FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES - The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.

SI-1.1 - Examine system and information integrity policy and procedures; other relevant documents or records, **and**

Interview organizational personnel with system and information integrity responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization develops and documents system and information integrity policy and procedures;				
(ii)	The organization disseminates system and information integrity policy and procedures to appropriate elements within the organization;				
(iii)	Responsible parties within the organization periodically review system and information integrity policy and procedures; and				
(iv)	The organization updates system and information integrity policy and procedures when organizational review indicates updates are required.				

SI-1.2 - Examine system and information integrity policy and procedures; other relevant documents or records, **and**

Interview organizational personnel with system and information integrity responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The system and information integrity policy addresses purpose, scope, roles and responsibilities, management commitment,				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
	coordination among organizational entities, and compliance;				
(ii)	The system and information integrity policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and				
(iii)	The system and information integrity procedures address all areas identified in the system and information integrity policy and address achieving policy-compliant implementations of all associated security controls.				

SI-2 FLAW REMEDIATION - The organization identifies, reports, and corrects information system flaws.

SI-2.1 - Examine system and information integrity policy; procedures addressing flaw remediation; NIST Special Publication 800-40; list of flaws and vulnerabilities potentially affecting the information system; list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws); test results from the installation of software to correct information system flaws; other relevant documents or records, **and**

Interview organizational personnel with flaw remediation responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization identifies, reports, and corrects information system flaws;				
(ii)	The organization installs newly released security patches, service packs, and hot fixes on the information system in a reasonable timeframe in accordance with organizational policy and procedures;				
(iii)	The organization addresses flaws discovered during security assessments, continuous monitoring, or incident response activities in an expeditious manner in accordance with organizational policy and procedures;				
(iv)	The organization tests information system patches, service packs, and hot fixes for effectiveness and potential side effects before installation; and				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(v)	The organization captures all appropriate information pertaining to the discovered flaws in the information system, including the cause of the flaws, mitigation activities, and lessons learned.				

SI-3 MALICIOUS CODE PROTECTION - The information system implements malicious code protection.

SI-3.1 - Examine system and information integrity policy; procedures addressing malicious code protection; NIST Special Publication 800-83; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The information system implements malicious code protection;				
(ii)	The organization employs malicious code protection mechanisms at critical information system entry and exit points, at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code;				
(iii)	The malicious code protection mechanisms detect and eradicate malicious code transported by electronic mail, electronic mail attachments, Internet access, removable media, or other common means, or by exploiting information system vulnerabilities;				
(iv)	The organization updates malicious code protection mechanisms whenever new releases are available; and				
(v)	The malicious code protection mechanisms are appropriately updated to include the latest malicious code definitions, configured to perform periodic scans of the information system as well as real-time scans of files from external sources as the files are downloaded, opened, or executed, and configured to disinfect and quarantine infected files.				

SI-3(1).1 - Examine system and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system

configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization centrally manages malicious code protection mechanisms.				

SI-4 INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES - The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.

SI-4.1 - Examine system and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.				

SI-5 SECURITY ALERTS AND ADVISORIES - The organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.

SI-5.1 - Examine system and information integrity policy; procedures addressing security alerts and advisories; NIST Special Publication 800-40; records of security alerts and advisories; other relevant documents or records, **and**

Interview organizational personnel with security alert and advisory responsibilities; organizational personnel implementing, operating, maintaining, administering, and using the information system to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization receives information system security alerts/advisories on a regular basis;				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(ii)	The organization issues security alerts/advisories to appropriate organizational personnel; and				
(iii)	The organization takes appropriate actions in response to security alerts/advisories.				

SI-6 SECURITY FUNCTIONALITY VERIFICATION -The information system verifies the correct operation of security functions [Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every [Assignment: organization-defined time-period]] and [Selection (one or more): notifies system administrator, shuts the system down, restarts the system] when anomalies are discovered.

SI-6.1 – Examine system and information integrity policy; procedures addressing security function verification; information system design documentation; information system security plan (for organization-defined conditions for conducting security function verification, organization-defined frequency of security function verifications (if periodic), and organization-defined information system responses to security function anomalies); information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines the appropriate conditions for conducting security function verification;				
(ii)	The organization defines, for periodic security function verification, the frequency of the verifications;				
(iii)	The organization defines information system responses to anomalies discovered during security function verification;				
(iv)	The information system verifies the correct operation of security functions in accordance with organization-defined conditions and in accordance with organization-defined frequency (if periodic verification); and				
(v)	The information system responds to security function anomalies in accordance with organization-defined responses.				

and

Test security function verification capability to determine if the following requirements are met:

Test Steps		S	N	Findings	Initials & Date
1	Verify that the system notification functions within accordance with documented security functions verification.				

SI-7 SOFTWARE AND INFORMATION INTEGRITY - The information system detects and protects against unauthorized changes to software and information.

SI-7.1 – Examine system and information integrity policy; procedures addressing software and information integrity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The information system detects and protects against unauthorized changes to software and information;				
(ii)	The organization employs effective integrity verification tools in accordance with good software engineering practices.				

and

Test software integrity protection and verification capability.

Test Steps		S	N	Findings	Initials & Date
1					

SI-8 SPAM PROTECTION - The information system implements spam protection.

SI-8.1 – Examine system and information integrity policy; procedures addressing spam protection; information system design documentation; SPAM protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The information system implements SPAM protection;				
(ii)	The organization employs SPAM protection mechanisms at critical information system entry points and at workstations, servers, or mobile computing devices on the network;				
(iii)	The organization employs SPAM protection mechanisms to detect and take appropriate action on unsolicited messages transported by electronic mail; and				
(iv)	The organization updates SPAM protection mechanisms whenever new releases are available in accordance with organizational policy and procedures.				

and

Test SPAM detection and handling capability to determine if the following requirements are met:

Test Steps		S	N	Findings	Initials & Date
1	Validate that the SPAM protection is compliant in accordance with documented security functions verification;				
2	Validate that the SPAM detection is enabled; and				
3	Validate that SPAM signatures are updated in accordance with the current SI SPAM policy.				

SI-9 INFORMATION INPUT RESTRICTIONS - The organization restricts the capability to input information to the information system to authorized personnel.

SI-9.1 – Examine system and information integrity policy; procedures addressing information input restrictions; access control policy and procedures; separation of duties policy and procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization restricts the capability to input information to the information system to authorized personnel.				

SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY - The information system checks information for accuracy, completeness, validity, and authenticity.

SI-10.1 – Examine system and information integrity policy; procedures addressing information accuracy, completeness, validity, and authenticity; access control policy and procedures; separation of duties policy and procedures; documentation for automated tools and applications to verify accuracy, completeness, validity, and authenticity of information; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The information system checks information for accuracy, completeness, validity, and authenticity;				
(ii)	Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible;				
(iii)	The information system employs rules to check the valid syntax of information inputs to verify that inputs match specified definitions for format and content; and				
(iv)	The information system prescreens information inputs passed to interpreters to prevent the content from being unintentionally interpreted as commands.				

and

Test information system capability for checking information for accuracy, completeness, validity, and authenticity.

Test Steps		S	N	Findings	Initials & Date
1					

SI-11 ERROR HANDLING - The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries.

SI-11.1 – Examine system and information integrity policy; procedures addressing information system error handling; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries;				
(ii)	The information system reveals only essential information to authorized individuals; and				
(iii)	The information system does not include sensitive information in error logs or associated administrative messages.				

and

Test information system error handling capability.

Test Steps		S	N	Findings	Initials & Date
1					

SI-12 INFORMATION OUTPUT HANDLING AND RETENTION - The organization handles and retains output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

SI-12.1 - Examine system and information integrity policy; procedures addressing information system output handling and retention; media protection policy and procedures; information retention records, other relevant documents or records, **and**

Interview organizational personnel with information output handling and retention responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization handles and retains output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements; and				
(ii)	The organization handles output from the information system in accordance with labeled or marked instructions on information system output (including paper and digital media) that includes, but not limited to, special instructions for dissemination, distribution, transport, or storage of information system output.				