

Job Aid: NISP Contract Classification System (NCCS)

Using this job aid



This job aid provides background information on the National Industrial Security Program (NISP) Contract Classification System (NCCS). Sections of the job aid cover user roles, the General Account Manager/Client Account Manager (GAM/CAM) determination, and NCCS technical requirements and access registration.

Table of Contents

Overview	1
NCCS User Roles.....	2
Government Account Managers (GAMs)/Contractor Account Managers (CAMs)	3
NCCS Technical Requirements	5
NCCS Access Registration	7

Overview

What is NCCS?

The National Industrial Security Program (NISP) Contract Classification System (NCCS) is an online system that allows government and contractor security offices or organizations to create an electronic equivalent of the DD Form 254, and route it between offices. Wide Area Workflow (WAWF) e-Business Suite has provided the ability for users to populate data onto DD Form 254 on the web.

NCCS interfaces with the System for Award Management (SAM), which the Federal Acquisition Regulation (FAR) requires that all prime contractors use. NCCS also uses the Defense Logistics Agency's (DLA's) CAGE Search & Inquiry (CSI) to register CAGE Codes, the Actual Performance Location, and subcontractor/tier DD Form 254s.

**Note: WAWF uses the term "vendor" for contractors.*

NCCS User Roles



There are several NCCS user roles that allow access to different system features.

For more information on NCCS user roles see: <https://wawfraid.nit.disa.mil/nccswbt/xhtml/wbt/nccs/nccs.xhtml>

Role	Access
Originator	This access allows Vendors/Contractors, Government Support Contractors, and Government users to Initiate, Save, Recall, Resubmit and Void the DD254 depending on the status. Vendors may create Subcontracts, Tier 1, Tier 2 and Tier 3. Government users may create Prime and Solicitations.
Reviewer	This access allows Vendors/Contractors, Government Support Contractors, and Government users to Recommend Certification, Reject, Hold or Recall the DD254 depending on the status.
Certifying Official	This access allows Vendors/Contractors and Government users to Certify, Reject, Hold or Recall the DD254 depending on the status.
Contracting Officer	This access allows Government and Government Support Contractors to perform an acceptance review of an NCCS Request for Approval to Subcontract document.
Government Account Manager (GAM)/ Contractor Account Manager (CAM)	This access allows selected Vendors/Contractors and Government users to administer the Groups, Users, and Roles for the NCCS location codes and users. <i>Note: NCCS will allow Vendors/Contractors to establish CAMs for their CAGE Codes.</i> For more information about GAMs/CAMs see section on Government Account Manager (GAM) and Contractor Account Manager (CAM) Determination.

Government Account Managers (GAMs)/Contractor Account Managers (CAMs)



The Government Account Manager (GAM) or Contractor Account Manager (CAM) enables and disables user access and authorization and approves other user roles for the organization.

For more information on GAM/CAMs see the [GAM/CAM Role Information PDF](#).

Organizational Hierarchy

The users of the WAWF e-Business Suite are broken down into groups on seven levels. Each group is administered by one or more GAM/CAMs.

- The GAM/CAM can edit user profile information for two levels: their own level and the level below their level
- The GAM/CAM has view-only access to user information for all other levels below their current level

Based on the size of the company or agency there may be tiered hierarchy GAM/CAM levels, similar to JPAS or e-QIP. The GAM/CAM role should be based on the company or agency structure and there can be sub-group GAM/CAMs for divisions and/or branches of a company or agency. The top GAM/CAM will oversee all subgroups, but the subgroup GAM/CAM will manage only their own users and DD Form 254s.

GAM/CAM Administrative Abilities

The GAM/CAM has eight major administrative abilities in WAWF e-Business Suite:

1. Manage Group Structure
2. Administer Location Codes
3. Look up group names and GAM/CAM information
4. View and edit User Profile Information
5. Activate (add) and deactivate users
6. Use Activation Reports
7. Reset user passwords
8. Reset certificates

*GAM/CAM
Selection and
Appointment*

A GAM/CAM must be selected before other user roles can be approved

- There should be a primary GAM/CAM and an alternate GAM/CAM
- Smaller companies can use a consultant as the alternate GAM/CAM

Typically, a GAM/CAM is appointed from among security-type individuals in an organization, but a GAM/CAM can also have other NCCS user roles including the role of Originator, Reviewer and/or Certifying Official depending upon organizational business practices.

The Supervisor/Authorizing Official (AO) provides a written statement for GAM/CAMs appointed for a particular DODAAC or CAGE Code. The GAM/CAM must sign the letter, acknowledging the responsibilities.

See attached copies of the [GAM Appointment Letter](#) and [CAM Appointment Letter](#) for details.

NCCS Technical Requirements



This section describes technical requirements for NCCS. For technical support, contact the DLA/DISA Help Desk:

CONUS ONLY: 1-866-618-5988

COMMERCIAL: 801-605-7095

DSN: 388-7095

FAX COMMERCIAL: 801-605-7453

FAX DSN: 388-7453

Email: disa.ogden.esd.mbx.cscassig@mail.mil

Minimum Hardware Requirements

- 233 MHz or more Pentium microprocessor (or equivalent)
- SVGA Color Monitor (minimum 256 color)
- 64 MB RAM (minimum)
- Internet Access (broadband recommended)

Minimum Software Requirements

- Operating System
 - Windows XP SP3+
 - Windows Vista SP1+ (32-bit and 64-bit OS, all versions)
 - Windows 7 Professional (32-bit and 64-bit OS, all versions)
 - Windows 8 Professional (32-bit and 64-bit OS, all versions)
- Internet Browser
 - Internet Explorer (128 bit or higher) Version 9.0 or later is recommended

For more information on configuring your machine to use Wide Area Workflow eBusiness Suite visit:

<https://wawf.eb.mil/xhtml/unauth/web/homepage/machineSetup.xhtml>

NOTE: If any software is required for installation/updating to become compliant with WAWF eBusiness Suite minimum requirements, you MUST have authorization/permission to load/install software on your local machine. If you do NOT have these permissions, contact your local network support personnel to assist you.

*Registration
Requirements*

- CAC/PKI cards and soft certificates are mandatory for all NCCS users to register and log in
- Registration for an NCCS account is based on Location Code. Location Code types vary:
 - Vendors/contractors: Use CAGE Code
 - Government (DoD): Use Department of Defense Activity Address Code (DoDAAC)
 - Government (non-DoD Agency): Use Agency Codes for non-DoD agencies.

For additional CAC/PKI troubleshooting see “CAC Help?” on the Login page:

<https://wawf.eb.mil/xhtml/unauth/web/homepage/cacSupport.xhtml>

NCCS Access Registration



This section provides step-by-step instructions for NCCS registration. Note that some steps may be different for industry and government/embedded contractor users.

Step 1: Access WAWF

- Go to <https://wawf.eb.mil/>
- Review the terms and conditions notification; Select “Accept” to proceed
- Select “Register”
- Review the privacy act statement; Select “Accept” to proceed

Step 2: Select NCCS

Industry/Vendors

- Select “Vendor” as the User Type
- Select “NCCS – NISP Contracts Classification System” as the Application Type; Select “Next”

Government or Embedded Contractors:

- Select “Government” or “Government Support Contractor”(embedded contractors) as the User Type
- Select “NCCS – NISP Contracts Classification System” as the Application Type; Select “Next”

Step 3: Complete User and Sponsor/ Supervisor Profiles

- Complete the required user profile Information. The blocks with an “*” are required fields; Select “Next”
 - *Note: the email you use for the User profile will be the notification email. If there will be multiple people who need to be notified, you may want to use a generic office email.*
- Complete the required Sponsor/Supervisor profile Information; Select “Next”
- *Note: For Industry/Vendors, this can be your supervisor information*

*Step 4a:
Select Roles
(GAM/CAM)*

The GAM/CAM role must be established before other user roles can be added. Contact DSS.NCCS@mail.mil to get the GAM/CAM role approved.

Note: DSS will only approve the GAM/CAM role (and no other user roles), unless the GAM/CAM will also have user roles. The GAM/CAM should approve their other sub-GAM/CAMs and other user roles.

Industry/Vendors

- Find the NISP Contract Classification System in the block of systems
- Select “Vendor Admin Roles”
- Enter valid CAGE Code as a Location Code
 - If you have multiple CAGE Codes, contact DSS.NCCS@mail.mil to set up a company group. You will register as a Group Name instead of the CAGE Code.
- Upload the GAM/CAM Approval Letter:
- Provide a justification why need the GAM/CAM account (short)
- Select “Save”; Select “Next”

Government or Embedded Contractors:

- Find the NISP Contract Classification System in the block of systems
- Select “Government Admin Roles”
- DoD users: Enter DoDAAC/Non-DoD users: Enter an Agency Code as a Location Code
- Upload the GAM/CAM Approval Letter
- Provide a justification why need the GAM/CAM account (short)
- Select “Save”; Select “Next”

*Step 4b:
Select Roles
(Users)*

Industry/Vendors

- Find the NISP Contract Classification System in the block of systems
- Select “Vendor User Roles” for the Originator, Reviewer, or Certifying Official roles
- Enter valid CAGE Code as a Location Code
- Select “Save”; Select “Next”

Government or Embedded Contractors:

- Find the NISP Contract Classification System in the block of systems
- Select “Government User Roles” for the Originator, Reviewer, Certifying Official, or Government Contract Office roles
- DoD users: Enter DoDAAC/Non-DoD users: Enter an Agency Code as a Location Code
- Select “Save”; Select “Next”

*Step 5:
Authenticate
Roles*

NCCS requires CAC/PKI/Soft Certificate authentication only; no ID/Passwords are allowed for the production site.

- Select “User CAC/PKI/Soft Certificate” as your authentication type; Select “Next”
- Select your certificate and/or pin information and select “Ok”; Select “Submit”