

(Music)

SLIDE 1

Welcome to SPRS NIST SP 800-171 Entry Tutorial.

SLIDE 2

This training covers User Access Roles for accessing the SPRS application as-well-as entering & editing NIST SP 800-171 Assessment Results.

This training is for entering and editing only.

SLIDE 3

It does not instruct on how to identify the NIST SP 800-171 Assessment score,

SLIDE 4

complete the NIST SP 800-171 Assessment methodology,

SLIDE 5

or create a company specific system security plan or SSP.

SLIDE 6

The References slide at the end of the presentation includes resource links for additional support entering, editing, and where to find the methodology and a System Security Plan template.

SLIDE 7

The purpose of the National Institute of Standards and Technology, commonly pronounced, NIST, Special Publication, SP, 800-171 is to protect Controlled Unclassified Information, CUI, in Nonfederal Systems and Organizations.

SPRS provides storage and retrieval capabilities for specific NIST SP 800-171 assessment details and results.

SLIDE 8

When selecting the user type in the Procurement Integrated Enterprise Environment, PIEE, choose Vendor.

SLIDE 9

User roles control what users have access to. There are two user role types for vendors. Select one or both roles depending upon the desired level of SPRS access.

SLIDE 10

The SPRS Cyber Vendor User is a privileged role that allows users the ability to view, enter, edit, or delete the NIST SP 800-171 Basic Confidence level assessment records for any CAGE within their company hierarchy. This user also has view-only access to any additional Confidence level records, for any CAGE within their company hierarchy.

The user responsibilities for the Cyber Vendor User role are:

Ensuring the CAGE Hierarchy is accurate, and  
Managing NIST assessment data.

SLIDE 11

The SPRS Contractor Vendor user role restricts users to only view NIST SP 800-171 assessments at their company's hierarchy level and of their subsidiaries. Furthermore,

the SPRS Contractor Vendor user role allows users access to additional SPRS Modules as discussed in detail in the SPRS Access training.

#### SLIDE 12

Remember, the “SPRS Cyber Vendor User” role is required to enter Basic NIST SP 800-171 Assessment information.

#### SLIDE 13

SPRS uses the PIEE platform for login verification and security. For information about account creation, refer to PIEE’s “Vendors - Getting Started Help” page, at the URL listed here:

<https://piee.eb.mil/xhtml/unauth/web/homepage/vendorGettingStartedHelp.xhtml>

Step-by-step SPRS-specific Access Instructions can be found at the URL listed here:

[https://www.sprs.csd.disa.mil/pdf/SPRS\\_Access\\_Instructions.pdf](https://www.sprs.csd.disa.mil/pdf/SPRS_Access_Instructions.pdf)

Note: PIEE is not managed by the SPRS program office.

#### SLIDE 14

All access role requests are reviewed and approved by the Contractor Account Administrator (CAM) associated with the Company CAGE.

If the CAM is the one requesting a specific user role, and there is only one CAM at the company, role activation must be completed by the SPRS Program Management Office PMO or PIEE, not both. Email the PIEE Help Desk, [disa.global.servicedesk.mbx.eb-ticket-requests@mail.mil](mailto:disa.global.servicedesk.mbx.eb-ticket-requests@mail.mil), OR the SPRS Help Desk, [WEBPTSMH.fct@navy.mil](mailto:WEBPTSMH.fct@navy.mil), to activate.

#### SLIDE 15

SPRS Access - PIEE Registration Step 5:  
Select SPRS from dropdown application list.  
Select the Role SPRS Cyber Vendor User.  
Click “+Add Roles”.

#### SLIDE 16

Enter location code/Commercial and Government Entity (CAGE), code for the company.

#### SLIDE 17

Repeat these steps to select multiple Roles or multiple CAGEs before moving on in the registration process.

Once the roles are activated, the SPRS Icon will appear on your PIEE dashboard, immediately.

#### SLIDE 18

A common error that suppliers encounter is: applying for a SPRS role before registering their company in PIEE and assigning a CAM. To resolve this, ensure the company is registered in PIEE and a CAM is assigned prior to role application.

#### SLIDE 19

Refer to the PIEE Getting Started Help page (<https://piee.eb.mil/xhtml/unauth/web/homepage/vendorGettingStartedHelp.xhtml>) for more assistance on how to assign a CAM.

## SLIDE 20

Now we will discuss SPRS application access. Open a browser session and go to the PIEE landing page: <https://piee.eb.mil/piee-landing/>  
Click “log-in” and follow prompted log-in steps.  
Select the SPRS Tile.  
The SPRS application will be displayed. Make selections from the SPRS Menu Items.

## SLIDE 21

Please note that the screenshots shown throughout this presentation have been modified for size and content.

## SLIDE 22

The NIST landing page displays the Header View. NIST Assessments are organized by corporate CAGE hierarchy Highest Level Owner, HLOs.

## SLIDE 23

The Header View displays HLO CAGE, Company name, number of assessments, and confidence level.

## SLIDE 24

Basic Confidence level records are company self-assessments.

## SLIDE 25

MEDIUM, HIGH VIRTUAL, and HIGH ON-SITE confidence level records are government assessments completed at the government’s discretion.

## SLIDE 26

Header creation is the first step to entering an assessment. If there is no header or the Total Assessments column shows 0, no assessment has been entered.

## SLIDE 27

Click “[Guidance](#)” above the Header View for a dropdown list containing links to: Assessment Methodology, Quick Entry Guide, and DFARS 252.204.

## SLIDE 28

Please note, the Export HLO CAGE(s) to Excel button does not export assessment summary results.

## SLIDE 29

HLO CAGE information for the company is defined by the hierarchy information that is registered in the System for Award Management (SAM) and CAGE DLA. The system defaults to the HLO associated with the CAGE entered. Creating the HLO for the parent company does not mean an assessment is being entered on their behalf. There will be an opportunity to select specific CAGES included in the assessment on a later screen. A “Header” is required for each HLO CAGE. This is a one-time step.

## SLIDE 30

If a Basic Confidence Level header does not already exist for the HLO CAGE, it may be created by selecting the “+ Create New HLO CAGE” button and following all associated steps, this will be covered on the following slides.

#### SLIDE 31

If there is no option for "+ Create New HLO CAGE", confirm the "SPRS Cyber Vendor User" role has been activated.

#### SLIDE 32

Note that once created, a header cannot be deleted.

#### SLIDE 33

CAGE Hierarchy is imported from the System for Award Management, SAM. Please contact the company's CAGE hierarchy authority to have the data updated in SAM.

Updates typically flow to SPRS within 48 hours.

#### SLIDE 34

Begin entering the information on this screen.

The first step is to select the HLO CAGE Code.  
Click the HLO CAGE Code dropdown to select.

Next, select the Assessment Standard from the Assessment Standard dropdown.

Finally, select the Confidence Level from the Confidence Level dropdown. Currently, BASIC is the only Confidence level available to Vendors.

#### SLIDE 35

A Basic NIST assessment is a self-assessment conducted by the company or organization hired by the company.

#### SLIDE 36

Click Create when completed.

If a header is being created for the first time, the user is directed to immediately enter assessment summary details. Enter Assessment Details and select Save.

#### SLIDE 37

If the Header, HLO and Confidence Level, has already been created, it cannot be created again. The error "CAGE and Confidence combination already exist. Click back link for Header View". Exit the entry window and click the gold "View Details" button next to company name in the Header record for the HLO and BASIC Confidence level combination.

#### SLIDE 38

Users with the SPRS Cyber Vendor User role may enter NIST SP 800-171 Assessment details for their company.  
Click the View Details button.

#### SLIDE 39

Click the Add New Assessment button to begin entering data.

#### SLIDE 40

This is the Assessment Entry input page.

#### SLIDE 41

Manually enter date using two digit month, two digit day and four digit year format or click the calendar icon to select Assessment Date.

#### SLIDE 42

Enter Score. The system will accept scores between negative two hundred five and one hundred ten points.

#### SLIDE 43

Click the dropdown to select scope. Enterprise - Company's Network under the CAGEs listed

Contracts - Contract specific SSP Review

Enclave - Standalone under Enterprise CAGE as a Business Unit (test enclave, hosted resources, etc.)

These definitions may be viewed by hovering over "Assessing Scope".

#### SLIDE 44

For specific questions about interpreting definitions please contact your Program Office or Contracts representative or the Defense Contract Management Agency (DCMA) general mailbox, [DCMA\\_7012\\_Assessment\\_Inquiry@mail.mil](mailto:DCMA_7012_Assessment_Inquiry@mail.mil) for assistance.

#### SLIDE 45

If the complete score of 110 has not been achieved, enter a Plan of Action Completion Date. If a score of 110 has been met, this is not a required field. Manually enter date using the correct format or click the calendar icon to select Plan of Action Completion Date.

#### SLIDE 46

Enter the document name of the company's System Security Plan or (SSP).

Note: In accordance with NIST SP 800-171 Assessment Methodology Version 1.2.1 dated June 24<sup>th</sup>, 2020,

#### SLIDE 47

"The contractor must have a system security plan, Basic Security Requirement 3.12.4, in place to describe each covered contractor information system, and a plan of action, Basic Security Requirement 3.12.2, in place for each unimplemented security requirement to describe how and when the security requirement will be met."

For help with creating the System Security Plan, DCMA has provided an SSP Guide and Template. Links have been provided at the end of this presentation.

#### SLIDE 48

A field is provided to identify the SSP Version, Revision if the company uses this for document control. This field is optional.

#### SLIDE 49

In the SSP Date field enter the date that the company's SSP was last updated. Manually enter date using the correct format or click the calendar icon to select SSP Date. This date should be prior to or the date of the assessment.

#### SLIDE 50

Click the Open CAGE Hierarchy Button to display a list of CAGEs for selection. Once selected, the CAGEs will be displayed in the Included CAGE(s) field. Click checkboxes directly or click the company name to include that CAGE in the CAGE Hierarchy Selection. Once satisfied with selected CAGEs click 'Ok'.

#### SLIDE 51

To include the Highest Level Owner (HLO) and did not select it in the CAGE tree, click the checkbox to add to the Included CAGE(s) list. Only CAGEs listed in the "Included CAGEs" field are considered assessed.

#### SLIDE 52

Click the Save button to save the Assessment details. Once an assessment has been submitted, it will be assigned a DoD Unique Identifier (UID).

#### SLIDE 53

Viewing the Assessment.

Columns may be sorted Ascending/Descending.

Columns may be toggled on/off.

Columns may be filtered.

#### SLIDE 54

To view all the information on the record, select Full Details and an additional screen will appear with the information in its entirety. This report may be printed and shared at the users' discretion. The printed report is time stamped.

#### SLIDE 55

As per NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1 "Assessment of contractors with contracts containing DFARS clause 252.204-7012 is anticipated to be once every three years..." Therefore, SPRS displays assessments that are over 3-years old as red.

#### SLIDE 56

After entering an assessment, it may be updated as necessary to reflect the company's current status.

To edit, select the pencil button within Details View. The original form will open pre-populated with the current details. Update fields as necessary.

#### Slide 57

NIST Resources Include:

NIST Information Page: <https://www.sprs.csd.disa.mil/nistsp.htm>

NIST Quick Entry Guide:

<https://www.sprs.csd.disa.mil/pdf/NISTSP800-171QuickEntryGuide.pdf>

NIST FAQ's: <https://www.sprs.csd.disa.mil/faqs.htm#nist>

Defense Contract Management Agency (DCMA) help desk:

[dcma.lee.hq.mbx.dibcac-scheduling-inbox@mail.mil](mailto:dcma.lee.hq.mbx.dibcac-scheduling-inbox@mail.mil)

NIST Assessment Methodology:

<https://www.acq.osd.mil/asda/dpc/cp/cyber/safeguarding.html#nistSP800171>

And SSP Guide & Template:

<https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final>

SLIDE 58

SPRS can be contacted by going to our website which is located at the URL listed here:

<https://www.sprs.csd.disa.mil>

Our Help Desk is available Monday through Friday 6:30am to 6:00pm Eastern Time.

The phone numbers and Help Desk Email are listed here: [webptsmh@navy.mil](mailto:webptsmh@navy.mil)

Slide 59

Within the application questions may be submitted via the Feedback/Customer Support link in the menu.

SLIDE 60

This concludes the SPRS NIST SP 800-171 Entry Tutorial.