USTRANSCOM NIST 800-171 Plan of Actions & Milestones POAM

INSTRUCTIONS

The FARS 52.204-21 tab highlights FAR Clause 52.204-21 the Basic Safeguarding of Covered Contractor Information Systems (DODI 8582.01)

The Carrier Info tab summarizes the NIST 800-171 controls from the control family tabs across the bottom of this workbook.

Please complete
Company name:
Contract number:
Cage code:
Date completed:
Submission Type (Annual or update?)
Point of contact (POC):
POC phone number:
POC e-mail address:

The remainder of tabs across the bottom of this workbook contains a NIST 800-171 control family.

Note: Certain areas of each sheet are not editable. These include "control compliance", "control/objective number", "control family", "DIBCAC score", "control/objective text" and "control type" (columns A through F). These are all locked out.

Overarching control compliance status is controlled by the subobjectives under each control number. Example: 3.1.1 can only be compliant ("yes") if objectives 3.1.1[a] through [f] are all compliant ("yes"). A noncompliant ("no") in any subobjective will automatically render the objective as noncompliant ("no"). Thus, when all subobjectives are in compliance ("yes"), the objective automatically is compliant ("yes").

Noncompilance Detection Date: self explanatory

Scheduled Completion Date: please provide an estimated time the noncompliant control/objective will be corrected.

Actual Completion Date: please annotate the date the noncompliant control/objective was corrected.

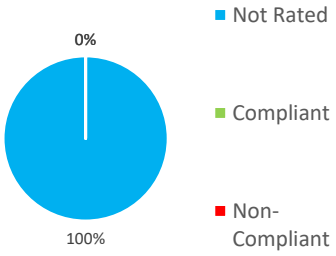
Supporting Documentation/System Controls: briefly describe those technology controls and/or process documents that will be used to achieve compliance with the control/objective requirement. Include details of the implementation/deployment plans and associated milestones. Description should be complete enough so assessors can clearly see a pathway to compliance.

Status/Comments: additional amplifying information regarding the control, objective, documentation, and/or the POAM itself.

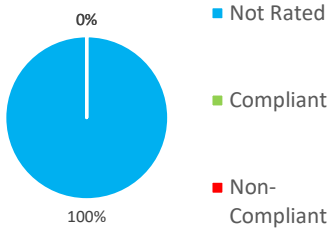
Company name:
Contract number:
Cage code:
Date completed:
Submission Type (Annual or update?)
Point of contact (POC):
POC phone number:
POC e-mail address:

Annual Submission

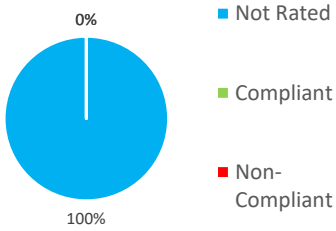
800-171 Controls



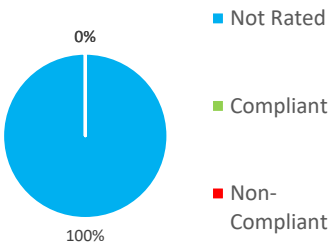
800-171 Objectives



FAR 52.204-21 Controls

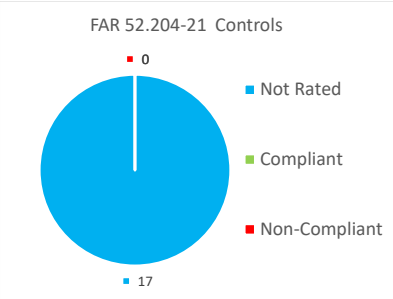


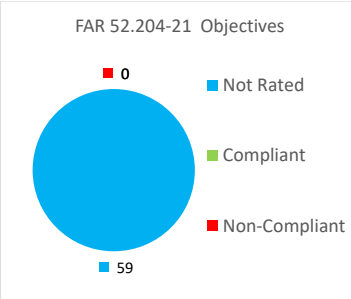
FAR 52.204-21 Objectives

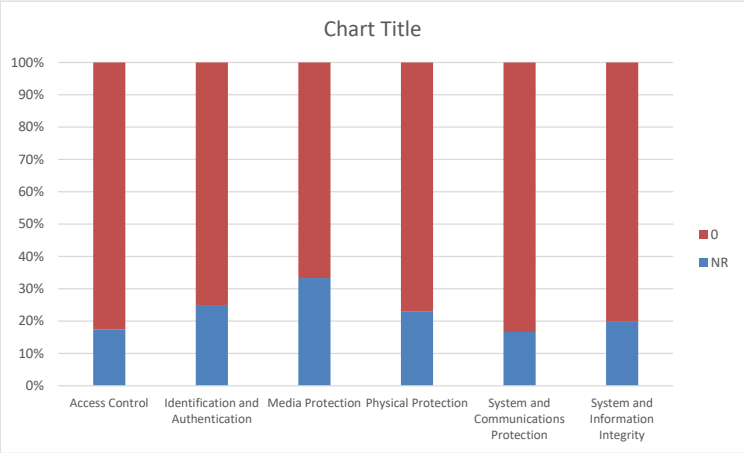


Controls marked requiring Plan of Action and Milestones	no

Controls	Scheduled Completion Date







Basic Safeguarding of Covered Contractor Information Systems	1
NIST 800-171 Control/Objective Number	(All)

Count of Compliant	Column Labels	
Row Labels	NR	0
Access Control	4	19
Identification and Authentication	2	6
Media Protection	1	2
Physical Protection	3	10
System and Communications Protection	2	10
System and Information Integrity	3	12
Grand Total	**15**	**59**

Basic Safeguarding of Covered Contractor Information Systems	1
FAR 52.204-21 Controls marked requiring Plan of Action and Milestones	no

Controls	Scheduled Completion Date

Compliant (Yes/No)	NIST 800-171 Control/Objective Number	Control Family	Control/Objective Text	Non-Compliance Detection Date	Scheduled Completion Date	Actual Completion Date	Supporting Documentation / System Controls	Status / Comments
NR	3.1.1	Access Control	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).					
	3.1.1[a]	Access Control	authorized users are identified.					
	3.1.1[b]	Access Control	processes acting on behalf of authorized users are identified.					
	3.1.1[c]	Access Control	devices (and other systems) authorized to connect to the system are identified.					
	3.1.1[d]	Access Control	system access is limited to authorized users.					
	3.1.1[e]	Access Control	system access is limited to processes acting on behalf of authorized users.					
	3.1.1[f]	Access Control	system access is limited to authorized devices (including other systems).					
NR	3.1.2	Access Control	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.					
	3.1.2[a]	Access Control	the types of transactions and functions that authorized users are permitted to execute are defined.					
	3.1.2[b]	Access Control	system access is limited to the defined types of transactions and functions for authorized users.					
NR	3.1.3	Access Control	Limit the flow of DoD information to organizations or individuals necessary for the performance of the operationally critical requirements of this contract.					
	3.1.3[a]	Access Control	information flow control policies are defined.					

	3.1.3[b]	Access Control	methods and enforcement mechanisms for controlling the flow of CUI are defined.					
	3.1.3[c]	Access Control	designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.					
	3.1.3[d]	Access Control	authorizations for controlling the flow of CUI are defined.					
	3.1.3[e]	Access Control	approved authorizations for controlling the flow of CUI are enforced.					
NR	3.1.4	Access Control	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.					
	3.1.4[a]	Access Control	the duties of individuals requiring separation are defined.					
	3.1.4[b]	Access Control	responsibilities for duties that require separation are assigned to separate individuals.					
	3.1.4[c]	Access Control	access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals.					
NR	3.1.5	Access Control	Employ the principle of least privilege, including for specific security functions and privileged accounts.					
	3.1.5[a]	Access Control	privileged accounts are identified.					
	3.1.5[b]	Access Control	access to privileged accounts is authorized in accordance with the principle of least privilege.					
	3.1.5[c]	Access Control	security functions are identified.					
	3.1.5[d]	Access Control	access to security functions is authorized in accordance with the principle of least privilege.					

NR	3.1.6	Access Control	Use non-privileged accounts or roles when accessing nonsecurity functions.					
	3.1.6[a]	Access Control	nonsecurity functions are identified.					
	3.1.6[b]	Access Control	users are required to use non-privileged accounts or roles when accessing nonsecurity functions.					
NR	3.1.7	Access Control	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.					
	3.1.7[a]	Access Control	privileged functions are defined.					
	3.1.7[b]	Access Control	non-privileged users are defined.					
	3.1.7[c]	Access Control	non-privileged users are prevented from executing privileged functions.					
	3.1.7[d]	Access Control	the execution of privileged functions is captured in audit logs.					
NR	3.1.8	Access Control	Limit unsuccessful logon attempts.					
	3.1.8[a]	Access Control	the means of limiting unsuccessful logon attempts is defined.					
	3.1.8[b]	Access Control	the defined means of limiting unsuccessful logon attempts is implemented.					
NR	3.1.9	Access Control	Provide privacy and security notices consistent with U.S. Government and/or local governmental regulations.					
	3.1.9[a]	Access Control	privacy and security notices required by CUI-specified rules are identified, consistent, and associated with the specific CUI category.					

	3.1.9[b]	Access Control	privacy and security notices are displayed.					
NR	3.1.10	Access Control	Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.					
	3.1.10[a]	Access Control	the period of inactivity after which the system initiates a session lock is defined.					
	3.1.10[b]	Access Control	access to the system and viewing of data is prevented by initiating a session lock after the defined period of inactivity.					
	3.1.10[c]	Access Control	previously visible information is concealed via a pattern-hiding display after the defined period of inactivity.					
NR	3.1.11	Access Control	Terminate (automatically) a user session after a defined condition.					
	3.1.11[a]	Access Control	conditions requiring a user session to terminate are defined.					
	3.1.11[b]	Access Control	a user session is automatically terminated after any of the defined conditions occur.					
NR	3.1.12	Access Control	Monitor and control remote access sessions.					
	3.1.12[a]	Access Control	remote access sessions are permitted.					
	3.1.12[b]	Access Control	the types of permitted remote access are identified.					
	3.1.12[c]	Access Control	remote access sessions are controlled.					
	3.1.12[d]	Access Control	remote access sessions are monitored.					

NR	3.1.13	Access Control	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.					
	3.1.13[a]	Access Control	cryptographic mechanisms to protect the confidentiality of remote access sessions are identified.					
	3.1.13[b]	Access Control	cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented.					
NR	3.1.14	Access Control	Route remote access via managed access control points.					
	3.1.14[a]	Access Control	managed access control points are identified and implemented.					
	3.1.14[b]	Access Control	remote access is routed through managed network access control points.					
NR	3.1.15	Access Control	Authorize remote execution of privileged commands and remote access to security-relevant information.					
	3.1.15[a]	Access Control	privileged commands authorized for remote execution are identified.					
	3.1.15[b]	Access Control	security-relevant information authorized to be accessed remotely is identified.					
	3.1.15[c]	Access Control	the execution of the identified privileged commands via remote access is authorized.					
	3.1.15[d]	Access Control	access to the identified security-relevant information via remote access is authorized.					
NR	3.1.16	Access Control	Authorize wireless access prior to allowing such connections.					
	3.1.16[a]	Access Control	wireless access points are identified.					

	3.1.16[b]	Access Control	wireless access is authorized prior to allowing such connections.					
NR	3.1.17	Access Control	Protect wireless access using authentication and encryption.					
	3.1.17[a]	Access Control	wireless access to the system is protected using authentication.					
	3.1.17[b]	Access Control	wireless access to the system is protected using encryption.					
NR	3.1.18	Access Control	Control connection of mobile devices.					
	3.1.18[a]	Access Control	mobile devices that process, store, or transmit CUI are identified.					
	3.1.18[b]	Access Control	mobile device connections are authorized.					
	3.1.18[c]	Access Control	mobile device connections are monitored and logged.					
NR	3.1.19	Access Control	Provide adequate technical protections on mobile devices and computing platforms that process and/or store contractual information.					
	3.1.19[a]	Access Control	mobile devices and mobile computing platforms that process, store, or transmit CUI are identified.					
	3.1.19[b]	Access Control	encryption is employed to protect CUI on identified mobile devices and mobile computing platforms.					
NR	3.1.20	Access Control	Verify and control/limit connections to and use of external information systems.					
	3.1.20[a]	Access Control	connections to external systems are identified.					

	3.1.20[b]	Access Control	the use of external systems is identified.					
	3.1.20[c]	Access Control	connections to external systems are verified.					
	3.1.20[d]	Access Control	the use of external systems is verified.					
	3.1.20[e]	Access Control	connections to external systems are controlled/limited.					
	3.1.20[f]	Access Control	the use of external systems is controlled/limited.					
NR	3.1.21	Access Control	Limit use of organizational portable storage devices on external information systems.					
	3.1.21[a]	Access Control	the use of portable storage devices containing CUI on external systems is identified and documented.					
	3.1.21[b]	Access Control	limits on the use of portable storage devices containing CUI on external systems are defined.					
	3.1.21[c]	Access Control	the use of portable storage devices containing CUI on external systems is limited as defined.					
NR	3.1.22	Access Control	Control DoD information posted or processed on publically accessible systems.					
	3.1.22[a]	Access Control	individuals authorized to post or process information on publicly accessible systems are identified.					
	3.1.22[b]	Access Control	procedures to ensure CUI is not posted or processed on publicly accessible systems are identified.					
	3.1.22[c]	Access Control	a review process is in place prior to posting of any content to publicly accessible systems.					

	3.1.22[d]	Access Control	content on publicly accessible systems is reviewed to ensure that it does not include CUI.					
	3.1.22[e]	Access Control	mechanisms are in place to remove and address improper posting of CUI.					

Compliant (Yes/No)	NIST 800-171 Control/Objective Number	Control Family	Control/Objective Text	Non-Compliance Detection Date	Scheduled Completion Date	Actual Completion Date	Supporting Documentation / System Controls	Status / Comments
NR	3.2.1	Awareness and Training	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.					
	3.2.1[a]	Awareness and Training	security risks associated with organizational activities involving CUI are identified.					
	3.2.1[b]	Awareness and Training	policies, standards, and procedures related to the security of the system are identified.					
	3.2.1[c]	Awareness and Training	managers, systems administrators, and users of the system are made aware of the security risks associated with their activities.					
	3.2.1[d]	Awareness and Training	managers, systems administrators, and users of the system are made aware of the applicable policies, standards, and procedures related to the security of the system.					
NR	3.2.2	Awareness and Training	Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.					
	3.2.2[a]	Awareness and Training	information security-related duties, roles, and responsibilities are defined.					
	3.2.2[b]	Awareness and Training	information security-related duties, roles, and responsibilities are assigned to designated personnel.					
	3.2.2[c]	Awareness and Training	personnel are adequately trained to carry out their assigned information security-related duties, roles, and responsibilities.					
NR	3.2.3	Awareness and Training	Provide security awareness training on recognizing and reporting potential indicators of insider threat.					
	3.2.3[a]	Awareness and Training	potential indicators associated with insider threats are identified.					
	3.2.3[b]	Awareness and Training	security awareness training on recognizing and reporting potential indicators of insider threat is provided to managers and employees.					

Compliant (Yes/No)	NIST 800-171 Control/Objective Number	Control Family	Control/Objective Text	Non-Compliance Detection Date	Scheduled Completion Date	Actual Completion Date	Supporting Documentation / System Controls	Status / Comments
NR	3.3.1	Audit and Accountability	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.					
	3.3.1[a]	Audit and Accountability	audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified.					
	3.3.1[b]	Audit and Accountability	the content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined.					
	3.3.1[c]	Audit and Accountability	audit records are created (generated).					
	3.3.1[d]	Audit and Accountability	audit records, once created, contain the defined content.					
	3.3.1[e]	Audit and Accountability	retention requirements for audit records are defined.					
	3.3.1[f]	Audit and Accountability	audit records are retained as defined.					
NR	3.3.2	Audit and Accountability	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.					
	3.3.2[a]	Audit and Accountability	the content of the audit records needed to support the ability to uniquely trace users to their actions is defined.					
	3.3.2[b]	Audit and Accountability	audit records, once created, contain the defined content.					
NR	3.3.3	Audit and Accountability	Review and update audited events.					
	3.3.3[a]	Audit and Accountability	a process for determining when to review logged events is defined.					
	3.3.3[b]	Audit and Accountability	event types being logged are reviewed in accordance with the defined review process.					
	3.3.3[c]	Audit and Accountability	event types being logged are updated based on the review.					
NR	3.3.4	Audit and Accountability	Alert in the event of an audit process failure.					

	3.3.4[a]	Audit and Accountability	personnel or roles to be alerted in the event of an audit logging process failure are identified.					
	3.3.4[b]	Audit and Accountability	types of audit logging process failures for which alert will be generated are defined.					
	3.3.4[c]	Audit and Accountability	identified personnel or roles are alerted in the event of an audit logging process failure.					
NR	3.3.5	Audit and Accountability	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.					
	3.3.5[a]	Audit and Accountability	audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity are defined.					
	3.3.5[b]	Audit and Accountability	defined audit record review, analysis, and reporting processes are correlated.					
NR	3.3.6	Audit and Accountability	Provide audit reduction and report generation to support on-demand analysis and reporting.					
	3.3.6[a]	Audit and Accountability	an audit record reduction capability that supports on-demand analysis is provided.					
	3.3.6[b]	Audit and Accountability	a report generation capability that supports on-demand reporting is provided.					
NR	3.3.7	Audit and Accountability	Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.					
	3.3.7[a]	Audit and Accountability	internal system clocks are used to generate time stamps for audit records.					
	3.3.7[b]	Audit and Accountability	an authoritative source with which to compare and synchronize internal system clocks is specified.					
	3.3.7[c]	Audit and Accountability	internal system clocks used to generate time stamps for audit records are compared to and synchronized with the specified authoritative time source.					
NR	3.3.8	Audit and Accountability	Protect audit information and audit tools from unauthorized access, modification, and deletion.					
	3.3.8[a]	Audit and Accountability	audit information is protected from unauthorized access.					
	3.3.8[b]	Audit and Accountability	audit information is protected from unauthorized modification.					

	3.3.8[c]	Audit and Accountability	audit information is protected from unauthorized deletion.					
	3.3.8[d]	Audit and Accountability	audit logging tools are protected from unauthorized access.					
	3.3.8[e]	Audit and Accountability	audit logging tools are protected from unauthorized modification.					
	3.3.8[f]	Audit and Accountability	audit logging tools are protected from unauthorized deletion.					
NR	3.3.9	Audit and Accountability	Limit management of audit functionality to a subset of privileged users.					
	3.3.9[a]	Audit and Accountability	a subset of privileged users granted access to manage audit logging functionality is defined.					
	3.3.9[b]	Audit and Accountability	management of audit logging functionality is limited to the defined subset of privileged users.					

Compliant (Yes/No)	NIST 800-171 Control/Objective Number	Control Family	Control/Objective Text	Non-Compliance Detection Date	Scheduled Completion Date	Actual Completion Date	Supporting Documentation / System Controls	Status / Comments
NR	3.4.1	Configuration Management	Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.					
	3.4.1[a]	Configuration Management	a baseline configuration is established.					
	3.4.1[b]	Configuration Management	the baseline configuration includes hardware, software, firmware, and documentation.					
	3.4.1[c]	Configuration Management	the baseline configuration is maintained (reviewed and updated) throughout the system development life cycle.					
	3.4.1[d]	Configuration Management	a system inventory is established.					
	3.4.1[e]	Configuration Management	the system inventory includes hardware, software, firmware, and documentation.					
	3.4.1[f]	Configuration Management	the inventory is maintained (reviewed and updated) throughout the system development life cycle.					
NR	3.4.2	Configuration Management	Establish and enforce security configuration settings for information technology products employed in organizational information systems.					
	3.4.2[a]	Configuration Management	security configuration settings for information technology products employed in the system are established and included in the baseline configuration.					
	3.4.2[b]	Configuration Management	security configuration settings for information technology products employed in the system are enforced.					
NR	3.4.3	Configuration Management	Track, review, approve/disapprove, and audit changes to information systems.					
	3.4.3[a]	Configuration Management	changes to the system are tracked.					
	3.4.3[b]	Configuration Management	changes to the system are reviewed.					
	3.4.3[c]	Configuration Management	changes to the system are approved or disapproved.					
	3.4.3[d]	Configuration Management	changes to the system are logged.					
	3.4.4	Configuration Management	Analyze the security impact of changes prior to implementation.					
NR	3.4.5	Configuration Management	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.					

	3.4.5[a]	Configuration Management	physical access restrictions associated with changes to the system are defined.					
	3.4.5[b]	Configuration Management	physical access restrictions associated with changes to the system are documented.					
	3.4.5[c]	Configuration Management	physical access restrictions associated with changes to the system are approved.					
	3.4.5[d]	Configuration Management	physical access restrictions associated with changes to the system are enforced.					
	3.4.5[e]	Configuration Management	logical access restrictions associated with changes to the system are defined.					
	3.4.5[f]	Configuration Management	logical access restrictions associated with changes to the system are documented.					
	3.4.5[g]	Configuration Management	logical access restrictions associated with changes to the system are approved.					
	3.4.5[h]	Configuration Management	logical access restrictions associated with changes to the system are enforced.					
NR	3.4.6	Configuration Management	Employ the principle of least functionality by configuring the information system to provide only essential capabilities.					
	3.4.6[a]	Configuration Management	essential system capabilities are defined based on the principle of least functionality.					
	3.4.6[b]	Configuration Management	the system is configured to provide only the defined essential capabilities.					
NR	3.4.7	Configuration Management	Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.					
	3.4.7[a]	Configuration Management	essential programs are defined.					
	3.4.7[b]	Configuration Management	the use of nonessential programs is defined.					
	3.4.7[c]	Configuration Management	the use of nonessential programs is restricted, disabled, or prevented as defined.					
	3.4.7[d]	Configuration Management	essential functions are defined.					
	3.4.7[e]	Configuration Management	the use of nonessential functions is defined.					
	3.4.7[f]	Configuration Management	the use of nonessential functions is restricted, disabled, or prevented as defined.					

	3.4.7[g]	Configuration Management	essential ports are defined.					
	3.4.7[h]	Configuration Management	the use of nonessential ports is defined.					
	3.4.7[i]	Configuration Management	the use of nonessential ports is restricted, disabled, or prevented as defined.					
	3.4.7[j]	Configuration Management	essential protocols are defined.					
	3.4.7[k]	Configuration Management	the use of nonessential protocols is defined.					
	3.4.7[l]	Configuration Management	the use of nonessential protocols is restricted, disabled, or prevented as defined.					
	3.4.7[m]	Configuration Management	essential services are defined.					
	3.4.7[n]	Configuration Management	the use of nonessential services is defined.					
	3.4.7[o]	Configuration Management	the use of nonessential services is restricted, disabled, or prevented as defined.					
NR	3.4.8	Configuration Management	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.					
	3.4.8[a]	Configuration Management	a policy specifying whether whitelisting or blacklisting is to be implemented is specified.					
	3.4.8[b]	Configuration Management	the software allowed to execute under whitelisting or denied use under blacklisting is specified.					
	3.4.8[c]	Configuration Management	whitelisting to allow the execution of authorized software or blacklisting to prevent the use of unauthorized software is implemented as specified.					
NR	3.4.9	Configuration Management	Control and monitor user-installed software.					
	3.4.9[a]	Configuration Management	a policy for controlling the installation of software by users is established.					
	3.4.9[b]	Configuration Management	installation of software by users is controlled based on the established policy.					
	3.4.9[c]	Configuration Management	installation of software by users is monitored.					

Compliant (Yes/No)	NIST 800-171 Control/Objective Number	Control Family	Control/Objective Text	Non-Compliance Detection Date	Scheduled Completion Date	Actual Completion Date	Supporting Documentation / System Controls	Status / Comments
NR	3.5.1	Identification and Authentication	Identify information system users, processes acting on behalf of users, or devices.					
	3.5.1[a]	Identification and Authentication	system users are identified.					
	3.5.1[b]	Identification and Authentication	processes acting on behalf of users are identified.					
	3.5.1[c]	Identification and Authentication	devices accessing the system are identified.					
NR	3.5.2	Identification and Authentication	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.					
	3.5.2[a]	Identification and Authentication	the identity of each user is authenticated or verified as a prerequisite to system access.					
	3.5.2[b]	Identification and Authentication	the identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access.					
	3.5.2[c]	Identification and Authentication	the identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access.					
NR	3.5.3	Identification and Authentication	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.					
	3.5.3[a]	Identification and Authentication	privileged accounts are identified.					
	3.5.3[b]	Identification and Authentication	multifactor authentication is implemented for local access to privileged accounts.					
	3.5.3[c]	Identification and Authentication	multifactor authentication is implemented for network access to privileged accounts.					
	3.5.3[d]	Identification and Authentication	multifactor authentication is implemented for network access to non-privileged accounts.					
	3.5.4	Identification and Authentication	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.					

NR	3.5.5	Identification and Authentication	Prevent reuse of identifiers for a defined period.					
	3.5.5[a]	Identification and Authentication	a period within which identifiers cannot be reused is defined.					
	3.5.5[b]	Identification and Authentication	reuse of identifiers is prevented within the defined period.					
NR	3.5.6	Identification and Authentication	Disable identifiers after a defined period of inactivity.					
	3.5.6[a]	Identification and Authentication	a period of inactivity after which an identifier is disabled is defined.					
	3.5.6[b]	Identification and Authentication	identifiers are disabled after the defined period of inactivity.					
NR	3.5.7	Identification and Authentication	Enforce a minimum password complexity and change of characters when new passwords are created.					
	3.5.7[a]	Identification and Authentication	password complexity requirements are defined.					
	3.5.7[b]	Identification and Authentication	password change of character requirements are defined.					
	3.5.7[c]	Identification and Authentication	minimum password complexity requirements as defined are enforced when new passwords are created.					
	3.5.7[d]	Identification and Authentication	minimum password change of character requirements as defined are enforced when new passwords are created.					
NR	3.5.8	Identification and Authentication	Prohibit password reuse for a specified number of generations.					
	3.5.8[a]	Identification and Authentication	the number of generations during which a password cannot be reused is specified.					
	3.5.8[b]	Identification and Authentication	reuse of passwords is prohibited during the specified number of generations.					

	3.5.9	Identification and Authentication	Allow temporary password use for system logons with an immediate change to a permanent password.					
NR	3.5.10	Identification and Authentication	Store and transmit only encrypted representation of passwords.					
	3.5.10[a]	Identification and Authentication	passwords are cryptographically protected in storage.					
	3.5.10[b]	Identification and Authentication	passwords are cryptographically protected in transit.					
	3.5.11	Identification and Authentication	Obscure feedback of authentication information.					

Compliant (Yes/No)	NIST 800-171 Control/Objective Number	Control Family	Control/Objective Text	Non-Compliance Detection Date	Scheduled Completion Date	Actual Completion Date	Supporting Documentation / System Controls	Status / Comments
NR	3.6.1	Incident Response	Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.					
	3.6.1[a]	Incident Response	an operational incident-handling capability is established.					
	3.6.1[b]	Incident Response	the operational incident-handling capability includes preparation.					
	3.6.1[c]	Incident Response	the operational incident-handling capability includes detection.					
	3.6.1[d]	Incident Response	the operational incident-handling capability includes analysis.					
	3.6.1[e]	Incident Response	the operational incident-handling capability includes containment.					
	3.6.1[f]	Incident Response	the operational incident-handling capability includes recovery.					
	3.6.1[g]	Incident Response	the operational incident-handling capability includes user response activities.					
NR	3.6.2	Incident Response	Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.					
	3.6.2[a]	Incident Response	incidents are tracked.					
	3.6.2[b]	Incident Response	incidents are documented.					
	3.6.2[c]	Incident Response	authorities to whom incidents are to be reported are identified.					
	3.6.2[d]	Incident Response	organizational officials to whom incidents are to be reported are identified.					
	3.6.2[e]	Incident Response	identified authorities are notified of incidents.					
	3.6.2[f]	Incident Response	identified organizational officials are notified of incidents.					
	3.6.3	Incident Response	Test the organizational incident response capability.					

Compliant (Yes/No)	NIST 800-171 Control/Objective Number	Control Family	Control/Objective Text	Non-Compliance Detection Date	Scheduled Completion Date	Actual Completion Date	Supporting Documentation / System Controls	Status / Comments
	3.7.1	Maintenance	Perform maintenance on organizational information systems.					
NR	3.7.2	Maintenance	Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.					
	3.7.2[a]	Maintenance	tools used to conduct system maintenance are controlled.					
	3.7.2[b]	Maintenance	techniques used to conduct system maintenance are controlled.					
	3.7.2[c]	Maintenance	mechanisms used to conduct system maintenance are controlled.					
	3.7.2[d]	Maintenance	personnel used to conduct system maintenance are controlled.					
	3.7.3	Maintenance	Ensure equipment removed for off-site maintenance is sanitized of DoD information.					
	3.7.4	Maintenance	Check media containing diagnostic and test programs for malicious code before the media are used in the information system.					
NR	3.7.5	Maintenance	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.					
	3.7.5[a]	Maintenance	multifactor authentication is used to establish nonlocal maintenance sessions via external network connections.					
	3.7.5[b]	Maintenance	nonlocal maintenance sessions established via external network connections are terminated when nonlocal maintenance is complete.					
	3.7.6	Maintenance	Supervise the maintenance activities of maintenance personnel without required access authorization.					

Compliant (Yes/No)	NIST 800-171 Control/Objective Number	Control Family	Control/Objective Text	Non-Compliance Detection Date	Scheduled Completion Date	Actual Completion Date	Supporting Documentation / System Controls	Status / Comments
NR	3.8.1	Media Protection	Protect (i.e., physically control and securely store) system media containing DoD information, both paper and digital.					
	3.8.1[a]	Media Protection	paper media containing CUI is physically controlled.					
	3.8.1[b]	Media Protection	digital media containing CUI is physically controlled.					
	3.8.1[c]	Media Protection	paper media containing CUI is securely stored.					
	3.8.1[d]	Media Protection	digital media containing CUI is securely stored.					
	3.8.2	Media Protection	Limit access to DoD information on system media to authorized users.					
NR	3.8.3	Media Protection	Sanitize or destroy system media containing DoD information before disposal or release for reuse.					
	3.8.3[a]	Media Protection	system media containing CUI is sanitized or destroyed before disposal.					
	3.8.3[b]	Media Protection	system media containing CUI is sanitized before it is released for reuse.					
NR	3.8.4	Media Protection	Mark media with privacy and security notices consistent with U.S. Government and/or local government regulations.					
	3.8.4[a]	Media Protection	media containing CUI is marked with applicable CUI markings.					
	3.8.4[b]	Media Protection	media containing CUI is marked with distribution limitations.					
NR	3.8.5	Media Protection	Control access to and maintain accountability for media containing DoD information.					
	3.8.5[a]	Media Protection	access to media containing CUI is controlled.					
	3.8.5[b]	Media Protection	accountability for media containing CUI is maintained during transport outside of controlled areas.					
	3.8.6	Media Protection	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	Media Protection	Control the use of removable media on information system components.					
	3.8.8	Media Protection	Prohibit the use of portable storage devices when such devices have no identifiable owner.					
	3.8.9	Media Protection	Provide information backup procedures (frequency, timeframe for storage, etc.) for DoD data located on contractor systems. Protect the confidentiality of backup materials containing DoD information.					

Compliant (Yes/No)	NIST 800-171 Control/Objective Number	Control Family	Control/Objective Text	Non-Compliance Detection Date	Scheduled Completion Date	Actual Completion Date	Supporting Documentation / System Controls	Status / Comments
	3.9.1	Personnel Security	Screen individuals prior to authorizing access to organizational systems containing DoD information.					
NR	3.9.2	Personnel Security	Ensure that DoD information and organizational systems containing DoD information are protected during and after personnel actions such as terminations and transfers.					
	3.9.2[a]	Personnel Security	a policy and/or process for terminating system access and any credentials coincident with personnel actions is established.					
	3.9.2[b]	Personnel Security	system access and credentials are terminated consistent with personnel actions such as termination or transfer.					
	3.9.2[c]	Personnel Security	the system is protected during and after personnel transfer actions.					

Compliant (Yes/No)	NIST 800-171 Control/Objective Number	Control Family	Control/Objective Text	Non-Compliance Detection Date	Scheduled Completion Date	Actual Completion Date	Supporting Documentation / System Controls	Status / Comments
NR	3.10.1	Physical Protection	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.					
	3.10.1[a]	Physical Protection	authorized individuals allowed physical access are identified.					
	3.10.1[b]	Physical Protection	physical access to organizational systems is limited to authorized individuals.					
	3.10.1[c]	Physical Protection	physical access to equipment is limited to authorized individuals.					
	3.10.1[d]	Physical Protection	physical access to operating environments is limited to authorized individuals.					
NR	3.10.2	Physical Protection	Protect and monitor the physical facility and support infrastructure for those information systems.					
	3.10.2[a]	Physical Protection	the physical facility where organizational systems reside is protected.					
	3.10.2[b]	Physical Protection	the support infrastructure for organizational systems is protected.					
	3.10.2[c]	Physical Protection	the physical facility where organizational systems reside is monitored.					
	3.10.2[d]	Physical Protection	the support infrastructure for organizational systems is monitored.					
NR	3.10.3	Physical Protection	Escort visitors and monitor visitor activity.					
	3.10.3[a]	Physical Protection	visitors are escorted.					
	3.10.3[b]	Physical Protection	visitor activity is monitored.					
	3.10.4	Physical Protection	Maintain audit logs of physical access.					
NR	3.10.5	Physical Protection	Control and manage physical access devices.					
	3.10.5[a]	Physical Protection	physical access devices are identified.					
	3.10.5[b]	Physical Protection	physical access devices are controlled.					
	3.10.5[c]	Physical Protection	physical access devices are managed.					
NR	3.10.6	Physical Protection	Enforce safeguarding measures for DoD Information at alternate work sites (e.g., telework sites).					
	3.10.6[a]	Physical Protection	safeguarding measures for CUI are defined for alternate work sites.					
	3.10.6[b]	Physical Protection	safeguarding measures for CUI are enforced for alternate work sites.					

Compliant (Yes/No)	NIST 800-171 Control/Objective Number	Control Family	Control/Objective Text	Non-Compliance Detection Date	Scheduled Completion Date	Actual Completion Date	Supporting Documentation / System Controls	Status / Comments
NR	3.11.1	Risk Assessment	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 DoD information.					
	3.11.1[a]	Risk Assessment	the frequency to assess risk to organizational operations, organizational assets, and individuals is defined.					
	3.11.1[b]	Risk Assessment	risk to organizational operations, organizational assets, and individuals resulting from the operation of an organizational system that processes, stores, or transmits CUI is assessed with the defined frequency.					
NR	3.11.2	Risk Assessment	Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.					
	3.11.2[a]	Risk Assessment	the frequency to scan for vulnerabilities in organizational systems and applications is defined.					
	3.11.2[b]	Risk Assessment	vulnerability scans are performed on organizational systems with the defined frequency.					
	3.11.2[c]	Risk Assessment	vulnerability scans are performed on applications with the defined frequency.					
	3.11.2[d]	Risk Assessment	vulnerability scans are performed on organizational systems when new vulnerabilities are identified.					
	3.11.2[e]	Risk Assessment	vulnerability scans are performed on applications when new vulnerabilities are identified.					
NR	3.11.3	Risk Assessment	Remediate vulnerabilities in accordance with assessments of risk.					
	3.11.3[a]	Risk Assessment	vulnerabilities are identified.					
	3.11.3[b]	Risk Assessment	vulnerabilities are remediated in accordance with risk assessments.					

Compliant (Yes/No)	NIST 800-171 Control/Objective Number	Control Family	Control/Objective Text	Non-Compliance Detection Date	Scheduled Completion Date	Actual Completion Date	Supporting Documentation / System Controls	Status / Comments
NR	3.12.1	Security Assessment	Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.					
	3.12.1[a]	Security Assessment	the frequency of security control assessments is defined.					
	3.12.1[b]	Security Assessment	security controls are assessed with the defined frequency to determine if the controls are effective in their application.					
NR	3.12.2	Security Assessment	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.					
	3.12.2[a]	Security Assessment	deficiencies and vulnerabilities to be addressed by the plan of action are identified.					
	3.12.2[b]	Security Assessment	a plan of action is developed to correct identified deficiencies and reduce or eliminate identified vulnerabilities.					
	3.12.2[c]	Security Assessment	the plan of action is implemented to correct identified deficiencies and reduce or eliminate identified vulnerabilities.					
	3.12.3	Security Assessment	Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.					
NR	3.12.4	Security Assessment	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.					

	3.12.4[a]	Security Assessment	a system security plan is developed.					
	3.12.4[b]	Security Assessment	the system boundary is described and documented in the system security plan.					
	3.12.4[c]	Security Assessment	the system environment of operation is described and documented in the system security plan.					
	3.12.4[d]	Security Assessment	the security requirements identified and approved by the designated authority as non-applicable are identified.					
	3.12.4[e]	Security Assessment	the method of security requirement implementation is described and documented in the system security plan.					
	3.12.4[f]	Security Assessment	the relationship with or connection to other systems is described and documented in the system security plan.					
	3.12.4[g]	Security Assessment	the frequency to update the system security plan is defined.					
	3.12.4[h]	Security Assessment	system security plan is updated with the defined frequency.					

Compliant (Yes/No)	NIST 800-171 Control/Objective Number	Control Family	Control/Objective Text	Non-Compliance Detection Date	Scheduled Completion Date	Actual Completion Date	Supporting Documentation / System Controls	Status / Comments
NR	3.13.1	System and Communications Protection	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.					
	3.13.1[a]	System and Communications Protection	the external system boundary is defined.					
	3.13.1[b]	System and Communications Protection	key internal system boundaries are defined.					
	3.13.1[c]	System and Communications Protection	communications are monitored at the external system boundary.					
	3.13.1[d]	System and Communications Protection	communications are monitored at key internal boundaries.					
	3.13.1[e]	System and Communications Protection	communications are controlled at the external system boundary.					
	3.13.1[f]	System and Communications Protection	communications are controlled at key internal boundaries.					
	3.13.1[g]	System and Communications Protection	communications are protected at the external system boundary.					
	3.13.1[h]	System and Communications Protection	communications are protected at key internal boundaries.					
NR	3.13.2	System and Communications Protection	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.					
	3.13.2[a]	System and Communications Protection	architectural designs that promote effective information security are identified.					
	3.13.2[b]	System and Communications Protection	software development techniques that promote effective information security are identified.					
	3.13.2[c]	System and Communications Protection	systems engineering principles that promote effective information security are identified.					

	3.13.2[d]	System and Communications Protection	identified architectural designs that promote effective information security are employed.					
	3.13.2[e]	System and Communications Protection	identified software development techniques that promote effective information security are employed.					
	3.13.2[f]	System and Communications Protection	identified systems engineering principles that promote effective information security are employed.					
NR	3.13.3	System and Communications Protection	Separate user functionality from information system management functionality.					
	3.13.3[a]	System and Communications Protection	user functionality is identified.					
	3.13.3[b]	System and Communications Protection	system management functionality is identified.					
	3.13.3[c]	System and Communications Protection	user functionality is separated from system management functionality.					
	3.13.4	System and Communications Protection	Prevent unauthorized and unintended information transfer via shared system resources.					
NR	3.13.5	System and Communications Protection	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.					
	3.13.5[a]	System and Communications Protection	publicly accessible system components are identified.					
	3.13.5[b]	System and Communications Protection	subnetworks for publicly accessible system components are physically or logically separated from internal networks.					
NR	3.13.6	System and Communications Protection	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).					
	3.13.6[a]	System and Communications Protection	network communications traffic is denied by default.					
	3.13.6[b]	System and Communications Protection	network communications traffic is allowed by exception.					

	3.13.7	System and Communications Protection	Prevent remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks.					
NR	3.13.8	System and Communications Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure of DoD information during transmission when possible unless otherwise protected by alternate physical safeguards.					
	3.13.8[a]	System and Communications Protection	cryptographic mechanisms intended to prevent unauthorized disclosure of CUI are identified.					
	3.13.8[b]	System and Communications Protection	alternative physical safeguards intended to prevent unauthorized disclosure of CUI are identified.					
	3.13.8[c]	System and Communications Protection	either cryptographic mechanisms or alternative physical safeguards are implemented to prevent unauthorized disclosure of CUI during transmission.					
NR	3.13.9	System and Communications Protection	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.					
	3.13.9[a]	System and Communications Protection	a period of inactivity to terminate network connections associated with communications sessions is defined.					
	3.13.9[b]	System and Communications Protection	network connections associated with communications sessions are terminated at the end of the sessions.					
	3.13.9[c]	System and Communications Protection	network connections associated with communications sessions are terminated after the defined period of inactivity.					
NR	3.13.10	System and Communications Protection	Establish and manage cryptographic keys for cryptography employed in the information system;					
	3.13.10[a]	System and Communications Protection	cryptographic keys are established whenever cryptography is employed.					
	3.13.10[b]	System and Communications Protection	cryptographic keys are managed whenever cryptography is employed.					
	3.13.11	System and Communications Protection	Employ FIPS-validated cryptography when used to protect the confidentiality of DoD information within the organization's systems and when possible when transmitting to external entities.					
NR	3.13.12	System and Communications Protection	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.					

	3.13.12[a]	System and Communications Protection	collaborative computing devices are identified.					
	3.13.12[b]	System and Communications Protection	collaborative computing devices provide indication to users of devices in use.					
	3.13.12[c]	System and Communications Protection	remote activation of collaborative computing devices is prohibited.					
NR	3.13.13	System and Communications Protection	Control and monitor the use of mobile code.					
	3.13.13[a]	System and Communications Protection	use of mobile code is controlled.					
	3.13.13[b]	System and Communications Protection	use of mobile code is monitored.					
NR	3.13.14	System and Communications Protection	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.					
	3.13.14[a]	System and Communications Protection	use of Voice over Internet Protocol (VoIP) technologies is controlled.					
	3.13.14[b]	System and Communications Protection	use of Voice over Internet Protocol (VoIP) technologies is monitored.					
	3.13.15	System and Communications Protection	Protect the authenticity of communications sessions.					
	3.13.16	System and Communications Protection	Protect the confidentiality of DoD information at rest.					

Compliant (Yes/No)	NIST 800-171 Control/Objective Number	Control Family	Control/Objective Text	Non-Compliance Detection Date	Scheduled Completion Date	Actual Completion Date	Supporting Documentation / System Controls	Status / Comments
NR	3.14.1	System and Information Integrity	Identify, report, and correct information and information system flaws in a timely manner.					
	3.14.1[a]	System and Information Integrity	the time within which to identify system flaws is specified.					
	3.14.1[b]	System and Information Integrity	system flaws are identified within the specified time frame.					
	3.14.1[c]	System and Information Integrity	the time within which to report system flaws is specified.					
	3.14.1[d]	System and Information Integrity	system flaws are reported within the specified time frame.					
	3.14.1[e]	System and Information Integrity	the time within which to correct system flaws is specified.					
	3.14.1[f]	System and Information Integrity	system flaws are corrected within the specified time frame.					
NR	3.14.2	System and Information Integrity	Provide protection from malicious code at appropriate locations within organizational information systems.					
	3.14.2[a]	System and Information Integrity	designated locations for malicious code protection are identified.					

	3.14.2[b]	System and Information Integrity	protection from malicious code at designated locations is provided.					
NR	3.14.3	System and Information Integrity	Monitor information system security alerts and advisories and take appropriate actions in response.					
	3.14.3[a]	System and Information Integrity	response actions to system security alerts and advisories are identified.					
	3.14.3[b]	System and Information Integrity	system security alerts and advisories are monitored.					
	3.14.3[c]	System and Information Integrity	actions in response to system security alerts and advisories are taken.					
	3.14.4	System and Information Integrity	Update malicious code protection mechanisms when new releases are available.					
NR	3.14.5	System and Information Integrity	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.					
	3.14.5[a]	System and Information Integrity	the frequency for malicious code scans is defined.					
	3.14.5[b]	System and Information Integrity	malicious code scans are performed with the defined frequency.					
	3.14.5[c]	System and Information Integrity	real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed.					

NR	3.14.6	System and Information Integrity	Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.					
	3.14.6[a]	System and Information Integrity	the system is monitored to detect attacks and indicators of potential attacks.					
	3.14.6[b]	System and Information Integrity	inbound communications traffic is monitored to detect attacks and indicators of potential attacks.					
	3.14.6[c]	System and Information Integrity	outbound communications traffic is monitored to detect attacks and indicators of potential attacks.					
NR	3.14.7	System and Information Integrity	Identify unauthorized use of the information system.					
	3.14.7[a]	System and Information Integrity	authorized use of the system is defined.					
	3.14.7[b]	System and Information Integrity	unauthorized use of the system is identified.					