



**NIRIS WORKGROUP**

**SOP Name: Obtaining NIRIS Access**

**Functional Area: Information Management**

**Sub-Area: Security and System Access**

SOP Date: January 11, 2008	Version: 2.0 Updated July 29, 2013	Authority: NIRIS Workgroup
-------------------------------	---------------------------------------	----------------------------

**Acronyms:**

CAC – Common Access Card

CADD – Computer Aided Design and Drafting

CERCLA – Comprehensive Environmental Response, Compensation, and Liability Act

CIP – Critical Infrastructure Protection

DEERS – Defense Enrollment and Eligibility Reporting System

DoD – Department of Defense

ECA – External Certification Authority

ER – Environmental Restoration

GIS – Geographic Information System

IA – Information Assurance

IASE – Information Assurance Support Environment



## NIRIS WORKGROUP

IR – Installation Restoration

NAVFAC – Naval Facilities Engineering Command

NIRIS – Naval Installation Restoration Information Solution

PII – Personally Identifiable Information

PKI – Public Key Infrastructure

RAPIDS – Real-Time Automated Personnel Identification System

RDM – Regional Database Manager

RPM – Remedial Project Manager

SAAR – System Authorization Access Request

SADA – Spatial Analysis and Decision Assistance

SDS – Spatial Data Standards

SOP – Standard Operating Procedure

SSO – Single Sign-On

URL – Universal Resource Locator

## **Purpose:**

This Standard Operating Procedure (SOP) specifies the procedures required to obtain system access to the Naval Installation Restoration Information Solution (NIRIS). NIRIS is a secure web-based application implemented to ensure continuity for the Environmental Restoration (ER) program. NIRIS provides users with desk-top access to information, and tools designed to collect and preserve data to meet Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA) requirements. Navy employees, environmental regulators, and government contractors whose jobs require recurring access to and compilation of environmental data may be eligible to become NIRIS users.



## NIRIS WORKGROUP

NIRIS was designed to standardize information and is compliant with the Computer Aided Design and Drafting (CADD)/ Geographic Information System (GIS) Technology Center's Spatial Data Standards (SDS) as required by Naval Facilities Engineering Command (NAVFAC) policy. The system provides software modules used to load, verify, and update data; query and report on the data; view the data using GIS tools; store electronic documents pertaining to the business line; and manage controls and inspections on land parcels during and after restoration. Data are presented in a controlled manner based on roles and user association with particular installations.

### **Scope:**

The scope of this SOP is to provide descriptive information and basic instructions for new users to complete the NIRIS registration process. To become a provisioned NIRIS user, new users must:

- Acquire a Department of Defense (DoD) Public Key Infrastructure (PKI) Medium Assurance Token Certificate (SmartCard)
- Complete DoD Cyber Awareness Challenge Training
- Obtain a NAVFAC Portal Account
- Request NIRIS Access



## NIRIS WORKGROUP

### **Procedure:**

#### Acquire DoD PKI Software Certificate

NIRIS is hosted on a DoD Private Web server which has been enabled to support user identification and authentication using a DoD PKI Token Certificate. To comply with DoD mandates, the site is restricted to only allow access to users that authenticate with a DoD PKI Token Certificate (SmartCard).

A Common Access Card (CAC) is not necessary to access NIRIS. CACs are available for DoD personnel and/or contractors only if their government sponsor deems it necessary. Contact your government sponsor (or NIRIS representative) with any questions regarding CACs.

A SmartCard reader and middleware are required for your Operating System to access the CAC or Medium Assurance Token PKI Certificates. A card reader is typically provided when you purchase a Token Certificate.

The DoD has established the External Certification Authority (ECA) program to support the issuance of DoD-approved certificates to industry partners and other external entities and organizations. The ECA program is designed to provide the mechanism for these entities to securely communicate with the DoD and authenticate to DoD Information Systems.

To purchase a DoD PKI Medium Assurance Token Certificate, visit the following Information Assurance Support Environment (IASE) site: <http://iase.disa.mil/pki/eca/> to see the list of approved ECA vendors. The requirements from each ECA vendor may vary slightly as well as the installation requirements. Contact the vendor directly regarding any issues installing the middleware and/or SmartCard reader.



## NIRIS WORKGROUP

### Complete DoD Cyber Awareness Challenge Training

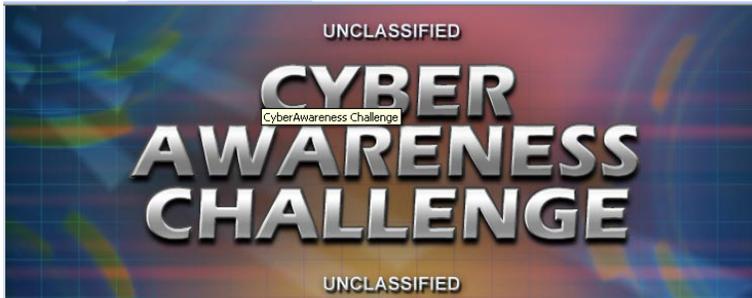
After obtaining a DoD PKI Medium Assurance Token Certificate, users are required to complete DoD Cyber Awareness Challenge Training. The training course can be completed by accessing the Internet and entering the Universal Resource Locator (URL):

<http://iase.disa.mil/eta/cyberchallenge/launchPage.htm>

This web-based Cyber Awareness Training provides expanded modules and topics to reflect the constantly changing world of information assurance as it relates to information technology. The user is introduced to the principles of Information Assurance, its evolution, IA-related policies and laws, and Critical Infrastructure Protection (CIP). The training explains the differences between threats and vulnerabilities and provides information regarding the insider threat, social engineering, and peer-to-peer applications. The user is presented with the concept of Malicious Code, including its impacts and the methods it uses to infect information systems. Important guidelines for ensuring a secure system, defining classification levels for DoD information, to include Personally Identifiable Information (PII), and outlining your role as a user in protecting this information is also provided. The course also introduces the threats associated with identity theft, spyware, and phishing and how you can protect yourself, as well as providing security tips to practice in your daily routine to increase your home computer security.



## NIRIS WORKGROUP



### Department of Defense Employees

[Launch New CyberAwareness Challenge Department of Defense Version](#)

[Continue Current CyberAwareness Challenge Department of Defense Version](#)

### Federal Employees

[Launch New CyberAwareness Challenge Federal Version](#)

[Continue Current CyberAwareness Challenge Federal Version](#)

**Product Functionality Caution:** To meet technical functionality requirements, this awareness product was developed to function with Windows operating systems (Windows 7, VISTA, and XP, when configured correctly) using either the Internet Explorer (IE) or Firefox browsers. Users employing another OS or browser may experience difficulties and may not be able to complete the training or print the certificate of completion. If you have questions regarding this requirement, please contact the [IASE Helpdesk](#).

Click on “Launch New CyberAwareness Challenge Department of Defense Version” to begin the course. Then follow the on-screen prompts to proceed through the learning modules.

At the end of the last module, click on the forward arrow again to get the certificate window to appear enter your name and print certificate. After the certificate is printed, click on the Exit button at the bottom of the screen. A digital copy should be sent to the NAVFAC Remedial Project Manager or NIRIS Workgroup representative who will process notification of the completion to the appropriate NAVFAC authorities.

### Note:

It is a DoD requirement that IA Training be completed on an annual basis.



## NIRIS WORKGROUP

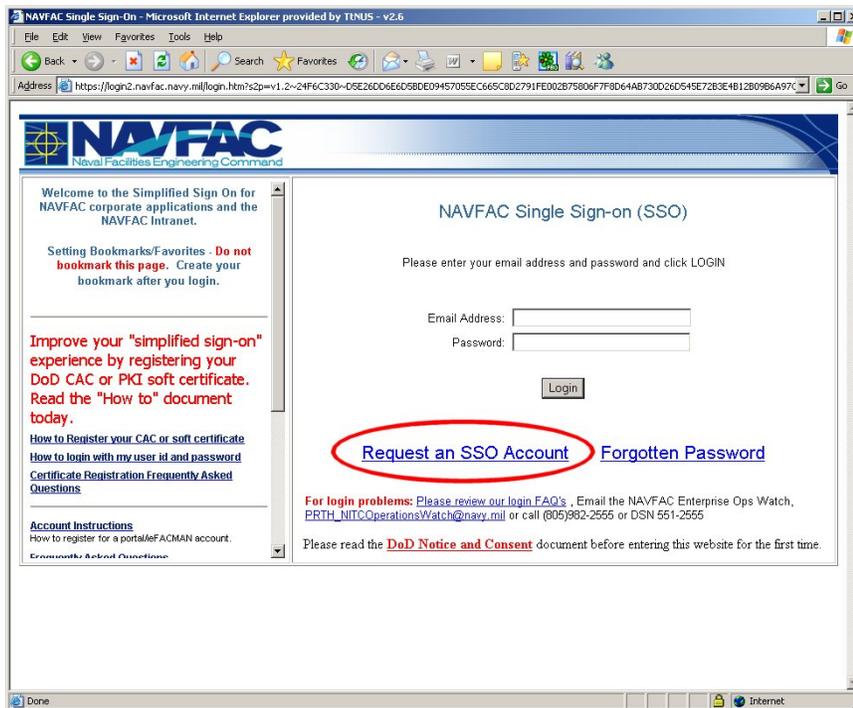
Obtain a NAVFAC Portal Account

Next users must register for a NAVFAC Single Sign-On (SSO). Registering and receiving a password for NAVFAC SSO does not give one access rights to NIRIS applications. Users must first register and receive their password and then follow the process described later in this document.

Anyone with a CAC card or DoD PKI Medium Assurance Token Certificate and a sponsor will be able to sign on to the NAVFAC Private Portal. If your affiliation is NAVFAC or "Other", your sponsor must be a NAVFAC associate. Your sponsor must have an active SSO account, because the sponsor will need to log in to SSO to approve your account.

Users can request an SSO by visiting the URL: <https://portal.navy.mil/private>.

The steps below walk you through what to do upon initial login to the system. When you first access the environment, click on the Request a Password/Account link, circled in red on the screen capture below.





## NIRIS WORKGROUP

The New SSO User Registration form must be completed and submitted as shown below. Fill in your information for validation purposes. A (\*) indicates required field. Enter all required fields and click on the Submit Registration button.

The screenshot shows a web browser window titled "New User Registration - Microsoft Internet Explorer provided by TINUS - v2.6". The address bar shows the URL: [https://portal.navfac.navy.mil/pls/portal/PORtal\\_vma\\_app\\_module.show?p\\_sessionid=2767150p\\_header=false](https://portal.navfac.navy.mil/pls/portal/PORtal_vma_app_module.show?p_sessionid=2767150p_header=false). The page header features the NAVFAC logo and the text "Naval Facilities Engineering Command".

The main heading is "New SSO User Registration". Below it, a message states: "Information collected on this page is required for Self Service registration to the NAVFAC Corporate Portal and supported applications. If you've forgotten your password, please go to the [Forgotten Password](#) Page for assistance."

The registration form contains the following fields and options:

- \* First Name: Text input field
- Middle Initial: Text input field
- \* Last Name: Text input field
- \* E-mail address: Text input field with a note: "Please use your military e-mail address whenever possible. (i.e. your.name@navy.mil)"
- \* Confirm E-mail address: Text input field
- \* Affiliation: Dropdown menu (selected: NAVFAC)
- \* Component: Dropdown menu (selected: NAVFAC ATLANTIC)
- \* Type: Dropdown menu (selected: Military)
- \* Password: Text input field with a note: "Passwords must be a minimum of 8 characters, with at least one upper case letter, one lower case letter, and one number."
- \* Verify Password: Text input field

At the bottom of the form, there are two buttons: "Submit Registration" (circled in red) and "Clear Registration". A note below the buttons says: "(\*) Asterisks indicate required fields".

At the bottom left of the page, there is a link: "Please read our [Privacy Page](#)".

All users **must** provide a sponsor to create an account. NAVFAC military and civilian employees may sponsor accounts for NAVFAC, contractors, and other employees. Complete the form and select Submit Sponsor.



## NIRIS WORKGROUP

Sponsor Information - Microsoft Internet Explorer provided by TNMS - v2.6

Address: [https://portal.navy.mil/private/portal/PORTAL\\_vvva\\_app\\_mod/le\\_show/p\\_sessionid=2767168p\\_header=false](https://portal.navy.mil/private/portal/PORTAL_vvva_app_mod/le_show/p_sessionid=2767168p_header=false)

**Sponsor Information**

Sorry, Mike, but we are unable to complete the self-registration process with your supplied credentials. You may hit the back button to correct any errors and try again. Alternatively, you may fill in the following information and we will manually verify your right to access.

\* Sponsor First and Last Name

\* Sponsor E-mail Address

\* Registrant Phone Number

\* Comments (reason for requesting access)

\* Asterisks indicate required fields

Users will then receive two subsequent emails, the first email will indicate that the request has been forwarded to the appropriate authorities for approval, and a second will indicate that the user's request for a portal account has been approved by the sponsor.

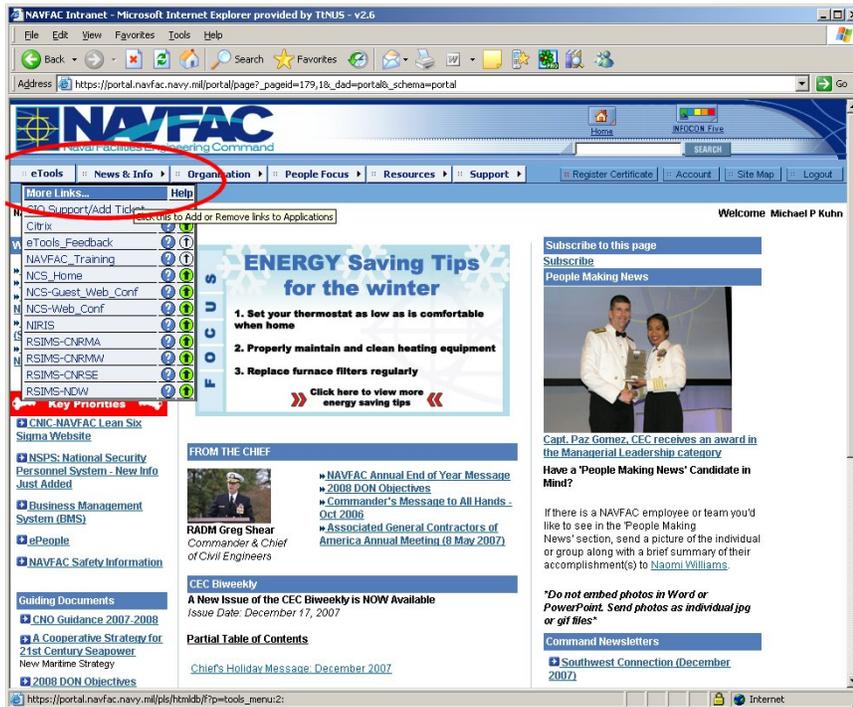
## Request NIRIS Access

To request access to NIRIS applications, the user must have completed their registration to NAVFAC's SSO and must have a User ID (email address) and assigned password. To start, go to the Internet and enter the URL <https://portal.navy.mil/private>. Log in by entering your User ID or PKI-enabled login.

After logging into the system, the NAVFAC Private Portal is displayed. Pan over the eTools button on the upper left corner of the screen.



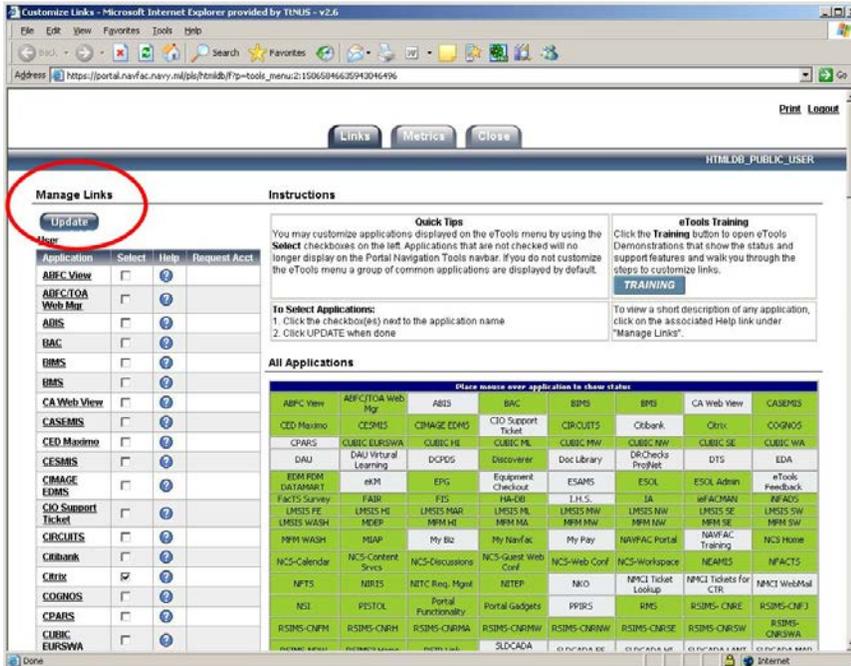
## NIRIS WORKGROUP



NAVFAC Private Portal eTools provides access to applications and links to applications that can be customized to suit your needs. Selecting the eTools menu displays the default applications. Additional information on eTools can be accessed through the Help menu that provides narrated demonstrations of eTools functionality.

From the eTools menu select More Links. The Manage Links window opens and on the left you will see the list of applications. Users may customize the applications that are displayed on the eTools menu by using the Select checkboxes on the left. Applications that are checked will be displayed on the eTools menu, and those not checked will no longer be displayed. Users may personalize the eTools menu at any time to reflect their changing work needs.

## NIRIS WORKGROUP



## NIRIS Provisioning Wizard

To access the NIRIS provisioning wizard, locate NIRIS from the list of applications on the Manage Links screen and select Acct Request. After clicking on the link, the NIRIS provisioning wizard window opens and the user profile screen is displayed.

The wizard will now walk you through the process to obtain the correct NIRIS access according to your role. All NIRIS access requests are routed for approval before activation and notifications will be delivered to your NAVFAC account email address. The steps are:

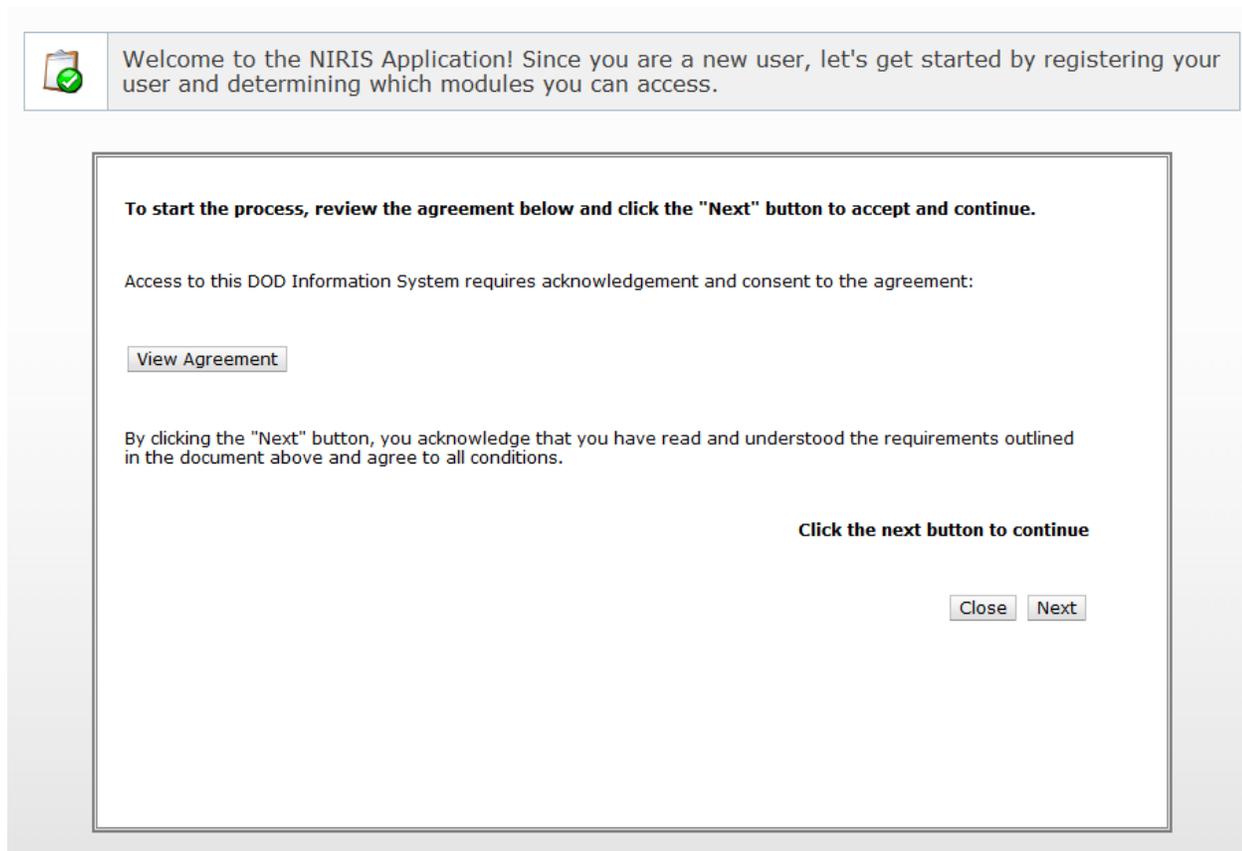
1. Accept the DOD system access agreement
2. Enter your organization, contact telephone, and Navy sponsor
3. Select the installation(s) you are requesting to access
4. Select your role in NIRIS



## NIRIS WORKGROUP

5. Review the recommended tools for your role and submit for approval

The initial wizard screen will display and request that you review the DOD Information System security agreement. Clicking the NEXT button signifies that you accept this agreement and wish to proceed.

A screenshot of the NIRIS Application welcome screen. At the top, there is a header bar with a clipboard icon and a green checkmark, followed by the text: "Welcome to the NIRIS Application! Since you are a new user, let's get started by registering your user and determining which modules you can access." Below this is a large white box with a thin border containing the following text: "To start the process, review the agreement below and click the 'Next' button to accept and continue." followed by "Access to this DOD Information System requires acknowledgement and consent to the agreement:". There is a "View Agreement" button. Below that, it says "By clicking the 'Next' button, you acknowledge that you have read and understood the requirements outlined in the document above and agree to all conditions." At the bottom right of the box, it says "Click the next button to continue" and there are "Close" and "Next" buttons.

Welcome to the NIRIS Application! Since you are a new user, let's get started by registering your user and determining which modules you can access.

**To start the process, review the agreement below and click the "Next" button to accept and continue.**

Access to this DOD Information System requires acknowledgement and consent to the agreement:

[View Agreement](#)

By clicking the "Next" button, you acknowledge that you have read and understood the requirements outlined in the document above and agree to all conditions.

**Click the next button to continue**

[Close](#) [Next](#)

The next screen will prompt you for your employment organization, your contact telephone number, and a Navy sponsor able to approve your access to NIRIS. Once this information has been entered, click the NEXT button to proceed.



## NIRIS WORKGROUP



Please provide the information required below and click the 'Next' button.

Organization:   
Phone Number:   
Sponsor:   
Sponsor Email:   
Sponsor Phone:

### What type of request? (navy.mil only)

This section is only available to users with a navy.mil email address and consists of two choices: Standard or Global. The Global choice will bypass the approval process and automatically set read-only access to all installations within the selected area. Clicking the NEXT button will complete the process and an email will be sent to you as confirmation that your provisioning is complete.

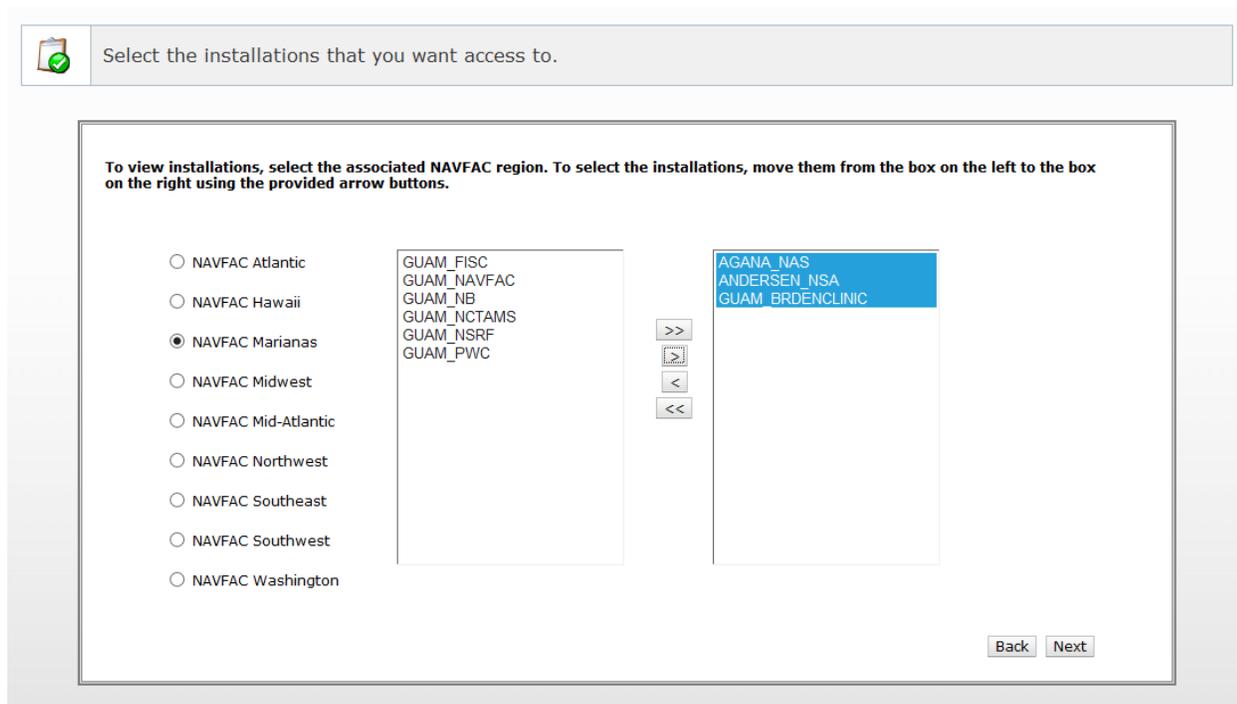
Note: Users that require the ability to write information or add data to NIRIS should choose the Standard type.



## NIRIS WORKGROUP

### Standard Provisioning

The wizard will now prompt for the NAVFAC regions and installations that you are requesting to access. You may select any combination of regions and installations on this screen. Click the region radio button to view the available installations and use the arrows to move the desired installations into the box on the right as depicted in the screen shot below. Click the NEXT button to continue.



The next step in the wizard identifies your role in NIRIS and will assign a recommended set of tools. Select your role and click the Next button to continue.



## NIRIS WORKGROUP



Select your primary role for the installations that you selected. Your primary role determines a default set of NIRIS modules that will be made available to you.

**Remedial Project Manager (RPM)**

Installation specific administration, referrer approval for user requests, SAP/ESS admin rights official RPM list maintenance

**Contractor**

Data submittal, view maps, view administrative records, query and download data

**Regulator**

View Administrative Records, Installation Maps

**Records Manager (RM)**

Administrative record librarian privileges and associated tasks

**Regional Data Manager (RDM)**

Regional user support, processing contractor data submittals, data calls, data maintenance, GIS setup

The default tool set will now display with an option of adding additional tools and features. Select any other tools that you feel are needed and click the NEXT button to continue.



## NIRIS WORKGROUP

 Listed below are the modules associated with your selected role. Select any additional modules you require and click 'Next'.

Modules granted by the selected role: CONTRACTOR

- Data Checker: Data Submission**  
Data Submission Tools: The NEDD Data Checker verifies NEDD submittals using data type, relationship and business rule checking stages. The uploaded files must pass all of the stages in order to be successfully submitted to the Navy.
- EDMS: ER Search AR**  
Data Management Tools: EDMS is used to manage/edit the Administrative Records portion of NIRIS: both the electronic documents themselves and the metadata which describe them.
- Query Tool: Query/Export Analytical Data**  
Analysis Tools: The Query Tool is the means by which analytical data is searched for and then downloaded from NIRIS. The tool is set up with a system of queries which allow the user to drill down successively into the data.
- Support Request: Support Request Screen**  
Analysis Tools: All NIRIS users are automatically provided access to the Support Request tool, which is the means for requesting help, reporting problems and perusing documentation.

At this point, the initial provisioning request is complete and an email will be sent to you and your sponsor for approval. Once the approval is complete, an additional email will be sent to you.

## Welcome to NIRIS

Users may elect to access NIRIS from the eTools menu located on the NAVFAC Private Portal or can log in directly to NIRIS by going to the URL <https://portal.navy.mil/portal/page/portal/niris>.

### Note:

The NIRIS Citrix server provides access to a number of applications for higher-end users that can be used to access NIRIS data. An additional account is needed to access these applications, which include Spatial Analysis and Decision Assistance (SADA) and the ESRI ArcGIS Suite.



## NIRIS WORKGROUP

To gain access to the Citrix server, the user will be required to fill out the top section and Part I of the System Authorization Access Request (SAAR) (DD FORM 2875). After completion, this form should be sent to your NAVFAC Remedial Project Manager (RPM) or NIRIS Workgroup representative. A copy of this form is attached, but it is recommended that the user verifies that it has not been replaced by a newer version.

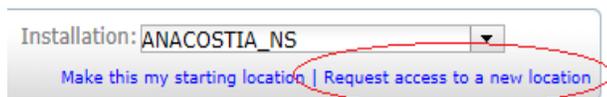
## Updating NIRIS Access

It may be necessary for a user to modify his/her NIRIS provisioning if additional permissions are required.

### Request a new Location

You can request access to a new NAVFAC installation quickly by clicking the “Request a new location” link below the installation selection drop down list (Figure 1). Clicking this link will display the installation selection screen. From this screen you can request access to one or more installations. When using the “Request access to a new location” link to request new installations, the request is made for all current approved tools for your user.

FIGURE 1



### Request a new Tool

You can request access to a new tool in the NIRIS Portal by clicking the “Request a new tool” link above the list of available tools in the NIRIS Portal (Figure 2). Clicking this link will display a list of available tools for your current role in the system. When using this link, you may only request one new



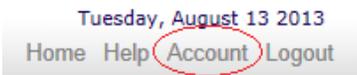
## NIRIS WORKGROUP

tool per request. If you need to change your role you can do so when requesting access to a new installation in the “Account” section described below.



### Account Menu Option

You can also make requests for new installations and new tools using the “Account” menu option at the top right in NIRIS Portal. Clicking the “Account” menu option will display a list of three choices, four for Navy users. The options available are “Add a New Installation”, “Request a New Tool”, and “Update User Information”. Navy users have an additional option that allows them to request global access at the NAVFAC footprint level.



Making provisioning requests through the account tab allows you to make more fine grained requests than the quick links from the NIRIS Portal. “Add a New Installation” allows you to specify which role you are requesting for the new installation(s). “Request a New Tool” allows you to select a specific subset of your installations where you would like to use the new tool. If you select the “Update User Information” option, you can update your Organization or Phone Number.



**NIRIS WORKGROUP**

Select the action you would like to perform

- Add a New Installation
- Request a New Tool
- Update User Information

As above, the wizard will walk you through each of these processes and a notification will be sent to you when the provisioning request has been completed.

**Revision Log:**

Revision Date: 8/21/13	Revision Detail: Updates for the new Provisioning Wizard.	Revised By: MIJARA
Revision Date: 7/17/09	Revision Detail: Modifications to provisioning form and process including the Standard and Global types.	Revised By: MIJARA
Approved By:		