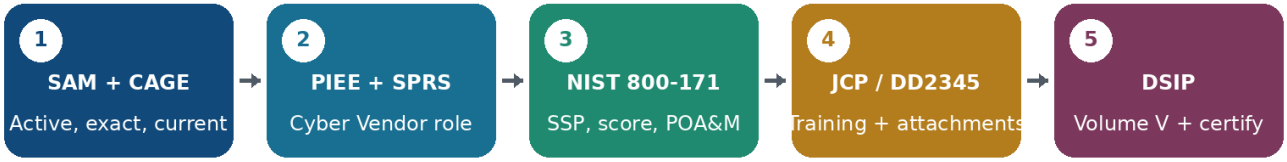
U.S. SMALL BUSINESS IMPLEMENTATION GUIDE

From SAM.gov to JCP / DD Form 2345

How to prepare for export-controlled DoD SBIR and STTR proposals - without false certifications



Version 1.0 | 21 July 2026

Built from current DLA, SPRS, DFARS, and Defense SBIR/STTR guidance. All portal screenshots are anonymized and flattened.

Scope and limitation

This guide explains the administrative, cybersecurity-documentation, and proposal-submission workflow. It does not guarantee approval or replace an export-control jurisdiction/classification determination, legal advice, or the exact instructions in a specific BAA/CSO topic.

Read this first: the critical correction

It is NIST SP 800-171 - not ISO 9000

The JCP cybersecurity gate is a NIST SP 800-171 DoD Basic Assessment posted in SPRS. ISO 9000/9001 quality-management certification is unrelated to this JCP prerequisite.

Do not check Yes before it is true

Current DLA guidance says an entity without a NIST SP 800-171 assessment documented in SPRS cannot apply for JCP certification. The JCP portal also asks you to certify that the assessment is documented and that the company complies with the cited DFARS clauses. An intent to assess later is not a valid substitute.

A company can perform the Basic Assessment internally, but the score must be based on a real System Security Plan (SSP), a review of the applicable NIST requirements, and the DoD Assessment Methodology. SPRS stores the result; it does not perform the assessment for you.

What JCP does - and does not do

JCP / DD Form 2345 helps with	JCP does not replace
Eligibility to receive certain nonpublic, unclassified military technical data	DDTC registration when required
Demonstrating a legitimate business need for controlled technical data	An ITAR or EAR export license / authorization
Supporting an ITAR-marked SBIR/STTR proposal when the solicitation requires DD Form 2345	A USML/ECCN classification decision
Identifying a responsible Data Custodian and certified physical CAGE location	NIST implementation, CMMC status, a Technology Control Plan, or access controls

Treat JCP as one component of an export-control and cybersecurity program. A JCP certificate is not a blanket statement that every product, service, employee, cloud system, transfer, or foreign-person interaction is authorized.

Use this guide in this order

1. Confirm the topic is export-controlled and identify the proposal-specific requirement.
2. Create a defensible NIST SP 800-171 assessment package and post the summary in SPRS.
3. Prepare the JCP applicant, Data Custodian, workstation/server details, and attachments.
4. Submit the JCP application truthfully and save evidence of actual submission.
5. Upload the approved DD Form 2345 or accepted application evidence to DSIP Volume V, then complete corporate certification.

Guide map

Part	What you will accomplish
1. Proposal decision	Determine whether the topic/work is ITAR, EAR, or neither; identify the exact DSIP requirement.
2. NIST package	Build the SSP, control assessment, score, evidence file, and POA&M needed for a Basic Assessment.
3. PIEE and SPRS	Obtain the SPRS Cyber Vendor User role and enter the assessment summary.
4. JCP package	Gather current proof of business, signed training certificate, Data Custodian information, and conditional attachments.
5. JCP portal	Link/create the organization, pass the pre-screen, complete the application, sign, and submit.
6. DSIP submission	Upload approved certification or permitted evidence in Volume V and complete final corporate certification.
7. Sustainment	Maintain SAM, NIST/SPRS, JCP, export-control controls, and revisions after submission.

Minimum readiness checklist

[ ] Active SAM registration; legal name, address, UEI, and CAGE are exact and current.
[ ] SAM will not expire within 90 days of the JCP application.
[ ] PIEE account and a Contractor Account Administrator (CAM) for the CAGE.
[ ] SPRS Cyber Vendor User role is active.
[ ] NIST SP 800-171 Basic Assessment completed from an SSP and posted in SPRS.
[ ] Primary Data Custodian selected and associated with the physical CAGE location.
[ ] Designated U.S.-located computer/server and permanent hardware MAC identified.
[ ] Secretary of State proof of business/good standing dated within the last 12 months.
[ ] Current DLA Proper Handling training reviewed; Page 15 completed and signed.
[ ] USML/CCL, DDTC registration, and license answers documented and supported.
[ ] JCP portal account with Google Authenticator.
[ ] Specific SBIR/STTR BAA, Component instructions, topic, and DSIP deadline reviewed.

> **Timing reality**
> DLA currently reports extended processing and advises initiating an initial JCP application well before the need date. Do not plan on same-day approval. A proposal may use evidence of application submission only when the controlling solicitation expressly allows it.

1. Determine what the SBIR/STTR topic actually requires

Start with the current program BAA/CSO, Component-specific instructions, topic text, amendments, and DSIP Topic Q&A. The topic-specific instructions control when they differ from general guidance.

1.1 Decision sequence

1. Does the topic identify ITAR, EAR, export-controlled data, controlled technical information, CUI, or U.S.-person restrictions?
2. Will the proposed work receive, generate, store, transmit, discuss, or deliver controlled technical data?
3. What documentation must be included at proposal submission versus before award?
4. Does the topic specify a projected CMMC level, facility clearance, foreign-national restriction, or approved system?
5. Does the Component accept an approved DD Form 2345 only, or an approved form OR evidence of a submitted JCP application?

> **2026 Defense SBIR BAA example**
>
> Section 3.2 of the supplied 2026 BAA states that when any portion of the proposed effort is subject to ITAR, the small business must provide a fully certified DD Form 2345 or evidence of application submission in Volume V. Always confirm the same language in the currently controlling solicitation.

1.2 Answer DSIP export-control questions from the facts

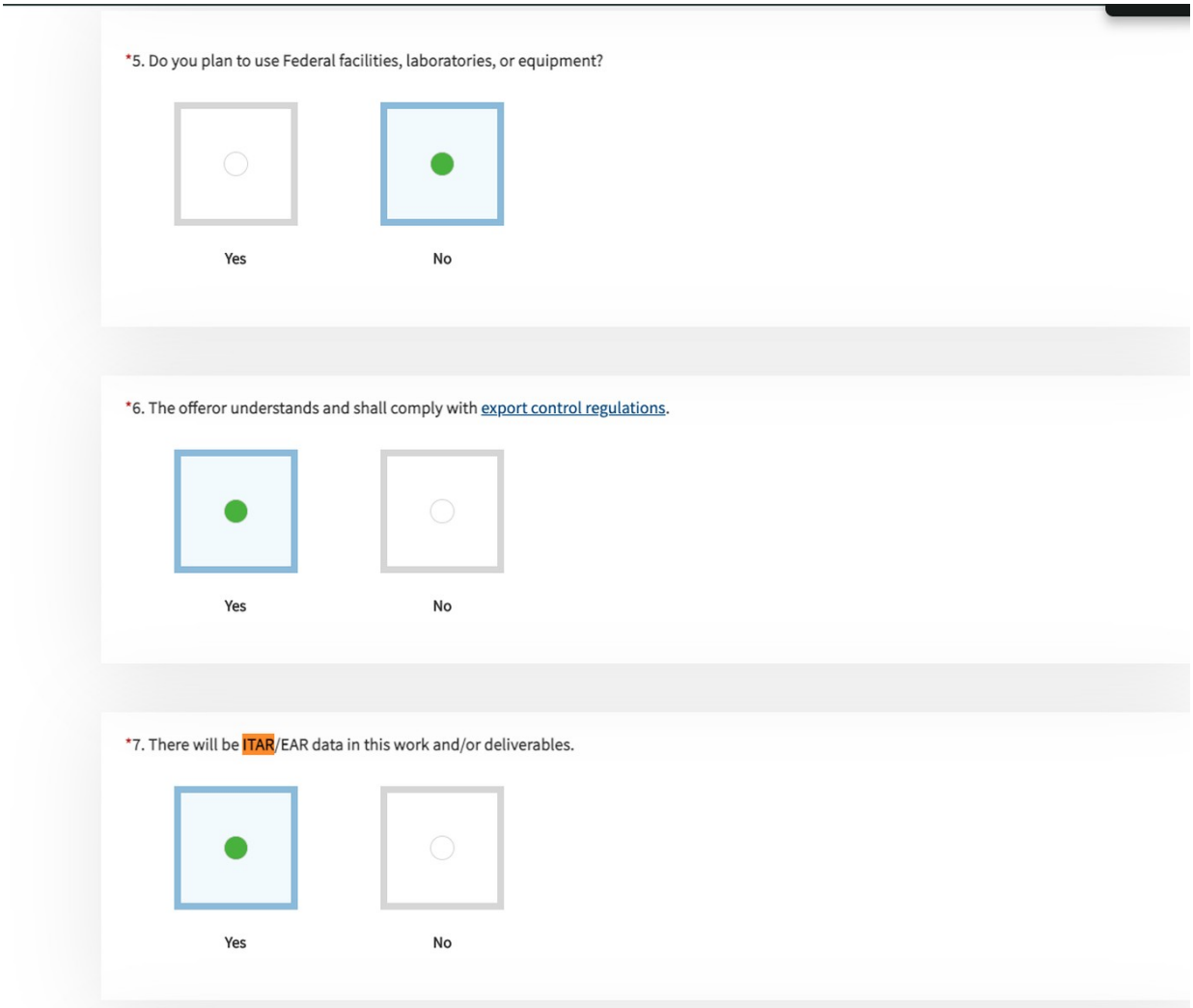


Figure 1. Typical DSIP export-control certification questions. The illustrated selections are not universal answers.

DSIP item	How to decide
Use Federal facilities/labs/equipment?	Select Yes only when the proposed work actually uses Government facilities, laboratories, or equipment.
Understand and comply with export-control regulations?	Select Yes only after the responsible corporate official accepts the obligation and the company has a workable compliance path.
ITAR/EAR data in work or deliverables?	Select Yes when the proposal will receive, generate, handle, or deliver controlled data. Do not select Yes merely because the customer is DoD.

> **Protect proposal content**
> Do not place export-controlled, classified, or sensitive technical details into public abstracts or other fields that may be publicly released. Follow proprietary markings and distribution instructions in the current BAA.

1.3 Separate JCP from ITAR/EAR classification and licensing

Question	Owner / system	Result
Is an item, software package, technical datum, or defense service on the USML?	State Department / DDTC	ITAR jurisdiction; registration or authorization may be required.
If not ITAR, what ECCN applies?	Commerce Department / BIS	CCL classification or EAR99; license analysis by destination, end user, and end use.
May this company receive certain nonpublic unclassified military technical data?	DLA Joint Certification Program	JCP / DD Form 2345 certification.
Is the contractor system prepared to safeguard covered defense information?	Company; NIST/DFARS; SPRS	SSP, Basic Assessment score, POA&M, and evidence.

The same project may involve both ITAR-controlled and EAR-controlled items. Answer the JCP USML/CCL questions from a documented classification analysis, not from the topic title alone.

1.4 Minimum export-control controls before access

- Written jurisdiction/classification record for hardware, software, technical data, and services.
- U.S.-person/foreign-person access review for employees, consultants, subcontractors, visitors, and cloud administrators.
- Technology Control Plan or equivalent procedures for repositories, meetings, travel, publishing, and releases.
- Approved systems and accounts; least privilege, MFA, logging, encryption, backups, and incident response.
- Review before sharing data with subcontractors, universities, foreign persons, or outside service providers.
- No controlled data in personal email, unapproved consumer file sharing, or public/consumer AI services.

USML (22 CFR Part 121): Open official resource

BIS classification and CCL: Open official resource

DDTC DECCS portal: Open official resource

2. Build the NIST SP 800-171 Basic Assessment package

> **SPRS is the filing cabinet, not the assessment tool**
> SPRS stores assessment summary data. It does not inspect your network, create the SSP, test controls, calculate the score, or generate a POA&M.

2.1 Define the system boundary first

Identify the actual information system that will process, store, or transmit covered defense information or export-controlled technical data. For a small business, a deliberately isolated enclave may reduce scope, but it must be real, documented, and technically separated from out-of-scope systems.

Boundary element	Document
People	Authorized users, administrators, contractors, support personnel, citizenship/access basis.
Devices	Laptops, desktops, mobile devices, servers, removable media, printers, network equipment.
Cloud/services	Identity provider, email, collaboration, repositories, hosting, ticketing, backup, security tools.
Connections	Internet, VPN, remote access, APIs, subcontractors, customer systems, backups, mobile hotspots.
Locations	Office, home office, data center, approved remote-work sites, travel restrictions.
Data flow	Where controlled data enters, is processed, is stored, is backed up, and leaves the boundary.

2.2 Required internal package

Artifact	What it must contain	Usually uploaded to JCP?
System Security Plan (SSP)	System boundary, architecture, roles, environment, and implementation narrative for each applicable security requirement.	No - retain internally unless requested.
Control assessment workbook	Requirement-by-requirement implementation status, objective evidence, owner, test date, and finding.	No.
DoD scoring sheet	Deductions calculated under the official DoD methodology; summary score and assessment date.	Summary entered in SPRS.
POA&M	Deficiencies, milestones, resources, owners, target dates, dependencies, and closure evidence.	No - completion date summarized in SPRS.
Evidence repository	Screenshots, configurations, policies, logs, training records, tickets, inventories, and test results.	No - preserve for review.
Asset/account/data-flow inventory	All in-scope components and authorized accounts, mapped to the SSP.	No.

2.3 Conduct and score the Basic Assessment

1. Use the NIST revision and DoD methodology required by the current solicitation and SPRS guidance. The supplied 2026 SBIR BAA references the 110 requirements in NIST SP 800-171 Revision 2.
2. For every requirement, verify implementation against objective evidence. A policy statement alone does not prove technical implementation.
3. Start from the methodology maximum score and apply the required deductions. Do not award partial credit when the methodology does not permit it.
4. Record unresolved requirements in the POA&M and assign a realistic completion date.
5. Have an accountable executive review the scope, SSP, evidence, score, and planned remediation before posting.

> **Do not enter an arbitrary 110**
>
> A score of 110 represents complete implementation under the methodology. A lower score can be posted, but the score, scope, SSP, and POA&M must be truthful. A posted score by itself does not prove full DFARS compliance or satisfy every contract/CMMC requirement.

2.4 Common small-business gaps to test

Area	Typical gap
Access control	Shared accounts, no separate admin account, uncontrolled remote access, stale users.
Authentication	MFA not enforced everywhere; weak service-account controls.
Logging	No centralized logs, insufficient retention, no review process.
Configuration	No secure baseline, unmanaged software, inconsistent patching.
Media	USB/removable media not restricted or tracked.
Incident response	No documented reporting, containment, evidence preservation, or cyber-incident workflow.
Cloud/subcontractors	No evaluation of provider responsibilities, location, foreign access, or flow-downs.
Training/personnel	No recurring security/export training or termination checklist.

2.5 Cybersecurity and CMMC are separate gates

A topic may require CMMC Level 1 or Level 2 in addition to the NIST Basic Assessment needed for JCP. Review the exact solicitation and award timing. Do not assume that a SPRS NIST score automatically creates a CMMC status or annual affirmation.

DFARS 252.204-7019/7020 and current policy: Open official resource

Official DoD Assessment Methodology: Open official resource

NIST SP 800-171 publication: Open official resource

DoD CMMC information: Open official resource

3. Obtain PIEE and SPRS access

3.1 Confirm the PIEE Contractor Account Administrator

Every CAGE group needs a Contractor Account Administrator (CAM). The CAM approves privileged roles for the company. A one-person company may still need to establish and use this role.

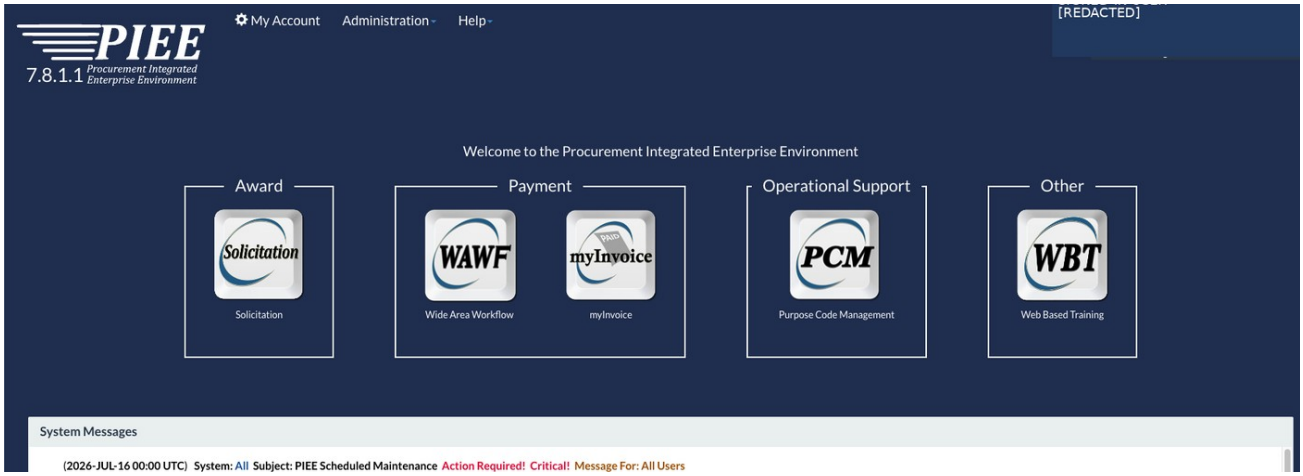


Figure 2. PIEE home before the SPRS tile/role is active.

3.2 Request the SPRS Cyber Vendor User role

1. Sign in to PIEE.
2. Open My Account > Add Additional Roles.
3. Select SPRS - Supplier Performance Risk System.
4. Select SPRS Cyber Vendor User.
5. Select the correct CAGE/vendor group and enter a business justification.
6. Submit the request; the CAM approves it. Log out and back in after activation.

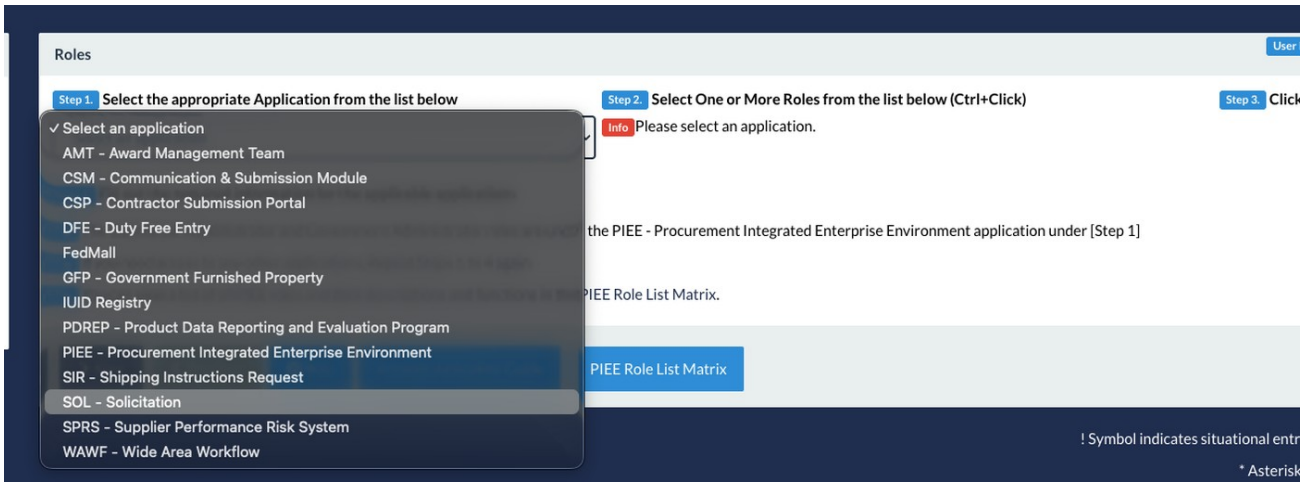


Figure 3. Select the SPRS application in PIEE.

> **Suggested role justification**
>
> Requesting SPRS Cyber Vendor User access to enter and maintain the company's NIST SP 800-171 Basic Assessment in support of JCP certification and DoD contracting requirements.

3.3 Verify the role is Active

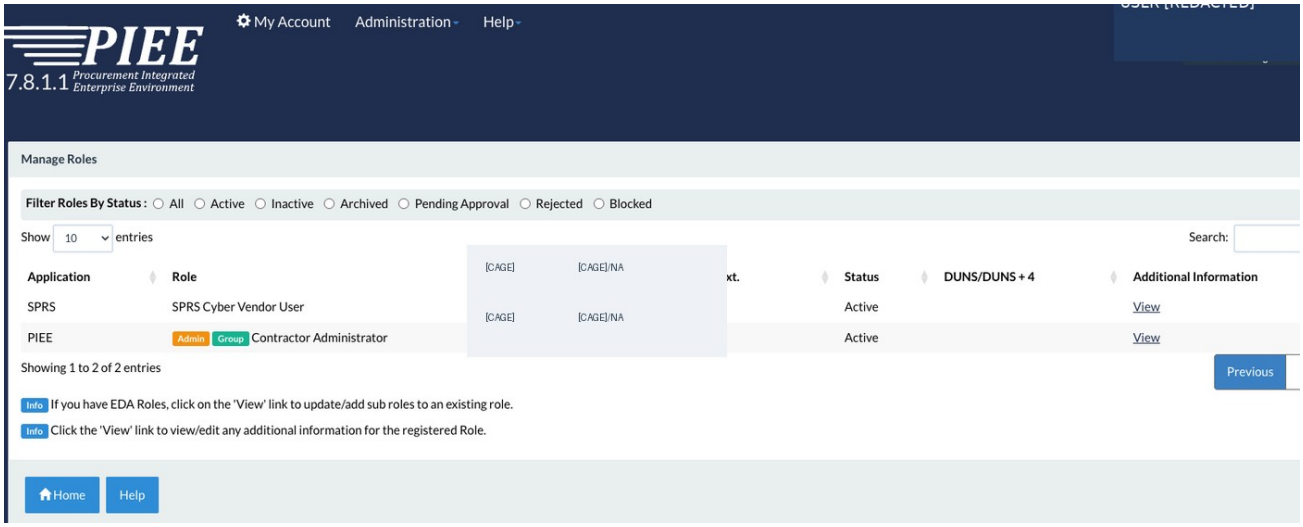


Figure 4. Manage Roles should show SPRS Cyber Vendor User - Active for the correct CAGE hierarchy.

If the SPRS tile is visible but the Add New NIST Assessment button is missing, verify that the privileged SPRS Cyber Vendor User role - not only a support/view role - is active. Sign out and back in after approval.

3.4 Open Cyber Reports in SPRS

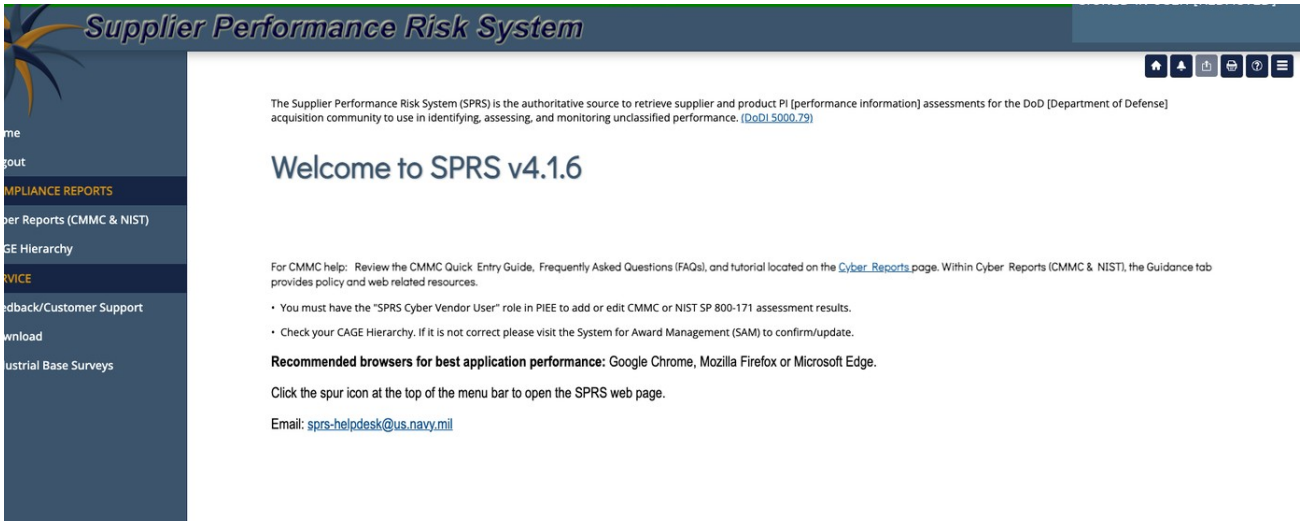


Figure 5. SPRS home. Open Cyber Reports (CMMC & NIST) from the left menu.

PIEE: Open official resource
SPRS access instructions: Open official resource
SPRS Cyber Reports role guide: Open official resource

4. Post the Basic Assessment summary in SPRS

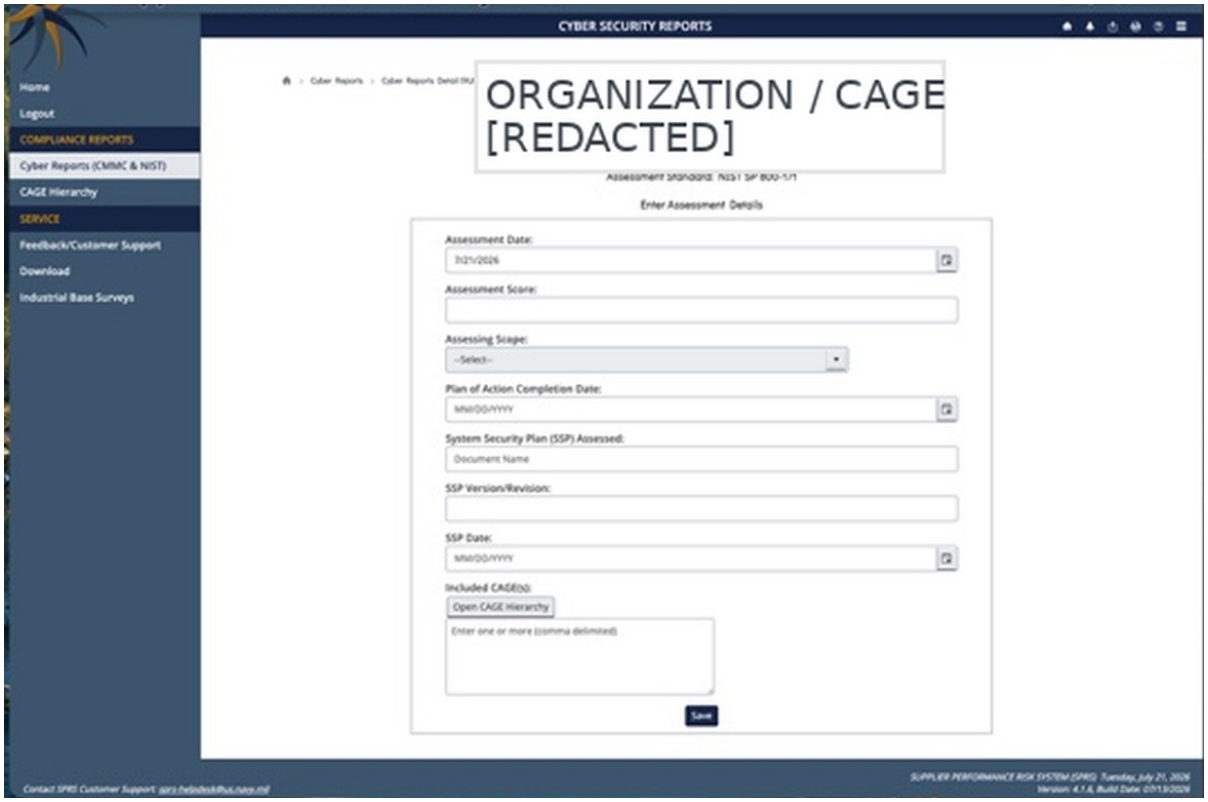


Figure 6. SPRS NIST assessment summary entry form. Organization and CAGE are redacted.

SPRS field	Enter
Assessment date	Date the assessment was actually completed.
Assessment score	DoD methodology summary score - not a percentage and not a planned score.
Assessing scope	Enterprise, Enclave, or Contract, matching the SSP and actual system boundary.
Plan of Action completion date	Target date supported by the associated POA&M, when applicable.
SSP assessed	Exact internal SSP title/document name.
SSP version/revision	Current approved revision.
SSP date	Effective/approval date of the assessed SSP.
Included CAGE(s)	CAGE codes actually supported by the assessed system/SSP.

4.1 Save evidence of the posted record

[ ] SPRS assessment details page showing the CAGE, date, score, scope, SSP name/version/date, and status.
[ ] Internal approval record identifying who reviewed the score.
[ ] The SSP, workbook, scoring sheet, POA&M, and evidence repository as of the assessment date.
[ ] Any later edits, closure evidence, and reassessment records.

> **Validity**
> DLA states the NIST assessment must be renewed every three years unless a solicitation or contract requires a shorter period. Reassess sooner after material changes to the system boundary or security posture.

SPRS NIST information: Open official resource
SPRS NIST Quick Entry Guide: Open official resource

5. Assemble the JCP / DD Form 2345 application package

5.1 Mandatory prerequisites before opening the application

Item	Acceptance standard
SAM/CAGE	Active and accurate; DLA says SAM should not expire within 90 days of application.
NIST in SPRS	Completed Basic Assessment summary actually posted for the relevant CAGE/system.
Data Custodian	Company employee/authorized person at the physical CAGE site who can control access and coordinate internally.
Portal 2FA	Google Authenticator installed and working.
Proof of business	Secretary of State good-standing/equivalent document from the state of incorporation in SAM, dated within 12 months.
Training certificate	Page 15 of the current DLA Proper Handling training completed and signed.

5.2 Mandatory and conditional attachments

Attachment	When required	Preparation rule
Proof of Business	All U.S. applicants	Current good-standing/equivalent PDF. Articles of Organization alone may not prove current status.
Certification Statement of Export Control Compliance	All applicants	Read current training and sign Page 15 as the Data Custodian/authorized signer indicated.
DDTC registration letter	If application says the entity is registered with DDTC	Current, matching legal name/address; include supporting form if directed for mismatches.
Export license	If application says the entity possesses one	Current license and relevant supporting documentation.
TAA / MLA / distribution agreement	When answers or business arrangement trigger it	Upload the current executed/approved document as directed.
Other evidence	When requested by analyst	Use the secure portal and avoid unnecessary PII.

> **Do not upload the internal NIST package by default**
>
> The SSP, control workbook, evidence repository, and POA&M are internal compliance records. The summary is posted in SPRS. Upload these documents only when an authorized Government reviewer requests them through an approved channel.

5.3 Complete the DLA Proper Handling training correctly

The generic DLA Customer Support training catalog is not the JCP training attachment. Use the current training PDF linked on the JCP page. Read the document, complete and sign the Certification Statement of Export Control Compliance on Page 15, and upload that signed page under the portal's training-certificate attachment type.

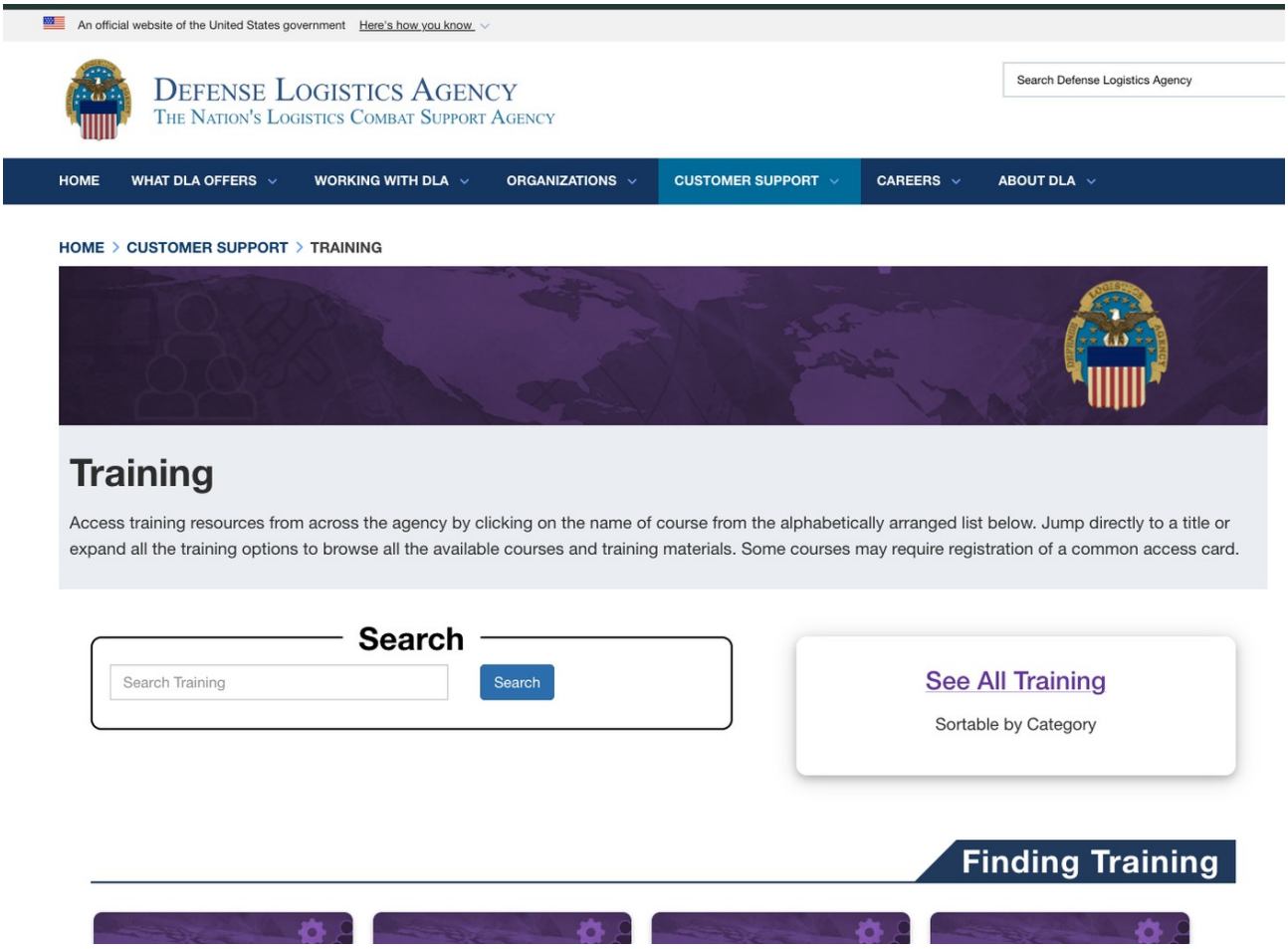


Figure 7. The general DLA training catalog is not the document the JCP attachment field is requesting.

Correct document

Introduction to Proper Handling of Export-Controlled Technical Data - current DLA PDF. Upload the completed Certification Statement on Page 15.

Current Proper Handling training PDF: Open official resource
Current JCP home/instructions: Open official resource
50-state proof-of-business examples: Open official resource

5.4 Select and document the Data Custodian

Requirement	Practical interpretation
Relationship	Use an employee/authorized company representative, not an outside proposal consultant with no operational authority.
CAGE/location	The person is associated with the certified physical site and can oversee data access for that CAGE.
Citizenship/status	Select only the statuses that are true and supported. Restrict access to authorized U.S. persons for a U.S. application.
Availability	Can respond to JCP analysts and coordinate with management, IT, contracts, security, and users.
Responsibility	Controls download, receipt, dissemination, storage, authorized-user list, training, and incident escalation.

5.5 Designated computer/server information

- Use a company-controlled computer or server physically located in the United States for a U.S. firm.
- Record the permanent hardware MAC address. Do not use 00:00:00:00:00:00, a placeholder, or a randomized/private Wi-Fi MAC.
- Follow the current portal help/JCP user guide for the IP address. Do not automatically substitute the public gateway IP for the device address. The current help guide directs Windows users to ipconfig /all.
- Record the physical street address where the designated device/server is located.
- Answer the server question from the actual architecture. A consumer cloud account is not automatically a company-controlled server for this field.
- If controlled data will be stored in a cloud enclave, confirm the architecture, location, provider responsibilities, and authorization before use.

> **Earlier-chat correction**
> A 192.168.x.x address may be the designated computer's local IPv4 address. It should not be replaced with a public IP merely because it is private. Follow the current JCP field help and the official user guide; provide additional network information only when requested.

6. Create or link the organization in the JCP portal

6.1 Register and sign in

1. Open the official JCP portal and register the individual user account.
2. Configure Google Authenticator and retain account-recovery information securely.
3. Search for the organization before creating a new one.
4. If it exists, request to join it. If it does not exist, create it using exact SAM/CAGE data.

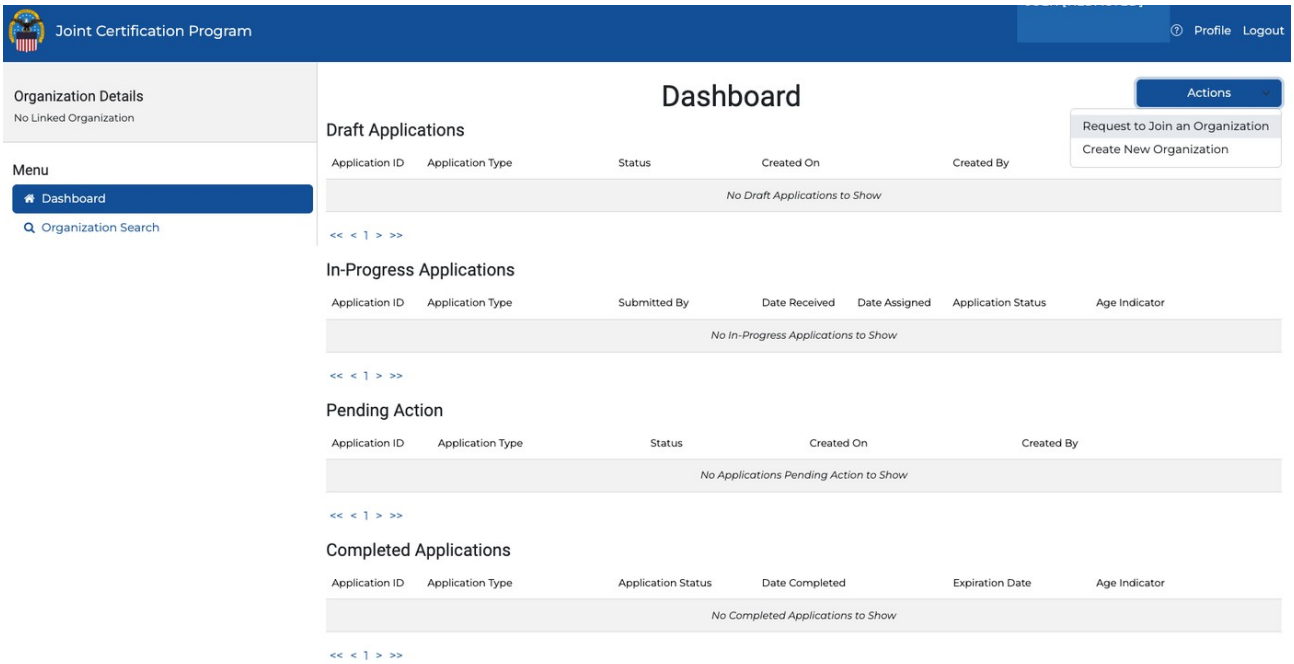


Figure 8. JCP dashboard before an organization is linked. Search first; request to join or create only when appropriate.

6.2 Organization-creation rules

Field	Rule
Legal business name	Exact legal name in SAM/CAGE - punctuation and suffix included.
Organization type	Choose the actual business model. A service-only software/R&D firm will commonly select Service Providers; a reseller/non-manufacturer should use the category that matches its operations.
Established date	Actual formation/incorporation date - not today's date.
Contact/address	Exact current business information consistent with SAM/CAGE.
Ownership	Mirror the company's SAM/FAR ownership disclosures. Do not invent a parent or automatically enter the applicant as both owners.

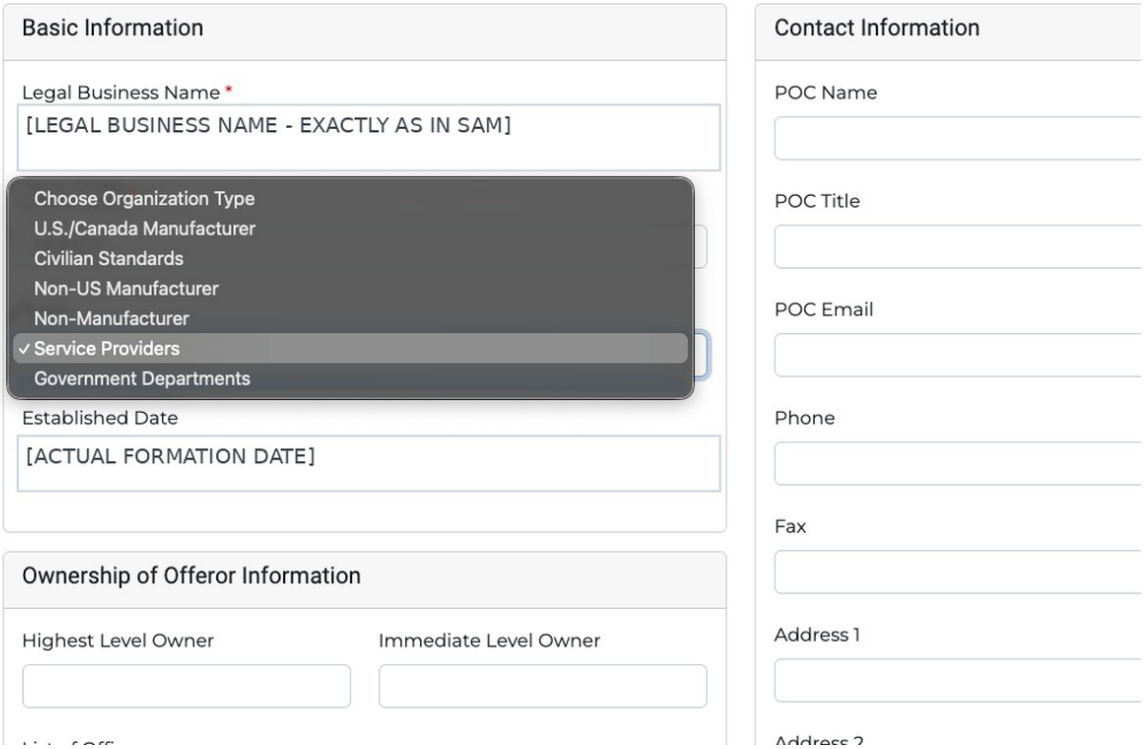


Figure 9. Example organization-type selection; use the category that matches the actual company.

6.3 Wait for SAM/CAGE synchronization

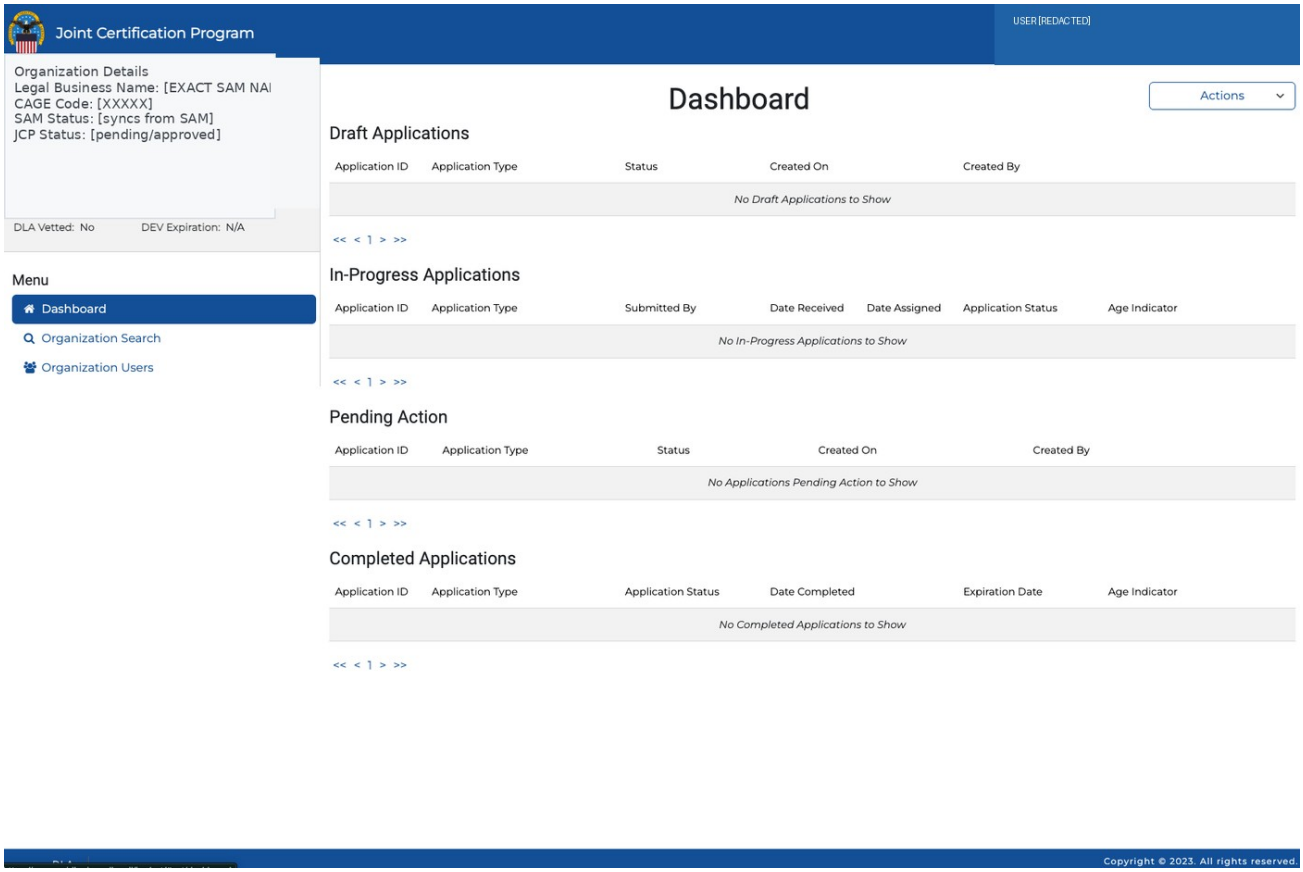


Figure 10. Linked organization dashboard. Verify exact SAM/CAGE data before starting the certification request.

The JCP user guide states that organization/SAM data can take up to 24 hours to populate. Do not submit when the legal name, address, UEI, CAGE, or SAM status is blank, stale, expired, or wrong. Correct the authoritative record first, then allow systems to synchronize.

6.4 Start a JCP Certification Request

From Actions, start the standard JCP Certification Request. Do not choose DLA Enhanced Validation (DEV) unless you also require DLA systems such as DIBBS/cFolders and meet those additional requirements.

> **DIBBS is not a standard Navy SBIR prerequisite**
> DIBBS is the DLA Internet Bid Board System. Standard JCP certification for a Navy/Army/Air Force SBIR does not by itself require DIBBS. DEV/DIBBS/cFolders access is a separate DLA path. Never claim DIBBS registration if it is not true.

JCP portal: Open official resource
JCP External User Guide (2026): Open official resource

7. Pass the JCP pre-screen truthfully

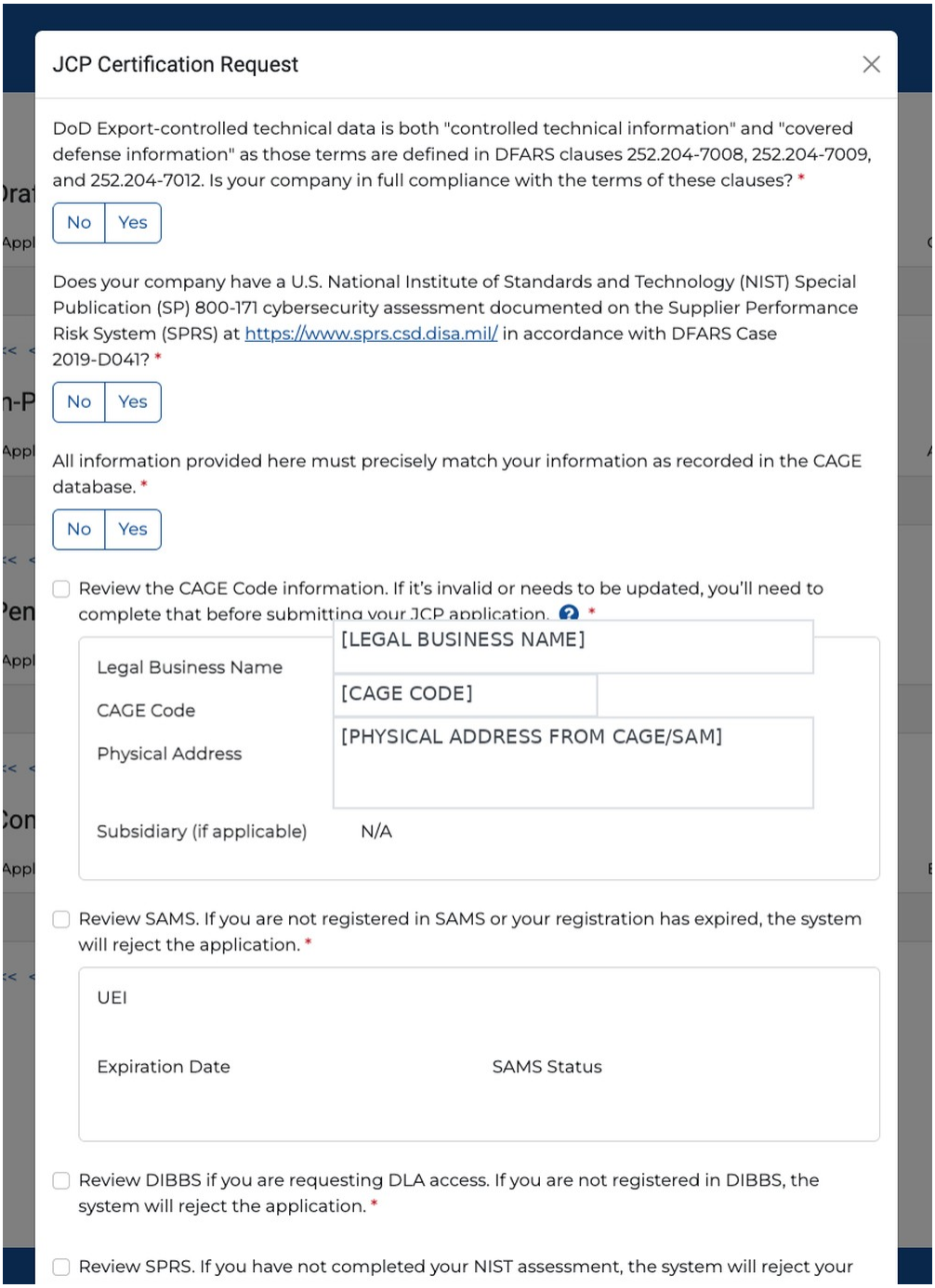


Figure 11. JCP pre-screen. The cybersecurity and CAGE/SAM statements are certifications, not future intentions.

Pre-screen statement	Select Yes only when
Full compliance with cited DFARS clauses	The company has evaluated the applicable clauses and its current SSP, implementation, POA&M, reporting, and safeguarding posture support the certification.
NIST SP 800-171 assessment documented in SPRS	The assessment summary is actually posted for the relevant CAGE/system and can be viewed in SPRS.
Information matches the CAGE database	Legal name, CAGE, physical address, and related information are exact.
SAM review	SAM is active, accurate, and sufficiently current for the application.
DIBBS review	Only when requesting DLA/DEV access and DIBBS registration actually applies. Contact JCP support if the portal forces this on a standard request.

No post-submission shortcut

Do not select Yes to the NIST/SPRS question on the theory that the assessment can be completed after the JCP application is submitted. DLA says the posted assessment is a prerequisite to applying.

8. Complete the JCP application - field by field

8.1 Applicant and submission type

Field	Company-agnostic entry rule
Current JCP certification?	No for a first application; otherwise enter the current number/expiration accurately.
Registered in SAM?	Yes only when the registration is active. Enter the current expiration date.
Submission type	Initial Submission for first certification; use Renewal or Revision only when applicable.
Physical address / CAGE	System-populated data must exactly match CAGE/SAM.

8.2 Data Custodian and device

Field	Entry rule
Name, title, direct phone, email	Business contact who will actually perform the Data Custodian role.
Citizenship/status checkboxes	Select every statement that is true and no statement that is not.
IP address	Designated device address per current portal help/JCP user guide.
MAC address	Permanent hardware-assigned MAC of the designated computer/server; no randomized value.
Physical address	Actual U.S. location of the designated computer/server.
Server?	Yes only when a server actually stores the data; provide its permanent MAC if requested.
Downloading/receiving/disseminating?	Yes only when the Data Custodian will perform and control those functions.

8.3 Contractor and business-activity answers

Field	How to answer
Prime / subcontractor / neither	Choose the relationship that supports the current legitimate business need. A company may have different roles across opportunities.

Field	How to answer
Describe what you do - 200 chars	State manufacturer, non-manufacturer, or service-only status and concise operations. Match SAM.
Items/products/services - 200 chars	List the actual offerings relevant to defense work.
NAICS/FSC	Use codes that actually appear in the company's SAM registration.
Manufacturers	For a service-only firm, leave blank when permitted and clearly state service-only/non-manufacturer. For resold products, list actual manufacturer names/CAGEs.

8.4 Export-control and access-purpose answers

Field	How to answer
Related to USML?	Yes only when the equipment/material/service is related to a documented USML category. Identify the category when requested.
Related to CCL?	Yes only when related to an identified ECCN/CCL category. ITAR and EAR answers are not automatically mutually exclusive across a portfolio.
Registered with DDTC?	Yes only with an active registration; upload current proof when required.
Possess export license?	Yes only with a current U.S. authorization; upload proof.
Purpose for access - 400 chars	Tie the need to U.S. Government solicitations/contracts/R&D and the controlled technical information required.
Specific U.S. system?	No unless a named Government system is actually required. Selecting DIBBS can trigger DEV/DLA prerequisites.
Government agency/contractor requiring JCP?	Identify the agency/topic/prime/POC when one exists; otherwise follow the portal guide for no current POC.

8.5 Safe sample narratives

Describe what you do - under 200 characters

Service-only small business providing software, engineering, research, systems integration, data analytics, prototype development, and technical services to U.S. Government customers.

Types of services - under 200 characters

Research and development, software engineering, data analytics, systems integration, testing, prototype development, and technical consulting aligned with NAICS codes in SAM.

Purpose for access - under 400 characters

We seek JCP certification to respond to and perform U.S. Department of Defense SBIR/STTR and other solicitations that require access to unclassified export-controlled technical information. Access will support proposal preparation, authorized research and development, engineering, testing, and contract performance.

Edit these samples so they are true. Do not add capabilities, products, classifications, customer relationships, or licenses the company does not have.

U.S. Relevant Business Activity Quick Guide: Open official resource

8.6 Authority to sign and Conditions of Certification

- Use the individual who can legally obligate the company to a binding contract.
- Use the same legal name/title consistently throughout the application and signature page.
- Read the Conditions of Certification in full before signing.
- Confirm the signer and Data Custodian understand access, dissemination, safeguarding, change-notification, and export-control obligations.
- Retain the signed application, attachment set, and submission confirmation.

> **Application evidence begins after Submit**
> A Draft application or screenshot of partially completed fields is not evidence of application submission. Evidence should show the application number, legal entity/CAGE, submitted status, and submission date/time.

9. Upload attachments, sign, and submit

9.1 Recommended file set

Filename	Portal use
01_Secretary_of_State_Good_Standing.pdf	Mandatory Proof of Business.
02_Proper_Handling_Page15_Signed.pdf	Mandatory training/certification statement.
03_DDTC_Registration_Letter.pdf	Only if DDTC answer is Yes.
04_Export_License_or_Authorization.pdf	Only if license answer is Yes.
05_TAA_MLA_or_Distribution_Agreement.pdf	Only when applicable.
06_Other_Analyst_Requested_Document.pdf	Only when specifically requested.

9.2 Submission sequence

1. Review every answer against SAM, CAGE, SPRS, the SSP, export-classification records, and the attachments.
2. Confirm attachments are legible, current, correctly categorized, and do not contain unnecessary PII.
3. Complete the Conditions of Certification and authorized signature.
4. Click Submit and wait for the success confirmation.
5. Save the confirmation page, application number, dashboard status, and submission email as a single evidence PDF.
6. Monitor Pending Action and email. Respond to analyst requests within the stated deadline; DLA currently requires responses within 90 days.

> **Processing time**
> DLA states that processing timelines are extended and recommends initiating an initial application at least 120 days before certification is needed. Approval is not immediate.

9.3 JCP submission-evidence cover sheet template

Field	Template
Document title	JCP / DD Form 2345 Application Submission Evidence
Applicant	[EXACT LEGAL NAME IN SAM]
CAGE	[CAGE CODE]
JCP application number	[APPLICATION ID]
Submitted	[DATE / TIME / TIME ZONE]
SBIR/STTR topic	[TOPIC NUMBER AND TITLE]
Attachments	Portal confirmation, submitted-status dashboard, confirmation email

10. Use the JCP result in the SBIR/STTR proposal

10.1 Decide which evidence the solicitation accepts

Situation	Volume V action
Approved/current JCP / DD Form 2345	Upload the approved certificate/form or official certification evidence as required.
JCP submitted; solicitation expressly accepts evidence of application	Upload the submission-evidence PDF with application number/status/date.
JCP only in Draft	Not acceptable evidence of submission.
Solicitation requires approval, not application evidence	Obtain approval before the deadline or follow the Component's official clarification process.

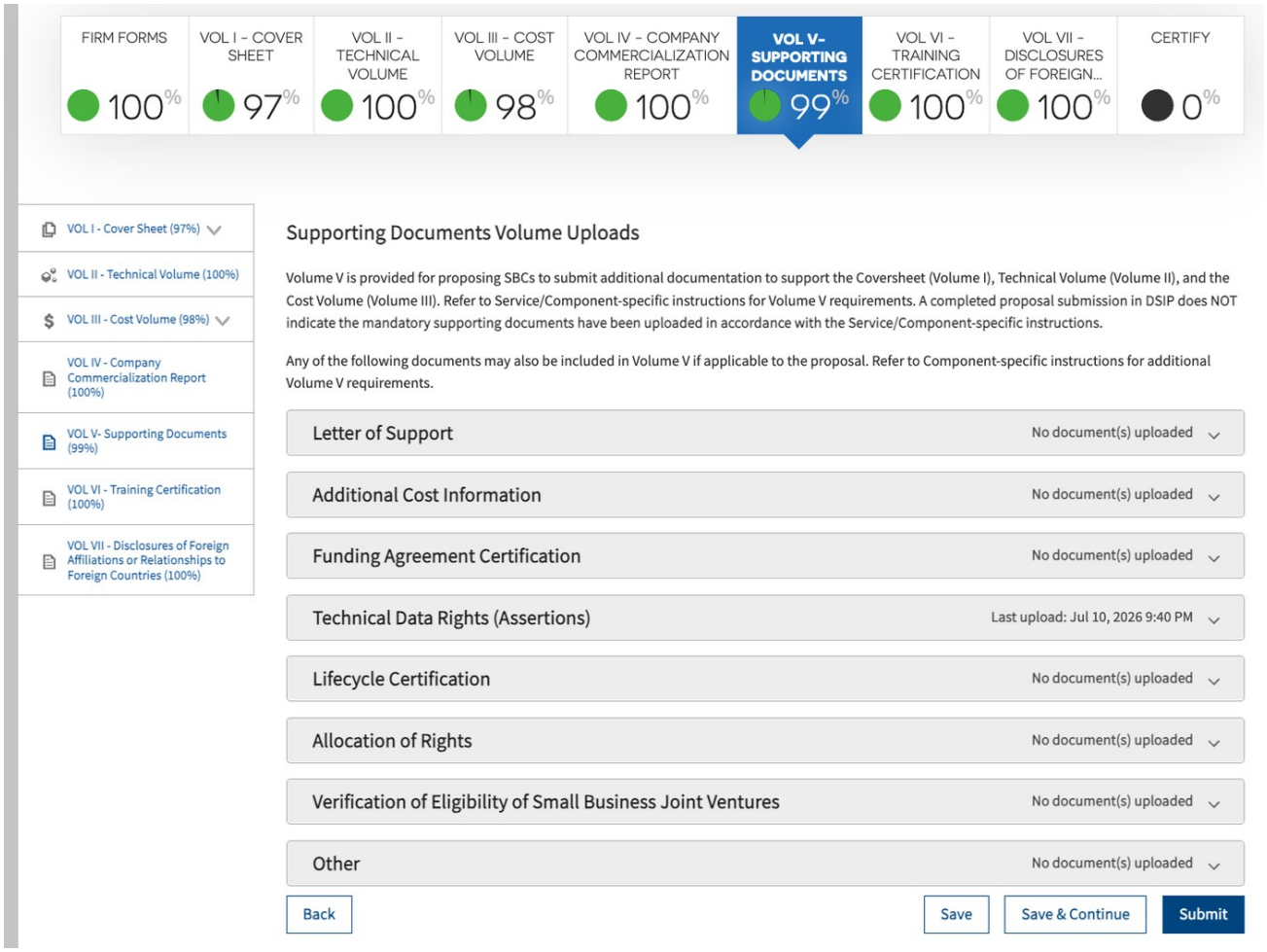


Figure 12. DSIP Volume V. When no dedicated DD Form 2345 row exists, the Other category is commonly used if consistent with the solicitation.

> **Do not use the Technical Data Rights slot**
>
> Technical data rights assertions and DD Form 2345/JCP evidence are different documents. Upload JCP evidence under the dedicated DD Form 2345 category when present, or under Other when the current Component instructions permit it.

10.2 Suggested DSIP filename

[LegalName]_[CAGE]_JCP-DD2345_Submission-Evidence_[YYYYMMDD].pdf

10.3 Complete the entire DSIP submission

[ ] Cover Sheet and all export-control questions are complete and factually correct.
[ ] Technical Volume follows page, marking, foreign-citizen, facilities, subcontractor, and data-rights instructions.
[ ] Cost Volume is complete and percentages of work are compliant.
[ ] Volume V includes every mandatory Component-specific supporting document.
[ ] Fraud, Waste, and Abuse training is complete.
[ ] Foreign affiliations/relationships webform is complete.
[ ] Corporate official has electronically certified the full proposal.
[ ] Final status is Submitted - not In Progress or Ready to Certify.
[ ] Submission confirmation and final proposal package are archived.

> **DSIP percentage is not a compliance determination**
> A 100% portal completion indicator does not prove that every mandatory Component-specific attachment or instruction has been satisfied. Read the BAA and topic instructions separately.

10.4 Same-day deadline triage

Can be completed quickly	Cannot be safely shortcut
PIEE role request if CAM approval is available	Actual NIST implementation, SSP, evidence review, and defensible scoring
SPRS summary entry after the assessment exists	Truthful DFARS compliance certification
JCP organization/account setup and attachments	JCP analyst approval
JCP submission confirmation after all gates are true	DDTC registration/license decisions when actually required
DSIP upload and corporate certification	A solicitation requirement for an approved DD Form 2345

Defense SBIR/STTR program and DSIP guidance: Open official resource
DSIP portal: Open official resource

11. Maintain compliance after submission and approval

Record / status	Maintenance
SAM	Renew annually and keep legal name, address, ownership, contacts, and representations current.
CAGE	Update authoritative CAGE information before changing JCP records.
NIST/SPRS	Reassess at least every three years or sooner when required/materially changed; maintain SSP/POA&M/evidence.
JCP	Current JCP guidance describes a five-year certification. Submit a Revision when required by entity, site, business type, signer, Data Custodian, or DDTC changes.
DDTC/licenses	Keep registrations/authorizations current and aligned with the application; revise JCP if required.
Users/data	Maintain authorized-user lists, citizenship/access determinations, training, logs, transfer approvals, and incident procedures.
Subcontractors	Flow down applicable cybersecurity/export requirements and verify authorization before releasing controlled data.

11.1 Internal operating controls

- Data Custodian approval before any person receives access.
- Unique accounts, MFA, least privilege, separate administrator accounts, and prompt termination.
- Approved repositories and secure transfer methods only.
- Logging, review, incident response, and required cyber-incident reporting.
- Prepublication, conference, marketing, customer-demo, and AI-tool review.
- International travel and remote-access controls.
- Periodic export-control and cybersecurity training.
- Annual management review of JCP, SAM, SPRS, DDTC, licenses, and controlled-data inventory.

> **Portal account maintenance**
> Current DLA guidance warns that JCP portal accounts can be locked after extended inactivity. Keep credentials, two-factor authentication, and designated contacts current.

12. Troubleshooting and rejection prevention

Problem	Likely cause / corrective action
SPRS tile missing	Role not approved, wrong role, stale session. Verify My Account > Manage Roles and re-login.
No Add New NIST Assessment button	SPRS Cyber Vendor User role is not active for the correct hierarchy.
JCP SAM fields blank/N/A	Wait up to 24 hours after organization creation/sync; verify SAM is active and exact.
JCP portal rejects NIST prerequisite	Assessment is not posted for the relevant CAGE/system or has expired.
Proof of business rejected	Wrong state, stale document, does not show good standing/equivalent, or legal name mismatch.
Training attachment rejected	Wrong DLA course, unsigned page, or not Page 15 of current training.
Application returned	Inconsistent USML/CCL, DDTC/license, business activity, NAICS, manufacturer, Data Custodian, or CAGE answers.
DSIP still not submitted	Corporate official has not completed final certification; status remains In Progress/Ready to Certify.

12.1 When to contact support

Issue	Contact
JCP policy, application status, analyst/document questions	JCP-Admin@dla.mil; include entity name, CAGE, and application ID.
General DLA/CAGE support	DLA Customer Interaction Center: 1-877-352-2255 or dlacontactcenter@dla.mil.
PIEE account/role/CAM	PIEE Vendor Customer Support / Find My Account Administrator.
SPRS entry/access	SPRS helpdesk and official access/quick-entry guides.
NIST assessment interpretation	Contracting/program office, DCMA, qualified assessor, or cybersecurity counsel.
ITAR/EAR classification/license	Qualified export-control counsel or empowered official; DDTC/BIS as appropriate.
DSIP technical issue	DSIP Learning & Support / official support channel before the deadline.

JCP support email: Open official resource
DLA general contact email: Open official resource

Appendix A. Complete package index

A.1 Internal cybersecurity file - do not submit unless requested

[ ] 01_System_Security_Plan.pdf
[ ] 02_NIST_800-171_Control_Assessment.xlsx
[ ] 03_DoD_Score_Calculation.xlsx
[ ] 04_POAM.xlsx
[ ] 05_Asset_Account_and_Data_Flow_Inventory.xlsx
[ ] 06_Network_and_System_Boundary_Diagram.pdf
[ ] 07_Policies_Procedures_and_Training/
[ ] 08_Objective_Evidence/
[ ] 09_Management_Approval_and_Assessment_Record.pdf
[ ] 10_SPRS_Posting_Evidence.pdf

A.2 JCP portal upload file

[ ] Secretary of State current good-standing/equivalent proof
[ ] Signed Page 15 Proper Handling Certification Statement
[ ] DDTC registration proof - if Yes
[ ] Export license/authorization - if Yes
[ ] TAA/MLA/distribution agreement - if applicable
[ ] Other analyst-requested documents

A.3 DSIP proposal file

[ ] Approved JCP/DD Form 2345 OR solicitation-permitted application-submission evidence
[ ] One-page transmittal/cover sheet identifying legal name, CAGE, topic, application number, and date
[ ] Every other Component-specific Volume V document
[ ] Final DSIP submission confirmation

Appendix B. One-page execution checklist

Done	Gate	Acceptance test
[ ]	SAM/CAGE	Active; exact; >90 days remaining for JCP
[ ]	PIEE CAM	Established for correct CAGE
[ ]	SPRS role	SPRS Cyber Vendor User - Active
[ ]	SSP	Approved and matches actual enclave/system
[ ]	Assessment	110 requirements reviewed with evidence
[ ]	Score/POA&M	Calculated and management-approved
[ ]	SPRS	Assessment summary posted and saved
[ ]	Data Custodian	Authorized, trained, U.S. site, direct contact
[ ]	Device/server	Permanent MAC, IP per guide, physical address
[ ]	Proof of business	Secretary of State, current within 12 months
[ ]	Training	Current PDF reviewed; Page 15 signed
[ ]	Export answers	USML/CCL/DDTC/license documented
[ ]	JCP organization	Search/join/create; SAM sync verified
[ ]	JCP pre-screen	Every Yes is currently true
[ ]	JCP application	All fields and attachments reviewed
[ ]	JCP submit	Application ID/status/email saved
[ ]	DSIP Volume V	Approved form or permitted evidence uploaded
[ ]	DSIP certify	Corporate official completed final certification
[ ]	Archive	Final package and confirmations retained

Stop condition

If any certification statement is not presently true, stop and correct the underlying condition or obtain authoritative clarification. Do not use a portal checkbox to create compliance that does not exist.

Appendix C. Official links and source documents

Links were checked on 21 July 2026. Government sites and file paths change; begin with the DLA JCP home page when a deep link stops working.

DLA Joint Certification Program home and current requirements: Open official resource

JCP Portal: Open official resource

JCP External Users Help Guide (2026): Open official resource

Introduction to Proper Handling training (March 2026): Open official resource

U.S. Relevant Business Activity Quick Guide: Open official resource

50-state Proof of Business examples: Open official resource

PIEE: Open official resource

SPRS access instructions: Open official resource

SPRS NIST SP 800-171 information: Open official resource

SPRS NIST Quick Entry Guide: Open official resource

SPRS Cyber Reports access guide: Open official resource

DFARS Part 204 cybersecurity provisions/clauses: Open official resource

DFARS 252.204-7020: Open official resource

DoD NIST SP 800-171 Assessment Methodology: Open official resource

NIST SP 800-171 Revision 2: Open official resource

DoD CMMC information: Open official resource

Defense SBIR/STTR program and DSIP guidance: Open official resource

DSIP proposal portal: Open official resource

USML - 22 CFR Part 121: Open official resource

BIS classify your item: Open official resource

Commerce Control List: Open official resource

BIS SNAP-R: Open official resource

DDTC DECCS: Open official resource

Source hierarchy

When sources conflict, use this order: (1) the current topic and Component-specific instructions; (2) the current program BAA/CSO and amendments; (3) the current contract clauses/provisions; (4) the official DLA JCP, SPRS, PIEE, DDTC, BIS, and DSIP instructions; (5) this guide.

Appendix D. Fast answers

Does a CAGE code make the company ITAR compliant?

No. A CAGE code identifies the entity; it is not an export-control authorization or cybersecurity assessment.

Can we submit a JCP application before posting NIST in SPRS?

Current DLA guidance says no. The assessment must be documented in SPRS before applying.

Can we check Yes and finish NIST later?

No. That would make the portal certification inaccurate.

Is ISO 9000 the cybersecurity requirement?

No. The relevant JCP prerequisite is NIST SP 800-171 in SPRS.

Does JCP registration with DLA require DIBBS?

Standard JCP does not. DIBBS/cFolders is relevant to DLA Enhanced Validation and DLA technical-data systems.

Do we need an outside assessor for the Basic Assessment?

Not necessarily. It is a contractor self-assessment, but it must follow the official methodology and be supported by an SSP and evidence.

Does a score below 110 prevent posting?

SPRS can store a Basic Assessment summary below 110. The separate JCP DFARS-compliance statement and any solicitation/CMMC minimum still must be answered truthfully.

Is JCP approval immediate?

No. DLA reports extended processing and advises starting well in advance.

Can application evidence be used in DSIP?

Only when the controlling solicitation permits evidence of application submission. A draft does not count.

Where does JCP evidence go in DSIP?

Use the dedicated DD Form 2345 category when present; otherwise use Other only when consistent with the current Component instructions. Do not use Technical Data Rights Assertions.

Does JCP authorize sharing data with foreign nationals?

No. Foreign-person releases require separate export-control analysis and authorization.

What changes require a JCP Revision?

Current DLA guidance identifies changes such as entity name, CAGE site/address, primary work, authorized signer, Data Custodian, and DDTC status.

> **Final rule**
> The fastest legitimate path is to reduce scope, document the real environment, implement and evidence the required controls, post the real assessment, and submit accurate application answers. Speed does not justify false certification.