Jean Stroisch 314-954-6816: <a href="mailto:Jean.A.Stroisch@irs.gov">Jean.A.Stroisch@irs.gov</a> Jean will forward to WA RS ISSO using either option b or c below:</p> <p>b. Via Email: Scan completed form into PDF format, encrypt file in a password protected WinZIP file and email to Carl Turner: <a href="mailto:Carl.Turner@treasury.gov">Carl.Turner@treasury.gov</a></p> <p>c. Via Fax (202 622-2981): Contact Carl Turner 202 622-1128 or via email <a href="mailto:Carl.Turner@treasury.gov">Carl.Turner@treasury.gov</a>, to inform of the time the fax was sent.</p> <p>Upon receipt and approval of action, the WA RS ISSO (box 22) and/or OCIO ISSM (box 23) will provide signatures. These blocks are to be signed by the WA RS 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.</p>
<p><b>5</b> Complete Action Taken section (boxes 15, 16, 17, 24). NT System Administrator/Security Officer (WA RS NT Administrator) may also fill in the effective date of the action in box 16. The NT System Administrator notifies the requester/WA RS Security Officer that network access activity is complete, and returns the original Completed request form and any attachments to the WA RS ISSO.</p>

**Contact for Help**

<b>Common Problems:</b>	<b>How to Get Help:</b>
Failure to submit signed Information Systems Security Rules and Privacy Act statement.	Obtain form from OCIO / CyberSecurity / WA RS ISSO.

**Attachments**

<b>Document Title(s) and References:</b>	<b>Location or Source:</b>
Access Request Procedure  Information Systems Security Rules and Privacy Act	OCIO/CyberSecurity, 1750 Pennsylvania Avenue, NW, Suite 13452, Washington DC, 20006.  The electronic file can be found on the J:\docs\Information Security drive under Forms- Policies & Procedures.

**Records**

Retention Period:	Contributors:	Revision History and Notes:
Indefinitely	Scott Cohen	01/22/08 - converted procedure from HRCPO Access Requests to handle all Workforce Analytics Reporting System access requests.
<b>Responsible:</b>		
Carl Turner		
Retention Period:	Contributors:	Revision History and Notes:
Indefinitely	Carl Turner	11/24/08 - reviewed, modified and approved instruction changes. 03/18/09 - 1.1 a Access types; 1.1 b -added Internal Roles. 1.2 Added SSN Masking 1.10 changed wording.
<b>Responsible:</b>		
Carl Turner		
Retention Period:	Contributors:	Revision History and Notes:
Indefinitely	Carl Turner	01/11/10 - Added TLMS selection box in section 1-A. - Added IRS ONLY approval box 21. - Moved ISSO AND ISSM Approval to boxes 22 and 23.
<b>Responsible:</b>		
Carl Turner		
Retention Period:	Contributors:	Revision History and Notes:
Indefinitely	Carl Turner	07/26/11 - Removed references to HRConnect, HRC, HRCPO - Inserted Workforce Analytics Reporting System (WA RS)
<b>Responsible:</b>		
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. Use a shredder 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

Please retain for you records.

<b>Workforce Analytics Reporting System Access or Change Request</b>		<b>1. a- Access Requested:</b> <input type="checkbox"/> Access to PII data <input type="checkbox"/> Report Builder (General) <input type="checkbox"/> Organization Lead <input type="checkbox"/> TLMS  <b>b- Internal Roles (WA RS Staff only):</b> <input type="checkbox"/> WADEV <input type="checkbox"/> WAPROD <input type="checkbox"/> WADEV no SBU/ PII data access		
<b>Section 1. User Information (See Security &amp; Privacy Statement)</b>				
<b>2. Employee SSN (Last 4 digits)</b> <b>XXX-XX-</b>		<b>3. User's Name (last, first, middle initial or nickname)</b>		
<b>4. User's Title</b> <input type="checkbox"/> Contractor <input type="checkbox"/> Intern <input type="checkbox"/> Federal Employee		<b>5. User's Mail and Email Addresses</b>		<b>6. User's Org.</b>
<b>7. Requested Access Hours:</b> 24 hrs day / 7 days a week: <u> X </u>		<b>8. User's Phone Number</b>		<b>9. Manager's Phone</b>
<b>10. Post of Duty (Agency/Bureau):</b>		<b>11. Office</b>		
<b>Section 2. Action Requested</b>				
<b>12. Name Change : Old Name</b>		<b>New Name</b>		
<b>A</b> <b>C</b> <b>C</b> <b>E</b> <b>S</b> <b>S</b>	<b>13. <input type="checkbox"/> New user (Check all that apply)</b> <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 environments <input type="checkbox"/> Other: _____		<b>14. Request Date</b>	<b>15. Effective Date</b>
			<b>16. User ID/Logon</b>	
<b>17. Special Instructions (If contractor, specify contract number and expiration date.)</b>  				
<b>User's Acknowledgement</b>				
<b>18. 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 WA RS PRODUCTION SYSTEM, AND/OR CRIMINAL PROSECUTION MAY BE TAKEN BASED ON VIOLATION OF THESE RULES.</b>  _____ <b>User's Signature</b> <span style="float:right">_____</span> <span style="float:right"><b>Date</b></span>				
<b>Section 3. Status of Background Investigation</b>				
<b>19. New Employees Only</b> <input type="checkbox"/> Initiated    Enter Date Initiated: _____ or <input type="checkbox"/> Enter on Duty Date: _____ <b>Existing/Returning Employee</b> <input type="checkbox"/> Completed    Enter Date Completed: _____ or <input type="checkbox"/> Initiated    Date Initiated: _____ <b>Contractors</b> <input type="checkbox"/> Completed    Enter Date Completed: _____ <b>Verified by: (Print Name)</b> _____ <b>Source:</b> <input type="checkbox"/> WA RS <input type="checkbox"/> Other _____				
<b>20. 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.</b>		<b>Print and sign name</b>		<b>Date</b>
<b>Section 4. Authorization</b>				
<b>21. IRS REQUESTS ONLY --- APPROVING OFFICIAL:</b>				<b>Date</b>
<b>22. WA RS Information System Security Officer (ISSO)</b>				<b>Date</b>
<b>23. OCIO Information System Security Manager (ISSM)</b>				<b>Date</b>
<b>Section 5. Action Taken</b>				
<b>24. System Administrator/ WA RS SQL Administrator)</b>				<b>Date</b>