



DARPA Contracts Management Office
NIST SP 800-171 Self-Assessment
How-To Guide

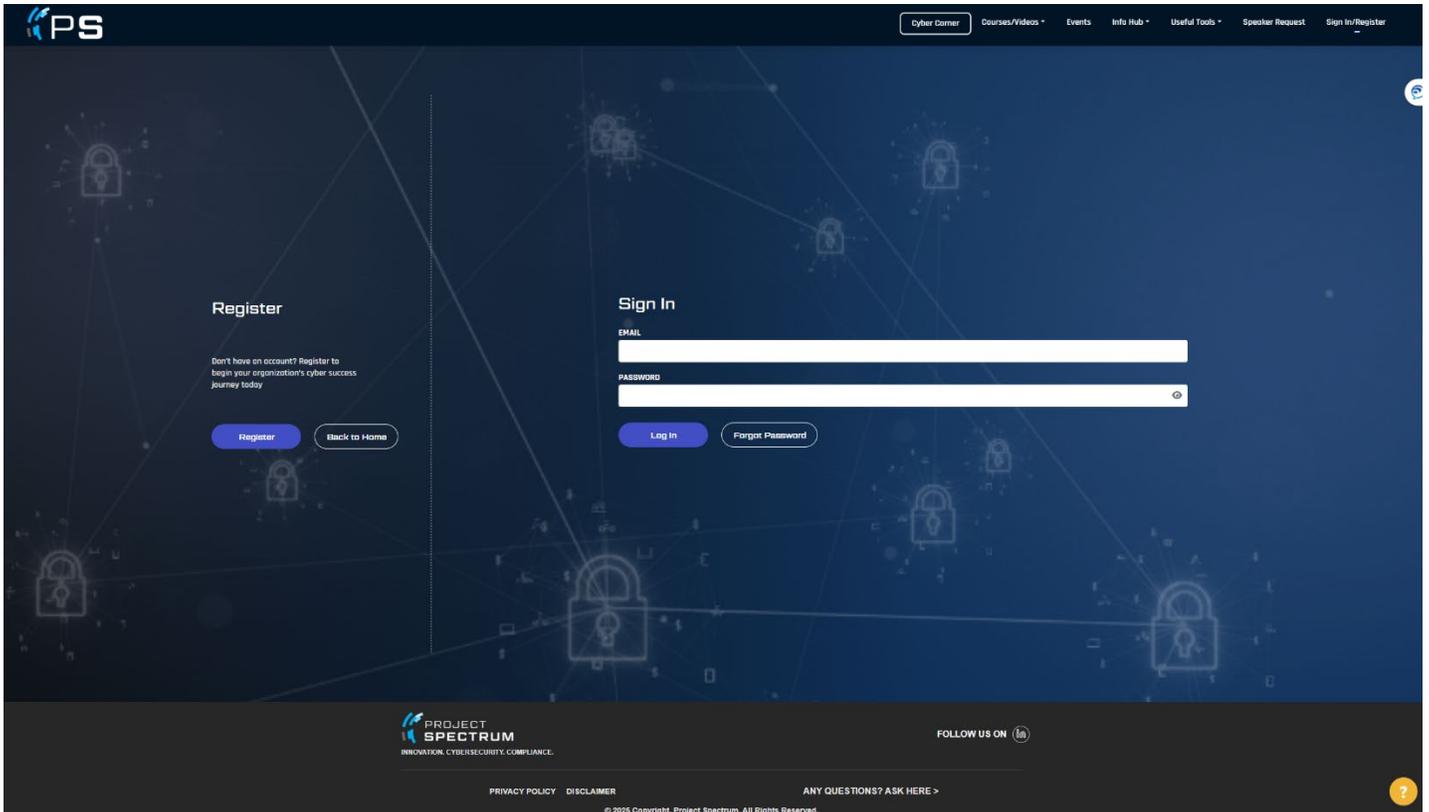


PART 1 – Generate NIST 800-171 Self- Assessment Score

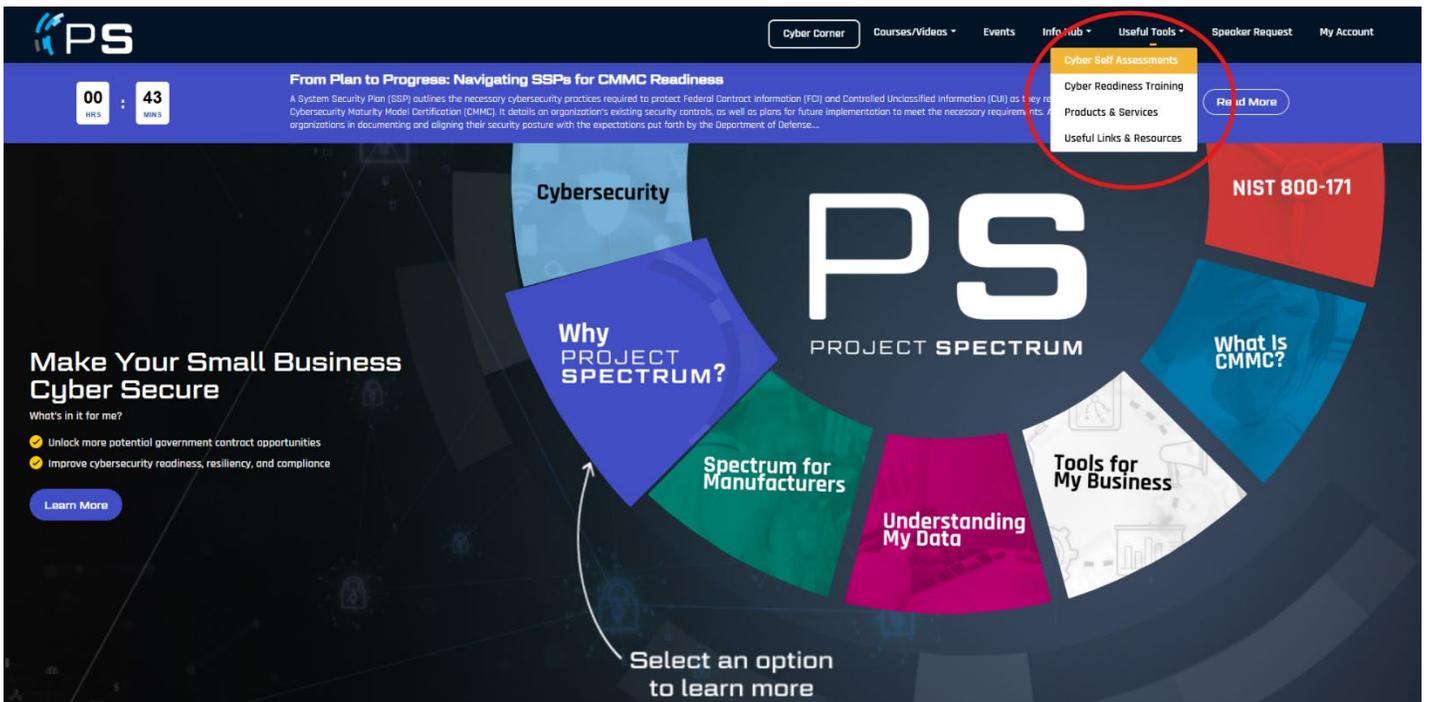
COMPLETE IN PROJECT SPECTRUM PORTAL

(<https://www.projectspectrum.io/#/>)

Step 1 – Create an Account on projectspectrum.io and log-in.



Step 2 – From the top ribbon select Useful Tools -> Cyber Self Assessments



Step 3 – Scroll down and select “Start Assessment” for the NIST 800 171 Self-Assessment

The screenshot shows the top navigation bar with 'PS' logo and links for Cyber Corner, Courses/Videos, Events, Info Hub, Useful Tools, Speaker Request, and My Account. Below are three assessment cards:

- CUI – Discovery Questionnaire**: We have provided a self-discovery questionnaire to assist you with starting your data discovery journey to find where Controlled Unclassified Information (CUI) is being accessed, processed, stored and transmitted within your organization. [Start Questionnaire](#)
- CMMC Level 2 - Self-Assessment**: Level 2 focuses on the protection of Controlled Unclassified Information (CUI) and encompasses the 110 security requirements specified in the NIST SP 800-171 Rev 2. [Start Assessment](#)
- NIST 800 171 - Self-Assessment**: NIST 800-171 provides agencies with recommended security requirements for protecting the confidentiality of Controlled Unclassified Information (CUI) and applies to all components of nonfederal systems and organizations that process, store, and/or transmit CUI. [Start Assessment](#)

Step 4 – Complete Self-Assessment

Note: The self-assessment is 110 questions and 14 pages, one page for each category as indicated by the gray bars at the top of the page. See next page for guidance on Q.86.

The screenshot shows the 'NIST 800-171' assessment page. The main heading is 'NIST 800-171' with a 'Back To Readiness Check' button. Below is a navigation bar with categories: Access Control, Awareness and Training, Audit and Account Manager, Configuration and Incident Response, Identification and Authentication, Maintenance, Media Protection, Personnel Security, Physical Protection, Risk Assessment, Security Assessment, System and Information Protection, and System and Information Integrity. The 'Access Control' category is selected.

Access Control

These questions ask about your policies to control access to your company's network systems.

1. Do you limit information system access to authorized users, processes acting on behalf of authorized users, and devices (including other information systems)?

[Tooltip](#) | [Explainer Video](#)

Authorized users are identified. Yes No Not Applicable Answer Later

Processes acting on behalf of authorized users are identified. Yes No Not Applicable Answer Later

Devices (and other systems) authorized to connect to the system are identified. Yes No Not Applicable Answer Later

System access is limited to authorized users. Yes No Not Applicable Answer Later

System access is limited to processes acting on behalf of authorized users. Yes No Not Applicable Answer Later

System access is limited to authorized devices (including other systems). Yes No Not Applicable Answer Later

2. Do you limit information system access to the types of transactions and functions that authorized users are permitted to execute?

[Tooltip](#) | [Explainer Video](#)

The types of transactions and functions that authorized users are permitted to execute are defined. Yes No Not Applicable Answer Later

System access is limited to the defined types of transactions and functions for authorized users. Yes No Not Applicable Answer Later

Note: You will not be able to complete the NIST Self-Assessment and have a score generated until you have a System Security Plan completed. If you already have a system security plan you are able to answer Q.86 and generate a score if all answers are marked “yes” If any answers are “no” you will need to update your System Security Plan to ensure all answers can be “yes.”

Q.85. Do you monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls?
 > [Tooltip](#) | [Explainer Video](#)
 Security controls are monitored on an ongoing basis to ensure the continued effectiveness of these controls. Yes No Not Applicable Answer Later

Q.86. Do you develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems?
Warning: If the System Security Plan is not developed or does not exist, the NIST 800-171 Assessment is incomplete and the final score will not be provided. You may continue as is without formal results.
 > [Tooltip](#) | [Explainer Video](#)

A system security plan is developed. Yes No Not Applicable Answer Later

The system boundary is described and documented in the system security plan. Yes No Not Applicable Answer Later

The system environment of operation is described and documented in the system security plan. Yes No Not Applicable Answer Later

The security requirements identified and approved by the designated authority as nonapplicable are identified. Yes No Not Applicable Answer Later

The method of security requirement implementation is described and documented in the system security plan. Yes No Not Applicable Answer Later

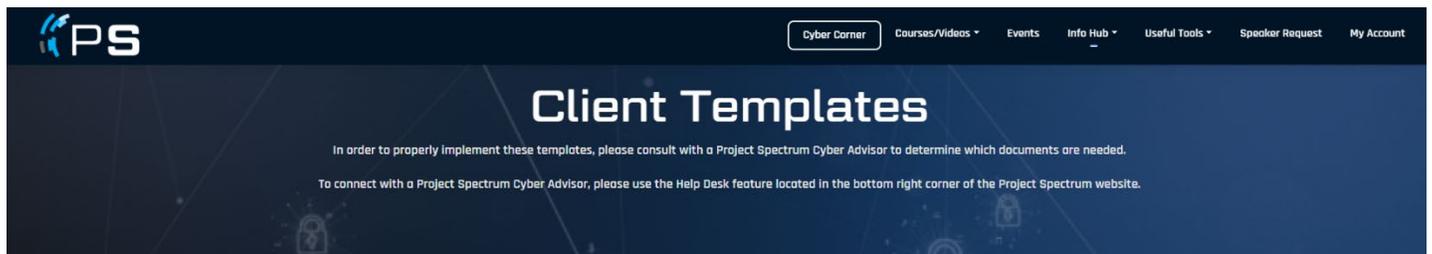
The relationship with or connection to other systems is described and documented in the system security plan. Yes No Not Applicable Answer Later

The frequency to update the system security plan is defined. Yes No Not Applicable Answer Later

System security plan is updated with the defined frequency. Yes No Not Applicable Answer Later

Step 5 – Download & Complete System Security Plan *(if applicable; if not applicable, skip to step 6)*

Note: A template System Security Plan is available on Project Spectrum. Navigate to window top ribbon “Info Hub” -> “Client Templates” -> Scroll down to System Security Plan (SSP) -> Check box & Click “Download Checked.”



Select up to 6 templates to download at a time

Search by Title

Categories:

Levels:

Selected Templates: (1)

- System Security Plan (SSP)

Template Title	Category	Level	Details
<input type="checkbox"/> System Configuration Settings...	Access Control	Level 1	<input type="button" value="Preview"/>
<input type="checkbox"/> System Scan Log	System and Information Integrity	Level 1	<input type="button" value="Preview"/>
<input checked="" type="checkbox"/> System Security Plan (SSP)	General		<input type="button" value="Preview"/>
<input type="checkbox"/> User Identification Policy	Identification and Authentication	Level 1	<input type="button" value="Preview"/>
<input type="checkbox"/> Visitor Management Policy	Physical Protection	Level 1	<input type="button" value="Preview"/>
<input type="checkbox"/> VPN Configuration Details	Access Control	Level 1	<input type="button" value="Preview"/>

Note: For assistance in understanding each requirement, you may use the “Explainer Video” linked with each requirement in the NIST 800-171 Self-Assessment Questionnaire

Step 6 – Complete NIST 800-171 Self-Assessment & Obtain Score

Note: If you needed to complete or update your System Security Plan please ensure you completed Q.86 before completing assessment or your score will not be generated.

PS Cyber Corner Courses/Videos Events Info Hub Useful Tools Speaker Request My Account

1.0B. Do you perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed?

[Tooltip](#) | [Explainer Video](#)

The frequency for malicious code scans is defined. Yes No Not Applicable Answer Later

Malicious code scans are performed with the defined frequency. Yes No Not Applicable Answer Later

Real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed. Yes No Not Applicable Answer Later

1.0B. Do you monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks?

[Tooltip](#) | [Explainer Video](#)

The system is monitored to detect attacks and indicators of potential attacks. Yes No Not Applicable Answer Later

Inbound communications traffic is monitored to detect attacks and indicators of potential attacks. Yes No Not Applicable Answer Later

Outbound communications traffic is monitored to detect attacks and indicators of potential attacks. Yes No Not Applicable Answer Later

1.1D. Do you identify unauthorized use of organizational systems?

[Tooltip](#) | [Explainer Video](#)

Authorized use of the system is defined. Yes No Not Applicable Answer Later

Unauthorized use of the system is identified. Yes No Not Applicable Answer Later

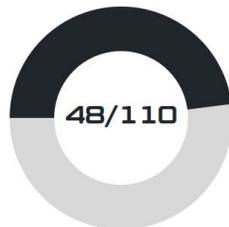
[Previous](#) [Complete](#)

PS Cyber Corner Courses/Videos Events Info Hub Useful Tools Speaker Request My Account

NIST 800-171 - Self-Assessment

Your Assessment is complete.

NIST 800-171 provides agencies with recommended security requirements for protecting the confidentiality of CUI and applies to all components of nonfederal systems and organizations that process, store, and/or transmit CUI. Your score: **48/110**



[Print Answers](#)

[Export to CSV](#)

[Go to Dashboard](#)

[Back to Cyber Readiness Check](#)

YOU DO NOT NEED A PERFECT SCORE TO SATISFY THE NIST REQUIREMENT IN THE SPRS PORTAL.

PART 2 – Input NIST 800-171 Self- Assessment Score into Supplier Performance Risk System (SPRS)

COMPLETE IN SUPPLIER PERFORMANCE RISK SYSTEM
(<https://www.sprs.csd.disa.mil/access.htm>)

Quick Entry Guide Source: <https://www.sprs.csd.disa.mil/nistsp.htm>

SPRS

Supplier Performance Risk System

NIST SP 800-171
Quick Entry Guide

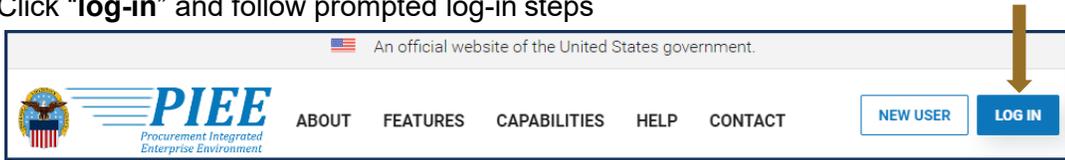
NIST SP 800-171 QUICK ENTRY GUIDE
VERSION 4.0



NSLC PORTSMOUTH BLDG. 153-2 PORTSMOUTH NAVAL SHIPYARD, PORTSMOUTH, NH 03804-5000

Approved for public release, distribution is unlimited.

1. **NIST SP 800-171 Assessment Database:** The purpose of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 is to protect Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations. This database contains data associated with NIST SP 800-171 Assessments.
2. **PIEE Access:** A “SPRS Cyber Vendor User” role is required to enter Basic Assessment information. Step-by-step PIEE Access Instructions can be found here. <https://www.sprs.csd.disa.mil/access.htm>
3. **SPRS Application Access:** To Access SPRS, follow the below steps:
 - a. **PIEE** landing page: <https://piee.eb.mil/>
 - b. Click “**log-in**” and follow prompted log-in steps



Screenshot Dtd 09 JAN 2024

- c. Select the **SPRS** icon:



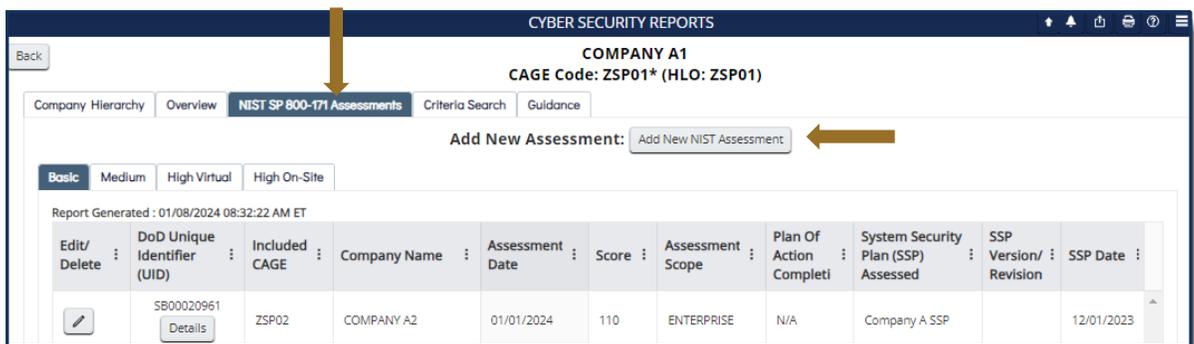
- d. Select the **Cyber Reports** module:

- 3.1 Select the desired Hierarchy from the drop down and click the **Run Cyber Reports** button. The first CAGE displayed 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, that the PIEE profile CAGE is associated with.

NOTE: An asterisk * indicates the user has the SPRS Cyber Vendor User role (access to add/edit) for this CAGE/Hierarchy.



- 3.2 Navigate to the NIST SP 800-171 Assessments tab and select the **Add New Assessment** button.



NOTE: CAGE Hierarchy is imported from the System for Award Management (SAM). Contact your company’s Electric Business Point of Contact (EBPOC) listed at SAM.gov so they can correct the hierarchy in SAM. Updates typically flow to SPRS within 48 hours.

3.3 Enter Assessment Details: Enter data in the form and select “Save”:

NOTE: The Assessment Methodology and System Security Plan should be completed prior to entering assessment summary results within SPRS.

A **DoD Unique Identifier (UID)** is automatically assigned to each newly saved assessment. The DoDUID is a 10-digit alphanumeric number where the first two letters delineate the confidence level of the assessment; Basic, Medium, and High confidence levels start with SB, SM, SH respectively.

3.4 Assessment Edit/Delete: The user may update as necessary to reflect the company’s current status. To edit assessment details, click the pencil icon located within the Basic tab of the NIST SP 800-171 Assessments tab.

NOTE: The Basic Confidence Level is the only assessment that can be maintained (add/edit/delete) by vendors.

Basic Medium High Virtual High On-Site

Report Generated : 03/07/2024 04:22:48 PM ET

Edit/ Delete	DoD Unique Identifier (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
	SB00020881 Details	ZSP01	COMPANY A1	12/20/2023	99	ENTERPRISE	12/18/2024	TEST SSP Document Name	1.2	12/20/2023
	SB00020407 Details	ZSP02	COMPANY A2	06/01/2019	110	ENTERPRISE	N/A	Test	v2.0	06/01/2018

NOTE: Assessments results turn red when the assessment date expands beyond three years.