Appendix J: NIST.SP.800-171 - POAM

		Date:	**Org Name**, Cage Code: Street City State Zip (XXX) XXX-XXXX									
Compliant (Yes/No)	**NIST 800-171 Control Number**	**Control Family**	**Control Text**	**Control Type**	**Non-Compliance Detection Date**	**Scheduled Completion Date**	**Actual Completion Date**	**Original Impact Level**	**Adjusted Impact Level**	**Adjusted Impact Rationale (If Applicable)**	**Supporting Documentation / System Controls**	**Status / Comments**
	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).	Basic								
	3.1.2	Access Control	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Derived								
	3.1.3	Access Control	Control the flow of CUI in accordance with approved authorizations.	Derived								
	3.1.4	Access Control	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Derived								
	3.1.5	Access Control	Employ the principle of least privilege, including for specific security functions and privileged accounts.	Derived								
	3.1.6	Access Control	Use non-privileged accounts or roles when accessing nonsecurity functions.	Derived								
	3.1.7	Access Control	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	Derived								
	3.1.8	Access Control	Limit unsuccessful logon attempts.	Derived								
	3.1.9	Access Control	Provide privacy and security notices consistent with applicable CUI rules.	Derived								
	3.1.10	Access Control	Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.	Basic								
	3.1.11	Access Control	Terminate (automatically) a user session after a defined condition.	Derived								
	3.1.12	Access Control	Monitor and control remote access sessions.	Derived								
	3.1.13	Access Control	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Derived								
	3.1.14	Access Control	Route remote access via managed access control points.	Derived								

	3.1.15	Access Control	Authorize remote execution of privileged commands and remote access to security-relevant information.	Derived								
	3.1.16	Access Control	Authorize wireless access prior to allowing such connections.	Derived								
	3.1.17	Access Control	Protect wireless access using authentication and encryption.	Derived								
	3.1.18	Access Control	Control connection of mobile devices.	Derived								
	3.1.19	Access Control	Encrypt CUI on mobile devices.	Derived								
	3.1.20	Access Control	Verify and control/limit connections to and use of external information systems.	Derived								
	3.1.21	Access Control	Limit use of organizational portable storage devices on external information systems.	Derived								
	3.1.22	Access Control	Control information posted or processed on publicly accessible information systems.	Derived								
	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.	Basic								
	3.2.2	Awareness and Training	Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.	Basic								
	3.2.3	Awareness and Training	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	Derived								
	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.	Basic								
	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.	Basic								
	3.3.3	Audit and Accountability	Review and update audited events.	Derived								
	3.3.4	Audit and Accountability	Alert in the event of an audit process failure.	Derived								
	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.	Derived								
	3.3.6	Audit and Accountability	Provide audit reduction and report generation to support on-demand analysis and reporting.	Derived								
	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.	Derived								
	3.3.8	Audit and Accountability	Protect audit information and audit tools from unauthorized access, modification, and deletion.	Derived								
	3.3.9	Audit and Accountability	Limit management of audit functionality to a subset of privileged users.	Derived								
	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.	Basic								

	3.4.2	Configuration Management	Establish and enforce security configuration settings for information technology products employed in organizational information systems.	Basic								
	3.4.3	Configuration Management	Track, review, approve/disapprove, and audit changes to information systems.	Derived								
	3.4.4	Configuration Management	Analyze the security impact of changes prior to implementation.	Derived								
	3.4.5	Configuration Management	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.	Derived								
	3.4.6	Configuration Management	Employ the principle of least functionality by configuring the information system to provide only essential capabilities.	Derived								
	3.4.7	Configuration Management	Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.	Derived								
	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.	Derived								
	3.4.9	Configuration Management	Control and monitor user-installed software.	Derived								
	3.5.1	Identification and Authentication	Identify information system users, processes acting on behalf of users, or devices.	Basic								
	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.	Basic								
	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.	Derived								
	3.5.4	Identification and Authentication	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	Derived								
	3.5.5	Identification and Authentication	Prevent reuse of identifiers for a defined period.	Derived								
	3.5.6	Identification and Authentication	Disable identifiers after a defined period of inactivity.	Derived								
	3.5.7	Identification and Authentication	Enforce a minimum password complexity and change of characters when new passwords are created.	Derived								
	3.5.8	Identification and Authentication	Prohibit password reuse for a specified number of generations.	Derived								
	3.5.9	Identification and Authentication	Allow temporary password use for system logons with an immediate change to a permanent password.	Derived								
	3.5.10	Identification and Authentication	Store and transmit only encrypted representation of passwords.	Derived								
	3.5.11	Identification and Authentication	Obscure feedback of authentication information.	Derived								
	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.	Basic								

	3.6.2	Incident Response	Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.	Basic								
	3.6.3	Incident Response	Test the organizational incident response capability.	Derived								
	3.7.1	Maintenance	Perform maintenance on organizational information systems.	Basic								
	3.7.2	Maintenance	Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.	Basic								
	3.7.3	Maintenance	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	Derived								
	3.7.4	Maintenance	Check media containing diagnostic and test programs for malicious code before the media are used in the information system.	Derived								
	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.	Derived								
	3.7.6	Maintenance	Supervise the maintenance activities of maintenance personnel without required access authorization.	Derived								
	3.8.1	Media Protection	Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.	Basic								
	3.8.2	Media Protection	Limit access to CUI on information system media to authorized users.	Basic								
	3.8.3	Media Protection	Sanitize or destroy information system media containing CUI before disposal or release for reuse.	Basic								
	3.8.4	Media Protection	Mark media with necessary CUI markings and distribution limitations.	Derived								
	3.8.5	Media Protection	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	Derived								
	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.	Derived								
	3.8.7	Media Protection	Control the use of removable media on information system components.	Derived								
	3.8.8	Media Protection	Prohibit the use of portable storage devices when such devices have no identifiable owner.	Derived								
	3.8.9	Media Protection	Protect the confidentiality of backup CUI at storage locations.	Derived								
	3.9.1	Personnel Security	Screen individuals prior to authorizing access to information systems containing CUI.	Basic								
	3.9.2	Personnel Security	Ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers.	Basic								

	3.10.1	Physical Protection	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	Basic								
	3.10.2	Physical Protection	Protect and monitor the physical facility and support infrastructure for those information systems.	Basic								
	3.10.3	Physical Protection	Escort visitors and monitor visitor activity.	Derived								
	3.10.4	Physical Protection	Maintain audit logs of physical access.	Derived								
	3.10.5	Physical Protection	Control and manage physical access devices.	Derived								
	3.10.6	Physical Protection	Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).	Derived								
	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 information systems and the associated processing, storage, or transmission of CUI.	Basic								
	3.11.2	Risk Assessment	Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.	Derived								
	3.11.3	Risk Assessment	Remediate vulnerabilities in accordance with assessments of risk.	Derived								
	3.12.1	Security Assessment	Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.	Basic								
	3.12.2	Security Assessment	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.	Basic								
	3.12.3	Security Assessment	Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.	Basic								
	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.	Basic								
	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.	Basic								
	3.13.3	System and Communications Protection	Separate user functionality from information system management functionality.	Derived								
	3.13.4	System and Communications Protection	Prevent unauthorized and unintended information transfer via shared system resources.	Derived								
	3.13.5	System and Communications Protection	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Derived								
	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).	Derived								

	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.	Derived								
	3.13.8	System and Communications Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	Derived								
	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.	Derived								
	3.13.10	System and Communications Protection	Establish and manage cryptographic keys for cryptography employed in the information system;	Derived								
	3.13.11	System and Communications Protection	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	Derived								
	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.	Derived								
	3.13.13	System and Communications Protection	Control and monitor the use of mobile code.	Derived								
	3.13.14	System and Communications Protection	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	Derived								
	3.13.15	System and Communications Protection	Protect the authenticity of communications sessions.	Derived								
	3.13.16	System and Communications Protection	Protect the confidentiality of CUI at rest.	Derived								
	3.14.1	System and Information Integrity	Identify, report, and correct information and information system flaws in a timely manner.	Basic								
	3.14.2	System and Information Integrity	Provide protection from malicious code at appropriate locations within organizational information systems.	Basic								
	3.14.3	System and Information Integrity	Monitor information system security alerts and advisories and take appropriate actions in response.	Basic								
	3.14.4	System and Information Integrity	Update malicious code protection mechanisms when new releases are available.	Derived								
	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.	Derived								
	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.	Derived								

	3.14.7	System and Information Integrity	Identify unauthorized use of the information system.	Derived								