(Music)

SLIDE 1
Welcome to SPRS version 4.0 NIST SP 800-171 Entry Tutorial.

SLIDE 2
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.

This training covers the user's ability to enter and edit NIST SP 800-171 Assessment Results.

SLIDE 3
It does not instruct on how to identify the NIST SP 800-171 Assessment score, complete the NIST SP 800-171 Assessment methodology, or create a company specific system security plan or SSP. Additional information can be found on the SPRS website listed here: https://www.sprs.csd.disa.mil/nistsp.htm

SLIDE 4
SPRS uses the Procurement Integrated Enterprise Environment (PIEE) for authentication and access. There are two PIEE user role types for vendors, Contractor/Vendor or Cyber Vendor User roles. Select one or both roles depending upon the desired level of SPRS access required.

SLIDE 5
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 6
The SPRS Contractor Vendor user role restricts users to view-only NIST SP 800-171 assessment scores at their company's hierarchy level and of their subsidiaries. Furthermore, the SPRS Contractor Vendor user role allows users access to additional SPRS report as discussed in detail in the SPRS Access training.

SLIDE 7
Please note that the screenshots shown throughout this presentation have been modified for size and content.

SLIDE 8
To access NIST SP 800-171 Assessments, select the Cyber Reports link from the menu.

Select the desired Company Hierarchy from the drop-down menu and click the Run Cyber Reports button.

The first CAGE displayed in the drop down list is the CAGE that is associated with the user's PIEE profile. The CAGE in parenthesis is the hierarchy; the Highest Level Owner (HLO) reported to SPRS.

An asterisk indicates the user has the SPRS Cyber Vendor User role for this CAGE Hierarchy.

SLIDE 9
The Company name and CAGE code selected from the drop down will be listed at the top.

SLIDE 10
The Company Hierarchy tab displays the company's complete hierarchy. SPRS receives this data from SAM.gov.

If the Corporate CAGE Hierarchy is not accurate, contact the Electric Business Point of Contact (EBPOC) listed in SAM registration for the CAGE at the website listed here: https://sam.gov/content/home. CAGE Hierarchy information typically flows from SAM to SPRS within 48 hours

SLIDE 11
The Overview tab displays the CAGE(s), within the hierarchy, that have Cyber assessments. Only CAGE(s) that have assessments, and that the user has access to view, will show within this tab. The number indicates how many current assessments for that CAGE and confidence level combination exist.

If records are greater than zero, the number will be linked. If selected, it will open to the Criteria Search tab with that CAGE pre-populated in the search criteria, the related confidence level tab opened, the search executed, and results listed. More information on this tab later in the training. If there are records older than 3 years, there will be a zero listed in brackets and it will be linked.

SLIDE 12
The NIST SP 800-171 Assessments tab displays logged assessment summary results. If the user has a SPRS Cyber Vendor User role, they will have visibility of an Add New NIST Assessment button as well as an Edit/Delete column with pencil icons. Users with Contractor/Vendor access will not see those two items.

SLIDE 13
Within the NIST SP 800-171 Assessments tab there are four tabs denoting the NIST confidence levels: High On-site, High Virtual, Medium, and Basic. The Basic is the only confidence level that is a self-assessment and the only one that can be maintained by a SPRS Cyber Vendor User.

SLIDE 14
Selecting the Details button opens a pop-up that contains a print friendly display of all information associated with that DoD Unique Identifier (UID). This can be downloaded and saved as a PDF.

SLIDE 15
NIST SP 800-171 Assessment Summary results include the following information: DoD UID, included CAGE, Company Name, Assessment Date, Score, Assessment Scope, Plan of Action Completion Date, System Security Plan (SSP) Assessed, SSP Version/Revision, SSP Date, and depending on the confidence level: Assessing CAGE or DoDAAC, and DFARS 252.204-7012 Compliance.

SLIDE 16
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 17
To Add an Assessment, users must have the SPRS Cyber Vendor User role.

Select the Add New NIST Assessment button, this is the Assessment Entry input page.

SLIDE 18
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 19
Enter Score. The system will accept scores between negative two hundred five and one hundred ten points.

SLIDE 20
Click the dropdown to select scope. Choices Include: Enterprise, for company’s Network under the CAGEs listed. Contracts, for contract specific company’s System Security Plan, and Enclave, for standalone under Enterprise CAGE as a Business Unit.

SLIDE 21
For specific questions about interpreting definitions please contact your Program Office, Contracts representative, or the Defense Contract Management Agency (DCMA) general mailbox, DCMA_7012_Assessment_Inquiry@mail.mil for assistance.

SLIDE 22
If a score of 110 is not achieved, a Plan of Action Completion Date is required.

SLIDE 23
Enter the document name of the company’s SSP.

“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 a System Security Plan, DCMA has provided an SSP Guide and Template. Links have been provided at the end of this presentation.

SLIDE 24
A field is provided to identify the SSP Version, Revision if the company uses this for document control. This field is optional.

SLIDE 25
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 the SSP Date. This date should be prior to or the date of the assessment.

SLIDE 26
Click the Open CAGE Hierarchy button to see the list of CAGEs in the Hierarchy, which allows users to select Included/assessed CAGEs. Users can also copy and paste a comma-delimited list of CAGEs into the CAGE text box provided.

SLIDE 27
Click the Save button to save the Assessment details. Once an assessment has been submitted, it will be assigned a DoD UID, which is a 10-digit alphanumeric identifier is automatically assigned to each newly saved assessment. The first two letters delineate the confidence level of the assessment. Basic, Medium, and High confidence levels start with SB, SM, SH respectively.

SLIDE 28
Assessment results entered will populate below the entry fields. To revise or update the assessment information below, update the information within the fields and select the Update button. To add additional assessments, select the Clear and Add Additional Assessment(s) button. This will clear the fields and allow additional assessments to be added. Clearing the fields does not delete the previously entered assessment. Select the Back button to go back or to view the entered assessment on the NIST SP 800-171 Assessments tab.

SLIDE 29
The Edit/Delete pencil icon will also bring the user to the Enter Assessment Details screen with the details populated. To edit, update the information within the fields and select the Update button.

SLIDE 30
To Delete an Assessment, select the Delete button. This will open a pop-up of the complete assessment details with a warning to confirm deletion. Deleting the assessment will delete it for all Included CAGEs. Select Confirm Delete to delete.

SLIDE 31
Viewing the Assessment table information, columns can be sorted and filtered by clicking the three dots at the top of each column.
Columns may be sorted Ascending or Descending.
Columns may be toggled on/off.
Columns may be filtered.
The Clear button will reset all selected filters.

SLIDE 32
For additional information on entering a NIST SP 800-171 assessment into SPRS. Review the NIST SP 800-171 Quick Entry Guide, located here:
https://www.sprs.csd.disa.mil/pdf/NISTSP800-171QuickEntryGuide.pdf

SLIDE 33
The Criteria Search tab allows the user to enter various data points and search all assessments based on the entered criteria. Enter desired search criteria and select the Search button. Applicable information will load below.

SLIDE 34
The Show/Hide Search Fields button will collapse or expand the criteria search fields for space saving considerations.

SLIDE 35
The Guidance tab provides General Guidance as well as NIST SP 800-171 specific Information and contains links to Assessment Methodology, Quick Entry Guide, DFARS 252.204, and more.

SLIDE 36
To obtain an Excel spreadsheet of report, select the Export button from the Toolbar. An indicator will pop up indicating the request has been received and select okay. An email will be sent when the report is available in the Download module, if the email is not received, check Junk or Spam mail.

SLIDE 37
The report will be available in the Downloads module for five (5) days before being removed. The report can be retrieved again by going to the module and using the Export Icon in the Toolbar again.

Slide 38
To print the browser screen currently available, use the print option in the Toolbar. This will allow the current report to be printed or saved as a PDF.

SLIDE 39
The informational question mark option on the Toolbar will open an additional tab with the SPRS home page displayed.

SLIDE 40
Additional NIST Resources for entering, editing, and where to find the methodology and a System Security Plan template. Are included here:
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
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 41
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.
Help Desk Email are listed here: sprs-helpdesk@us.navy.mil

Slide 42
Within the application questions may be submitted via the Feedback/Customer Support link in the menu or via the Toolbar.

SLIDE 43
This concludes the SPRS version 4.0 NIST SP 800-171 Entry Tutorial.