Welcome

3.1.Access Control

Welcome to the NIST SP 800-171 Questionnaire (Ref:1.1)

This questionnaire is based on cyber requirements as specified by the United States National Institute of Standards and Technology Standards (NIST).The cybersecurity control statements in this questionnaire are solely from NIST Special Publication 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. NIST SP 800-171 is a requirement for contracts with the Defense Federal Acquisition Regulation Supplement(DFARS) 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting.

By responding to this questionnaire, you represent that you have appropriate authority to complete the questionnaire on behalf of your company. The Exostar partners may separately use the information to assess your compliance with applicable DFARs.Your answers to the questionnaire will be treated as your company's proprietary information by Exostar or the Exostar partnersand can only be changed by your company. Please do not include any competitively sensitive information or proprietary information of any customer including any subscriber company in your answers in the questionnaire. The questionnaire will be amended to reflect NIST SP 800-171 changes.

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Welcome	3.1.Access Control

Instructions for NIST SP 800-171 as required by DFARS 252.204-7012 (Ref:2.1)

On August 26, 2015, and updated December 30, 2015, the United States Department of Defense(DoD) issued a new interim rule making significant changes to the way the US DoD addresses cybersecurity. As a supplier, you should be aware of the significantly expanded obligations on defense contractors and subcontractors with regard to the protection of unclassified Covered Defense Information (CDI) and the reporting of cyber incidents occurring on unclassified information systems that contain such information. The applicable Defense Federal Acquisition Regulation Supplement *(DFARS) 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting*. Key changes are summarized below.It is imperative that all suppliers fully understand their obligations required under this new clause.
The following summary focuses on a few requirements.

1. The covered data is expanded beyond unclassified controlled technical information to include other types of data.
2. Contractors have until December 2017 to be in full compliance with the requirements outlined in the clause and NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

For new contracts awarded prior to December 2017 areas of non-compliance need to be reported to the DoD CIOs office within 30 days of contract award

Answers for each Control Question

Please indicate the current status for each of the controls in this questionnaire. The choices for the status are described below and only one can be selected:

If the control is implemented as per the NIST 800-171 specification, select IMPLEMENTED

If not IMPLEMENTED but you have documented your plan to become compliant in an SSP & POAM, select ADDRESSED WITH SSP & POAM

If you have been given approval by the DoD to: [1] treat this control as not applicable or [2] provide an equally effective alternate control, select APPROVED EXCEPTION

If the control has not been implemented, nor is there any plan to implement as part of an SSP/POAM, select NOT IMPLEMENTED

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Welcome	3.1.Access Control

Who in your organization is responsible for providing the answers to this cybersecurity questionnaire? (Ref:2.2)

Name :

Job Title :

Email :

Name :

Job Title :

Email :

Name :

Job Title :

Email :

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Welcome	3.1.Access Control

Does your organization have a NIST SP 800-171 DoD Assessment Methodology score in the DoD's Supplier Performance Risk System (SPRS)? (Ref:2.3.0)

- Yes
- No

Guidance

The DFARS Interim Rule, for NIST SP 800-171, requires that a contractor organization which handles Controlled Unclassified Information (CUI) must have its NIST SP 800-171 DoD Assessment Methodology score (that is not more than 3 years old) within the DoD's Supplier Performance Risk System (SPRS) for all covered contractor information systems relevant to its offer.

For more information, please see the "NIST SP 800-171" section of the Form Resources page in myExostar.com which contains useful external resource links that provide information regarding the following:

1. The DFARS Interim Rule

2. Accessing and using SPRS

3. The DoD Assessment Methodology for calculating NIST SP 800-171 scores

If you do not currently know your NIST SP 800-171 DoD Assessment Methodology score, once you complete and submit this NIST SP 800-171 form in PIM, you can import the .csv file of this form into Exostar's Certification Assistant (CA) tool to get your DoD Assessment Methodology score in a few steps. For more information on how to do this, please see the Guide Link.

Welcome	3.1.Access Control

What is the date of your organization's most recent NIST SP 800-171 DoD Assessment Methodology score, as input into SPRS? (Ref:2.4.0)

Guidance

Within DoD's Supplier Performance Risk System (SPRS), your organization may have data for more than one assessment for NIST SP 800-171 that has already been completed. Per this question, please only input the date of your organization's most recent assessment only.

Welcome	3.1.Access Control

What is the Confidence Level of your most recent NIST SP 800-171 DoD Assessment Methodology score, as input into SPRS? (Ref:2.5.0)

- Basic
- Medium
- High Virtual
- High On-Site

Guidance

The response options provided for this question directly correlated to the Confidence Level values for the NIST SP 800-171 assessments that exist within DoD's Supplier Performance Risk System (SPRS). Please note that the following Confidence Levels are only applicable if your organization's assessment was performed by the Defense Contract Management Agency (DCMA): Medium; High Virtual; High On-Site.

For more information regarding SPRS and the DoD Assessment Methodology in particular, please see the “NIST SP 800-171” section of the Form Resources page in myExostar.com.

Welcome	3.1.Access Control

What is the CAGE code(s) of your most recent NIST SP 800-171 DoD Assessment Methodology score, as input into SPRS? (Ref:2.6.0)

Guidance

For each of your organization's NIST SP 800-171 assessments whose information already exists in within DoD's Supplier Performance Risk System (SPRS), a CAGE code(s) is associated with each particular assessment. Please input that CAGE code value for your most recent assessment only for this form question. If entering multiple CAGE codes, please separate each entry with a "space". For US organizations, a cage code will be represented by three alpha/numerical characters prefixed and suffixed by a numeral (#***#). For other countries, it may be referenced as an NCAGE code where the leading and trailing character may be alpha or numerical characters. Of additional note: The letter "I" must be used only in the first position of International NCAGEs assigned by NSPA, the letter "O" must not be used in CAGE nor NCAGEs.

Welcome	3.1.Access Control

What is the Scope of Assessment as recorded in SPRS? (Ref:2.7.0)

- Enterprise
- Enclave
- Contract

Guidance

For each of your organization's NIST SP 800-171 assessments whose information already exists in within DoD's Supplier Performance Risk System (SPRS), a Scope of Assessment is associated with each particular assessment. Per guidance from SPRS:

Enterprise - Entire Company's Network under the CAGEs listed

Enclave - Standalone under Enterprise CAGE as Business Unit (test enclave, hosted resources, etc.)

Contract - Contract specific SSP Review

Are you willing to share your most recent NIST 800-171 DoD Assessment Methodology score, as input into SPRS, with your buyers (partners) in PIM? (Ref:2.8.0)

- Yes
- No

Guidance

Please note that you are not required to share your most recent NIST 800-171 DoD Assessment Methodology score with your buyers in PIM. This question is purely for informational purposes for your PIM buyers/partners.

Welcome	3.1.Access Control

What is your expected Cybersecurity Maturity Model Certification (CMMC) maturity level your organization is planning to achieve? (Ref:2.10.0)

- None
- Level 1
- Level 2
- Level 3
- Level 4
- Level 5

Guidance

The Cybersecurity Maturity Model Certification (CMMC) is a set of cybersecurity standards developed by the Department of Defense (DoD). It consists of several maturity levels that range from basic cyber hygiene to advanced. For a given CMMC level, the associated controls and processes, when implemented, are intended to reduce risk against a specific set of cyber threats.

For more information and resource links on CMMC, please see the “CMMC” section of the Form Resources page in myExostar.com, or the CMMC page on Exostar's website.

Welcome	3.1.Access Control

What is your targeted Cybersecurity Maturity Model Certification (CMMC) Certification Date? (Ref:2.11.0)

Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems). (Ref:3.1.1.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Limit system access to the types of transactions and functions that authorized users are permitted to execute. (Ref:3.1.2.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Control the flow of CUI in accordance with approved authorizations. (Ref:3.1.3.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Separate the duties of individuals to reduce the risk of malevolent activity without collusion. (Ref:3.1.4.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Employ the principle of least privilege, including for specific security functions and privileged accounts. (Ref:3.1.5.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Use non-privileged accounts or roles when accessing nonsecurity functions. (Ref:3.1.6.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Prevent non-privileged users from executing privileged functions and audit the execution of such functions. (Ref:3.1.7.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Limit unsuccessful logon attempts. (Ref:3.1.8.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Provide privacy and security notices consistent with applicable CUI rules. (Ref:3.1.9.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity. (Ref:3.1.10.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Terminate (automatically) a user session after a defined condition. (Ref:3.1.11.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Monitor and control remote access sessions. (Ref:3.1.12.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. (Ref:3.1.13.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Route remote access via managed access control points. (Ref:3.1.14.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Authorize remote execution of privileged commands and remote access to security-relevant information. (Ref:3.1.15.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Authorize wireless access prior to allowing such connections. (Ref:3.1.16.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Protect wireless access using authentication and encryption. (Ref:3.1.17.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Control connection of mobile devices. (Ref:3.1.18.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Encrypt CUI on mobile devices and mobile computing platforms. (Ref:3.1.19.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Verify and control/limit connections to and use of external systems. (Ref:3.1.20.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Limit use of organizational portable storage devices on external systems. (Ref:3.1.21.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Control CUI posted or processed on publicly accessible systems. (Ref:3.1.22.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

3.1.Access Control	**3.2.Awareness and Training**	3.3.Audit and Accountability

Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems. (Ref:3.2.1.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities. (Ref:3.2.2.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

3.1.Access Control	**3.2.Awareness and Training**	3.3.Audit and Accountability

Provide security awareness training on recognizing and reporting potential indicators of insider threat. (Ref:3.2.3.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity. (Ref:3.3.1.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. (Ref:3.3.2.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Review and update audited events. (Ref:3.3.3.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Alert in the event of an audit process failure. (Ref:3.3.4.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Use automated mechanisms to integrate and correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity. (Ref:3.3.5.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Provide audit reduction and report generation to support on-demand analysis and reporting. (Ref:3.3.6.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records. (Ref:3.3.7.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Protect audit information and audit tools from unauthorized access, modification, and deletion. (Ref:3.3.8.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Limit management of audit functionality to a subset of privileged users. (Ref:3.3.9.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. (Ref:3.4.1.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

3.3.Audit and Accountability	**3.4.Configuration Management**	3.5.Identification and Authentication

Establish and enforce security configuration settings for information technology products employed in organizational systems. (Ref:3.4.2.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Track, review, approve/disapprove, and audit changes to organizational systems. (Ref:3.4.3.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Analyze the security impact of changes prior to implementation. (Ref:3.4.4.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational system. (Ref:3.4.5.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Employ the principle of least functionality by configuring organizational system to provide only essential capabilities. (Ref:3.4.6.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services. (Ref:3.4.7.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software. (Ref:3.4.8.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Control and monitor user-installed software. (Ref:3.4.9.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Identify system users, processes acting on behalf of users, or devices. (Ref:3.5.1.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems. (Ref:3.5.2.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. (Ref:3.5.3.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. (Ref:3.5.4.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Prevent reuse of identifiers for a defined period. (Ref:3.5.5.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Disable identifiers after a defined period of inactivity. (Ref:3.5.6.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Enforce a minimum password complexity and change of characters when new passwords are created. (Ref:3.5.7.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Prohibit password reuse for a specified number of generations. (Ref:3.5.8.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Allow temporary password use for system logons with an immediate change to a permanent password. (Ref:3.5.9.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Store and transmit only cryptographically-protected passwords. (Ref:3.5.10.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Obscure feedback of authentication information. (Ref:3.5.11.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Establish an operational incident-handling capability for organizational systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities. (Ref:3.6.1.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization. (Ref:3.6.2.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Test the organizational incident response capability. (Ref:3.6.3.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Perform maintenance on organizational systems. (Ref:3.7.1.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. (Ref:3.7.2.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Ensure equipment removed for off-site maintenance is sanitized of any CUI. (Ref:3.7.3.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Check media containing diagnostic and test programs for malicious code before the media are used in organizational system. (Ref:3.7.4.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. (Ref:3.7.5.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Supervise the maintenance activities of maintenance personnel without required access authorization. (Ref:3.7.6.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. (Ref:3.8.1.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Limit access to CUI on system media to authorized users. (Ref:3.8.2.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Sanitize or destroy system media containing CUI before disposal or release for reuse. (Ref:3.8.3.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Mark media with necessary CUI markings and distribution limitations (Ref:3.8.4.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. (Ref:3.8.5.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. (Ref:3.8.6.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Control the use of removable media on system components. (Ref:3.8.7.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Prohibit the use of portable storage devices when such devices have no identifiable owner. (Ref:3.8.8.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Protect the confidentiality of backup CUI at storage locations. (Ref:3.8.9.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Screen individuals prior to authorizing access to organizational systems containing CUI. (Ref:3.9.1.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Ensure that CUI and organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers. (Ref:3.9.2.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals. (Ref:3.10.1.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Protect and monitor the physical facility and support infrastructure for organizational systems (Ref:3.10.2.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Escort visitors and monitor visitor activity. (Ref:3.10.3.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Maintain audit logs of physical access. (Ref:3.10.4.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Control and manage physical access devices. (Ref:3.10.5.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites). (Ref:3.10.6.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. (Ref:3.11.1.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. (Ref:3.11.2.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Remediate vulnerabilities in accordance with assessments of risk. (Ref:3.11.3.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

3.11.Risk Assessment	**3.12.Security Assessment**	3.13.System and Communications Protection

Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. (Ref:3.12.1.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

3.11.Risk Assessment	**3.12.Security Assessment**	3.13.System and Communications Protection

Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. (Ref:3.12.2.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. (Ref:3.12.3.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Develop, document, and periodically updatesystem security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. (Ref:3.12.4.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. (Ref:3.13.1.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. (Ref:3.13.2.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

3.12.Security Assessment	**3.13.System and Communications Protection**	3.14.System and Information Integrity

Separate user functionality from system management functionality. (Ref:3.13.3.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Prevent unauthorized and unintended information transfer via shared system resources. (Ref:3.13.4.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. (Ref:3.13.5.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). (Ref:3.13.6.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks. (Ref:3.13.7.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

3.12.Security Assessment	**3.13.System and Communications Protection**	3.14.System and Information Integrity

Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. (Ref:3.13.8.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. (Ref:3.13.9.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Establish and manage cryptographic keys for cryptography employed in organizational systems. (Ref:3.13.10.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.*** (Ref:3.13.11.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device. (Ref:3.13.12.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Control and monitor the use of mobile code. (Ref:3.13.13.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Control and monitor the use of Voice over Internet Protocol (VoIP) technologies (Ref:3.13.14.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

3.12.Security Assessment	**3.13.System and Communications Protection**	3.14.System and Information Integrity

Protect the authenticity of communications sessions (Ref:3.13.15.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Protect the confidentiality of CUI at rest. (Ref:3.13.16.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

3.13.System and Communications Protection	**3.14.System and Information Integrity**	Additional Details

Identify, report, and correct information and system flaws in a timely manner. (Ref:3.14.1.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

3.13.System and Communications Protection	**3.14.System and Information Integrity**	Additional Details

Provide protection from malicious code at appropriate locations within organizational systems. (Ref:3.14.2.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Monitor system security alerts and advisories and take appropriate actions in response. (Ref:3.14.3.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

3.13.System and Communications Protection	**3.14.System and Information Integrity**	Additional Details

Update malicious code protection mechanisms when new releases are available. (Ref:3.14.4.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

3.13.System and Communications Protection	**3.14.System and Information Integrity**	Additional Details

Perform periodic scans of organizational system and real-time scans of files from external sources as files are downloaded, opened, or executed. (Ref:3.14.5.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

3.13.System and Communications Protection	**3.14.System and Information Integrity**	Additional Details

Monitor organizational system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. (Ref:3.14.6.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Identify unauthorized use of organizational system. (Ref:3.14.7.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

3.14.System and Information Integrity	**Additional Details**	Submission

If your organization has not implemented all of the NIST 800-171 controls, please provide an Estimated Completion Date (ECD) of when your organization expects to operationally implement all of the controls. (Ref:4.1)

ECD :

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar

Submission

Thank you for your responses, the NIST SP 800-171 Subscriber with whom you have a business relationship will use this information as an input to manage risk. (Ref:5.1)

First Name :

Last Name :

Job Title :

Email :

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST SP 800-171 section of the PIM Form Resources page in myExostar