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. The purpose of NIST SP 800-171 as stated in section 1.1 of the standard:

"is to provide federal agencies with recommended requirements for protecting the confidentiality of CUI:
(i) when the CUI is resident in nonfederal information systems and organizations;(ii) when the information systems where the CUI resides are not used or operated by contractors of federal agencies or other organizations on behalf of those agencies;8 and (iii) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government wide policy for the CUI category or subcategory listed in the CUI Registry. The requirements apply only to components9 of nonfederal information systems that process, store, or transmit CUI, or that provide security protection for such components."

NIST 800-171 Rev.1 states:

"Nonfederal organizations describe in a system security plan (SSP), how the CUI requirements are met or how organizations plan to meet the requirements. The SSP describes the boundary of the information system; the operational environment for the system; how the security requirements are implemented; and the relationships with or connections to other systems. When requested, the SSP and any associated plans of action and milestones (POAM) for any planned implementations or mitigations should be submitted to the responsible federal agency or contracting officer to demonstrate the nonfederal organization’s implementation or planned implementation of the CUI requirements. Federal agencies may consider the submitted SSPs and POAMs as critical inputs to an overall risk management decision to process, store, or transmit CUI on an information system hosted by a nonfederal organization and whether or not to pursue an agreement or contract with the nonfederal organization."

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 partners and 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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
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 R1 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.

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th>Welcome</th>
<th>3.1. Access Control</th>
<th>3.2. Awareness and Training</th>
</tr>
</thead>
</table>

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th>Welcome</th>
<th>3.1. Access Control</th>
<th>3.2. Awareness and Training</th>
</tr>
</thead>
</table>

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th>Welcome</th>
<th>3.1. Access Control</th>
<th>3.2. Awareness and Training</th>
</tr>
</thead>
</table>

**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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th>Welcome</th>
<th>3.1. Access Control</th>
<th>3.2. Awareness and Training</th>
</tr>
</thead>
</table>

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th>Welcome</th>
<th>3.1. Access Control</th>
<th>3.2. Awareness and Training</th>
</tr>
</thead>
</table>

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th>Welcome</th>
<th>3.1. Access Control</th>
<th>3.2. Awareness and Training</th>
</tr>
</thead>
</table>

**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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th>Welcome</th>
<th>3.1. Access Control</th>
<th>3.2. Awareness and Training</th>
</tr>
</thead>
</table>

### 3.1. Access Control
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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
### 3.1. Access Control

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th>Welcome</th>
<th>3.1. Access Control</th>
<th>3.2. Awareness and Training</th>
</tr>
</thead>
</table>

**3.1. Access Control**

- 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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th>Welcome</th>
<th>3.1. Access Control</th>
<th>3.2. Awareness and Training</th>
</tr>
</thead>
</table>

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
### Welcome

<table>
<thead>
<tr>
<th>3.1. Access Control</th>
<th>3.2. Awareness and Training</th>
</tr>
</thead>
</table>

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
### 3.1. Access Control

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th>Welcome</th>
<th>3.1. Access Control</th>
<th>3.2. Awareness and Training</th>
</tr>
</thead>
</table>

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
### 3.1. Access Control

**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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th>Welcome</th>
<th><strong>3.1. Access Control</strong></th>
<th><strong>3.2. Awareness and Training</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify and control/limit connections to and use of external systems. (Ref: 3.1.20.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Implemented</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Addressed with SSP &amp; POAM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Approved Exception (by DoD)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Not Implemented</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Welcome</td>
<td>3.1. Access Control</td>
<td>3.2. Awareness and Training</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------</td>
<td>----------------------------</td>
</tr>
</tbody>
</table>

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th>Welcome</th>
<th>3.1. Access Control</th>
<th>3.2. Awareness and Training</th>
</tr>
</thead>
</table>

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
3.2. Awareness and Training

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
### 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. NIST 800-171 Revision 1

3. Exostar Resource Center for NIST SP 800-171
### 3.2. Awareness and Training

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

### 3.3. Audit and Accountability

<table>
<thead>
<tr>
<th>Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:</td>
</tr>
<tr>
<td>1. The supply chain representative for the company with which you are working.</td>
</tr>
<tr>
<td>2. NIST 800-171 Revision 1</td>
</tr>
<tr>
<td>3. Exostar Resource Center for NIST SP 800-171</td>
</tr>
</tbody>
</table>

### 3.4. Configuration Management
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.)

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
### 3.2. Awareness and Training

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

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

### 3.3. Audit and Accountability

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171

### 3.4. Configuration Management

Guidance
### 3.2. Awareness and Training

**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. NIST 800-171 Revision 1

3. Exostar Resource Center for NIST SP 800-171

---

<table>
<thead>
<tr>
<th>Implemented</th>
<th>Addressed with SSP &amp; POAM</th>
<th>Approved Exception (by DoD)</th>
<th>Not Implemented</th>
</tr>
</thead>
</table>

Alert in the event of an audit process failure. (Ref: 3.3.4.)
| 3.2. Awareness and Training | 3.3. Audit and Accountability | 3.4. Configuration Management |

**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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th>3.2.Awareness and Training</th>
<th>3.3.Audit and Accountability</th>
<th>3.4.Configuration Management</th>
</tr>
</thead>
</table>

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th>3.2. Awareness and Training</th>
<th>3.3. Audit and Accountability</th>
<th>3.4. Configuration Management</th>
</tr>
</thead>
</table>

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
3.2. Awareness and Training

3.3. Audit and Accountability

3.4. Configuration Management

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th>3.2. Awareness and Training</th>
<th>3.3. Audit and Accountability</th>
<th>3.4. Configuration Management</th>
</tr>
</thead>
</table>

**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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
| 3.3.Audit and Accountability | 3.4.Configuration Management | 3.5.Identification and Authentication |

**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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
### 3.3. Audit and Accountability

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

---

### 3.4. Configuration Management

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171

---

### 3.5. Identification and Authentication

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

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
### 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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171

---

#### 3.3. Audit and Accountability

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

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented
### 3.3. Audit and Accountability

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th>3.3.Audit and Accountability</th>
<th>3.4.Configuration Management</th>
<th>3.5.Identification and Authentication</th>
</tr>
</thead>
</table>

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
### 3.3. Audit and Accountability

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

### 3.4. Configuration Management

### 3.5. Identification and Authentication

**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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
### 3.3. Audit and Accountability

**Summary:**
- 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.)

<table>
<thead>
<tr>
<th>Implemented</th>
<th>Addressed with SSP &amp; POAM</th>
<th>Approved Exception (by DoD)</th>
<th>Not Implemented</th>
</tr>
</thead>
</table>

### 3.4. Configuration Management

**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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th>3.3. Audit and Accountability</th>
<th>3.4. Configuration Management</th>
<th>3.5. Identification and Authentication</th>
</tr>
</thead>
</table>

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
### 3.4. Configuration Management

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

### 3.5. Identification and Authentication

#### 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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th>3.4.Configuration Management</th>
<th>3.5.Identification and Authentication</th>
<th>3.6.Incident Response</th>
</tr>
</thead>
</table>

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th>3.4.Configuration Management</th>
<th>3.5.Identification and Authentication</th>
<th>3.6.Incident Response</th>
</tr>
</thead>
</table>

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th>3.4.Configuration Management</th>
<th>3.5.Identification and Authentication</th>
<th>3.6.Incident Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. (Ref: 3.5.4.)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- 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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
| 3.4. Configuration Management | 3.5. Identification and Authentication | 3.6. Incident Response |

**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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th>3.4.Configuration Management</th>
<th>3.5.Identification and Authentication</th>
<th>3.6.Incident Response</th>
</tr>
</thead>
</table>

- **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. NIST 800-171 Revision 1

3. Exostar Resource Center for NIST SP 800-171

---

Disables identifiers after a defined period of activity. (Ref: 3.5.6.)

- Implemented
- Addressed with SSP & POAM
- Approved Exception (by DoD)
- Not Implemented
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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th>3.4.Configuration Management</th>
<th>3.5.Identification and Authentication</th>
<th>3.6.Incident Response</th>
</tr>
</thead>
</table>

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th>3.4. Configuration Management</th>
<th>3.5. Identification and Authentication</th>
<th>3.6. Incident Response</th>
</tr>
</thead>
</table>

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th>3.4.Configuration Management</th>
<th>3.5.Identification and Authentication</th>
<th>3.6.Incident Response</th>
</tr>
</thead>
</table>

**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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171

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

Store and transmit only cryptographically-protected passwords. (Ref: 3.5.10.)
<table>
<thead>
<tr>
<th>3.4.Configuration Management</th>
<th>3.5.Identification and Authentication</th>
<th>3.6.Incident Response</th>
</tr>
</thead>
</table>

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th>3.5. Identification and Authentication</th>
<th>3.6. Incident Response</th>
<th>3.7. Maintenance</th>
</tr>
</thead>
</table>

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th>3.5. Identification and Authentication</th>
<th>3.6. Incident Response</th>
<th>3.7. Maintenance</th>
</tr>
</thead>
</table>

**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. NIST SP 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th>3.5. Identification and Authentication</th>
<th>3.6. Incident Response</th>
<th>3.7. Maintenance</th>
</tr>
</thead>
</table>

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
### 3.7. Maintenance

**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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
### 3.6 Incident Response

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

### 3.7 Maintenance

<table>
<thead>
<tr>
<th>Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:</td>
</tr>
<tr>
<td>1. The supply chain representative for the company with which you are working.</td>
</tr>
<tr>
<td>2. NIST 800-171 Revision 1</td>
</tr>
<tr>
<td>3. Exostar Resource Center for NIST SP 800-171</td>
</tr>
</tbody>
</table>

### 3.8 Media Protection
3.6.Incident Response

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

3.7.Maintenance

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. NIST 800-171 Revision 1

3. Exostar Resource Center for NIST SP 800-171

3.8.Media Protection
### 3.6. Incident Response

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

<table>
<thead>
<tr>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implemented</td>
</tr>
<tr>
<td>Addressed with SSP &amp; POAM</td>
</tr>
<tr>
<td>Approved Exception (by DoD)</td>
</tr>
<tr>
<td>Not Implemented</td>
</tr>
</tbody>
</table>

### 3.7. Maintenance

#### 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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
### 3.6. Incident Response

- 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

### 3.7. Maintenance

- **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. NIST 800-171 Revision 1
  3. Exostar Resource Center for NIST SP 800-171
3.6 Incident Response

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
3.7. Maintenance

3.8. Media Protection

3.9. Personnel Security

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Limit access to CUI on system media to authorized users. (Ref:3.8.2.)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- 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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
|------------------|----------------------|------------------------|

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
### 3.7. Maintenance

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

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

### 3.8. Media Protection

#### 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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
### 3.7. Maintenance
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

### 3.8. Media Protection

### 3.9. Personnel Security

---

**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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
### 3.7. Maintenance

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

### 3.8. Media Protection

**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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Control the use of removable media on system components. (Ref: 3.8.7.)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Implemented</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Addressed with SSP &amp; POAM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Approved Exception (by DoD)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Not Implemented</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Prohibit the use of portable storage devices when such devices have no identifiable owner. (Ref: 3.8.8.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>![Q] Implemented</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Addressed with SSP &amp; POAM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Approved Exception (by DoD)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Implemented</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
3.8. Media Protection

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

3.9. Personnel Security

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
### 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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
|------------------------|--------------------------|----------------------|

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)
- [X] 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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
### 3.9. Personnel Security

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

<table>
<thead>
<tr>
<th>Implemented</th>
<th>Addressed with SSP &amp; POAM</th>
<th>Approved Exception (by DoD)</th>
<th>Not Implemented</th>
</tr>
</thead>
</table>

### 3.10. Physical Protection

### 3.11. Risk Assessment

**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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
3.9. Personnel Security

3.10. Physical Protection

3.11. Risk Assessment

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
### 3.9. Personnel Security

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

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

### 3.10. Physical Protection

**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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
3.10. Physical Protection

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites). (Ref: 3.10.6.)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
### 3.10. Physical Protection

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

### 3.11. Risk Assessment

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
3.10. Physical Protection

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

3.11. Risk Assessment

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171

3.12. Security Assessment

NIST 800-171 R1 1.2
3.10. Physical Protection

3.11. Risk Assessment

3.12. Security Assessment

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
3.11. Risk Assessment

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

3.12. Security Assessment

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171

**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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
|--------------------------|------------------------------------------|--------------------------------------|

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
|--------------------------|------------------------------------------|-------------------------------------|

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
|--------------------------|------------------------------------------|--------------------------------------|

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
3.12. Security Assessment

3.13. System and Communications Protection

3.14. System and Information Integrity

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
|--------------------------|------------------------------------------|--------------------------------------|

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
### 3.12. Security Assessment

<table>
<thead>
<tr>
<th><strong>Guidance</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. (Ref: 3.13.9.)</td>
</tr>
<tr>
<td><strong>Implemented</strong></td>
</tr>
<tr>
<td><strong>Addressed with SSP &amp; POAM</strong></td>
</tr>
<tr>
<td><strong>Approved Exception (by DoD)</strong></td>
</tr>
<tr>
<td><strong>Not Implemented</strong></td>
</tr>
</tbody>
</table>

**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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
|-------------------------|------------------------------------------|--------------------------------------|

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
3.12. Security Assessment

3.13. System and Communications Protection

3.14. System and Information Integrity

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
### 3.12. Security Assessment

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
|--------------------------|------------------------------------------|--------------------------------------|

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
|--------------------------|------------------------------------------|-------------------------------------|

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
3.13. System and Communications Protection

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

3.14. System and Information Integrity

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
|------------------------------------------|---------------------------------------|------------------|

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Update malicious code protection mechanisms when new releases are available. (Ref: 3.14.4.)</td>
<td></td>
<td>Guidance</td>
</tr>
<tr>
<td>☐ Implemented</td>
<td>☐ Addressed with SSP &amp; POAM</td>
<td>For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:</td>
</tr>
<tr>
<td>☐ Approved Exception (by DoD)</td>
<td>☐ Not Implemented</td>
<td>1. The supply chain representative for the company with which you are working.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. NIST 800-171 Revision 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Exostar Resource Center for NIST SP 800-171</td>
</tr>
</tbody>
</table>
### 3.13. System and Communications Protection

<table>
<thead>
<tr>
<th>Additional Details</th>
</tr>
</thead>
</table>

**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

### 3.14. System and Information Integrity

**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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
|------------------------------------------|--------------------------------------|-------------------|

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
|------------------------------------------|-----------------------------------------|-------------------|

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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171
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. NIST 800-171 Revision 1
3. Exostar Resource Center for NIST SP 800-171