

WAWF Registration

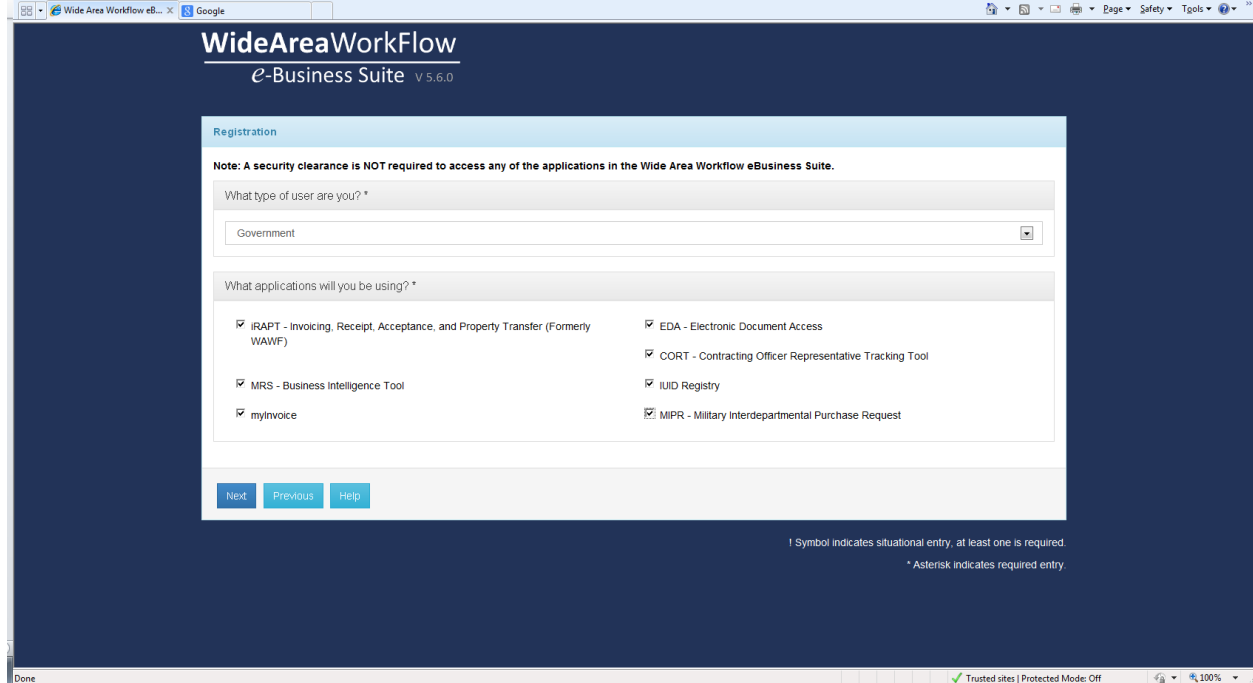
Go to <https://wawf.eb.mil/> and click on “Register”

The screenshot shows the WideAreaWorkflow e-Business Suite V 5.6.0 homepage. The header includes the logo and navigation links. The main content area features a 'Certificate Login' section, a 'User ID Login' section with fields for 'User ID' and 'Password', and a 'System Messages' section. A red box highlights the 'Register' button in the top right corner. Below the login sections, there are logos for various systems (iRAPT, EDA, mytwice, IUID, CORT TOOL, eMIPR, MRS) and a 'Quick Links' section with links to 'Security and Privacy', 'Accessibility', 'Government Customer Support', and 'Vendor Customer Support'. The 'Getting Started Help' section includes links for 'Machine Setup', 'Vendors Getting Started', 'Government Users Getting Started', and 'Government Contractor Users Getting Started'. The 'iRAPT Mobile' section provides links to the 'Apple App Store', 'Google Play', and 'Blackberry'.

Read and agree to terms and conditions, click “Agree”

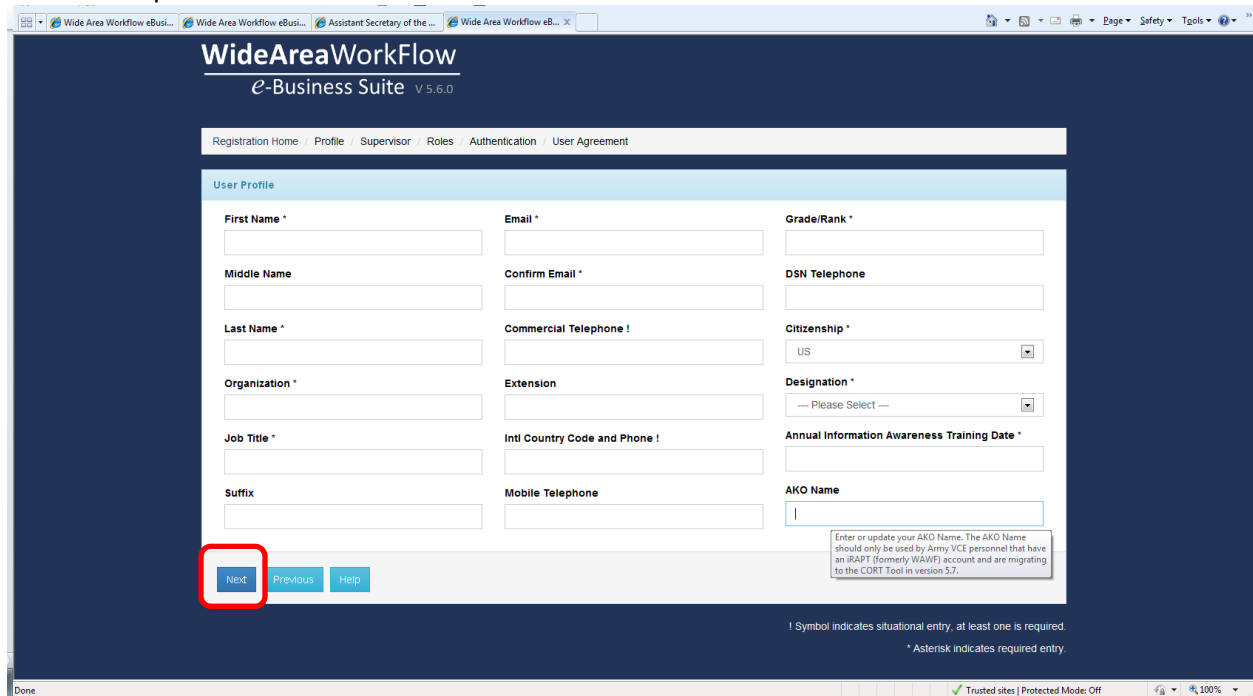
The screenshot shows the WideAreaWorkflow e-Business Suite V 5.6.0 Privacy Act Statement page. The page displays the 'Privacy Act Statement' with sections for 'AUTHORITY', 'PRINCIPAL PURPOSE', 'ROUTINE USES', and 'DISCLOSURE'. Below the statement, there is a checkbox labeled 'I have read and understand the terms and conditions for use of this website.' and an 'Agree' button, which is highlighted with a red box. At the bottom right, there are footnotes: '† Symbol indicates situational entry, at least one is required.' and '* Asterisk indicates required entry.'

Select user type (Government, Government Support Contractor, or Vendor) and select module(s) to register for, click “Next”



The screenshot shows the 'Registration' page of the WideAreaWorkFlow e-Business Suite (V 5.6.0). The page has a dark blue header with the logo and version. Below the header, a light blue box contains the title 'Registration'. A note states: 'Note: A security clearance is NOT required to access any of the applications in the Wide Area Workflow eBusiness Suite.' The main form area is white and contains two sections. The first section, 'What type of user are you? *', has a dropdown menu with 'Government' selected. The second section, 'What applications will you be using? *', contains two columns of checkboxes. The first column has: 'IRAPT - Invoicing, Receipt, Acceptance, and Property Transfer (Formerly WAWF)' (checked), 'MRS - Business Intelligence Tool' (checked), and 'myInvoice' (checked). The second column has: 'EDA - Electronic Document Access' (checked), 'CORT - Contracting Officer Representative Tracking Tool' (checked), 'IUID Registry' (checked), and 'MIPR - Military Interdepartmental Purchase Request' (checked). At the bottom of the form are three buttons: 'Next' (highlighted in blue), 'Previous', and 'Help'. Below the form, there are two footnotes: '† Symbol indicates situational entry, at least one is required.' and '* Asterisk indicates required entry.'

Fill out user profile and click “Next”



The screenshot shows the 'User Profile' page of the WideAreaWorkFlow e-Business Suite (V 5.6.0). The page has a dark blue header with the logo and version. Below the header, a light blue box contains the title 'User Profile'. A breadcrumb trail at the top reads: 'Registration Home / Profile / Supervisor / Roles / Authentication / User Agreement'. The main form area is white and contains a grid of input fields. The fields are: 'First Name *', 'Middle Name', 'Last Name *', 'Organization *', 'Job Title *', 'Suffix', 'Email *', 'Confirm Email *', 'Commercial Telephone !', 'Extension', 'Intl Country Code and Phone !', 'Mobile Telephone', 'Grade/Rank *', 'DSN Telephone', 'Citizenship *' (with a dropdown menu showing 'US'), 'Designation *' (with a dropdown menu showing '--- Please Select ---'), 'Annual Information Awareness Training Date *', and 'AKO Name'. At the bottom of the form are three buttons: 'Next' (highlighted in blue and circled in red), 'Previous', and 'Help'. A tooltip box is visible over the 'AKO Name' field, containing the text: 'Enter or update your AKO Name. The AKO Name should only be used by Army VCE personnel that have an IRAPT (formerly WAWF) account and are migrating to the CORT Tool in version 5.7.' Below the form, there are two footnotes: '† Symbol indicates situational entry, at least one is required.' and '* Asterisk indicates required entry.'

Fill out supervisor information and click “Next”

Note: An email will be sent to the provided supervisor email address, please ensure that it is correct

The screenshot shows the 'WideAreaWorkflow e-Business Suite' registration page. The navigation bar includes 'Registration Home', 'Profile', 'Supervisor', 'Roles', 'Authentication', and 'User Agreement'. The 'Supervisor' section is active, displaying 'Additional Profile Information'. This section is divided into two parts: 'Supervisor Information' and 'Agency Information'. The 'Supervisor Information' part contains fields for First Name, Last Name, Job Title, Email, Confirm Email, DSN Telephone, Phone, Extension, and Intl Country Code and Phone. The 'Agency Information' part contains fields for Agency Name, Address, City, State, Zip, Country, Organization, and Office Symbol. The browser's address bar shows the URL 'Wide Area Workflow eBusi...' and the status bar indicates 'Trusted sites | Protected Mode: Off'.

Supervisor Information		
First Name *	Email *	Phone !
<input type="text"/>	<input type="text"/>	<input type="text"/>
Last Name *	Confirm Email *	Extension
<input type="text"/>	<input type="text"/>	<input type="text"/>
Job Title *	DSN Telephone	Intl Country Code and Phone !
<input type="text"/>	<input type="text"/>	<input type="text"/>

Agency Information		
Agency Name *	City *	Country *
<input type="text"/>	<input type="text"/>	<input type="text"/>
Address *	State *	Organization
<input type="text"/>	<input type="text"/>	<input type="text"/>
	Zip *	Office Symbol
	<input type="text"/>	<input type="text"/>

Select Role(s)

The screenshot shows the 'WideAreaWorkflow e-Business Suite' registration page, specifically the 'Roles' section. The navigation bar is the same as the previous screenshot. The 'Roles' section is active, displaying a list of roles with expandable options. The roles listed are: IRAPT, Government User Roles, Admin User Roles, COR Tracking Tool, CORT Role, Electronic Document Access, EDA Role, UID Registry, Government User Roles, Admin User Roles, Management Reporting System, MRS Role, and Military Interdepartmental Purchase Request. The browser's address bar shows the URL 'Wide Area Workflow eBusi...' and the status bar indicates 'Trusted sites | Protected Mode: Off'.

Roles	
IRAPT	
+ Government User Roles	+ Admin User Roles
COR Tracking Tool	
+ CORT Role	
Electronic Document Access	
+ EDA Role	
UID Registry	
+ Government User Roles	+ Admin User Roles
Management Reporting System	
+ MRS Role	
Military Interdepartmental Purchase Request	
+ Government User Roles	+ Admin User Roles

Enter additional information for appropriate role(s), click “Save”

WideAreaWorkflow
e-Business Suite V 5.6.0

Registration Home / Profile / Supervisor / Roles / Authentication / User Agreement

CORT Role

Role *
--- Please Select ---

Location Code Type *
DoDAAC

Home Organization *
[Text Field]

Home Department *
--- Please Select ---

Justification
[Text Field]

Attachments
Browse Upload

Save Cancel Help

! Symbol indicates situational entry, at least one is required.
* Asterisk indicates required entry.

Add any additional role, if applicable, and click “Next” when finished

COR Tracking Tool

+ CORT Role

Role	Home Organization	Home Department	Action
Contracting Officer Representative	N48142	MDA	Justification/Attachments Delete

Electronic Document Access

+ EDA Role

IUID Registry

+ Government User Roles + Admin User Roles

Management Reporting System

+ MRS Role

Military Interdepartmental Purchase Request

+ Government User Roles + Admin User Roles

myInvoice

Government - Selected

Next Previous Help

Select access method (most users should be “Common Access Card”), click “Certificate Login”

WideAreaWorkflow
e-Business Suite V 5.6.0

Registration Home / Profile / Supervisor / Roles / Authentication / User Agreement

Authentication

How will you be accessing the Wide Area Workflow eBusiness Suite applications? *

Common Access Card

Please click on the Certificate Login button to select the appropriate certificate.

Certificate Login

Previous Help

! Symbol indicates situational entry, at least one is required.
* Asterisk indicates required entry.

Select certificate, enter PIN which will take the user to the statement of accountability, go to the bottom of the page

WideAreaWorkflow
e-Business Suite V 5.6.0

Registration Home / Profile / Supervisor / Roles / Authentication / 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.

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

Enter organization and click “Signature”

Pill 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

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.

Signature Date

2014/11/10

Government Organization *

[I accept the System User Agreement and Rules of Behavior / Acceptable Use Policy.](#)

Signature

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

! Symbol indicates situational entry, at least one is required.
* Asterisk indicates required entry.

Select certificate and receive a success message

WideAreaWorkflow
e-Business Suite V 5.6.0

Successful Registration

You have successfully registered for the following applications. You will receive an e-mail containing your User ID.

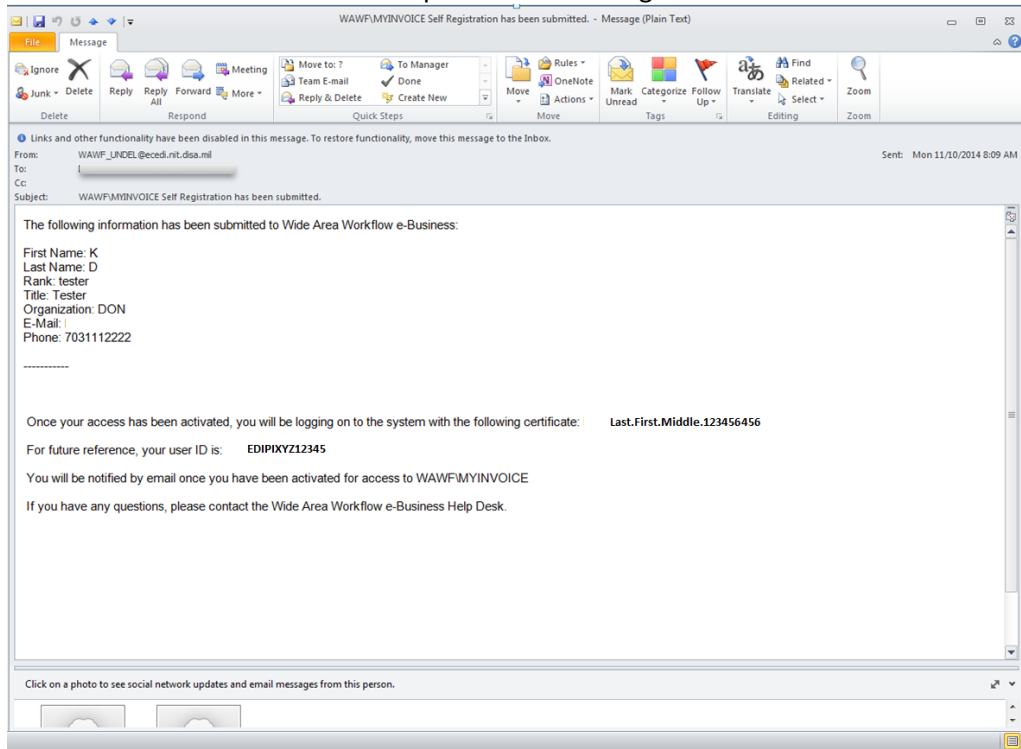
- iRAPT - Invoicing, Receipt, Acceptance, and Property Transfer (Formerly WAWF)
- myInvoice

The approval request will go to your Supervisor/Sponsor.
Once you have been approved by your Supervisor/Sponsor, the approval request will go to an administrator.
Once you have been activated by an administrator, you will receive another email notifying you of the role(s) for which you have been activated.
You may log into Wide Area Workflow e-Business Suite to check the status of your request or make changes to your profile information.
If you have any questions, please contact the Customer Support.

[Home](#) [Help](#)

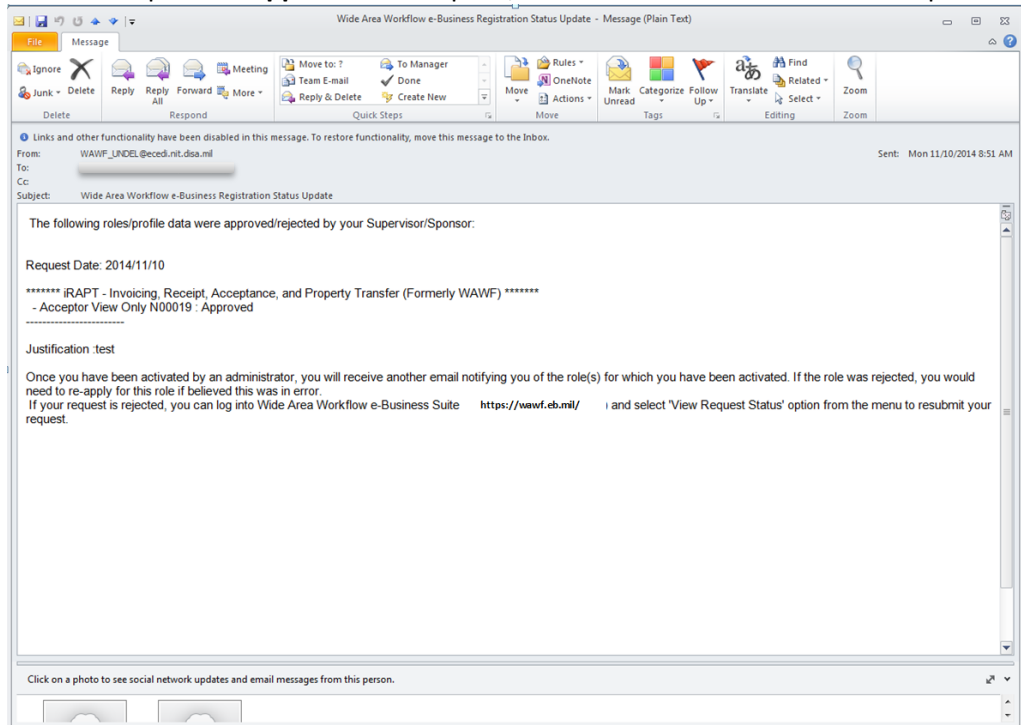
An email approval request will be sent to the supervisor.

The user receives an email status update after self-registration

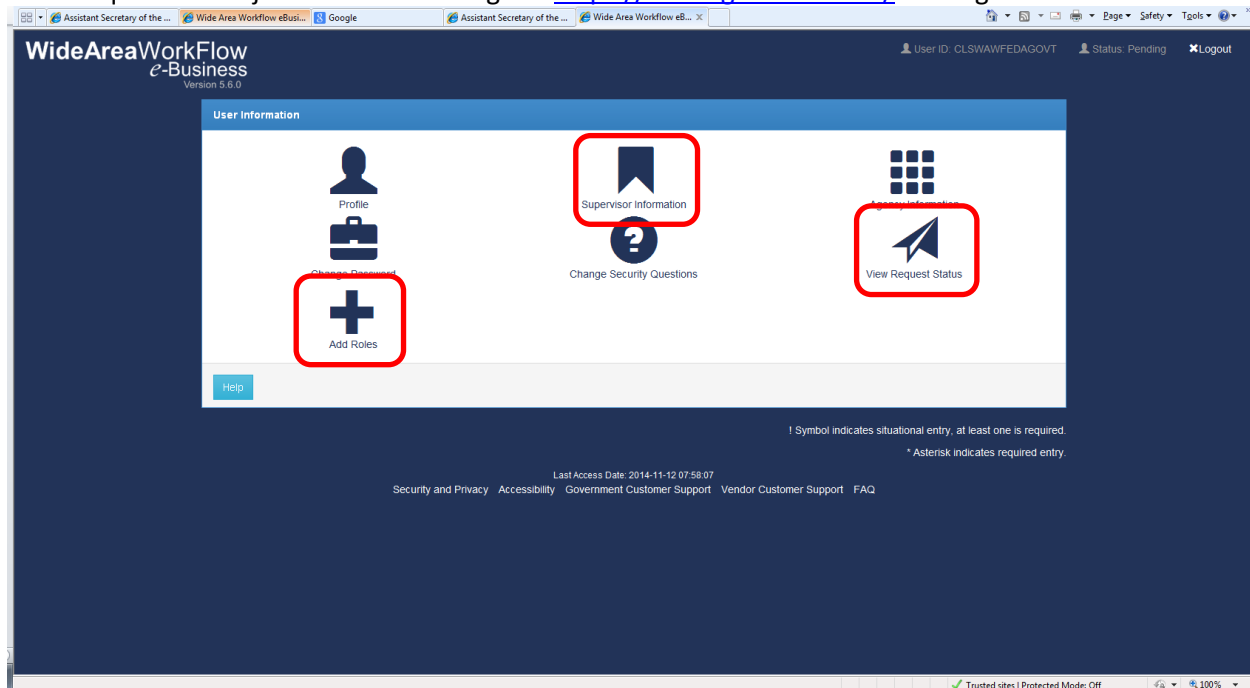


Supervisor Approves

After the supervisor **approves** the request, the user receives another status update email



If the request was rejected the user can go to <https://wawf-gt.nit.disa.mil/> and log on



View Request Status: New users who were originally rejected can log in as a pending user and add justification comments and resubmit their original access request to their supervisor.

REVIEW_REQUIRED: Supervisor needs to approve/reject electronic DD2875

APPROVER_REJECTED: User can add a justification and resubmit request or self-register for a different role, if necessary

APPROVER_ACPTED: Supervisor approved DD2875 and now the Group Administrator (GAM) needs to activate the account

ACTIVE: User role is active

Add Roles: To completely change their access request the user will need log into the pending page and click the Add Roles icon. A new request will need to be submitted.

Supervisor Information: The user also sees the option to change their supervisor info and resubmit their access request to the correct supervisor, if needed.

After role activation by the GAM, the user will receive a status update email.