



Wide Area Workflow

System Messages

(2013-JUL-25) System: *All* Subject: *Posting Docs Action Required! Critical! Message For: All Users*

[Open folder.](#)

(2013-JUL-24) This demonstration provides an overview of ECP0728, Electronic User Agreement.

Testing v5.5.0 Sy This presentation contains audio narrative. Please adjust your volume accordingly.

(2013-JAN-17) System: *All* Subject: *Message For: All Users*

Version:	5.5.0 Test BUILD02_8
Build Date:	09/24/2013
Application Server:	WebSphere 8.5.5.0
HTTP Server:	IBM IHS 8.5.5.0

Login



New User



Help / Training





Wide Area Workflow

System Messages

(2013-JUL-25) System: **All** Subject: **Posting Docs Action Required! Critical!** Message For: All Users

[Open folder.](#)

(2013-JUL-24) System: **All** Subject: **Test Action Required! Critical!** Message For: All Users

Testing v5.5.0 System Messages

(2013-JAN-17) System: **All** Subject:

The user clicks the New User button or icon to access the Registration link.

Version:	5.5.0 Test
Build Date:	09/24/2013
Application Server:	WebSphere 8.5.5.0
HTTP Server:	IBM IHS 8.5.5.0

Login



New User



Help / Training



New WAWF / EDA / CORT Tool / BI Users

Vendors Getting Started

- [WAWF - Getting Started Help](#)
- [Help - WAWF Vendor User Roles](#)
- [Help - EDA User Vendor Role](#)

Government and Government Support Contractors Getting Started

- [WAWF - Government Getting Started Help](#)
- [WAWF - Support Contractor Getting Started Help](#)
- [CORT Tool - Getting Started Help](#)
- [EDA - Government Getting Started Help](#)
- [EDA - Support Contractor Getting Started Help](#)
- [Help - WAWF Government User Roles](#)
- [Help - CORT Tool Government User Roles](#)
- [Help - EDA Government User Roles](#)
- [Help - Administration User Roles](#)

WAWF / EDA / CORT Tool / BI Tool User Registration

[Registration](#)



The user clicks the Registration link to access the Registration page.

Help

Registration

User Authentication Type >> Data Capture >> User Agreement >> Registration Success

* Asterisk indicates required entry.

Note: A security clearance is NOT required to access Wide Area Workflow, Electronic Document Access, Business Intelligence Tool, or Contract Officer Representative Tracking Tool.

What is your user type? *

- Government
- Government Support Contractor
- Vendor

What systems will you be using? * (You must check at least one)

- WAWF (Wide Area Workflow)
- EDA (Electronic Document Access)
- CORT Tool (Contracting Officer Representative Tracking Tool)
- Business Intelligence Tool

How will you be accessing these systems? *

- User ID \ Password
- Common Access Card
- Software Certificate

The user selects user type, system and how they will be accessing the system. Then clicks the "Next" button to continue.

Next

Help

Next (access key N)

Registration

User Authentication Type >> Data Capture >> **User Agreement** >> Registration Success

* Asterisk indicates required entry.

INFO: DoD has mandated that all Government users use CAC to access WAWF unless some work condition prohibits the use of CAC. The User ID, Location Code, or C/S/A (Commands/Services/Agency) must be on the CAC exemption table prior to registering with User ID/Password. If your User ID, Location Code, or C/S/A needs to be added to this table, please contact your Administrator (GAM, Site assistance). If you are unable to contact your Administrator, please contact your appropriate Service/ Agency Help Desk via the Government Customer Support link.

User Profile * [\(Edit\)](#)

First Name	Middle Name	Last Name	Organization	Title	Email Address	Mobile Telephone	Commercial Telephone	DSN Telephone
------------	-------------	-----------	--------------	-------	---------------	------------------	----------------------	---------------

User Authentication * [\(Edit\)](#)

User ID

User Security Questions * [\(Edit\)](#)

Security Question

WAWF Government User Roles * [\(Add\)](#)

WAWF Administrative User Roles * [\(Add\)](#)

The User Agreement has been added to the breadcrumb section and the "Next" button has replaced the "Registration" button.

Clicking the "Next" button will take the user to the User Agreement page.

Next

Previous

Help

Registration

User Authentication Type >> Data Capture >> **User Agreement** >> Registration Success

The User Agreement page is displayed.

The user scrolls to the bottom of the page.

STATEMENT OF ACCOUNTABILITY *

I understand my obligation to protect my password/certificate. I assume the responsibility for the data and system I am granted access to. I will not exceed my authorized access.

Standard Mandatory Notice & Consent Provision For All DoD Information System User Agreements 9 May 2008

Security and Privacy Rules of Behavior (ROB) / Acceptable Use Policy (AUP) 14 Jan 2010

STANDARD MANDATORY NOTICE AND CONSENT PROVISION FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS

You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.

You consent to the following conditions:

The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counter-intelligence (CI) investigations.

At any time, the U.S. Government may inspect and seize data stored on this information system.

Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.

Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

Nothing in the User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U. S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

[Register](#)[Previous](#)[Help](#)

Registration

User Authentication Type >> Data Capture >> **User Agreement** >> Registration Success

and DoD 5400.11-R, paragraph C1.4.

Place the standard Privacy Act warning label on the top of your computer monitor if names and social security numbers/personal bank account numbers, etc., are on your computer screen while you do your work. These labels can be generated on a plain white label that must read: "Personal Data, Privacy Act of 1974, as Amended, 5 U.S.C. 552a."

PII in DoD systems must be protected from unauthorized access especially when the system is in use and when the information is printed. The Privacy Act of 1974, As amended, 5 U.S.C. § 552a(i) also provides for criminal penalties.

(1) Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain personally identifiable information the disclosure of which is prohibited by this section or by rules or regulations established there under, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, may be found guilty in a court of law of a misdemeanor and fined not more than \$5,000.

(2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e) (4) of this section shall be guilty of a misdemeanor and fined not more than \$5,000.

(3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses may be found guilty in a court of law of a misdemeanor and fined not more than \$5,000.

If you have any questions or comments about the information presented here, please contact the Service Desk.

User's Acknowledgement of Standard Agreement, Security and Privacy Training

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

I have read and consent to the terms in the Standard Mandatory Notice Consent Provision For All DoD Information System User Agreements (Standard Agreement Training).

I have read and consent to the terms in the System Security Rules of Behavior (ROB)/Acceptable Use Policy (AUP) Training.

I have read and consent to the terms in the Privacy Rules of Behavior (ROB)/Acceptable Use Policy (AUP) Training.

I also agree to follow the standard agreement and these rules as a condition of being granted system access.

I understand that I may be subject to civil, criminal or administrative action for failure to follow the DoD Standard User Agreement, and the System Security and Privacy Rules of Behavior (ROB) / Acceptable Use Policy (AUP) applicable to me.

* Asterisk indicates required entry.

Signature Date

2013/07/16

DoD Component/Office *

DoD Component/Office and Signature
are required for Government Users.

I accept the System User Agreement and Rules of Behavior / Acceptable Use Policy. *

Signature

Previous

Help

Registration

User Authentication Type >> Data Capture >> User Agreement >> Registration Success

ERROR: DoD Component/Office is Mandatory.



STATEMENT OF ACCOUNTABILITY *

I understand my obligation to protect my password/certificate. I assume the responsibility for the data and system I am granted access to. I will not exceed my authorized access.

Government Users must enter the DoD Component/Office before signing the agreement. An Error message will be displayed if the DoDComponent/Office field is left blank.

Standard Mandatory Notice & Consent Provision For All DoD Information System User Agreements 9 May 2008

Security and Privacy Rules of Behavior (ROB) / Acceptable Use Policy (AUP) 14 Jan 2010

STANDARD MANDATORY NOTICE AND CONSENT PROVISION FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS (STANDARD AGREEMENT TRAINING)

You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government-authorized use only.

You consent to the following conditions:

The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counter-intelligence (CI) investigations.

At any time, the U.S. Government may inspect and seize data stored on this information system.

Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.

Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential as further explained below:

Nothing in the User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U. S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counter-intelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.

A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected

Registration

User Authentication Type >> Data Capture >> **User Agreement** >> Registration Success

(2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e) (4) of this section shall be guilty of a misdemeanor and fined not more than \$5,000.

(3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses may be found guilty in a court of law of a misdemeanor and fined not more than \$5,000.

User's Acknowledgement of this Agreement:

By signing, or otherwise acknowledging, this agreement, you acknowledge and consent that when you access Department of Defense (DoD) information systems you have:

Read and consent to the terms in the System Security Rules of Behavior (ROB) / Acceptable Use Policy (AUP) applicable to you.

Read and consent to the terms in the Privacy Rules of Behavior (ROB) / Acceptable Use Policy (AUP) applicable to you.

Agree to follow the rules described in this user agreement as a condition of being granted system access.

I understand that I may be subject to civil, criminal or administrative action for failure to follow the DoD Standard User Agreement, and the System Security and Privacy Rules of Behavior (ROB) / Acceptable Use Policy (AUP) applicable to me.

* Asterisk indicates required entry.

Signature Date

2013/09/26

Vendors are required to sign the agreement.

I accept the System User Agreement and Rules of Behavior / Acceptable Use Policy. *

Signature

[Previous](#)

[Help](#)

WAWF Password Confirmation

User ID	carla_test111
Password *	<input type="password"/>

Next, the User enters their password and clicks the "Next" button.

[Next](#)[Previous](#)[Help](#)

Wide Area Workflow

Home

Registration

User Authentication Type >> Data Capture >> **User Agreement** >> Registration Success

Printed output products must be properly labeled with "For Official Use Only" "Privacy Act of 1974, As amended." The policy for labeling output products containing Privacy Act information is in DoD 5200.1-R, Appendix 3, page 141 and DoD 5400.11-R, paragraph C1.4.

Place the standard Privacy Act warning label on the top of your computer monitor if names and social security numbers/personal bank account numbers, etc., are on your computer screen while you do your work. These labels can be generated on a plain white label that must read: "Personal Data, Privacy Act of 1974, as Amended, 5 U.S.C. 552a."

PII in DoD systems must be protected from unauthorized access especially when the system is in use and when the information is printed. The Privacy Act of 1974, As amended, 5 U.S.C. § 552a(i) also provides for criminal penalties.

(1) Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain personally identifiable information the disclosure of which is prohibited by this section or by rules or regulations established there under, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, may be found guilty in a court of law of a misdemeanor and fined not more than \$5,000.

(2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e) (4) of this section shall be guilty of a misdemeanor and fined not more than \$5,000.

(3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses may be found guilty in a court of law of a misdemeanor and fined not more than \$5,000.

If you have any questions or comments about the information presented here, please contact the Service Desk.

User's Acknowledgement of Standard Agreement, Security and Privacy Training

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

I have read and consent to the terms in the Standard Mandatory Notice Consent Provision For All DoD Information System User Agreements (Standard Agreement Training).

I have read and consent to the terms in the System Security Rules of Behavior (ROB)/Acceptable Use Policy (AUP) Training.

I have read and consent to the terms in the Privacy Rules of Behavior (ROB)/Acceptable Use Policy (AUP) Training.

I also agree to follow the standard agreement and these rules as a condition of being granted system access.

I understand that I may be subject to civil, criminal or administrative action for failure to follow the DoD Standard User Agreement, and the System Security and Privacy Rules of Behavior (ROB) / Acceptable Use Policy (AUP) applicable to me.

* Asterisk indicates required entry.

Signature Date

2013/07/16

DoD Component/Office

Air Force

I accept the System User Agreement and Rules of Behavior / Acceptable Use Policy.

John Doe

Register

Previous

Help

The "Register" button will be available once the User Agreement has been signed. The User must select this button to complete the registration process.

View & Accept Information System User Agreement

STATEMENT OF ACCOUNTABILITY *

I understand my obligation to protect my password/certificate. I assume the responsibility for the data and system I am granted access to. I will not exceed my authorized access.

Standard Mandatory Notice & Consent Provision For All DoD Information System User Agreements 9 May 2008

Security and Privacy Rules of Behavior (ROB) / Acceptable Use Policy (AUP) 14 Jan 2010

STANDARD MANDATORY NOTICE AND CONSENT PROVISION FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS

You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.

You consent to the following conditions:

When a user logs into WAWF with a CAC/Certificate/UserID and Password, the User Agreement page will be displayed if it has been a year or longer since the user has signed it.

The U.S. Government routinely intercepts and monitors communications for purposes including, but not limited to, penetration testing, communications security (COMSEC)

At any time, the U.S. Government may inspect and

Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.

Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

Nothing in the User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U. S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law

Cancel

Help

View & Accept Information System User Agreement

(1) Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain personally identifiable information the disclosure of which is prohibited by this section or by rules or regulations established there under, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, may be found guilty in a court of law of a misdemeanor and fined not more than \$5,000.

(2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e) (4) of this section shall be guilty of a misdemeanor and fined not more than \$5,000.

(3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses may be found guilty in a court of law of a misdemeanor and fined not more than \$5,000.

User's Acknowledgement of this Agreement:

By signing, or otherwise acknowledging, this agreement, you acknowledge and consent that when you access Department of Defense (DoD) information systems you have:

Read and consent to the terms in the System Security Rules of Behavior (ROB) / Acceptable Use Policy (AUP) applicable to you.

Read and consent to the terms in the Privacy Rules of Behavior (ROB) / Acceptable Use Policy (AUP) applicable to you.

Agree to follow the rules described in this user agreement as a condition of being granted system access.

I understand that I may be subject to civil, criminal or administrative action for failure to follow the DoD Standard User Agreement, and the System Security and Privacy Rules of Behavior (ROB) / Acceptable Use Policy (AUP) applicable to me.

* Asterisk indicates required entry.

Signature Date

2013/09/26

The user views and accepts the agreement by clicking the "Signature" button.

I accept the System User Agreement and Rules of Behavior / Acceptable Use Policy. *

Signature

Cancel

Help

View & Accept Information System User Agreement

User's Acknowledgement of Standard Agreement, Security and Privacy Training

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

I have read and consent to the terms in the Standard Mandatory Notice Consent Provision For All DoD Information System User Agreements (Standard Agreement Training).

I have read and consent to the terms in the System Security Rules of Behavior (ROB)/Acceptable Use Policy (AUP) Training.

I have read and consent to the terms in the Privacy Rules of Behavior (ROB)/Acceptable Use Policy (AUP) Training.

I also agree to follow the standard agreement and these rules as a condition of being granted system access.

I understand that I may be subject to civil, criminal or administrative action for failure to follow the DoD Standard User Agreement, and the System Security and Privacy Rules of Behavior (ROB) / Acceptable Use Policy (AUP) applica

* Asterisk indicates required entry.

Signature Date

2013/07/16

DoD Component/Office

Test

Select the "Submit" button to save the User Agreement and complete the logon process.

I accept the System User Agreement and Rules of Behavior / Acceptable Use Policy.

John Doe

Submit

Cancel

Help

[**Back to Final Changes**](#)

User Administration

- [User Information](#)
- [Reset Password](#)
- [Reset Certificate](#)

The SAM/GAM accesses the User Administration.

The "User Information" link is clicked.

User Information

Search For

Current Roles

UserId (case sensitive)

equal to

First Name

equal to

Last Name

equal to

Group Name

Location Code

equal to

Extension

equal to

Role

Email

equal to

Active Status

A UserId is entered in the Search field and the "Submit" button is clicked.

Search for user information. Data must be entered in at least one search field. Enter search data then click the 'Submit' link.

[Submit](#) [Return](#) [Reset](#)

User Information

Users Found: 3 User Status: CURRENT

Item	Userid	First Name	Last Name ▲	X509 Subject Name	Actions
1	cora_DLA_Energy				View Edit Roles
2	carlagov			CN=CACI.Tester4.9000040796,OU=CONTRACTOR,OU=PKI,OU=DoD,O=U.S.Government,C=US	View Edit Roles
3	cora_govt				View Edit Roles

10 [Resize](#)

3 items found, displaying 1 - 3.

[Return](#)

Click the "View" link to view the Signed Date for the User Agreement.

User Information - View

User ID

cora_DLA_Energy

First Name

Cora

Middle Name

Energy

Last Name

Leung

Suffix

XYZ

Email Address

coleung@caci.com

Commercial Phone

704-956-8426

DSN Phone

Extension

Intl Country Code and Phone

Mobile Phone

Title

DLA Energy

Organization

CACI

Rank/Grade

111a

Certificate Issuer

Certificate Valid From Date

Certificate Valid To Date

Certificate Subject

Archived Roles/DoDAACs

Attempted Logon Date

Locked Date

Last Access Date

Attempted Password Reset Date

The "User Agreement Signed Date" is displayed.

User Agreement Signed Date

EDI Attachment location path

2013-08-29 09:36:32

2013-08-28 17:38:07



Wide Area Workflow

System Messages

(2013-JUL-25) System: **All** Subject: **Posting Docs Action Required! Critical!** Message For: All Users

[Open folder.](#)

(2013-JUL-24) System: **All** Subject: **Test Action Required! Critical!** Message For: All Users

Testing v5.5.0 System Messages

(2013-JAN-17) System: **All** Subject: **This concludes the overview of ECP0728, Electronic User Agreement.**

Version:	5.5.0 Test BUILD02_8
Build Date:	09/24/2013
Application Server:	WebSphere 8.5.5.0
HTTP Server:	IBM IHS 8.5.5.0

Login



New User



Help / Training

