

How to Obtain a NIST (National Institute of Standards and Technology) Self-assessment Score

MAY2025

Sherrie Cordi

- Small Business Deputy
- USACE Memphis District



U.S. ARMY



US Army Corps
of Engineers®





U.S. ARMY

1. CREATE A PROJECT SPECTRUM ACCOUNT

2. LOGIN



<https://www.projectspectrum.io>

Register

Don't have an account? Register to begin your organization's cyber success journey today

Sign In

EMAIL

PASSWORD

Sign up for a free Project Spectrum account

Project Spectrum provides companies, institutions, and organizations with a comprehensive, cost-effective platform of cybersecurity information, resources, tools, and training. Our mission is to improve cybersecurity readiness, resiliency, and compliance of small/medium-sized businesses and the Defense Industrial Base (DIB) manufacturing supply chain.

1 Account Info **2 Account Type** **3 Contact Info**

First Name*

First Name

Last Name*

Last Name

Your Email*

Email Address

Forum Username*

Username

Password*

Password

Confirm Password*

Confirm Password

Must be at least 8 characters and contain a lowercase, uppercase, number and special character.

☐ * By creating an account, you agree to our Limited Liability Agreement (LLA). Please review it before proceeding [Limited Liability Agreement \(LLA\)](#).

PRIVACY

CBIL Help



U.S. ARMY

3. CLICK ON “NIST” AND THEN “WHAT IS NIST?”

3



PS PROJECT SPECTRUM

Zero Trust for Small Manufacturing Industries
Imagine a world where every device, user, and application is treated as a potential threat. That's the core idea behind Zero Trust Architecture - a security framework that assumes threats could exist both outside and inside the network.
The fundamental principle? "Never trust, always verify..." [Read More](#)

Make Your Small Business Cyber Secure
What's in it for me?
✓ Unlock more potential government contract opportunities
✓ Improve cybersecurity readiness, resiliency, and compliance
[Learn More](#)

Select an option

- Cybersecurity
- Why PROJECT SPECTRUM?
- Spectrum for Manufacturers
- Understanding My Data
- Tools for My Business
- What Is CMMC?
- NIST 800-171**

[Back To All Options](#)

Cyber Resources for the Supply Chain

What's in it for me?

- ✓ Understand government information security standards and guidelines
- ✓ Stay abreast of contracting requirements for small- and medium-sized businesses

What is NIST?

NIST 800-171



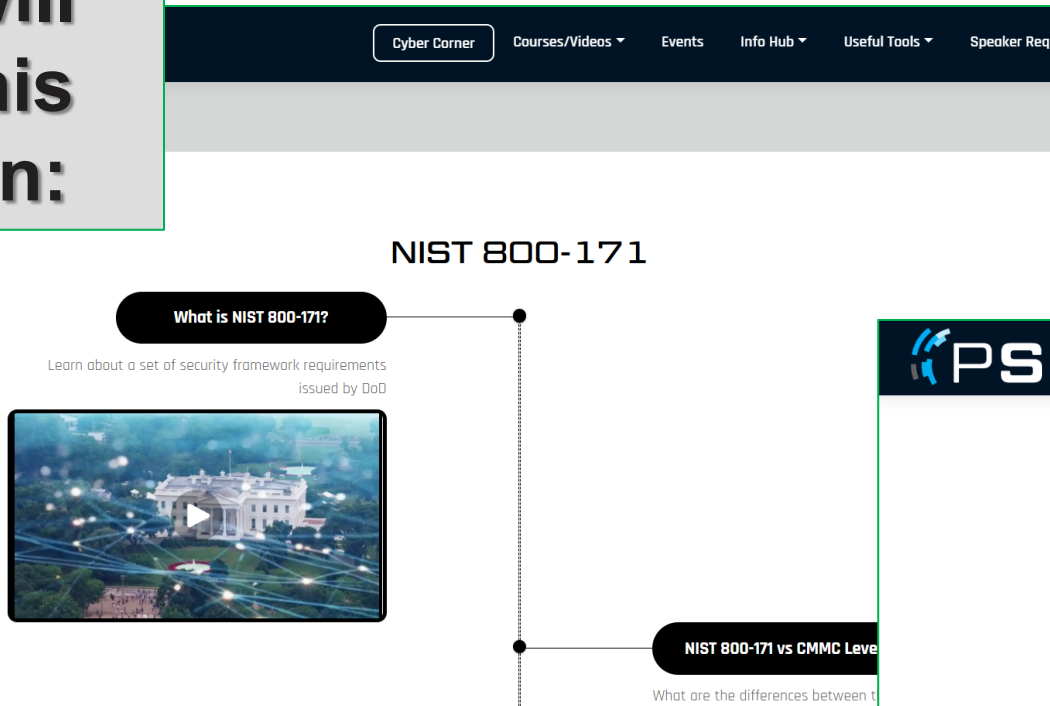
U.S. ARMY

4

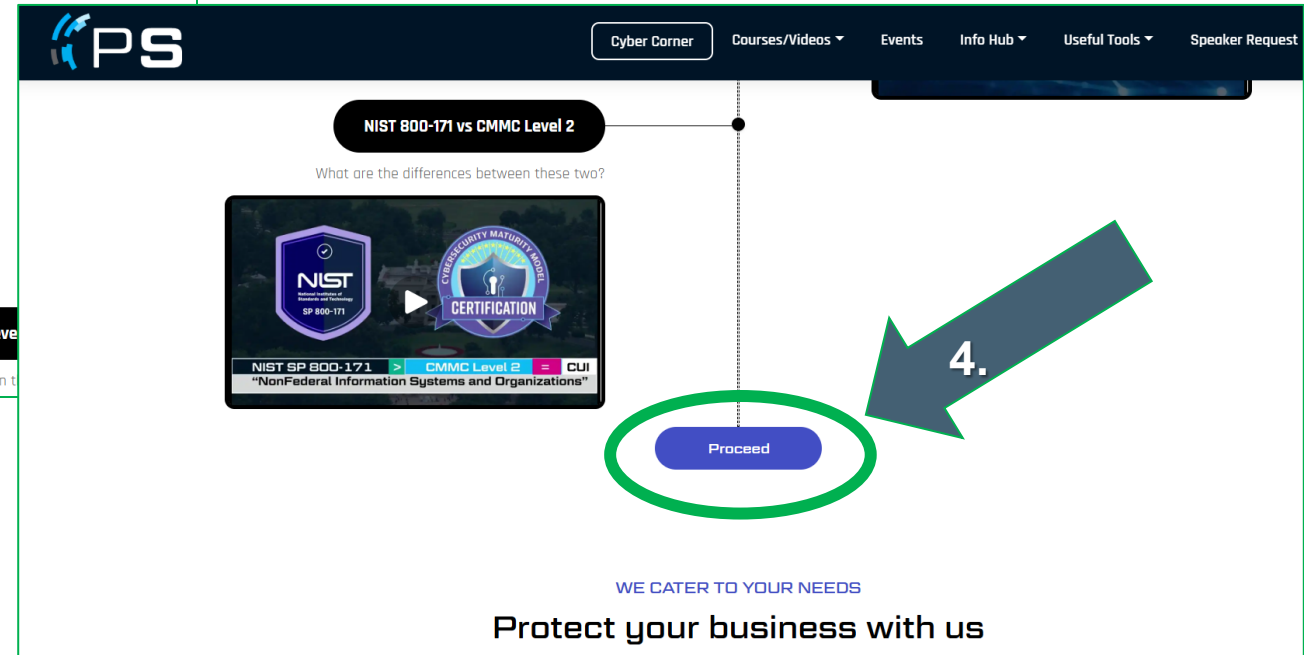


4. NAVIGATE TO THE SELF-ASSESSMENT

You will see this screen:



Scroll down and click "Proceed":





U.S. ARMY

5. BEGIN SELF-ASSESSMENT

5



Click “Start Now”

Cyber Self Assessments

If you are handling Controlled Unclassified Information (CUI) or Federal Contract Information (FCI) on your network or information systems, there are compliance standards you are required to meet. Taking one of our Cyber Self Assessments will help you determine your current level of security based on NIST 800-171, CMMC Level 1, and CMMC Level 2 requirements. These self assessments serve as a great first step in your cybersecurity journey. Need more help? Click the yellow question mark in the bottom right-hand corner of the webpage to have a Cyber Advisor contact you.

5.

Start Now

CYBER SELF ASSESSMENT

How secure is your organization?

Select the NIST 800-171 or CMMC self-assessments to evaluate your organization



Cyber Corner

Courses/

y Account

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.

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...

Start Assessment

Scroll down to the NIST section and click “Start Assessment”



U.S. ARMY

6



6. CONDUCT SELF-ASSESSMENT

PS

Cyber Corner

Courses/Videos

Events

Info Hub

Useful Tools

Speaker Request

My Account

NIST 800-171 - Self-Assessment

Access Control

Awareness and Training

Audit and Accountability

Configuration Management

Identification and Authentication

Incident Response

Maintenance

Media Protection

Personnel Security

Physical Protection

Risk Assessment

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, or both?

> Tooltip

|

Explainer Video

Authorized users are identified.

Processes acting on behalf of authorized users are identified.

Devices (and other systems) authorized to connect to the system are identified.

System access is limited to authorized users.

System access is limited to processes acting on behalf of authorized users.

System access is limited to authorized devices (including other systems).

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.

System access is limited to the defined types of transactions and functions for authorized users.

☐ Yes

☐ No

☐ Not Applicable

☐ Answer Later

☐ Yes

☐ No

☐ Not Applicable

☐ Answer Later

3. Do you control the flow of CUI in accordance with approved authorizations?

> Tooltip

|

Explainer Video

Information flow control policies are defined.

Methods and enforcement mechanisms are defined.

Designated sources and destinations for CUI in interconnected systems are identified.

Authorizations for controlling the flow of CUI are defined.

Approved authorizations for controlling the flow of CUI are defined.

4. Does your organization separate the duties of individuals to reduce the risk of malevolent activity without collusion?

> Tooltip

|

Explainer Video

The duties of individuals requiring separation are defined.

Responsibilities for duties that require separation are assigned to separate individuals.

Access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals.

☐ Yes

☐ No

☐ Not Applicable

☐ Answer Later

☐ Yes

☐ No

☐ Not Applicable

☐ Answer Later

☐ Yes

☐ No

☐ Not Applicable

☐ Answer Later

5. Does your organization employ the principle of least privilege, including for specific security functions and privileged accounts?

> Tooltip

|

Explainer Video

Privileged accounts are identified for security.

Access to privileged accounts is authorized in accordance with the principle of least privilege.

Security functions are identified.

Access to security functions is authorized in accordance with the principle of least privilege.

☐ Yes

☐ No

☐ Not Applicable

☐ Answer Later

☐ Yes

☐ No

☐ Not Applicable

☐ Answer Later

☐ Yes

☐ No

☐ Not Applicable

☐ Answer Later

☐ Yes

☐ No

☐ Not Applicable

☐ Answer Later

6. Do you use non-privileged accounts or roles when accessing non-security functions?

> Tooltip

|

Explainer Video

Need help? Click on
“Tooltip” or “Explainer
Video”

and so forth..... there are **109** sections total



U.S. ARMY

7. COMPLETE SELF-ASSESSMENT AND NAVIGATE TO DASHBOARD



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

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

109. Do you identify unauthorized use of organizational systems?

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

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

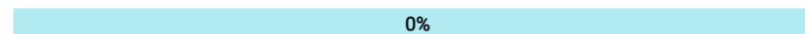
Unauthorized use of the system is identified. ☐ Yes ☐ No ☐ Not Applicable ☒ Answer Later

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

NIST 800-171 - Self-Assessment

Your responses are saved.

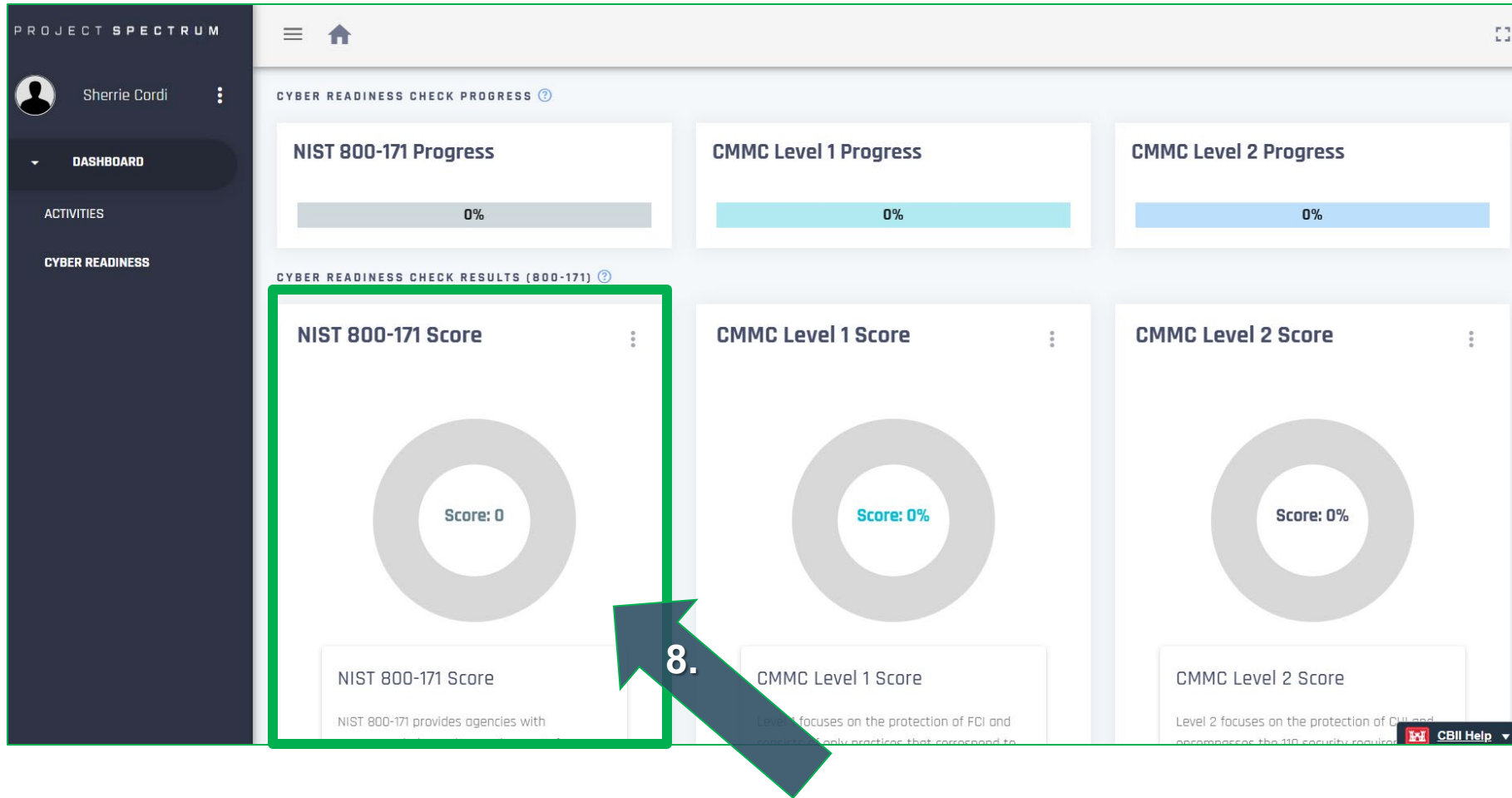
Progress:



[Go to Dashboard](#)

[Back to Cyber Readiness Check](#)

8. VIEW YOUR NIST SCORE





U.S. ARMY

9. NAVIGATE TO SPRS (SUPPLIER PERFORMANCE RISK SYSTEM)



CYBERSECURITY MATURITY MODEL CERTIFICATION

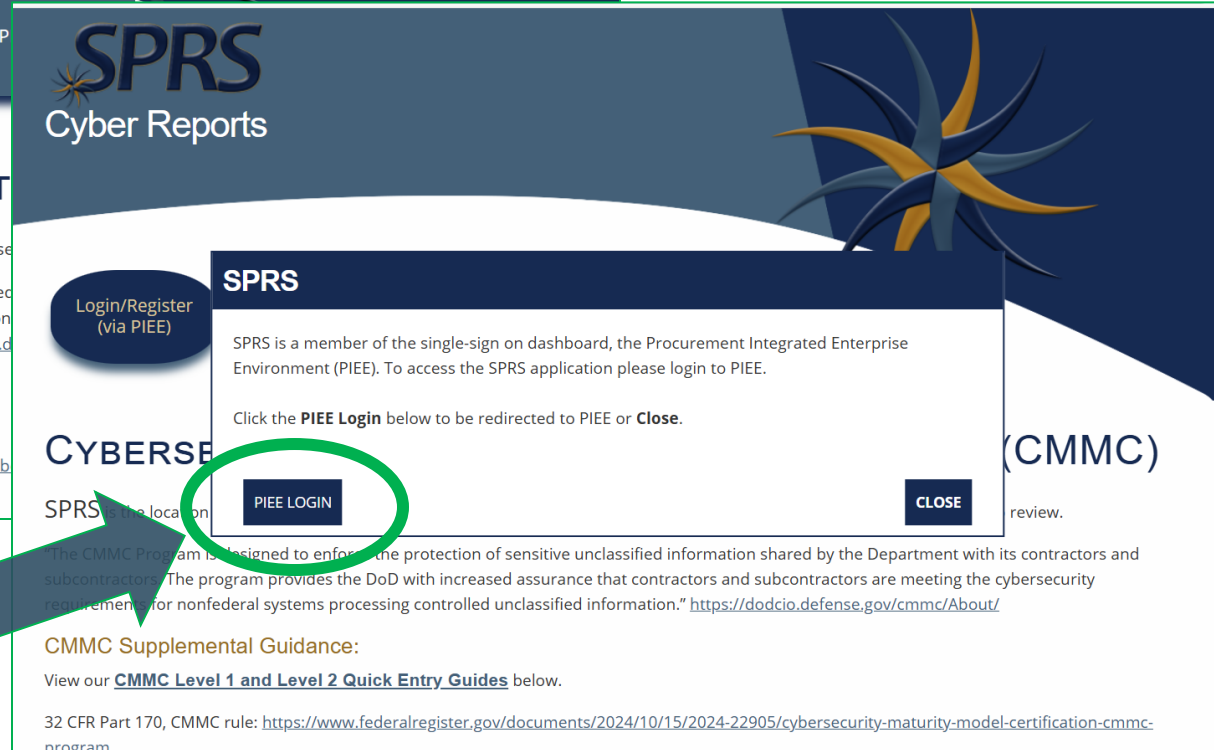
SPRS is the location for vendors to certify CMMC Level 1 and Level 2 compliance and for the defense

"The CMMC Program is designed to enforce the protection of sensitive unclassified information shared by the Department 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." <https://dodcio.defense.gov/cmmc/About/>

CMMC Supplemental Guidance:

View our [CMMC Level 1 and Level 2 Quick Entry Guides](#) below.

32 CFR Part 170, CMMC rule: <https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program>

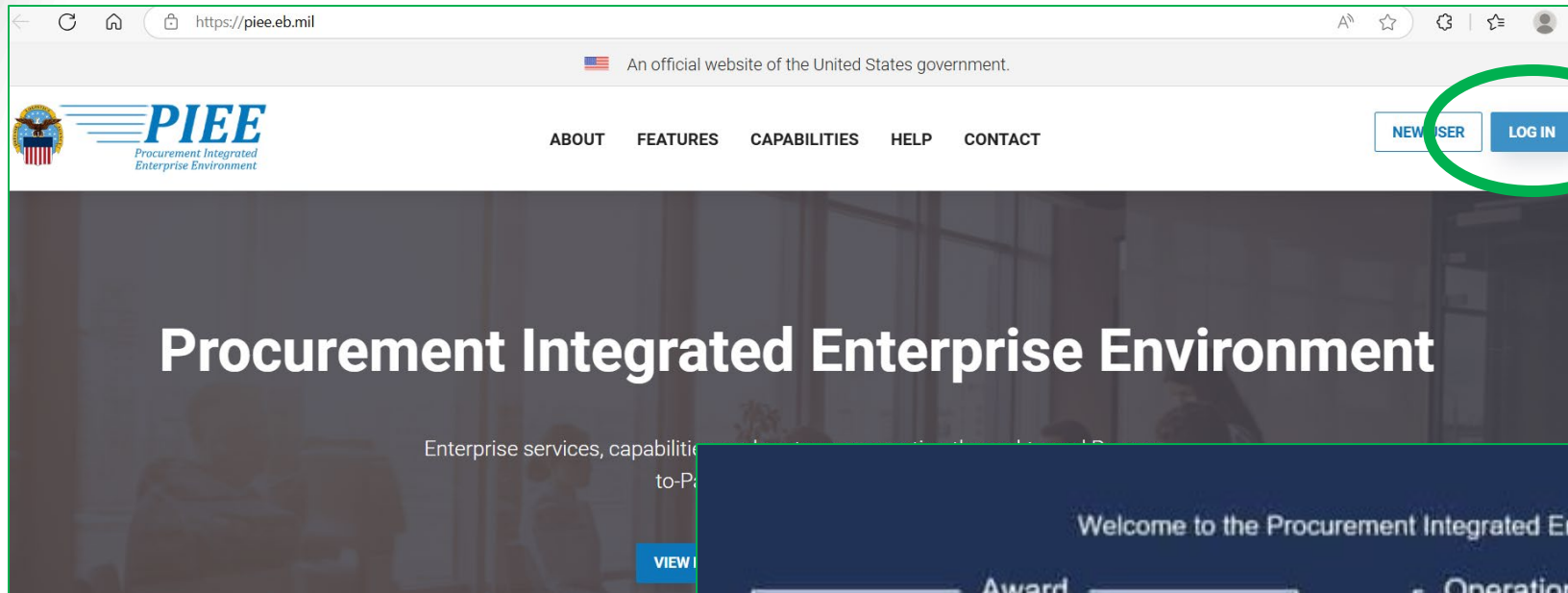




U.S. ARMY

9. CONT.

10





U.S. ARMY

HOW TO UPLOAD YOUR NIST SCORE

YOU MUST BE REGISTERED IN SAM.GOV AND HAVE A CAGE CODE



11

1. Get Access to SPRS

You must use the Procurement Integrated Enterprise Environment (PIEE) to access SPRS.

- Go to: <https://piee.eb.mil/>
- Click "Register" if you don't already have an account.
- During registration: Choose "SPRS" as the application.
- Select your appropriate role (usually "Contractor").
- Enter your CAGE Code (company identifier). *Your account must be approved by your company's Electronic Business Point of Contact (EB POC) in SAM.gov.*

2. Prepare Your NIST Score Submission

- Have the following info ready:
 - Your CAGE Code
 - The NIST 800-171 score
 - Date of the assessment
 - A Plan of Action & Milestones (POA&M) *if you have not implemented all 110 controls*
 - The expected date for achieving a perfect score (*if applicable*)

3. Submit the Score in SPRSLog into

- <https://piee.eb.mil/>
- Navigate to SPRS > NIST SP 800-171 Assessment
- Click "Create New Assessment"
- Enter all required data and submit

💡 Tips:

You do **not** upload a document — you just input your score and related information.

Only self-assessments are required for CMMC Level 1 and some Level 2 (until 2026).

Your score is valid for 3 years, unless your cybersecurity posture changes significantly.



U.S. ARMY



SUMMARY FOR SB CONTRACTORS

12



If you're just starting:

1. **Use Project Spectrum** to get free guidance and tools.
2. **Talk to your local APEX Accelerator** for personal help.
3. **Use the NIST templates** to perform a self-assessment.
4. **Submit your score in SPRS via PIEE.**
5. **Start planning now** for CMMC Level 1 by Oct 2025.



U.S. ARMY

RESOURCES FOR SMALL BUSINESS CONTRACTORS

CMMC & NIST 800-171

Resource	Description	Link
Business & Local Support		
APEX Accelerators (formerly PTACs)	Free one-on-one help for contractors on compliance, contracting, and cybersecurity	apexaccelerators.us
SBA Small Business Development Centers (SBDCs)	Help with business growth, federal readiness, and cybersecurity readiness	americassbdc.org
Government & Official Resources		
Project Spectrum	Free tools, templates, training, and self-assessments specifically for small businesses	projectspectrum.io
Cyber AB (Accreditation Body)	Authoritative CMMC info, list of assessors (C3PAOs), and training	cyberab.org
NIST 800-171	Official requirements for protecting Controlled Unclassified Information (CUI)	csrc.nist.gov/publications/detail/sp/800-171
NIST 800-171A	Assessment procedures to evaluate compliance	csrc.nist.gov/publications/detail/sp/800-171a
Defense Contract Management Agency (DCMA) DIBCAC	Conducts DoD assessments and publishes scoring methodology	dcma.mil
Supplier Performance Risk System (SPRS)	Required portal to submit your NIST score	sprs.csd.disa.mil (login via PIEE)
Procurement Integrated Enterprise Environment (PIEE)	Register to access SPRS and upload NIST scores	piee.eb.mil
CMMC Assessors (C3PAOs)	Independent third parties for Level 2c or Level 3 certification	Cyber AB Marketplace



U.S. ARMY

RESOURCES FOR SMALL BUSINESS CONTRACTORS (CONT.)

CMMC & NIST 800-171



Other Resources of Interest

Resource	Purpose
NSA Cybersecurity Guidance	Advanced hardening tips and public cybersecurity advisories
US Cybersecurity & Infrastructure Security Agency (CISA)	Alerts, best practices, and risk management tools



Additional Tools & Templates

Tool	Use
NIST 800-171 DoD Assessment Scoring Template (Excel)	Used to calculate your NIST score before submission
POA&M Template (Plan of Action & Milestones)	Used to document incomplete controls and mitigation plans



QUESTIONS?

(I'M NOT A CMMC EXPERT, BUT
I CAN HELP YOU FIND ONE!)



Sherrie Cordi

Sherrie.cordi@usace.army.mil

(901) 568-0614 (call or text)