YourIT!
Your Logo Goes Here

NIST SP 800-171 DoD Assessment Score Report

CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Prepared for: Client Company

Prepared by: YourIT Company

NIST SP 800-171 DoD Assessment Score Report

1 - Overview

We perform a periodic assessment of our information system environment with regards to the principles and functions set as part of the CMMC and NIST 800-171. The assessment consists of automated scans in conjunction with a review by an Internal Assessor.

The report contains an overview of the NIST 800-171 Rev. 2 security requirements and the current state of compliance with the requirements.

The methodology for the review and supporting documentation can be found in the various assessment worksheets and documents. Issues are noted in the Plan of Action and Milestones report.

2 - Assessment Methodology and NIST SP 800-171 DoD Assessment Scoring

2.1 - DoD Assessment Score Determination

We have performed a Security Plan Risk Assessment as part of our routine CMMC and NIST 800-171 Rev. 2 compliance review.

Based on the results of the Risk Assessment, we formulated an assessment score. This score is derived from our documented compliance with the NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1 published on June 24, 2020.

See the System Security Plan, NIST 800-181 Assessment Report (or the CMMC 2.0 - Level 2 Assessment Report) and the Plan of Action and Milestones report associated with the System assessed.

2.2 - NIST SP 800-171 DoD Assessment Score

Below is the DoD assessment score.

Maximum Assessment Score Value	110
Accumulated Control Point Value Deduction	-43

DoD Assessment Score	67

See section 3 of this report for the individual score value determined for each NIST SP 800-171 security control requirement.

2.3 - Accumulated Security Control Point Value Deductions by NIST 800-171 Control Family

NIST 800-171 Control Family	Accumulated Control Point Value Deductions
3.1 - Access Control	-13
3.2 - Awareness and Training	-1
3.3 - Audit and Accountability	-7
3.4 - Configuration Management	-5
3.5 - Identification and Authentication	-6
3.6 - Incident Response	0
3.7 - Maintenance	0
3.8 - Media Protection	0
3.9 - Personnel Security	0
3.10 - Physical Protection	0
3.11 - Risk Management	0
3.12 - Security Assessment	0
3.13 - System and Communications Protection	-1
3.14 - System and Information Integrity	-10
Total Scores	**-43**

3 - System Security Requirements and Scoring

We assessed our implementation of security requirements using the NIST 800-171 DoD Assessment Methodology.

When a NIST 800-171 security control is determined to be either "Not Implemented" or "Planned" to be implemented, point values are deducted from a total score of 110. The value 110 reflects the total number of NIST 800-171 security control requirements.

The Control Point Value deductions are based on the point values referenced in the following document published by the DoD:

NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1, June 24, 2020

A score resulting in a negative value can be determined based on the DoD Assessment's weighted scoring methodology.

The following is a key of "Control Implementation Status" types referenced in the assessment of the NIST 800-171 security requirements. This key presents how the control implementation status types impact the number of points that may be deducted during the DoD Assessment scoring process.

Control Implementation Status	Control Point Values Deducted?
Implemented	**No**
Not Implemented	**Yes**
Planned	**Yes**
Not Applicable	**No**

Below is an overview of NIST 800-171 control implementation status associated with each security requirement for the system assessed.

3.1 - Access Control

Security Requirement	Control Implementation Status	Control Point Value Deducted	Comments (DoD Supplied Guidance)
3.1.1: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Implemented	0	
3.1.2: Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Planned	-5	
3.1.3: Control the flow of CUI in accordance with approved authorizations.	Implemented	0	
3.1.4: Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Implemented	0	
3.1.5: Employ the principle of least privilege, including for specific security functions and privileged accounts.	Implemented	0	
3.1.6: Use non-privileged accounts or roles when accessing nonsecurity functions.	Implemented	0	
3.1.7: Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	Implemented	0	
3.1.8: Limit unsuccessful logon attempts.	Not Implemented	-1	
3.1.9: Provide privacy and security notices consistent	Implemented	0	

Security Requirement	Control Implementation Status	Control Point Value Deducted	Comments (DoD Supplied Guidance)
with applicable CUI rules.			
3.1.10: Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.	Implemented	0	
3.1.11: Terminate (automatically) a user session after a defined condition.	Implemented	0	
3.1.12: Monitor and control remote access sessions.	Planned	-5	Do not subtract points if remote access not permitted
3.1.13: Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Implemented	0	Do not subtract points if remote access not permitted
3.1.14: Route remote access via managed access control points.	Implemented	0	
3.1.15: Authorize remote execution of privileged commands and remote access to security-relevant information.	Implemented	0	
3.1.16: Authorize wireless access prior to allowing such connections.	Implemented	0	Do not subtract points if wireless access not permitted
3.1.17: Protect wireless access using authentication and encryption.	Implemented	0	Do not subtract points if wireless access not permitted
3.1.18: Control connection of mobile devices.	Implemented	0	Do not subtract points if connection of mobile devices is not permitted
3.1.19: Encrypt CUI on mobile devices.	Implemented	0	Exposure limited to CUI on mobile platform

Security Requirement	Control Implementation Status	Control Point Value Deducted	Comments (DoD Supplied Guidance)
3.1.20: Verify and control/limit connections to and use of external information systems.	Planned	-1	
3.1.21: Limit use of organizational portable storage devices on external information systems.	Implemented	0	
3.1.22: Control information posted or processed on publicly accessible information systems.	Not Implemented	-1	
Total Points to be Deducted for this Control Family		**-13**	

3.2 - Awareness and Training

Security Requirement	Control Implementation Status	Control Point Value Deducted	Comments (DoD Supplied Guidance)
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.	Implemented	0	
3.2.2: Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.	Implemented	0	

Security Requirement	Control Implementation Status	Control Point Value Deducted	Comments (DoD Supplied Guidance)
3.2.3: Provide security awareness training on recognizing and reporting potential indicators of insider threat.	Not Implemented	-1	
Total Points to be Deducted for this Control Family		**-1**	

3.3 - Audit and Accountability

Security Requirement	Control Implementation Status	Control Point Value Deducted	Comments (DoD Supplied Guidance)
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.	Implemented	0	
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.	Implemented	0	
3.3.3: Review and update audited events.	Not Implemented	-1	
3.3.4: Alert in the event of an audit process failure.	Implemented	0	

Security Requirement	Control Implementation Status	Control Point Value Deducted	Comments (DoD Supplied Guidance)
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.	**Not Implemented**	-5	
3.3.6: Provide audit reduction and report generation to support on-demand analysis and reporting.	**Not Implemented**	-1	
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.	**Implemented**	0	
3.3.8: Protect audit information and audit tools from unauthorized access, modification, and deletion.	**Implemented**	0	
3.3.9: Limit management of audit functionality to a subset of privileged users.	**Implemented**	0	
Total Points to be Deducted for this Control Family		**-7**	

3.4 - Configuration Management

Security Requirement	Control Implementation Status	Control Point Value Deducted	Comments (DoD Supplied Guidance)

Security Requirement	Control Implementation Status	Control Point Value Deducted	Comments (DoD Supplied Guidance)
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.	Not Implemented	-5	
3.4.2: Establish and enforce security configuration settings for information technology products employed in organizational information systems.	Implemented	0	
3.4.3: Track, review, approve/disapprove, and audit changes to information systems.	Implemented	0	
3.4.4: Analyze the security impact of changes prior to implementation.	Implemented	0	
3.4.5: Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.	Implemented	0	
3.4.6: Employ the principle of least functionality by configuring the information system to provide only essential capabilities.	Implemented	0	
3.4.7: Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.	Implemented	0	
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	Implemented	0	

Security Requirement	Control Implementation Status	Control Point Value Deducted	Comments (DoD Supplied Guidance)
execution of authorized software.			
3.4.9: Control and monitor user-installed software.	**Implemented**	0	
Total Points to be Deducted for this Control Family		**-5**	

3.5 - Identification and Authentication

Security Requirement	Control Implementation Status	Control Point Value Deducted	Comments (DoD Supplied Guidance)
3.5.1: Identify information system users, processes acting on behalf of users, or devices.	**Implemented**	0	
3.5.2: Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	**Implemented**	0	
3.5.3: Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	**Planned**	-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.	**Not Implemented**	-1	

Security Requirement	Control Implementation Status	Control Point Value Deducted	Comments (DoD Supplied Guidance)
3.5.5: Prevent reuse of identifiers for a defined period.	**Implemented**	0	
3.5.6: Disable identifiers after a defined period of inactivity.	**Implemented**	0	
3.5.7: Enforce a minimum password complexity and change of characters when new passwords are created.	**Implemented**	0	
3.5.8: Prohibit password reuse for a specified number of generations.	**Implemented**	0	
3.5.9: Allow temporary password use for system logons with an immediate change to a permanent password.	**Implemented**	0	
3.5.10: Store and transmit only encrypted representation of passwords.	**Implemented**	0	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.	**Implemented**	0	
Total Points to be Deducted for this Control Family		**-6**	

3.6 - Incident Response

Security Requirement	Control Implementation Status	Control Point Value Deducted	Comments (DoD Supplied Guidance)
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.	**Implemented**	0	
3.6.2: Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.	**Implemented**	0	
3.6.3: Test the organizational incident response capability.	**Implemented**	0	
Total Points to be Deducted for this Control Family		**0**	

3.7 - Maintenance

Security Requirement	Control Implementation Status	Control Point Value Deducted	Comments (DoD Supplied Guidance)
3.7.1: Perform maintenance on organizational information systems.	**Implemented**	0	
3.7.2: Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.	**Implemented**	0	

Security Requirement	Control Implementation Status	Control Point Value Deducted	Comments (DoD Supplied Guidance)
3.7.3: Ensure equipment removed for off-site maintenance is sanitized of any CUI.	Implemented	0	
3.7.4: Check media containing diagnostic and test programs for malicious code before the media are used in the information system.	Implemented	0	
3.7.5: Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	Implemented	0	
3.7.6: Supervise the maintenance activities of maintenance personnel without required access authorization.	Implemented	0	
Total Points to be Deducted for this Control Family		**0**	

3.8 - Media Protection

Security Requirement	Control Implementation Status	Control Point Value Deducted	Comments (DoD Supplied Guidance)
3.8.1: Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.	Implemented	0	Exposure limited to CUI on media

Security Requirement	Control Implementation Status	Control Point Value Deducted	Comments (DoD Supplied Guidance)
3.8.2: Limit access to CUI on information system media to authorized users.	**Implemented**	0	Exposure limited to CUI on media
3.8.3: Sanitize or destroy information system media containing CUI before disposal or release for reuse.	**Implemented**	0	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.	**Implemented**	0	
3.8.5: Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	**Implemented**	0	
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.	**Implemented**	0	
3.8.7: Control the use of removable media on information system components.	**Implemented**	0	
3.8.8: Prohibit the use of portable storage devices when such devices have no identifiable owner.	**Implemented**	0	
3.8.9: Protect the confidentiality of backup CUI at storage locations.	**Implemented**	0	
Total Points to be Deducted for this Control Family		**0**	

3.9 - Personnel Security

Security Requirement	Control Implementation Status	Control Point Value Deducted	Comments (DoD Supplied Guidance)
3.9.1: Screen individuals prior to authorizing access to information systems containing CUI.	Implemented	0	
3.9.2: Ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers.	Implemented	0	
Total Points to be Deducted for this Control Family		**0**	

3.10 - Physical Protection

Security Requirement	Control Implementation Status	Control Point Value Deducted	Comments (DoD Supplied Guidance)
3.10.1: Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	Implemented	0	
3.10.2: Protect and monitor the physical facility and support infrastructure for those information systems.	Implemented	0	
3.10.3: Escort visitors and monitor visitor activity.	Implemented	0	

Security Requirement	Control Implementation Status	Control Point Value Deducted	Comments (DoD Supplied Guidance)
3.10.4: Maintain audit logs of physical access.	**Implemented**	0	
3.10.5: Control and manage physical access devices.	**Implemented**	0	
3.10.6: Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).	**Implemented**	0	
Total Points to be Deducted for this Control Family		**0**	

3.11 - Risk Management

Security Requirement	Control Implementation Status	Control Point Value Deducted	Comments (DoD Supplied Guidance)
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.	**Implemented**	0	
3.11.2: Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.	**Implemented**	0	
3.11.3: Remediate vulnerabilities in accordance with	**Implemented**	0	

Security Requirement	Control Implementation Status	Control Point Value Deducted	Comments (DoD Supplied Guidance)
assessments of risk.			
Total Points to be Deducted for this Control Family		**0**	

3.12 - Security Assessment

Security Requirement	Control Implementation Status	Control Point Value Deducted	Comments (DoD Supplied Guidance)
3.12.1: Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.	**Implemented**	0	
3.12.2: Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.	**Implemented**	0	
3.12.3: Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.	**Implemented**	0	
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	**Not Applicable**	N/A	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.'

Security Requirement	Control Implementation Status	Control Point Value Deducted	Comments (DoD Supplied Guidance)
with or connections to other systems.			
Total Points to be Deducted for this Control Family		**0**	

3.13 - System and Communications Protection

Security Requirement	Control Implementation Status	Control Point Value Deducted	Comments (DoD Supplied Guidance)
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.	**Implemented**	0	
3.13.2: Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	**Implemented**	0	
3.13.3: Separate user functionality from information system management functionality.	**Implemented**	0	
3.13.4: Prevent unauthorized and unintended information transfer via shared system resources.	**Implemented**	0	

Security Requirement	Control Implementation Status	Control Point Value Deducted	Comments (DoD Supplied Guidance)
3.13.5: Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Implemented	0	
3.13.6: Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	Implemented	0	
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.	Implemented	0	
3.13.8: Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	Implemented	0	
3.13.9: Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	Implemented	0	
3.13.10: Establish and manage cryptographic keys for cryptography employed in the information system.	Implemented	0	
3.13.11: Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	Implemented	0	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.	Implemented	0	

Security Requirement	Control Implementation Status	Control Point Value Deducted	Comments (DoD Supplied Guidance)
3.13.13: Control and monitor the use of mobile code.	**Implemented**	0	
3.13.14: Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	**Not Implemented**	-1	
3.13.15: Protect the authenticity of communications sessions.	**Implemented**	0	
3.13.16: Protect the confidentiality of CUI at rest.	**Implemented**	0	
Total Points to be Deducted for this Control Family		**-1**	

3.14 - System and Information Integrity

Security Requirement	Control Implementation Status	Control Point Value Deducted	Comments (DoD Supplied Guidance)
3.14.1: Identify, report, and correct information and information system flaws in a timely manner.	**Not Implemented**	-5	
3.14.2: Provide protection from malicious code at appropriate locations within organizational information systems.	**Implemented**	0	
3.14.3: Monitor information system security alerts and advisories and take appropriate actions in response.	**Not Implemented**	-5	

Security Requirement	Control Implementation Status	Control Point Value Deducted	Comments (DoD Supplied Guidance)
3.14.4: Update malicious code protection mechanisms when new releases are available.	Implemented	0	
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.	Implemented	0	
3.14.6: Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	Implemented	0	
3.14.7: Identify unauthorized use of the information system.	Implemented	0	
Total Points to be Deducted for this Control Family		**-10**	

4 - Number of NIST 800-171 Security Requirements Implemented

Below is a summary of the number of NIST 800-171 security requirements that have been identified as being implemented based upon the NIST SP 800-171 DoD Assessment process.

Number of Security Requirements Implemented	**94 out of 110**