NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1

Table of Contents

1) Background

a) Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, requires contractors and subcontractors to provide 'adequate security' to safeguard covered defense information, hereto referred to, for the purposes of this methodology, as Department of Defense (DoD) controlled unclassified information (CUI)[1], when residing on or transiting through a contractor's/subcontractor's internal information system or network, and to report cyber incidents that affect that system or network to DoD. DFARS clause 252.204-7012 further states that to provide adequate security, the Contractor shall implement, at a minimum, the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations. Contractors are also required to flow down DFARS Clause 252.204-7012 to all subcontracts for operationally critical support, or for which subcontract performance will involve DoD CUI. Contractors must mark or otherwise identify, in accordance with direction contained within the specific contract, DoD CUI that is collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of performance of the contract.

b) DFARS provision 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls, requires, among other things, offerors to represent they will implement the security requirements in NIST SP 800-171 in effect at the time the solicitation is issued or as authorized by the contracting officer. To document implementation of NIST SP 800-171, the contractor must develop, document, and periodically update a system security plan that describes system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. If implementation of the security requirements is not complete, companies must develop and implement plans of action to describe when and how any unimplemented security requirements will be met.

c) Under Secretary of Defense (Acquisition and Sustainment) (USD(A&S)) memorandum, "Strategically Implementing Cybersecurity Contract Clauses," dated February 5, 2019, directed the Defense Contract Management Agency (DCMA) to pursue, with companies for which they administer contracts, the application of a standard methodology and approach to assess a contractor's implementation of NIST SP 800-171 at a strategic (corporate-wide) level as an alternative to the requirement for

[1] DoD is transitioning from the use of the term 'covered defense information' in the DFARS to "DOD Controlled Unclassified Information (CUI), consistent with DoDI 5200.48, Controlled Unclassified Information (CUI)"

contractors to document implementation of NIST SP 800-171 on a contract-by-contract basis.

2) Purpose

   a) The *NIST SP 800-171 DoD Assessment Methodology, Version 1.2* documents a standard methodology that enables a strategic assessment of a contractor's implementation of NIST SP 800-171, a requirement for compliance with DFARS clause 252.204-7012.

   b) This methodology is used for assessment purposes only and does not, and is not intended to, add any substantive requirements to either NIST SP 800-171 or DFARS clause 252.204-7012.

   c) DoD will use this methodology to assess the implementation of NIST SP 800-171 by its prime contractors. Prime contractors may use this methodology to assess the implementation status of NIST SP 800-171 by subcontractors.

   d) This methodology informed the conduct of pilot *NIST SP 800-171 DoD Assessments* performed by DCMA, in partnership with the Defense Counterintelligence and Security Agency (DCSA) and the DoD Components, during 2019. DoD will update and codify this methodology in policy/regulation.

3) Strategically Assessing a Contractor's Implementation of NIST SP 800-171

   a) The *NIST SP 800-171 DoD Assessment Methodology* enables DoD to strategically assess a contractor's implementation of NIST SP 800-171 on existing contracts which include DFARS clause 252.204-7012, and to provide DoD Components with visibility to the summary level scores of strategic assessments completed by DoD, thus providing an alternative to the contract-by-contract approach.

   b) The *NIST SP 800-171 DoD Assessment* consists of three levels of assessments (see Section 4 of this document). These three types of assessments reflect the depth of the assessment, and the associated level of confidence in the assessment results.

   c) Assessment of contractors with contracts containing DFARS clause 252.204-7012 is anticipated to be once every three years unless other factors, such as program criticality/risk or a security-relevant change, drive the need for a different assessment frequency.

4) Levels of Assessment

   a) Basic (Contractor Self-Assessment) *NIST SP 800-171 DoD Assessment*

      i) The Basic Assessment is the Contractor's self- assessment of NIST SP 800-171 implementation status, based on a review of the system security plan(s) associated with covered contractor information system(s), and conducted in accordance with

NIST SP 800-171A, "Assessing Security Requirements for Controlled Unclassified Information" and Section 5 and Annex A of this document.

ii) The Basic Assessment results in a confidence level of 'Low' in the resulting score because it is a self-generated score.

iii) The summary level scores resulting from Basic *NIST SP 800-171 DoD Assessments* should be documented as indicated in Section 6 and Annex B of this document.

b) Medium *NIST SP 800-171 DoD Assessment*

i) The Medium Assessment is conducted by DoD personnel who have been trained in accordance with DoD policy and procedures to conduct the assessment. It is anticipated that Medium Assessments will be conducted primarily by Program Management Office cybersecurity personnel, as part of a separately scheduled visit (e.g., for a Critical Design Review).

ii) The assessment will consist of a review of the system security plan description of how each requirement is met to identify any descriptions which may not properly address the security requirements.

iii) The Medium Assessment results in a confidence level of 'Medium' in the resulting score.

iv) The DoD assessor will document summary level scores resulting from Medium *NIST SP 800-171 DoD Assessments* as indicated in Section 6 of this document.

c) High (On-Site or Virtual) *NIST SP 800-171 DoD Assessment*

i) The High Assessment, conducted by DoD personnel who have been trained in accordance with DoD policy and procedures to conduct the assessment, requires a thorough on-site or virtual[2] verification/examination/demonstration of the Contractor's system security plan and implementation of the NIST SP 800-171 security requirements.

ii) The High Assessment is conducted using NIST SP 800-171A, "Assessing Security Requirements for Controlled Unclassified Information." The assessment will determine if the implementation meets the requirements by reviewing appropriate evidence and/or demonstration (e.g., recent scanning results, system inventories, configuration baselines, demonstration of multifactor authentication).

iii) An on-site High *NIST SP 800-171 DoD Assessment* is the preferred methodology for a full evaluation of the risk to DoD CUI because of the ability to verify and validate the effectiveness of the safeguards that implement security

[2] A virtual High Assessment was developed in response to the COVID-19 epidemic to allow protections of assessors and DIB personal to limit travel and exposure of staffs whilst still being able to assess contractor risk. The government may utilize this methodology in the future as required in response to similar or other scenarios.

requirements defined in NIST Special Publication 800-171. While a High Assessment maybe be conducted virtually in lieu of onsite, a virtual assessment will not fully cover all the NIST SP 800-171 requirements, resulting in a less than full understanding of overall risk.

iv) A virtual High Assessment utilizes the same methodology as the on-site with added data protections processes enacted to protect the DIB data that is shared with assessment teams. All data is transmitted through DoD Secure Access File Exchange (SAFE), is only reviewed locally on each assessor's computer (screen sharing is conducted utilizing DoD collaboration mediums that are approved for processing CUI) and contractor data is destroyed post assessment using NSA guidance for data destruction. With concurrence from the DIB companies being assessed, the assessment verifies and examines all documents utilizing the NIST SP 800-171A methodology minus the demonstration or testing of some requirements. In some cases, a follow-up on-site assessment of the items not assessed may be required or requested.

v) The first step in a High Assessment is for the contractor to conduct a Basic Assessment and submit results to the Department using the procedures in Annex B of this document. The High Assessment consists of a review of the Basic Assessment, a thorough document review and discussion with the contractor regarding the results to obtain additional information or clarification as needed, combined with government validation that the security requirements have been implemented as described in the system security plan. Network access by the assessor(s) is not required.

vi) The High Assessment results in a confidence level of 'High' in the resulting score.

vii) The DoD assessor will document summary level scores resulting from High *NIST SP 800-171 DoD Assessments* as indicated in Section 6 of this document.

5) *NIST SP 800-171 DoD Assessment* Scoring Methodology

a) This scoring methodology is designed to provide an objective assessment of a contractor's NIST SP 800-171 implementation status. With the exception of requirements for which the scoring of partial implementation is built-in (e.g., multi-factor authentication, security requirement 3.5.3) the methodology is not designed to credit partial implementation.

b) Conduct of the *NIST SP 800-171 DoD Assessment* will result in a score reflecting the net effect of security requirements not yet implemented. If all security requirements are implemented, a contractor is awarded a score of 110, consistent with the total number of NIST SP 800-171 security requirements. For each security requirement not met, the associated value is subtracted from 110. The score of 110 is reduced by each requirement not implemented, which may result in a negative score.

c) While NIST SP 800-171 does not prioritize security requirements, certain requirements have more impact on the security of the network and its data than others. This scoring methodology incorporates this concept by weighting each security requirement based on the impact to the information system and the DoD CUI created on or transiting through that system, when that requirement is not implemented.

d) Weighted requirements include all of the fundamental NIST SP 800-171 'Basic Security Requirements' - high-level requirements which, if not implemented, render ineffective the more numerous 'Derived Security Requirements'; and a subset of the 'Derived Security Requirements'- requirements that supplement the Basic Security Requirements - which, if not implemented, would allow for exploitation of the network and its information.

   i) For security requirements that, if not implemented, could lead to significant exploitation of the network, or exfiltration of DoD CUI, 5 points are subtracted from the score of 110. For example, failure to limit system access to authorized users (Basic Security Requirement 3.1.1) renders all the other Access Control requirements ineffective, allowing easy exploitation of the network; failure to control the use of removable media on system components (Derived Security Requirement 3.8.7) could result in massive exfiltration of CUI and introduction of malware.

      (1) Basic Security Requirements with a value of 5 points include 3.1.1, 3.1.2, 3.2.1, 3.2.2, 3.3.1, 3.4.1, 3.4.2, 3.5.1, 3.5.2, 3.6.1, 3.6.2, 3.7.2, 3.8.3, 3.9.2, 3.10.1, 3.10.2, 3.12.1, 3.12.3, 3.13.1, 3.13.2, 3.14.1, 3.14.2, and 3.14.3.

      (2) Derived Security Requirements with a value of 5 points include 3.1.12, 3.1.13, 3.1.16, 3.1.17, 3.1.18, 3.3.5, 3.4.5, 3.4.6, 3.4.7, 3.4.8, 3.5.10, 3.7.5, 3.8.7, 3.11.2, 3.13.5, 3.13.6, 3.13.15, 3.14.4, and 3.14.6.

   ii) For Basic and Derived Security Requirements that, if not implemented, have a specific and confined effect on the security of the network and its data, 3 points are subtracted from the score of 110. For example, failure to limit access to CUI on system media to authorized users (Security Requirement 3.8.2) or failure to encrypt CUI stored on a mobile device (Security Requirement 3.1.19), put the CUI stored on the system media or mobile device at risk, but not the CUI stored on the network itself.

      (1) Basic Security Requirements with a value of 3 points include 3.3.2, 3.7.1, 3.8.1, 3.8.2, 3.9.1, 3.11.1, and 3.12.2.

      (2) Derived Security Requirements with a value of 3 points include 3.1.5, 3.1.19, 3.7.4, 3.8.8, 3.13.8, 3.14.5, and 3.14.7.

   iii) All remaining Derived Security Requirements, if not implemented, have a limited or indirect effect on the security of the network and its data. For these, 1 point

is subtracted from the score of 110. For example, failing to prevent reuse of identifiers for a defined period (Security Requirement 3.5.5) could allow a user access to CUI to which they were not approved.

e) Two Derived Security Requirements can be partially effective even if not completely or properly implemented, and the points deducted should be adjusted depending on how the security requirement is implemented.

   i) Multi-factor authentication (MFA) (Security Requirement 3.5.3) is typically implemented first for remote and privileged users (since these users are both limited in number and more critical) and then for the general user, so 3 points are subtracted from the score of 110 if MFA is implemented only for remote and privileged users; 5 points are subtracted from the score of 110 if MFA is not implemented for any users.

   ii) FIPS validated encryption (Security Requirement 3.13.11) is required to protect the confidentiality of CUI. If encryption is employed, but is not FIPS validated, 3 points are subtracted from the score of 110; if encryption is not employed, 5 points are subtracted from the score of 110.

f) Although not common, future revisions of NIST SP 800-171 may add, delete or substantively revise security requirements. When this occurs, a value will be assigned to any new or modified requirements in accordance with this scoring methodology.

g) The contractor must have a system security plan (Basic Security Requirement 3.12.4) in place to describe each covered contractor information system, and a plan of action (Basic Security Requirement 3.12.2) in place for each unimplemented security requirement to describe how and when the security requirement will be met.

   i) Since the NIST SP 800-171 DoD Assessment scoring methodology is based on the review of a system security plan describing how the security requirements are met, it is not possible to conduct the assessment if the information is not available. The absence of a system security plan would result in a finding that 'an assessment could not be completed due to incomplete information and noncompliance with DFARS clause 252.204-7012.'

   ii) Plans of action addressing unimplemented security requirements are not a substitute for a completed requirement. Security requirements not implemented, whether a plan of action is in place or not, will be assessed as 'not implemented.' For example, if the initial roll-out of 3.5.3, multifactor authentication, is only 75% complete, and there is a plan of action still being implemented, 3.5.3 will be considered 'not implemented', as the requirement has not been fully implemented.

   iii) A lack of plan of action for unimplemented security requirements will result in Security Requirement 3.12.2 being assessed as 'not implemented.'

h) Temporary deficiencies and/or isolated enduring exceptions which occur during initial implementation, or arise after implementation, are to be expected in most complex environments.

   i) Temporary deficiencies that are appropriately addressed in plans of action (i.e., include deficiency reviews, milestones, and show progress towards the implementation of corrections to reduce or eliminate identified vulnerabilities) should be assessed as 'implemented.' For example, when a plan of action addresses a 'temporary deficiency' that arises after implementation (e.g., 3.13.11, employ FIPS validated cryptography, had been implemented, but subsequently a patch invalidated the FIPS validation of a particular cryptographic module), the requirement will be scored 'as implemented.' A 'temporary deficiency' may also arise during initial implementation of a NIST SP 800-171 requirement if, during roll-out, specific issues with certain equipment is discovered that has to be separately addressed (e.g., certain specific hardware or software unexpectedly needs to be changed for the requirement to be successfully applied). If the implementation roll-out has otherwise been completed, this 'temporary deficiency' plan of action would be considered, and the requirement scored 'as implemented.' There is no standard duration for which a 'temporary deficiency' may be active. It is what is reasonable, which would take into consideration the availability of the solution, the cost and time to implement, the overall risk and whether any mitigations are applied in the interim. Generally, deficiencies should be resolved as soon as is reasonably possible.

   ii) Isolated enduring exceptions encountered during implementation, such as unique equipment or environments (e.g., specialized manufacturing equipment or a unique laboratory environment) may prevent the implementation of certain security requirements. Isolated enduring exceptions are typically not suitable to address in plans of action, but when described, along with any mitigations, in the system security plan such exceptions should be assessed as 'implemented.'

i) For certain requirements, questions often arise on whether or not they are actually implemented. These situations are addressed below:

   i) Security Requirements 3.1.12, 3.1.16, 3.1.18: Companies commonly do not allow remote access, wireless access or connection of mobile devices and may indicate these requirements as 'Not Applicable' or 'Not Implemented' in the system security plan. The evaluator should not deduct points in such cases. However, if the company disallows use of remote, wireless, or mobile access, they should also have a policy and procedure in place to insure these capabilities are not enabled inadvertently. This should be discussed as part of the Medium-

Level assessment, and if such policy and procedures are not in place a point should be assessed.

ii) Security Requirement 3.13.8: When implementing this requirement, encryption, though preferred, is not required if using common-carrier provided Multiprotocol Label Switching (MPLS), as the MPLS separation provides sufficient protection without encryption.

iii) Security Requirement 3.13.11: Cryptography used to protect the confidentiality of CUI must be FIPS-validated, which means the cryptographic module has to have been tested and validated to meet FIPS 140-1 or-2 requirements. Simply using an approved algorithm (e.g., FIPS 197 for AES) is not sufficient - the module (software and/or hardware) used to implement the algorithm must be separately validated under FIPS 140. Note however, that this is required when encryption is required for protection, which is typically external to the contractor's covered information system (assuming the system meets NIST SP 800-171). Cryptography used for other purposes within the protected information system need not be FIPS validated. When required, if encryption is not employed (FIPS validated or otherwise), 5 points are subtracted from the score of 110. If encryption is employed, but is not FIPS validated, 3 points are subtracted from the score of 110. Isolated use of non-FIPS validated cryptography, with an associated Plan of Action, should be treated as a temporary deficiency and assessed as 'implemented.'

j) If a contractor received a favorable adjudication from the DoD CIO indicating that a requirement is not applicable or that an alternative security measure is equally effective in accordance with DFARS 252.204-7008 or 7012, the DoD CIO assessment should be included in the Contractor's system security plan. Implemented security measures adjudicated by the DoD CIO as equally effective, and security requirements approved by the DoD CIO as 'not applicable,' will be assessed as 'implemented.' Once DOD CIO assessments approving "not applicable" requirements or "alternative security measures" are included in the Contractor's system security plan, the contractor does not need to submit that documentation for every current contract with the DFARS 252.204-7012 clause unless specifically requested to do so by the contracting officer. When completing the Basic (Contractor Self-Assessment) NIST SP 800-171 DoD Assessment Results Format, the contractor shall score any security requirements for which an assessment of "not applicable" or "alternative security measures" was previously approved by DoD CIO as 'implemented'.

k) A template illustrating the application of this scoring methodology is provided at Annex A of this document.

l) DoD will provide medium and high assessment results to the Contractor and offer the opportunity for rebuttal and adjudication of assessment results. Upon completion of

each assessment, the assessed contractor has 14 business days to provide additional information to the assessment team, to demonstrate that they meet any security requirements not observed by the assessment team or to rebut the findings that may be of question.

6) Documenting *NIST SP 800-171 DoD Assessment* Results

a) A summary level score for basic assessments completed by the Contractor, and for medium and high assessments conducted by DoD, will be posted in the Supplier Performance Risk System (SPRS) to provide DoD Components with visibility to the results of strategic assessments.

i) SPRS is defined by DoD Instruction (DoDI) 5000.79, Defense-wide Sharing and Use of Supplier and Product Performance Information, October 15, 2019 available at https:\\www.esd.whs.mil/DD/.

ii) SPRS is the authoritative source to retrieve supplier and product performance information for the DoD acquisition community to assess and monitor unclassified performance, and to assess corporate business practices related to DoD contracts and the supplier's management of risk.

b) Assessment results posted in SPRS are available to DoD personnel, and are protected, in accordance with the standards set forth in DoD Instruction 5000.79, Defense-wide Sharing and Use of Supplier and Product Performance Information (PI), available at https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500079p.PDF?ver=2019-10-15-115609-957. Authorized representatives of the Contractor for which the assessment was conducted may access SPRS to view their own results in accordance with the SPRS Software User's Guide for Awardees/Contractors available at https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf.

c) A contractor may post the results of their Basic Assessments conducted in accordance with Section 5 and Annex B of this document in SPRS (via the Procurement Integrated Enterprise Environment (PIEE)).

d) DoD will post the following Medium and/or High *NIST SP 800-171 DoD Assessment* results to SPRS for each system security plan assessed:

i) The standard assessed (e.g., NIST SP 800-171 Rev 1).

ii) Organization conducting the assessment, e.g., DCMA, or a specific organization (identified by Department of Defense Activity Address Code (DoDAAC) or Commercial and Government Entity (CAGE) Code).

iii) Each system security plan assessed, mapped to the specific industry CAGE code(s) associated with the information system(s) addressed by the system security plan. All corporate CAGE codes must be mapped to all appropriate

system security plan(s) if the contractor has more than one system security plan and CAGE code. Additionally, a brief description of the system security plan architecture may be required if more than one plan exists.

iv) Date and level of the assessment, i.e., basic, medium, or high.

v) Summary level score (e.g., 105 out of 110), but not the individual value assigned for each requirement.

vi) Date a score of 110 is expected to be achieved (i.e., all requirements implemented) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800-171.

e) Department policy/procedures/guidance will be updated to direct acquisition/procurement officials and contractors to access SPRS to determine if a strategic assessment has been conducted.

f) DoD Components should rely on assessment results posted in SPRS in lieu of including requirements to assess implementation of NIST SP 800-171 on a contract-by-contract basis.

g) A High *NIST SP 800-171 DoD Assessment* may result in documentation in addition to that listed in 6) d) of this document. DoD will retain and protect any such documentation as For Official Use Only (FOUO) and intended for internal DoD use only. The information will be protected against unauthorized use and release, including through the exercise of applicable exemptions under the Freedom of Information Act (e.g., Exemption 4 covers trade secrets and commercial or financial information obtained from a contractor that is privileged or confidential).

7) Glossary of Terms

a) Enduring exception. Remediation is not feasible; no plan of action required; must be documented within a system security plan.

b) Temporary deficiency. Remediation of deficiency is feasible; known fix is in process; requires a plan of action. For the purposes of a DoD NIST SP 800-171 DoD Assessment, a 'temporary deficiency' is not based on an 'in progress' initial implementation of the requirement. A temporary deficiency arises after implementation. A Temporary deficiency may also apply during the initial implementation of a NIST SP 800-171 requirement if, during roll-out, specific issues with certain equipment is discovered that has to be separately addressed.

Annex A - *NIST SP 800-171 DoD Assessment* Scoring Template

- The following template illustrates the scoring methodology described in Section 5. If all requirements are met, a score of 110 is awarded. For each requirement not met, the associated value is subtracted from 110. Consistency results from the fact that the assessments are based on what is not yet implemented, or document that all requirements have been met.
- It is important to note an assessment is about the extent to which the company has implemented the requirements. It is not a value judgement about the specific approach to implementing – in other words, all solutions that meet the requirements are acceptable. This is not an assessment of one solution compared to another.
- Scoring for Basic, Medium, and High *NIST SP 800-171 DoD Assessments* is the same.
- While NIST does not prioritize requirements in terms of impact, certain requirements do have more impact than others. In this scoring methodology security requirements are weighted based on their effect on the information system and DoD CUI created on or transiting that system.

NIST SP 800-171 DoD Assessment Scoring Template

Security Requirement		Value	Comment
3.1.1*	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	5	
3.1.2*	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	5	
3.1.3	Control the flow of CUI in accordance with approved authorizations.	1	
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	1	
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	3	
3.1.6	Use non-privileged accounts or roles when accessing non-security functions.	1	
3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	1	
3.1.8	Limit unsuccessful logon attempts.	1	

Security Requirement		Value	Comment
3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	1	
3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	1	
3.1.11	Terminate (automatically) a user session after a defined condition.	1	
3.1.12	Monitor and control remote access sessions.	5	Do not subtract points if remote access not permitted
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	5	Do not subtract points if remote access not permitted
3.1.14	Route remote access via managed access control points.	1	
3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	1	
3.1.16	Authorize wireless access prior to allowing such connections.	5	Do not subtract points if wireless access not permitted
3.1.17	Protect wireless access using authentication and encryption.	5	Do not subtract points if wireless access not permitted
3.1.18	Control connection of mobile devices.	5	Do not subtract points if connection of mobile devices is not permitted
3.1.19	Encrypt CUI on mobile devices and mobile computing platforms	3	Exposure limited to CUI on mobile platform
3.1.20*	Verify and control/limit connections to and use of external systems.	1	
3.1.21	Limit use of portable storage devices on external systems.	1	
3.1.22*	Control CUI posted or processed on publicly accessible systems.	1	
3.2.1	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.	5	

Security Requirement		Value	Comment
3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	5	
3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	1	
3.3.1	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	5	
3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	3	
3.3.3	Review and update logged events.	1	
3.3.4	Alert in the event of an audit logging process failure.	1	
3.3.5	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	5	
3.3.6	Provide audit record reduction and report generation to support on-demand analysis and reporting.	1	
3.3.7	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	1	
3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	1	
3.3.9	Limit management of audit logging functionality to a subset of privileged users.	1	
3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	5	

Security Requirement		Value	Comment
3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational systems.	5	
3.4.3	Track, review, approve or disapprove, and log changes to organizational systems.	1	
3.4.4	Analyze the security impact of changes prior to implementation.	1	
3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	5	
3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	5	
3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	5	
3.4.8	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	5	
3.4.9	Control and monitor user-installed software.	1	
3.5.1*	Identify system users, processes acting on behalf of users, and devices.	5	
3.5.2*	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	5	
3.5.3	Use multifactor authentication (MFA) for local and network access to privileged accounts and for network access to non-privileged accounts.	3 to 5	Subtract 5 points if MFA not implemented. Subtract 3 points if implemented for remote and privileged users, but not the general user
3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	1	
3.5.5	Prevent reuse of identifiers for a defined period.	1	
3.5.6	Disable identifiers after a defined period of inactivity.	1	

Security Requirement		Value	Comment
3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	1	
3.5.8	Prohibit password reuse for a specified number of generations.	1	
3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.	1	
3.5.10	Store and transmit only cryptographically-protected passwords.	5	Encrypted representations of passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords
3.5.11	Obscure feedback of authentication information.	1	
3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	5	
3.6.2	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	5	
3.6.3	Test the organizational incident response capability.	1	
3.7.1	Perform maintenance on organizational systems.	3	
3.7.2	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	5	
3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	1	
3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	3	
3.7.5	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	5	

Security Requirement		Value	Comment
3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization.	1	
3.8.1	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	3	Exposure limited to CUI on media
3.8.2	Limit access to CUI on system media to authorized users.	3	Exposure limited to CUI on media
3.8.3*	Sanitize or destroy system media containing CUI before disposal or release for reuse.	5	While exposure limited to CUI on media, failure to sanitize can result in continual exposure of CUI
3.8.4	Mark media with necessary CUI markings and distribution limitations.	1	
3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	1	
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.	1	
3.8.7	Control the use of removable media on system components.	5	
3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	3	
3.8.9	Protect the confidentiality of backup CUI at storage locations.	1	
3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI.	3	
3.9.2	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	5	
3.10.1*	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	5	
3.10.2	Protect and monitor the physical facility and support infrastructure for organizational systems.	5	

Security Requirement		Value	Comment
3.10.3*	Escort visitors and monitor visitor activity.	1	
3.10.4*	Maintain audit logs of physical access.	1	
3.10.5*	Control and manage physical access devices.	1	
3.10.6	Enforce safeguarding measures for CUI at alternate work sites.	1	
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 systems and the associated processing, storage, or transmission of CUI.	3	
3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	5	
3.11.3	Remediate vulnerabilities in accordance with risk assessments.	1	
3.12.1	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	5	
3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	3	
3.12.3	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	5	
3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	NA	The absence of a system security plan would result in a finding that 'an assessment could not be completed due to incomplete information and noncompliance with DFARS clause 252.204-7012.'
3.13.1*	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.	5	

Security Requirement		Value	Comment
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	5	
3.13.3	Separate user functionality from system management functionality.	1	
3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.	1	
3.13.5*	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	5	
3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	5	
3.13.7	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).	1	
3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	3	
3.13.9	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	1	
3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems.	1	
3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	3 to 5	Subtract 5 points if no cryptography is employed; 3 points if mostly not FIPS validated
3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	1	

Security Requirement		Value	Comment
3.13.13	Control and monitor the use of mobile code.	1	
3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	1	
3.13.15	Protect the authenticity of communications sessions.	5	
3.13.16	Protect the confidentiality of CUI at rest.	1	
3.14.1*	Identify, report, and correct system flaws in a timely manner.	5	
3.14.2*	Provide protection from malicious code at designated locations within organizational systems.	5	
3.14.3	Monitor system security alerts and advisories and take action in response.	5	
3.14.4*	Update malicious code protection mechanisms when new releases are available.	5	
3.14.5*	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.	3	
3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	5	
3.14.7	Identify unauthorized use of organizational systems	3	

* Basic safeguarding requirements and procedures to protect covered contractor information systems per Federal Acquisition Regulation (FAR) clause 52.204-21, Basic Safeguarding of Covered Contractor Information Systems.

Annex B - Basic (Contractor Self-Assessment) NIST SP 800-171 DoD Assessment Results Format

- Score your implementation of the security requirements in NIST SP 800-171 based on Section 5 and Annex A of this document.
- Document your Basic (self) NIST SP 800-171 DoD Assessment score in Supplier Performance Risk System (SPRS). A Procurement Integrated Enterprise Environment (PIEE) account with a SPRS "Cyber Vendor" role will be required to enter Basic Assessment information into SPRS. This role may be requested through PIEE.
- Information required for entering results of a Basic NIST SP 800-171 DoD Assessment into SPRS include:
    - Date of the assessment
    - Summary level score (e.g., 95 out of 110, NOT the individual value for each requirement)
    - Scope of the Basic Assessment - Identify each system security plan (security requirement 3.12.4) supporting the performance of this contract. All company CAGE codes must be mapped to the appropriate system security plan(s). Additionally, a brief description of the plan architecture may be required, if more than one plan exists.
        - Select Open CAGE Hierarchy to choose CAGEs covered by the system security plan.
        - Note: if a CAGE does not appear in the hierarchy, update your company's records in the System for Award Management (SAM); ensure immediate/ highest level owner CAGEs are correctly indicated. SPRS will normally be updated within 24 hours.
    - Plan of Action Completion Date – date that a score of 110 is expected to be achieved for each system security plan assessed (i.e., all requirements implemented) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800-171 (security requirement 3.12.2).
- Informational links include:
    - PIEE Landing Page: https://wawf.eb.mil/piee-landing/
    - Information on requesting access via PIEE may be found here: https://www.sprs.csd.disa.mil/access.htm
    - Information on entering Cyber assessment scores into SPRS may be found here: https://www.sprs.csd.disa.mil/reference.htm
    - SPRS Homepage: https://www.sprs.csd.disa.mil/default.htm