(Music)

SLIDE 1
Welcome to SPRS Cybersecurity Maturity Model Certification (CMMC) Entry Tutorial.

SLIDE 2
The purpose of CMMC, "...is to enforce the protection of sensitive unclassified information shared by the Department of Defense with its contractors and subcontractors. The program provides the DoD with increased assurance that contractors and subcontractors are meeting the cybersecurity requirements for nonfederal systems processing controlled unclassified information (CUI)." (DoD CIO)

This training covers the vendor's ability to enter and affirm a CMMC Assessment.

SLIDE 3
SPRS uses the Procurement Integrated Enterprise Environment (PIEE) for authentication and access.

The SPRS Cyber Vendor User is a privileged role that allows users the ability to view, enter, and affirm a CMMC Assessment.

The user responsibilities for the Cyber Vendor User role are:
Ensuring the CAGE Hierarchy is accurate and Managing Cyber Reports.

SLIDE 4
The SPRS Contractor Vendor user role restricts users to view-only Cyber Report results at their company's hierarchy level and of their subsidiaries. In addition, the SPRS Contractor/Vendor Support role allows users access to SPRS performance reports as discussed in detail in the SPRS Access training.

SLIDE 5
Please note that the screenshots shown throughout this presentation have been modified for size and content.

SLIDE 6
To access CMMC, select the Cyber Reports link from the menu.

Use the drop-down list to identify the Company hierarchy. The CAGEs on the list will be paired; the first CAGE in the pair 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 and Hierarchy. Select the CAGE and Hierarchy combination and click the Run Cyber Reports button.

SLIDE 7
The CMMC 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 CMMC Level 1 Self-Assessment button as well as Edit and Delete columns. Users with only Contractor/Vendor Support access will not see those items.

To Add a CMMC Level 1 Assessment, select the Add New CMMC Level 1 Self-Assessment button.

SLIDE 8
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 9
Click the dropdown to select scope. Choices Include: Enterprise, an organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. Or Enclave, a set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter (NIST).

SLIDE 10
Enter the number employees that are in the organization for which this CMMC Level 1 Self-assessment applies. For a more in-depth detail of the fields, select the blue Information button next to the fields for quick access to definitions.

SLIDE 11
Select Yes or No to reflect if you are compliant with FAR clause 52.204-21, met mandatory CMMC Assessment requirements. For additional information the regulation clause is listed at the website here: https://www.ecfr.gov/current/title-48/chapter-1/subchapter-H/part-52/section-52.204-21

SLIDE 12
Click the Open CAGE Hierarchy button to see the list of CAGEs in the Hierarchy, this allows users to select Included CAGEs. Users can also copy and paste a comma-delimited list of CAGEs into the provided text box. CAGE Hierarchy information is fed into SPRS from SAM.

Questions related to technical interpretation of these CMMC Level 1 supplemental guidance documents may be directed to the email listed here: osd.pentagon.dod-cio.mbx.cmmc-inquiries@mail.mil. Do not submit questions requesting interpretation or modification of NIST source documents, which are outside the CMMC Program's purview.

SLIDE 13
Each assessment requires affirmation by a company’s Affirming Official (AO). As defined in 32 CFR 170.4, the AO is the senior level representative from within each Organization Seeking Assessment (OSA) who is responsible for ensuring the OSA’s compliance with the CMMC Program requirements and has the authority to affirm the OSA’s continuing compliance with the security requirements for their respective organization. (CMMC-custom term 170.4)

SLIDE 14
Assessments in progress can be saved and can be edited or affirmed at a later date. These assessments will not be assigned a CMMC UID until the assessment is Affirmed.

Once the assessment detail information is correct, select Continue to Affirmation.

SLIDE 15

If the user entering the CMMC Self-Assessment is not the AO, enter the AO's email address and select Transfer to AO. The AO will receive an email that an assessment is waiting for their affirmation.

SLIDE 16
If the user is the AO, select Continue to Affirmation.

This information for the Affirming Official is transferred from the user's PIEE profile. Any changes must be made in PIEE and cannot be changed on this screen. Enter any additional emails that need to be associated with this record and click Continue to Affirmation.

SLIDE 17
Review the information and statement and click the check box to certify. Select Affirm to complete or Cancel if information on the form needs to be updated or if the user is not the AO.

SLIDE 18
When affirming an assessment, if 'Yes' was selected for compliance with the security requirements specified in FAR clause 52.204-21, the assessment will receive CMMC Status Type "Final Level 1 Self-Assessment". If 'No' was selected, the assessment will receive CMMC Status Type "No CMMC Status" and will appear red.

Additional CMMC Status Types include "Pending Affirmation" which is a completed record that is waiting for the AO to affirm, "Incomplete", which is a saved record with partial assessment information, and "No CMMC Status (Expired Assessment)" which is an expired "Final Level 1 Self-Assessment". The only CMMC Status Type that will be visible to government personnel, will be "Final Level 1 Self-Assessment."

SLIDE 19
If an assessment has edit capability, there will be a pencil icon within the edit column. CMMC Status Types "Incomplete" and "Pending Affirmation" are the only status types that can be edited.
If the data within a "Final Level 1 Self-Assessment" or a "No CMMC Status", needs to change, this assessment type will need to be deleted and reentered.

SLIDE 20
If an assessment has delete capability, there will be a trashcan icon within the delete column located on the far right. All CMMC Status Types can be deleted with the exception of the "No CMMC Status (Expired Assessment)."

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

SLIDE 21
Selecting the Detail button in the CMMC Unique Identifier (UID) column, opens a pop-up that contains a print friendly display of all information associated with that record. This can be downloaded and saved as a PDF. The Export feature in the toolbar will not include CMMC assessment results at this time.

SLIDE 22
Viewing the Assessment table information, hover over the column title to see definitions of each of the column headers.
Columns can be sorted and filtered by clicking the three dots at the top of each column.

For additional information on entering a CMMC assessment in SPRS, review the CMMC Quick Entry Guide and website information:
https://www.sprs.csd.disa.mil/nistsp.htm

SLIDE 23
Reviewing the additional tabs, the Company Hierarchy tab displays the company's complete hierarchy. SPRS receives this data from SAM.

If the Corporate CAGE Hierarchy is not accurate, contact the Electronic 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 24
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 Support access will not see those items.

SLIDE 25
The Criteria Search tab allows the user to enter various data fields and search all assessments associated with that company based on the entered criteria. Enter desired search criteria and select the Search button. Applicable information will load in respective tabs below.

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

SLIDE 26
The Guidance tab provides General Guidance as well as CMMC specific Information and contains links to the FAR clause 52.204-21, supplemental guidance, and an email address for additional questions.

Slide 27
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 28
The informational question mark option on the Toolbar will open an additional tab with the SPRS home page displayed.

SLIDE 29
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 30
Within the application questions may be submitted via the Feedback/Customer Support link in the menu or via the Toolbar.

SLIDE 31
This concludes the CMMC Entry Tutorial.