

NIST SP 800-171 Questionnaire

Welcome

3.1 Access Control

0%

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; 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 components of nonfederal information systems that process, store, or transmit CUI, or that provide security protection for such components."

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

You are in the 'Welcome' section of this questionnaire.

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 special publication [NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations](#)
3. The US Department of Defense [Frequently Asked Questions regarding NIST SP 800-171](#)

NIST SP 800-171 Questionnaire

Welcome

3.1 Access Control

5%

**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

Guidance

You are in the 'Welcome' section of this questionnaire.

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 special publication [NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations](#)
3. The US Department of Defense [Frequently Asked Questions regarding NIST SP 800-171](#)

NIST SP 800-171 Questionnaire

Welcome

3.1 Access Control

11%



Who in your organization is responsible for providing the answers to NIST SP 800-171 questionnaire? (ref:2.2)

Name

Title

Email

Name

Title

Email

Name

Title

Email

Guidance

You are in the 'Welcome' section of this questionnaire.

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 special publication [NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations](#)
3. The US Department of Defense [Frequently Asked Questions regarding NIST SP 800-171](#)

NIST SP 800-171 Questionnaire

Welcome

3.1 Access Control

3.2 Awareness and Training

16%

Q

Which of the following NIST 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company. If you would like to add comments regarding the controls (i.e. to offer compensating controls that meet a control on this page, or to note which controls do not apply to your company and the reason why they do not apply) please refer to the last page of this questionnaire. (ref:3.1)

- 3.1.1.Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
- 3.1.2.Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
- 3.1.3.Control the flow of CUI in accordance with approved authorizations.
- 3.1.4.Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
- 3.1.5.Employ the principle of least privilege, including for specific security functions and privileged accounts.
- 3.1.6.Use non-privileged accounts or roles when accessing nonsecurity functions.
- 3.1.7.Prevent non-privileged users from executing privileged functions and audit the execution of such functions.
- 3.1.8.Limit unsuccessful logon attempts.
- 3.1.9.Provide privacy and security notices consistent with applicable CUI rules.
- 3.1.10.Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.
- 3.1.11.Terminate (automatically) a user session after a defined condition.
- 3.1.12.Monitor and control remote access sessions.
- 3.1.13.Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
- 3.1.14.Route remote access via managed access control points.
- 3.1.15.Authorize remote execution of privileged commands and remote access to security-relevant information.
- 3.1.16.Authorize wireless access prior to allowing such connections.
- 3.1.17.Protect wireless access using authentication and encryption.
- 3.1.18.Control connection of mobile devices.
- 3.1.19.Encrypt CUI on mobile devices.
- 3.1.20.Verify and control/limit connections to and use of external information systems.
- 3.1.21.Limit use of organizational portable storage devices on external information systems.
- 3.1.22.Control information posted or processed on publicly accessible information systems.

Guidance

You are in the '3.1 Access Control' section of this questionnaire.

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 special publication [NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations](#)
3. The US Department of Defense [Frequently Asked Questions regarding NIST SP 800-171](#)

NIST SP 800-171 Questionnaire

3.1 Access Control

3.2 Awareness and Training

3.3 Audit and Accountab...

21%

Q

Which of the following NIST 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company. If you would like to add comments regarding the controls (i.e. to offer compensating controls that meet a control on this page, or to note which controls do not apply to your company and the reason why they do not apply) please refer to the last page of this questionnaire. (ref:3.2)

- 3.2.1.Ensure that managers, systems administrators, and users of organizational information 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 organizational information systems.
- 3.2.2.Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.
- 3.2.3.Provide security awareness training on recognizing and reporting potential indicators of insider threat.

Guidance

You are in the '3.2 Awareness and Training' section of this questionnaire.

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 special publication [NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations](#)
3. The US Department of Defense [Frequently Asked Questions regarding NIST SP 800-171](#)

NIST SP 800-171 Questionnaire

3.2 Awareness and Training

3.3 Audit and Accountability

3.4 Configuration Manag...

26%

Q

Which of the following NIST 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company. If you would like to add comments regarding the controls (i.e. to offer compensating controls that meet a control on this page, or to note which controls do not apply to your company and the reason why they do not apply) please refer to the last page of this questionnaire. (ref:3.3)

- 3.3.1.Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.
- 3.3.2.Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.
- 3.3.3.Review and update audited events.
- 3.3.4.Alert in the event of an audit process failure.
- 3.3.5.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.
- 3.3.6.Provide audit reduction and report generation to support on-demand analysis and reporting.
- 3.3.7.Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.
- 3.3.8.Protect audit information and audit tools from unauthorized access, modification, and deletion.
- 3.3.9.Limit management of audit functionality to a subset of privileged users.

Guidance

You are in the '3.3 Audit and Accountability' section of this questionnaire.

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 special publication [NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations](#)
3. The US Department of Defense [Frequently Asked Questions regarding NIST SP 800-171](#)

NIST SP 800-171 Questionnaire

3.3 Audit and Accountab...

3.4 Configuration Management

3.5 Identification and...

32%

Q

Which of the following NIST 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company. If you would like to add comments regarding the controls (i.e. to offer compensating controls that meet a control on this page, or to note which controls do not apply to your company and the reason why they do not apply) please refer to the last page of this questionnaire. (ref:3.4)

- 3.4.1. Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
- 3.4.2. Establish and enforce security configuration settings for information technology products employed in organizational information systems.
- 3.4.3. Track, review, approve/disapprove, and audit changes to information systems.
- 3.4.4. Analyze the security impact of changes prior to implementation.
- 3.4.5. Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.
- 3.4.6. Employ the principle of least functionality by configuring the information system to provide only essential capabilities.
- 3.4.7. Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.
- 3.4.8. 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.
- 3.4.9. Control and monitor user-installed software.

Guidance

You are in the '3.4 Configuration Management' section of this questionnaire.

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 special publication [NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations](#)
3. The US Department of Defense [Frequently Asked Questions regarding NIST SP 800-171](#)

NIST SP 800-171 Questionnaire

3.4 Configuration Manag...

3.5 Identification and Authentication

3.6 Incident Response

37%

Q

Which of the following NIST 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company. If you would like to add comments regarding the controls (i.e. to offer compensating controls that meet a control on this page, or to note which controls do not apply to your company and the reason why they do not apply) please refer to the last page of this questionnaire. (ref:3.5)

- 3.5.1. Identify information system users, processes acting on behalf of users, or devices.
- 3.5.2. Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
- 3.5.3. Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
- 3.5.4. Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
- 3.5.5. Prevent reuse of identifiers for a defined period.
- 3.5.6. Disable identifiers after a defined period of inactivity.
- 3.5.7. Enforce a minimum password complexity and change of characters when new passwords are created.
- 3.5.8. Prohibit password reuse for a specified number of generations.
- 3.5.9. Allow temporary password use for system logons with an immediate change to a permanent password.
- 3.5.10. Store and transmit only encrypted representation of passwords.
- 3.5.11. Obscure feedback of authentication information.

Guidance

You are in the '3.5 Identification and Authentication' section of this questionnaire.

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 special publication [NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations](#)
3. The US Department of Defense [Frequently Asked Questions regarding NIST SP 800-171](#)

NIST SP 800-171 Questionnaire

3.5 Identification and...

3.6 Incident Response

3.7 Maintenance

42%

Q

Which of the following NIST 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company. If you would like to add comments regarding the controls (i.e. to offer compensating controls that meet a control on this page, or to note which controls do not apply to your company and the reason why they do not apply) please refer to the last page of this questionnaire. (ref:3.6)

- 3.6.1. Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.
- 3.6.2. Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.
- 3.6.3. Test the organizational incident response capability.

Guidance

You are in the '3.6 Incident Response' section of this questionnaire.

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 special publication [NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations](#)
3. The US Department of Defense [Frequently Asked Questions regarding NIST SP 800-171](#)

NIST SP 800-171 Questionnaire

3.6 Incident Response

3.7 Maintenance

3.8 Media Protection

47%

Q

Which of the following NIST 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company. If you would like to add comments regarding the controls (i.e. to offer compensating controls that meet a control on this page, or to note which controls do not apply to your company and the reason why they do not apply) please refer to the last page of this questionnaire. (ref:3.7)

- 3.7.1.Perform maintenance on organizational information systems.
- 3.7.2.Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.
- 3.7.3.Ensure equipment removed for off-site maintenance is sanitized of any CUI.
- 3.7.4.Check media containing diagnostic and test programs for malicious code before the media are used in the information system.
- 3.7.5.Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.
- 3.7.6.Supervise the maintenance activities of maintenance personnel without required access authorization.

Guidance

You are in the '3.7 Maintenance' section of this questionnaire.

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 special publication [NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations](#)
3. The US Department of Defense [Frequently Asked Questions regarding NIST SP 800-171](#)

NIST SP 800-171 Questionnaire

3.7 Maintenance

3.8 Media Protection

3.9 Personnel Security

53%

Q

Which of the following NIST 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company. If you would like to add comments regarding the controls (i.e. to offer compensating controls that meet a control on this page, or to note which controls do not apply to your company and the reason why they do not apply) please refer to the last page of this questionnaire. (ref:3.8)

- 3.8.1.Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.
- 3.8.2.Limit access to CUI on information system media to authorized users.
- 3.8.3.Sanitize or destroy information system media containing CUI before disposal or release for reuse.
- 3.8.4.Mark media with necessary CUI markings and distribution limitations
- 3.8.5.Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.
- 3.8.6.Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
- 3.8.7.Control the use of removable media on information system components.
- 3.8.8.Prohibit the use of portable storage devices when such devices have no identifiable owner.
- 3.8.9.Protect the confidentiality of backup CUI at storage locations.

Guidance

You are in the '3.8 Media Protection' section of this questionnaire.

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 special publication [NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations](#)
3. The US Department of Defense [Frequently Asked Questions regarding NIST SP 800-171](#)

NIST SP 800-171 Questionnaire

3.8 Media Protection

3.9 Personnel Security

3.10 Physical Protection

58%

Q

Which of the following NIST 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company. If you would like to add comments regarding the controls (i.e. to offer compensating controls that meet a control on this page, or to note which controls do not apply to your company and the reason why they do not apply) please refer to the last page of this questionnaire. (ref:3.9)

- 3.9.1. Screen individuals prior to authorizing access to information systems containing CUI.
- 3.9.2. Ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers.

Guidance

You are in the '3.9 Personnel Security' section of this questionnaire.

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 special publication [NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations](#)
3. The US Department of Defense [Frequently Asked Questions regarding NIST SP 800-171](#)

NIST SP 800-171 Questionnaire

3.9 Personnel Security

3.10 Physical Protection

3.11 Risk Assessment

63%

Q

Which of the following NIST 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company. If you would like to add comments regarding the controls (i.e. to offer compensating controls that meet a control on this page, or to note which controls do not apply to your company and the reason why they do not apply) please refer to the last page of this questionnaire. (ref:3.10)

- 3.10.1.Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
- 3.10.2.Protect and monitor the physical facility and support infrastructure for those information systems
- 3.10.3.Escort visitors and monitor visitor activity.
- 3.10.4.Maintain audit logs of physical access.
- 3.10.5.Control and manage physical access devices.
- 3.10.6.Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).

Guidance

You are in the '3.10 Physical Protection' section of this questionnaire.

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 special publication [NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations](#)
3. The US Department of Defense [Frequently Asked Questions regarding NIST SP 800-171](#)

NIST SP 800-171 Questionnaire

3.10 Physical Protection

3.11 Risk Assessment

3.12 Security Assessment

68%

Q

Which of the following NIST 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company. If you would like to add comments regarding the controls (i.e. to offer compensating controls that meet a control on this page, or to note which controls do not apply to your company and the reason why they do not apply) please refer to the last page of this questionnaire. (ref:3.11)

- 3.11.1.Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of CUI.
- 3.11.2.Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.
- 3.11.3.Remediate vulnerabilities in accordance with assessments of risk.

Guidance

You are in the '3.11 Risk Assessment' section of this questionnaire.

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 special publication [NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations](#)
3. The US Department of Defense [Frequently Asked Questions regarding NIST SP 800-171](#)

NIST SP 800-171 Questionnaire

3.11 Risk Assessment

3.12 Security Assessment

3.13 System and Communi...

74%

Q

Which of the following NIST 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company. If you would like to add comments regarding the controls (i.e. to offer compensating controls that meet a control on this page, or to note which controls do not apply to your company and the reason why they do not apply) please refer to the last page of this questionnaire. (ref:3.12)

- 3.12.1.Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.
- 3.12.2.Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.
- 3.12.3.Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Guidance

You are in the '3.12 Security Assessment' section of this questionnaire.

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 special publication [NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations](#)
3. The US Department of Defense [Frequently Asked Questions regarding NIST SP 800-171](#)

NIST SP 800-171 Questionnaire

3.12 Security Assessment

3.13 System and Communications Prot...

3.14 System and Informa...

79%

Q

Which of the following NIST 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company. If you would like to add comments regarding the controls (i.e. to offer compensating controls that meet a control on this page, or to note which controls do not apply to your company and the reason why they do not apply) please refer to the last page of this questionnaire. (ref:3.13)

- 3.13.1. Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
- 3.13.2. Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.
- 3.13.3. Separate user functionality from information system management functionality.
- 3.13.4. Prevent unauthorized and unintended information transfer via shared system resources.
- 3.13.5. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
- 3.13.6. Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).
- 3.13.7. Prevent remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks.
- 3.13.8. Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
- 3.13.9. Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.
- 3.13.10. Establish and manage cryptographic keys for cryptography employed in the information system
- 3.13.11. Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.***
- 3.13.12. Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.
- 3.13.13. Control and monitor the use of mobile code.
- 3.13.14. Control and monitor the use of Voice over Internet Protocol (VoIP) technologies
- 3.13.15. Protect the authenticity of communications sessions
- 3.13.16. Protect the confidentiality of CUI at rest.

Guidance

You are in the '3.13 System and Communications Protection' section of this questionnaire.

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 special publication [NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations](#)
3. The US Department of Defense [Frequently Asked Questions regarding NIST SP 800-171](#)

NIST SP 800-171 Questionnaire

3.13 System and Communi...

3.14 System and Information Integrity

Additional Details

84%

Q

Which of the following NIST 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company. If you would like to add comments regarding the controls (i.e. to offer compensating controls that meet a control on this page, or to note which controls do not apply to your company and the reason why they do not apply) please refer to the last page of this questionnaire. (ref:3.14)

- 3.14.1. Identify, report, and correct information and information system flaws in a timely manner.
- 3.14.2. Provide protection from malicious code at appropriate locations within organizational information systems.
- 3.14.3. Monitor information system security alerts and advisories and take appropriate actions in response.
- 3.14.4. Update malicious code protection mechanisms when new releases are available.
- 3.14.5. Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.
- 3.14.6. Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
- 3.14.7. Identify unauthorized use of the information system.

Guidance

You are in the '3.14 System and Information Integrity' section of this questionnaire.

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 special publication [NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations](#)
3. The US Department of Defense [Frequently Asked Questions regarding NIST SP 800-171](#)

NIST SP 800-171 Questionnaire

3.14 System and Informa...

Additional Details

Submission

89%



If your organization has not fully implemented all NIST 800-171 controls please provide an Estimated Completion Date (ECD) of when your organization expects to be compliant with the NIST 800-171 controls. According to the United States Department of Defense this date shall not exceed December 31, 2017. If applicable please provide a summary of your organization's **Remediation Plan** and a description of any **Compensating Controls** your organization has implemented in place of specific NIST controls or describe those controls that do not apply to your company and the basis for this determination. When referring to NIST controls please utilize the control number assigned by NIST to the particular control. Your organization may also upload a document in support of either and / or the Remediation Plan and Compensating Controls. (ref:4.1)

ECD

Month Day Year

Remediation Plan

Max. File Size allowed is 50MB.

Upload File

No file selected

Compensating Controls

Max. File Size allowed is 50MB.

Upload File

No file selected

Guidance

You are in the 'Additional Details' section of this questionnaire.

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 special publication [NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations](#)
3. The US Department of Defense [Frequently Asked Questions regarding NIST SP 800-171](#)

NIST SP 800-171 Questionnaire

Additional Details

Submission

95%



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)

By clicking "**Send Response**", I certify that to the best of my knowledge the information entered about my organization on the NIST SP 800-171 questionnaire is correct.

Please confirm your details below and amend as necessary.

Name

Title

Email

You are about to send the information provided in this assessment.

To review your answers and make any final amendments prior to sending, please click "**View Answers**" below.

To send your responses, please click "**Send Response**" below.

Guidance

You are in the 'Submission' section of this questionnaire.

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 special publication [NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations](#)
3. The US Department of Defense [Frequently Asked Questions regarding NIST SP 800-171](#)