Appendix C - Comparing the Office of the Chief Information Officer's IT Security Standards with leading practices	
This appendix provides a comparison of the state's IT security standards to leading practices including:	
- National Institute of Standards and Technology (NIST), Special Publication 800-53, Revision 4	
"Security and Privacy Controls for Federal Information Systems and Organizations"	
- International Organization for Standardization (ISO) IT Security Standards ISO 27001	
OCIO Standard No. 141.10 - Securing Information Technology Assets	**Standard incorporates leading practice(s) (Y/N)**
Standard 1 - IT Security Program	
1.1(1)-Agency IT Security Program-Documentation-The agency IT Security Program documentation must: Align with the agency's risk management strategy.	
ISO 5.1.1, IS Policies:Policies for IS	Y
ISO 6.1.1, Organization of IS:IS roles and responsibilities	Y
NIST PM-1:IS Program Plan	Y
1.1(2)-Agency IT Security Program-Documentation-The agency IT Security Program documentation must: Clearly identify the security objectives for agency systems.	
ISO 5.1.1, IS Policies:Policies for IS	Y
ISO 6.1.1, Organization of IS:IS roles and responsibilities	Y
NIST PM-11:Mission/Business Process Definition	Y
1.1(3)-Agency IT Security Program-Documentation-The agency IT Security Program documentation must: Contain policies, processes and procedures for all sections of OCIO IT security standards.	
ISO 5.1.1, IS Policies:Policies for IS	Y
ISO 6.1.1, Organization of IS:IS roles and responsibilities	Y
NIST PL-2:System Security Plan	Y
NIST PL-9:Central Management	Y
1.1(4)-Agency IT Security Program-Documentation-The agency IT Security Program documentation must: Contain detail commensurate with the size, complexity, and potential business exposure based on the results of the agency's IT Risk Assessment process.	
ISO 5.1.1, IS Policies:Policies for IS	Y
ISO 6.1.1, Organization of IS:IS roles and responsibilities	Y
NIST PM-7:Enterprise Architecture	Y
1.1(5)-Agency IT Security Program-Documentation-The agency IT Security Program documentation must: Contain details of the security controls applied to agency systems.	
ISO 14.1.1, System Acquisition, Development & Maintenance:IS requirements analysis and specification	Y
ISO 9.1.1, Access Control:Access control policy	Y

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
ISO 9.1.2, Access Control:Access to networks and network services	Y
NIST PM-1:IS Program Plan	Y
1.1(6)-Agency IT Security Program-Documentation-The agency IT Security Program documentation must: Contain details, justifications and approvals by OCIO for any deviation from the OCIO IT security standards.	
ISO 5.1.1, IS Policies:Policies for IS	Y
ISO 6.1.3, Organization of IS:Contact with authorities	Y
NIST PL-2:System Security Plan	Y
NIST SA-22:Unsupported System Components	Y
1.1(7)-Agency IT Security Program-Documentation-The agency IT Security Program documentation must: Contain results, logs, and records from risk and security assessments to demonstrate that the assessments performed met the intended security objectives of the agency.	
ISO 12.4.1, Operations Security:Event Logging	Y
ISO 18.2.1, Compliance:Independent review of IS	Y
ISO 18.2.2, Compliance:Compliance with security policies and standards	Y
ISO 18.2.3, Compliance:Technical compliance review	Y
NIST PM-6:IS Measures of Performance	Y
1.1(8)-Agency IT Security Program-Documentation-The agency IT Security Program documentation must: Identify mechanisms for receiving, documenting, and responding to reported security issues.	
ISO 16.1.1, IS Incident Management:Responsibilities and procedures	Y
NIST PM-4:Plan of Action and Milestones Process	Y
1.2(1)-Agency IT Security Program-IT Risk Assessment-The agency must: Define and implement a formal IT Risk Assessment process to evaluate risks resulting from the use of information systems to agency operations, systems and personnel.	
ISO 8.1 (ISO/IEC 27005:2011), IS Risk Assessment:General description of IS risk management	Y
NIST PM-9:Risk Management Strategy	Y
NIST RA-1:Risk Assessment Policy and Procedures	Y
1.2(2)-Agency IT Security Program-IT Risk Assessment-The agency must: Conduct an IT Risk Assessment when introducing new systems. When changes are made to an existing computing environment that impacts risk, conduct an IT Risk Assessment with a scope that is in proportion to the changes made.	
ISO 8.2.4 (ISO/IEC 27005:2011), IS Risk Assessment:Identification of existing controls	Y
NIST RA-3:Risk Assessment	Y

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
1.2(3)-Agency IT Security Program-IT Risk Assessment-The agency must: Identify assets that are within the scope of the agency IT Security Program and the entity that has responsibility for the production, development, maintenance, use, and security of the assets.	
ISO 8.2.2 (ISO/IEC 27005:2011), IS Risk Assessment:Identification of assets	Y
NIST RA-2:Security Categorization	Y
1.2(4)-Agency IT Security Program-IT Risk Assessment-The agency must: Identify potential threats to assets identified as within scope.	
ISO 8.2.3 (ISO/IEC 27005:2011), IS Risk Assessment:Identification of threats	Y
NIST RA-3:Risk Assessment	Y
1.2(5)-Agency IT Security Program-IT Risk Assessment-The agency must: Identify the vulnerabilities that might be exploited by the threats.	
ISO 8.2.5 (ISO/IEC 27005:2011), IS Risk Assessment:Identification of vulnerabilities	Y
NIST RA-5:Vulnerability Scanning	Y
1.2(6)-Agency IT Security Program-IT Risk Assessment-The agency must: Identify the impacts that losses of confidentiality, integrity, and availability may have on assets identified as within scope.	
ISO 8.2.6 (ISO/IEC 27005:2011), IS Risk Assessment:Identification of consequences	Y
NIST RA-5:Vulnerability Scanning	Y
1.2(7)-Agency IT Security Program-IT Risk Assessment-The agency must: Assess the likelihood that security failures may occur based on prevailing threats and vulnerabilities.	
ISO 8.3.3 (ISO/IEC 27005:2011), IS Risk Assessment:Assessment of incident likelihood	Y
NIST RA-5:Vulnerability Scanning	Y
1.2(8)-Agency IT Security Program-IT Risk Assessment-The agency must: Conduct an IT Risk Assessment on Systems processing Category 3 data or higher once every three years. Please refer to Section 4 for data categories.	
ISO 8.4 (ISO/IEC 27005:2011), IS Risk Assessment:Risk evaluation	Y
NIST RA-1:Risk Assessment Policy and Procedures	Y
1.2(9)-Agency IT Security Program-IT Risk Assessment-The agency must: Take into account business, legal, or regulatory requirements, and contractual security obligations.	
ISO 8.4 (ISO/IEC 27005:2011), IS Risk Assessment:Risk evaluation	Y
NIST RA-5:Vulnerability Scanning	Y

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
1.2.1-Agency IT Security Program-IT Risk Assessment-Design Review-The agency must request a security design review for maintenance and new development of systems and infrastructure projects when one or more of the following conditions exist:(1) An agency is required to submit an investment plan to OCIO commensurate with the IT Investment Standards, (2) An agency project or initiative requires OCIO or OCIO oversight as determined by OCIO policy and standards, (3) An agency project or initiative impacts risk to state IT assets outside the agency, or (4) An agency project or initiative meets criteria for a Design Review as defined and documented by the agency IT security program.	
ISO 14.1.1, System Acquisition, Development & Maintenance:IS requirements analysis and specification	Y
NIST PL-1:Security Planning Policy and Procedures	Y
NIST PL-2:System Security Plan	Y
NIST PL-7:Security Concept of Operations	Y
NIST PM-3:IS Resources	Y
1.2.1.1-Agency IT Security Program-IT Risk Assessment-The agency must provide the following to the state Chief Information Security Officer at CTS for the design review:(1) The IT Security Checklist for the system. Please refer to Section 1.5, (2) A system architecture diagram showing security controls and information flows, (3) The Security risks identified for the system and IT infrastructure, and (4) The planned security controls and how they will be implemented.	
ISO 14.1.1, System Acquisition, Development & Maintenance:IS requirements analysis and specification	Y
NIST SA-2:Allocation of Resources	Y
NIST SA-3:System Development Life Cycle	Y
NIST SA-5:Information System Documentation	Y
1.2.1.2-Agency IT Security Program-IT Risk Assessment-The Chief Information Security Officer at CTS must:(1) Review the results of the agency IT Security Checklist and other documents specific to the System, (2) Determine whether the security design complies with OCIO IT security standards, and (3) Provide design recommendations as necessary for the agency to satisfy OCIO IT security standards.	
NIST CA-6:Security Authorization	Y
NIST PM-10: Security Authorization Process	Y
NIST PM-2: Senior Information Security Officer	Y
1.3-Agency IT Security Program-IT Security Assessment-IT Security Assessments must be conducted periodically to review and assess the effectiveness of existing security controls. These assessments must include testing of security controls to make sure unauthorized access attempts can be identified or stopped. Examples of periodic testing include penetration tests, vulnerability assessments and system code analysis.	
ISO 12.7.1, Operations Security:Information systems audit controls	Y
ISO 18.2.2, Compliance:Compliance with security policies and standards	Y

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
ISO 6.1.5, Organization of IS:IS in project management	Y
1.3(1)-Agency IT Security Program-IT Security Assessment-The agency must: Establish an IT Security Assessment framework and schedule to identify a sampling of agency systems, applications, and IT infrastructure to test.	
NIST CA-1:Security Assessment and Authorization Policies and Procedures	Y
1.3(2)-Agency IT Security Program-IT Security Assessment-The agency must: Conduct IT Security Assessments against the sample in the framework to verify security controls and identify weaknesses at least once every three years.	
NIST CA-2:Security Assessments	Y
1.3(3)-Agency IT Security Program-IT Security Assessment-The agency must: Conduct an assessment through testing scenarios relevant to changes made when the following conditions exist:(a)A significant IT infrastructure upgrade or modification since the last IT Security Assessment was performed. Examples of a significant infrastructure upgrade or modification include but are not limited to:(a)the addition of a new sub-network, DMZ or security perimeter device; upgrades to firewalls, switches or routers, or (b) Applications have been added or significantly modified.	
NIST CA-5:Plan of Action and Milestones	Y
1.3(4)-Agency IT Security Program-IT Security Assessment-The agency must: Correct weaknesses identified with appropriate controls.	
NIST PM-4:Plan of Action and Milestones Process	Y
1.4-Agency IT Security Program-Education & Awareness	
ISO 7.2.2, Human Resource Security:IS awareness, education and training	Y
1.4(1)-Agency IT Security Program-Education & Awareness-The agency must: Ensure that personnel assigned responsibilities defined in the agency IT Security Program are competent to perform the required tasks.	
NIST AT-3:Role-Based Security Training	Y
NIST SA-16:Developer-Provided Training	Y
1.4(2)-Agency IT Security Program-Education & Awareness-The agency must: Document the knowledge, skills, and abilities required for personnel performing work affecting the agency IT Security Program.	
NIST AT-1:Security Awareness and Training Policy and Procedures	Y
1.4(3)-Agency IT Security Program-Education & Awareness-The agency must: Require that all employees receive annual security awareness training that includes the risks of data compromise, their role in prevention, and how to respond in the event of an incident as relevant to the individual's job function.	
NIST AT-2:Security Awareness Training	Y
NIST PM-12:Insider Threat Program	Y
NIST PM-14:Testing, Training, and Monitoring	Y
NIST PM-16:Threat Awareness Program	Y

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
1.4(4)-Agency IT Security Program-Education & Awareness-The agency must ensure that personnel assigned responsibilities defined in the agency IT Security Program must, at a minimum, receive training that addresses the OCIO Security Policy and Standard and the agency's security policies and procedures	
ISO 7.2.2, Human Resource Security:IS awareness, education and training	Y
NIST AT-2:Security Awareness Training	Y
NIST PM-12:Insider Threat Program	Y
NIST PM-14:Testing, Training, and Monitoring	Y
NIST PM-16:Threat Awareness Program	Y
1.5(1)-Agency IT Security Program-Compliance-The agency must: Ensure compliant implementation of systems and IT infrastructure funded and approved after adoption of these IT security standards.	
ISO 14.2.5, System Acquisition, Development & Maintenance:Secure system engineering principles	Y
ISO 14.2.8, System Acquisition, Development & Maintenance:System acceptance testing	Y
ISO 18.1.1, Compliance:Identification of applicable legislation and contractual requirements	Y
ISO 6.1.3, Organization of IS:Contact with authorities	Y
NIST CM-2:Baseline Configuration	Y
1.5(2)-Agency IT Security Program-Compliance-The agency must: Include estimates to implement these IT security standards and resulting security controls in schedules, budgets, and funding requests for maintenance and new development of applications, infrastructure, and operations.	
ISO 18.1.1, Compliance:Identification of applicable legislation and contractual requirements	Y
NIST CM-1:Configuration Management Policy and Procedures	Y
1.5(3)-Agency IT Security Program-Compliance-The agency must: Complete the IT Security Checklist and include results in budgets and schedules of new development or maintenance when:(a) Significant changes are made to the application, IT infrastructure or operations, (b)An IT Investment Plan must be prepared, or (c)The IT Security Checklist is required by the agency IT security program.	
ISO 14.2.5, System Acquisition, Development & Maintenance:Secure system engineering principles	Y
NIST CA-2:Security Assessments	Y
1.5(4)-Agency IT Security Program-Compliance-The agency must: Include in the agency investment plan the signed off copy of the IT Security Checklist from the Design Review itemizing the security controls and associated budget, schedule and resource estimates. If the agency investment plan is submitted to OCIO, the IT Security Checklist will be returned to the agency when processing is complete and securely filed in the agency.	
ISO 14.2.5, System Acquisition, Development & Maintenance:Secure system engineering principles	Y
NIST SA-1:System and Services Acquisition Policy and Procedures	Y

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
1.5(5)-Agency IT Security Program-Compliance-The agency must: Attain full compliance with these IT security standards by August 2012.	
ISO 18.1.1, Compliance:Identification of applicable legislation and contractual requirements	Y
NIST CM-1:Configuration Management Policy and Procedures	Y
1.5(6)-Agency IT Security Program-Compliance-The agency must: Select and apply the appropriate security controls commensurate with the risk and complexity of the system after completing the agency IT Risk Assessment (Section 1.2), IT Security Assessment (Section 1.3), the IT Security Checklist, and the Design Review (when required) to comply with the requirements in the OCIO IT security standards.	
ISO 14.2.1, System Acquisition, Development & Maintenance:Secure development policy	Y
ISO 9.1.1, Access Control:Access control policy	Y
NIST SA-8:Security Engineering Principles	Y
1.5(7)-Agency IT Security Program-Compliance-The agency must require contractor's compliance with OCIO IT security standards relative to the services provided when (a) The scope of work affects a state IT resource or asset, or (b) The agency contracts for IT resources or services with an entity not subject to the OCIO IT security standards.	
ISO 14.2.7, System Acquisition, Development & Maintenance:Outsourced development	Y
ISO 15.2.2, Supplier Relationships:Managing changes to supplier services	Y
NIST CM-3:Configuration Change Control	Y
NIST SA-9:External Information System Services	Y
1.5(8)-Agency IT Security Program-Compliance-The agency must: Confirm in writing that the agency is in compliance with OCIO IT security standards. The head of each agency will provide annual verification to the OCIO by August 31 of each year or Office of Financial Management budget submittal date, whichever is later, that an agency IT Security Program has been developed and implemented according to the OCIO IT security standards. The annual security verification letter will be included in the agency IT portfolio and submitted to OCIO. The verification indicates review and acceptance of agency security policies, procedures, and practices as well as updates since the prior verification.	
ISO 18.1.1, Compliance:Identification of applicable legislation and contractual requirements	Y
NIST SA-5:Information System Documentation	Y
1.5(9)-Agency IT Security Program-Compliance-The agency must: Document instances of non-compliance with OCIO IT security standards beginning no later than August 2010 and during the funding and approval process for new initiatives referenced above in Section 1.5. For those components that do not comply, agencies complete the IT Security Non-Compliance/Deviation Form, Appendix C. Update the form and submit annually with the annual security verification letter. The form is submitted to the state CIO for approval through the state Chief Information Security Officer at CTS. For security reasons, please submit only hardcopy IT Security Non-Compliance/Deviation Forms. Do not submit these forms via email. Agencies may submit appeals to the OCIO.	

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
ISO 18.1.1, Compliance:Identification of applicable legislation and contractual requirements	Y
NIST SA-1:System and Services Acquisition Policy and Procedures	Y
NIST SA-22:Unsupported System Components	Y
1.6(1)-Agency IT Security Program-Audit-The agency must: Ensure an independent audit is performed once every three years to assess compliance with OCIO IT security standards.	
ISO 18.2.1, Compliance:Independent review of IS	Y
1.6(2)-Agency IT Security Program-Audit-The agency must: Ensure the audit is performed by qualified parties independent of the agency's IT organization.	
ISO 18.2.1, Compliance:Independent review of IS	Y
1.6(3)-Agency IT Security Program-Audit-The agency must: Submit the results of the audit to the state chief information security officer at CTS.	
ISO 6.1.3, Organization of IS:Contact with authorities	Y
1.6(4)-Agency IT Security Program-Audit-The agency must: Maintain documentation showing the results of the audit according to applicable records retention requirements.	
ISO 18.2.1, Compliance:Independent review of IS	Y
1.6(5)-Agency IT Security Program-Audit-The agency must: Validate that security controls are implemented appropriately based on OCIO IT security standards, the agency security program, and applicable regulatory requirements.	
ISO 18.2.1, Compliance:Independent review of IS	Y
1.6(6)-Agency IT Security Program-Audit-The agency must: Identify nonconformities and related causes.	
ISO 18.2.1, Compliance:Independent review of IS	Y
1.6(7)-Agency IT Security Program-Audit-The agency must: Track progress to correct nonconformities.	
ISO 18.2.1, Compliance:Independent review of IS	Y
1.6(8)-Agency IT Security Program-Audit-The agency must: Implement the corrective action needed.	
ISO 18.2.1, Compliance:Independent review of IS	Y
1.7(1)-Agency IT Security Program-Maintenance-The agency must: Conduct an annual maintenance and review of the agency IT Security Program.	
ISO 5.1.2, IS Policies:Review of the policies for IS	Y
NIST MA-1:System Maintenance Policy and Procedures	Y
1.7(2)-Agency IT Security Program-Maintenance-The agency must: Identify areas to improve the effectiveness of the agency IT Security Program.	
ISO 5.1.2, IS Policies:Review of the policies for IS	Y
NIST MA-2:Controlled Maintenance	Y

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
Standard 2 - Personnel Security	
2-Personnel Security-These Personnel Security controls are designed to reduce risks of human error, theft, fraud, or misuse of facilities. They help agencies ensure that users are aware of information security threats and are equipped to support the OCIO security policy in the course of their normal work.	
NIST PS-1:Personnel Security Policy and Procedures	Y
2(1)-Personnel Security-Agencies must: Provide IT security orientation and supervision of employees and monitor contractors who have access to agency IT Assets.	
ISO 7.2.1, Human Resource Security:Management responsibilities	Y
NIST PS-7:Third-Party Personnel Security	Y
2(2)-Personnel Security-Agencies must: Ensure that appropriate staff conduct is achieved and maintained related to security matters.	
ISO 7.2.1, Human Resource Security:Management responsibilities	Y
NIST PS-2:Position Risk Designation	Y
NIST PS-7:Third-Party Personnel Security	Y
2(3)-Personnel Security-Agencies must: Conduct reference checks and background investigations as required by the agency IT security program and authorized by the agency.	
ISO 7.1.1, Human Resource Security:Screening	Y
NIST PS-3:Personnel Screening	Y
2(4)-Personnel Security-Agencies must: Require employees to receive appropriate awareness training and regular updates on agency and OCIO IT Security Policies and standards as described in Section 1.4.	
ISO 7.2.2, Human Resource Security:IS awareness, education and training	Y
NIST AT-2:Security Awareness Training	Y
2(5)-Personnel Security-Agencies must: Provide opportunities for IT Security support staff to obtain technical training.	
ISO 7.2.2, Human Resource Security:IS awareness, education and training	Y
NIST AT-3:Role-Based Security Training	Y
2(6)-Personnel Security-Agencies must: Impose appropriate sanctions for security violations.	
ISO 7.2.3, Human Resource Security:Disciplinary process	Y
NIST PS-8:Personnel Sanctions	Y
2(7)-Personnel Security-Agencies must: Establish processes for the timely removal of system access for employees and contractors when duties change or when separating from service.	
ISO 9.2.5, Access Control:Review of user access rights	Y
NIST PS-4:Personnel Termination	Y
NIST PS-5:Personnel Transfer	Y

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
2(8)-Personnel Security-Agencies must: Include appropriate language in vendor contracts to require compliance with OCIO and agency security policies, standards, and requirements.	
ISO 7.1.2, Human Resource Security:Terms and conditions of employment	Y
NIST PS-7:Third-Party Personnel Security	Y
2(9)-Personnel Security-Agencies must: Require employees and contractors to comply with these IT security standards and agency IT policies and procedures. Each user should be made clearly aware of this responsibility.	
ISO 7.1.2, Human Resource Security:Terms and conditions of employment	Y
NIST PS-6:Access Agreements	Y
2(10)-Personnel Security-Agencies must: Identify, document, and implement rules for the acceptable use of IT assets consistent with rules provided by the Washington State Executive Ethics Board.	
ISO 8.1.3, Asset Management:Acceptable use of assets	Y
NIST PL-4:Rules of Behavior	Y
Standard 3 - Physical & Environmental Security	
3-Physical & Environmental Protection-Agencies are responsible for ensuring that adequate physical security and environmental protections are implemented to maintain the confidentiality, integrity, and availability of the agency's computer systems. Agencies must prevent unauthorized access, damage, or compromise of IT assets. Investments in physical and environmental security must be commensurate with the risks, threats, and vulnerabilities unique to each physical site and location.	
ISO 11.1.3, Physical & Environmental Security:Securing offices, rooms and facilities	N
ISO 11.1.4, Physical & Environmental Security:Protecting against external and environmental threats	N
ISO 11.1.6, Physical & Environmental Security:Delivery and loading areas	N
ISO 11.2.2, Physical & Environmental Security:Supporting utilities	N
ISO 11.2.3, Physical & Environmental Security:Cabling security	N
NIST PE-10:Emergency Shutoff	N
NIST PE-11:Emergency Power	N
NIST PE-12:Emergency Lighting	N
NIST PE-13:Fire Protection	N
NIST PE-14:Temperature and Humidity Controls	N
NIST PE-15:Water Damage Protection	N
NIST PE-16:Delivery and Removal	N
NIST PE-17:Alternate Work Site	N
NIST PE-18:Location of Information System Components	N
NIST PE-2:Physical Access Authorization	N

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
NIST PE-20:Asset Monitoring and Tracking	N
NIST PE-5:Access Control for Output Devices	N
NIST PE-6:Monitoring Physical Access	N
NIST PE-8:Visitor Access Records	N
NIST PE-9:Power Equipment and Cabling	N
NIST SC-42:Sensor Capability and Data	N
3.1(1)-Physical & Environmental Protection-Facilities-Agencies must develop, document, and implement policies and procedures for the following: Location and layout of the facility.	
ISO 11.1.1, Physical & Environmental Security:Physical security perimeter	Y
NIST PE-1:Physical & EnvironmentalProtection Policy and Procedures	Y
3.1(2)-Physical & Environmental Protection-Facilities-Agencies must develop, document, and implement policies and procedures for the following: Physical security attributes for computer or telecommunications rooms.	
ISO 11.1.2, Physical & Environmental Security:Physical entry controls	Y
NIST PE-3:Physical Access Control	Y
3.1(3)-Physical & Environmental Protection-Facilities-Agencies must develop, document, and implement policies and procedures for the following: Design and enforcement of physical protection and guidelines for working in secure areas.	
ISO 11.1.5, Physical & Environmental Security:Working in secure areas	Y
NIST PE-3:Physical Access Control	Y
3.1(4)-Physical & Environmental Protection-Facilities-Agencies must develop, document, and implement policies and procedures for the following: Facility access control.	
ISO 11.1.2, Physical & Environmental Security:Physical entry controls	Y
NIST PE-3:Physical Access Control	Y
3.1(5)-Physical & Environmental Protection-Facilities-Agencies must develop, document, and implement policies and procedures for the following: Physical data storage and telecommunications controls.	
ISO 11.2.1, Physical & Environmental Security:Equipment siting and protection	Y
NIST PE-4:Access Control for Transmission Medium	Y
3.1(6)-Physical & Environmental Protection-Facilities-Agencies must develop, document, and implement policies and procedures for the following: Off-site media storage.	
ISO 11.2.6, Physical & Environmental Security:Security of equipment and assets off-premises	Y
NIST PE-4:Access Control for Transmission Medium	Y
3.1(7)-Physical & Environmental Protection-Facilities-Agencies must develop, document, and implement policies and procedures for the following: Physical security controls for mobile devices.	

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
ISO 11.2.1, Physical & Environmental Security:Equipment siting and protection	Y
ISO 6.2.1, Organization of IS:Mobile device policy	Y
NIST SA-18:Tamper Resistance and Detection	Y
Standard 4 - Data Security	
4.1(1-3)-Data Security-Data Classification-Agency data classifications must translate to or include the following classification categories: Category 1-Public Information, Category 2-Sensitive Information, Category 3-Confidential Information and Category 4-Confidential Information Requiring Special Handling	
ISO 18.1.4, Compliance:Privacy and protection of personally identifiable information	Y
ISO 8.2.1, Asset Management:Classification of information	Y
ISO 8.2.2, Asset Management:Identification of assets	Y
ISO 8.2.3 (ISO/IEC 27005:2011), IS Risk Assessment:Identification of threats	Y
NIST RA-2:Security Categorization	Y
4.2(1-9)-Data Security-Data Sharing-Agencies must ensure that sharing data with the public at large complies with the OCIO Public Records Privacy Protection Policy and other applicable statutes or regulations. When sharing Category 3 and above data outside the agency, an agreement must be in place unless otherwise prescribed by law. The agreement (such as a contract, a service level agreement, or a dedicated data sharing agreement) must address standards 4.2(1-9).	
ISO 13.2.1, Communications Security:Information transfer policies and procedures	Y
ISO 13.2.3, Communications Security:Electronic messaging	Y
ISO 13.2.4, Communications Security:Confidentialiy or non-disclosure agreements	Y
ISO 15.1.1, Supplier Relationships:IS in supplier relationships	Y
ISO 15.1.2, Supplier Relationships:Addressing security within supplier agreements	Y
ISO 15.1.3, Supplier Relationships:Information and communication technology supply chain	Y
ISO 15.2.1, Supplier Relationships:Monitoring and review of supplier services	Y
ISO 15.2.2, Supplier Relationships:Managing changes to supplier services	Y
ISO 7.3.1, Human Resource Security:Termination or change of employment responsibilities	Y
NIST AC-21:Information Sharing	Y
NIST AC-22:Publicly Accessible Content	Y
NIST CA-3:System Interconnections	Y
NIST SA-9:External Information System Services	Y
ISO 11.2.5, Physical & Environmental Security:Removal of assets	Y

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
4.3(1)-Data Security-Secure Management & Encryption of Data-The storage of Category 3 and above information requires agencies to select and apply encryption, at the discretion of the agency, after completing an agency IT Security Risk Assessment. Agencies must use industry standard algorithms or cryptographic modules validated by the National Institute of Standards and Technology (NIST).	
ISO 10.1.1, Cryptography:Policy on the use of cryptographic controls	Y
ISO 10.1.2, Cryptography:Cryptographic controls	N
ISO 18.1.5, Compliance:Regulation of cryptographic controls	Y
NIST AC-16:Security Attributes	Y
NIST SC-12:Cryptographic Key Establishment and Management	Y
NIST SC-13:Cryptographic Protection	Y
NIST SC-17:Public Key Infrastructure Certificates	Y
NIST SC-28:Protection of Information at Rest	Y
4.4-Data Security-Secure Data Transfer-Agencies must appropriately protect information transmitted electronically.	
ISO 11.2.5, Physical & Environmental Security:Removal of assets	Y
ISO 13.2.2, Communications Security:Agreements on information transfer	Y
ISO 13.2.3, Communications Security:Electronic messaging	Y
ISO 7.3.1, Human Resource Security:Termination or change of employment responsibilities	Y
4.4(1)-Data Security-Secure Data Transfer-The transmission of Category 3 and above information outside of the SGN requires encryption such that: All manipulations or transmissions of data during the exchange are secure.	
NIST SC-13:Cryptographic Protection	Y
NIST SC-16:Transmission of Security Attributes	Y
4.4(2)-Data Security-Secure Data Transfer-The transmission of Category 3 and above information outside of the SGN requires encryption such that: If intercepted during transmission the data cannot be deciphered.	
NIST SC-8:Transmission Confidentiality and Integrity	Y
NIST SI-1:System and Information Integrity Policy and Procedure	Y
4.4(3)-Data Security-Secure Data Transfer-The transmission of Category 3 and above information outside of the SGN requires encryption such that: When necessary, confirmation is received when the intended recipient receives the data.	
NIST AC-4:Information Flow Enforcement	Y
4.4(4)-Data Security-Secure Data Transfer-The transmission of Category 3 and above information outside of the SGN requires encryption such that: Agencies must use industry standard algorithms, or cryptographic modules validated by the National Institute of Standards and Technology (NIST).	
NIST SC-13:Cryptographic Protection	Y

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
4.4(5)-Data Security-Secure Data Transfer-The transmission of Category 3 and above information outside of the SGN requires encryption such that: For agencies not on the SGN, this standard applies when transmitting Category 3 and above information outside of the agency's secure network.	
NIST AC-4:Information Flow Enforcement	Y
Standard 5 - Network Security	
5.1-Network Security-Secure Segmentation-Agencies must:(1) Define and implement logical boundaries to segment networks as determined by system risk and data classification, (2) Enforce controls to protect segments and individual assets within each segment. The methods to achieve secure segmentation include but are not limited to those detailed in Sections 5.1.1-5.1.3.	
ISO 13.1.3, Communications Security:Segregation in networks	Y
NIST SC-7:Boundary Protection	Y
5.1.1-Network Security-Secure Segmentation-Network Devices	
NIST CA-9:Internal System Connections	Y
NIST SA-22:Unsupported System Components	Y
NIST SC-11:Trusted Path	Y
NIST SC-15:Collaborative Computing Devices	Y
NIST SC-24:Fail in Known State	Y
NIST SC-3:Security Function Isolation	Y
NIST SC-39:Process Isolation	Y
NIST SC-4:Information in Shared Resources	Y
NIST SI-17:Fail-Safe Procedures	Y
5.1.1(1)-Network Security-Secure Segmentation-Network Devices-Agencies must: Securely segment Internet-available systems from internal networks.	
ISO 13.1.1, Communications Security:Network controls	Y
ISO 13.1.3, Communications Security:Segregation in networks	Y
NIST SC-32:Information System Partitioning	Y
NIST SC-7:Boundary Protection	Y
5.1.1(2)-Network Security-Secure Segmentation-Network Devices-Agencies must: Disable unnecessary functionality such as scripts, drivers, features, subsystems, file systems and services.	
ISO 13.1.2, Communications Security:Security of network services	Y
NIST CM-7:Least Functionality	Y
NIST SC-25:Thin Nodes	Y
NIST SC-41:Port and I/A Devices Access	Y

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
5.1.1(3)-Network Security-Secure Segmentation-Network Devices-Agencies must: Harden devices based on industry best practice such as NIST, SANS, and vendor configuration standards.	
ISO 13.1.2, Communications Security:Security of network services	Y
NIST CM-2:Baseline Configuration	Y
NIST CM-6:Configuration Settings	Y
5.1.1(4)-Network Security-Secure Segmentation-Network Devices-Agencies must: Change default or initial passwords upon installation.	
ISO 9.2.4, Access Control:Management of secret authentication information of users	Y
ISO 9.4.3, Access Control:Password management system	Y
NIST IA-5:Authenticator Management	Y
5.1.1(5)-Network Security-Secure Segmentation-Network Devices-Agencies must: Display banner text conveying appropriate use at system entry points and at access points where initial user logon occurs.	
ISO 9.4.2, Access Control:Secure log-on procedures	Y
NIST AC-8:System Use Notification	N
5.1.1(6)-Network Security-Secure Segmentation-Network Devices-Agencies must: Disable remote communications where no business need exists.	
ISO 13.1.2, Communications Security:Security of network services	Y
NIST AC-17:Remote Access	Y
NIST CM-7:Least Functionality	Y
5.1.1(7)-Network Security-Secure Segmentation-Network Devices-Agencies must: Standardize and document the device configurations deployed.	
ISO 12.1.1, Operations Security:Documented operating procedures	Y
NIST CM-6:Configuration Settings	Y
5.1.1(8)-Network Security-Secure Segmentation-Network Devices-Agencies must: Document deviations from device configuration standards along with the approval.	
ISO 5.1.1, IS Policies:Policies for IS	Y
NIST CM-3:Configuration Change Control	Y
5.1.1(9)-Network Security-Secure Segmentation-Network Devices-Agencies must: Mask internal addresses from exposure on the Internet as necessitated by the risk and complexity of the system.	
ISO 13.1.3, Communications Security:Segregation in networks	Y
NIST SC-7:Boundary Protection	Y
5.1.1(10)-Network Security-Secure Segmentation-Network Devices-Agencies must: Implement controls to prevent unauthorized computer connections and information flows through methods such as:	

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
ISO 13.1.2, Communications Security:Security of network services	Y
NIST SI-4:Information System Monitoring	Y
5.1.1(10)(a)-Network Security-Secure Segmentation-Network Devices-Agencies must: Implement controls to prevent unauthorized computer connections and information flows through methods such as: Authentication of routing protocols.	
NIST SC-7:Boundary Protection	Y
5.1.1(10)(b)-Network Security-Secure Segmentation-Network Devices-Agencies must: Implement controls to prevent unauthorized computer connections and information flows through methods such as: Ingress filtering at network edge locations.	
NIST SC-7:Boundary Protection	Y
5.1.1(10)(c)-Network Security-Secure Segmentation-Network Devices-Agencies must: Implement controls to prevent unauthorized computer connections and information flows through methods such as: Internal route filtering.	
NIST SC-7:Boundary Protection	Y
5.1.1(10)(d)-Network Security-Secure Segmentation-Network Devices-Agencies must: Implement controls to prevent unauthorized computer connections and information flows through methods such as: Routing protocols are enabled only on necessary interfaces.	
NIST CM-7:Least Functionality	Y
5.1.1(10)(e)-Network Security-Secure Segmentation-Network Devices-Agencies must: Implement controls to prevent unauthorized computer connections and information flows through methods such as: Restrict routing updates on access ports.	
NIST CM-7:Least Functionality	Y
5.1.1(10)(f)-Network Security-Secure Segmentation-Network Devices-Agencies must: Implement controls to prevent unauthorized computer connections and information flows through methods such as: Secure or disable physical network connections in public areas.	
NIST SC-7:Boundary Protection	Y
5.1.2-Network Security-Secure Segmentation-Firewalls	
NIST SC-20:Secure Name /Address Resolution Service (Authoritative Source)	Y
NIST SC-21:Secure Name /Address Resolution Service (Recursive or Caching Resolver)	Y
NIST SC-22:Architecture and Provisioning for Name/Address Resolution Service	Y
NIST SC-5:Denial of Service Protection	Y
5.1.2(1)-Network Security-Secure Segmentation-Firewalls-Agencies must: Securely segment DMZ interfaces, where utilized, from interfaces connected directly to the internal network.	
ISO 13.1.3, Communications Security:Segregation in networks	Y

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
NIST SC-7:Boundary Protection	Y
5.1.2(2)-Network Security-Secure Segmentation-Firewalls-Agencies must: Configure network firewalls protecting production systems	
ISO 13.1.2, Communications Security:Security of network services	Y
5.1.2(2)(a)-Network Security-Secure Segmentation-Firewalls-Agencies must: Configure network firewalls protecting production systems to: Allow system administration only through secure encrypted protocols.	
NIST CM-7:Least Functionality	Y
NIST SC-13:Cryptographic Protection	Y
5.1.2(2)(b)-Network Security-Secure Segmentation-Firewalls-Agencies must: Configure network firewalls protecting production systems to: Prevent access by unauthorized source IP addresses or subnets.	
NIST SC-7:Boundary Protection	Y
5.1.2(2)(c)-Network Security-Secure Segmentation-Firewalls-Agencies must: Configure network firewalls protecting production systems to: Block ingress of internal addresses from an external interface into the DMZ or internal interface.	
NIST SC-7:Boundary Protection	Y
5.1.2(2)(d)-Network Security-Secure Segmentation-Firewalls-Agencies must: Configure network firewalls protecting production systems to: Block services, protocols, and ports not specifically allowed.	
NIST SC-7:Boundary Protection	Y
5.1.2(2)(e)-Network Security-Secure Segmentation-Firewalls-Agencies must: Configure network firewalls protecting production systems to: Allow only necessary egress communications from the internal network to the DMZ, Internet, wireless networks and SGN.	
NIST SC-7:Boundary Protection	Y
5.1.2(2)(f)-Network Security-Secure Segmentation-Firewalls-Agencies must: Configure network firewalls protecting production systems to: Allow only necessary ingress communications to the internal network from the DMZ, Internet, wireless networks and SGN.	
NIST SC-7:Boundary Protection	Y
5.1.2(2)(g)-Network Security-Secure Segmentation-Firewalls-Agencies must: Configure network firewalls protecting production systems to: Maintain comprehensive audit trails.	
NIST AU-11:Audit Record Retention	N
NIST AU-14:Session Audit	N
NIST AU-2:Audit Events	N
NIST AU-3:Content of Audit Records	N
NIST AU-8:Time Stamps	N

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
5.1.2(2)(h)-Network Security-Secure Segmentation-Firewalls-Agencies must: Configure network firewalls protecting production systems to: Fail in a closed state if failure occurs.	
NIST SC-24:Fail in Known State	Y
5.1.2(2)(i)-Network Security-Secure Segmentation-Firewalls-Agencies must: Configure network firewalls protecting production systems to: Operate boundary/perimeter firewalls on a platform specifically dedicated to firewalls.	
NIST SC-7:Boundary Protection	Y
5.1.2(3)-Network Security-Secure Segmentation-Firewalls-Agencies must: Document services, ports and protocols allowed through firewalls, with supporting business purposes, in the agency IT security program.	
ISO 12.1.1, Operations Security:Documented operating procedures	Y
NIST CM-6:Configuration Settings	Y
5.1.2(4)-Network Security-Secure Segmentation-Firewalls-Agencies must: Review configurations annually.	
ISO 5.1.2, IS Policies:Review of the policies for IS	Y
NIST CM-6:Configuration Settings	Y
5.1.3(1)-Network Security-Secure Segmentation-Device Administration	
ISO 9.4.1, Access Control:Information access restriction	Y
NIST CM-3:Configuration Change Control	Y
NIST AC-3:Access Enforcement	Y
5.1.3(2)-Network Security-Secure Segmentation-Device Administration-Agencies must: Encrypt non-console administrative access using technologies such as Secure Shell (SSH), Virtual Private Network (VPN), or Secure Sockets Layer (SSL)/ Transport Layer Security (TLS) for Web-based management and other non-console administrative access.	
NIST IA-7:Cryptographic Module Authentication	Y
5.2-Network Security-Restricted Services-Agencies must implement controls to prohibit the use of the following service and application types listed in this section unless specifically authorized. The use of restricted services must be documented in the agency IT security program and approved by agency management.	
ISO 13.1.2, Communications Security:Security of network services	Y
ISO 9.4.4, Access Control:Use of privileged security programs	Y
NIST CM-10:Software Usage Restrictions	Y
NIST CM-11:User-Installed Software	Y
NIST SC-43:Usage Restrictions	Y
5.3-Network Security-External Connections-Agencies with devices connected to the SGN must:(1) Prohibit direct public access between external networks and internal systems, (2) Connect agency networks to the SGN through a CTS-managed security layer, and (3) Connect internal networks to external networks through a CTS-managed or CTS-approved security layer. The CTS-managed security layer is defined as firewalls, proxy servers and security gateways.	

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
ISO 9.4.1, Access Control:Information access restriction	Y
NIST SC-7:Boundary Protection	Y
5.4-Network Security-Wireless Connections-Agencies are responsible for the secure deployment of wireless networks.	
ISO 13.1.3, Communications Security:Segregation in networks	Y
NIST CM-6:Configuration Settings	Y
NIST SC-40:Wireless Link Protection	Y
5.4(1)-Network Security-Wireless Connections-Agencies must ensure: The agency IT Security Program addresses the use of wireless technologies including but not limited to:(a)802.11, (b)Bluetooth	
NIST AC-18:Wireless Access	Y
5.4(2)(a)-Network Security-Wireless Connections-Agencies must ensure: Wireless devices that extend their Local Area Networks (LANs):Securely segment wireless access point connections from the agency network and the SGN.	
NIST SC-7:Boundary Protection	Y
5.4(2)(b)-Network Security-Wireless Connections-Agencies must ensure: Wireless devices that extend their Local Area Networks (LANs):Use WPA or its successor for authentication and encryption. Use WPA2 Enterprise on all new equipment purchased and existing equipment that supports the protocol.	
NIST IA-7:Cryptographic Module Authentication	Y
5.4(2)(c)-Network Security-Wireless Connections-Agencies must ensure: Wireless devices that extend their Local Area Networks (LANs):Change wireless vendor defaults including but not limited to pre-shared keys and passwords.	
NIST IA-5:Authenticator Management	Y
5.4(2)(d)-Network Security-Wireless Connections-Agencies must ensure: Wireless devices that extend their Local Area Networks (LANs):Disable Simple Network Management Protocol (SNMP) unless there is a clear business need. If enabled, change the vendor defaults.	
NIST CM-7:Least Functionality	Y
5.4(2)(e)-Network Security-Wireless Connections-Agencies must ensure: Wireless devices that extend their Local Area Networks (LANs):Follow wireless access security practices developed within the agency.	
NIST AC-18:Wireless Access	Y
5.4(2)(f)-Network Security-Wireless Connections-Agencies must ensure: Wireless devices that extend their Local Area Networks (LANs):Continuously monitor for rogue wireless devices.	
NIST AC-18:Wireless Access	Y
5.4(3)(a)-Network Security-Wireless Connections-Agencies must ensure: Wireless devices that do not extend the agency's local area network or connect to the SGN:Securely segment wireless access point connections from the Internet.	

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
NIST SC-7:Boundary Protection	Y
5.4(3)(b)-Network Security-Wireless Connections-Agencies must ensure: Wireless devices that do not extend the agency's local area network or connect to the SGN:Use authentication and encryption appropriate for the environment.	
NIST IA-7:Cryptographic Module Authentication	Y
5.4(3)(c)-Network Security-Wireless Connections-Agencies must ensure: Wireless devices that do not extend the agency's local area network or connect to the SGN:Change wireless vendor defaults including but not limited to pre-shared keys and passwords.	
NIST IA-5:Authenticator Management	Y
5.4(3)(d)-Network Security-Wireless Connections-Agencies must ensure: Wireless devices that do not extend the agency's local area network or connect to the SGN:Disable Simple Network Management Protocol (SNMP) unless there is a clear business need. If enabled, change the vendor defaults.	
NIST CM-7:Least Functionality	Y
5.4(3)(e)-Network Security-Wireless Connections-Agencies must ensure: Wireless devices that do not extend the agency's local area network or connect to the SGN:Follow wireless access security practices developed within the agency.	
NIST AC-18:Wireless Access	Y
5.4(3)(f)-Network Security-Wireless Connections-Agencies must ensure: Wireless devices that do not extend the agency's local area network or connect to the SGN:Monitor for rogue wireless devices as defined in the agency security program.	
NIST AC-18:Wireless Access	Y
5.4(4)-Network Security-Wireless Connections-Agencies must ensure: Open or public access wireless environments do not share assets or traverse infrastructure components that connect to the agency network or SGN unless wireless traffic is securely segmented, encapsulated or tunneled over shared infrastructure.	
NIST SC-7:Boundary Protection	Y
5.4(5)-Network Security-Wireless Connections-If wireless networks are prohibited, the agency IT Security Program documentation must define how this is periodically verified and enforced.	
ISO 13.1.3, Communications Security:Segregation in networks	Y
NIST CM-6:Configuration Settings	Y
5.5-Network Security-Security Patch Management-Agencies must develop and document in the agency IT Security Program a patch management process commensurate with the risk and complexity of the IT environment.	
ISO 12.5.1, Operations Security:Installation of software on operational systems	Y
ISO 12.6.1, Operations Security:Management of technical vulnerabilities	N

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
NIST CM-1:Configuration Management Policy and Procedures	N
NIST CM-3:Configuration Change Control	N
5.5(1)-Network Security-Security Patch Management-At a minimum, this process must include: Identification of the responsibilities required for patch management.	
NIST CM-1:Configuration Management Policy and Procedures	Y
NIST CM-3:Configuration Change Control	Y
NIST SI-2:Flaw Remediation	Y
5.5(2)-Network Security-Security Patch Management-At a minimum, this process must include: Identification of the authorized software and information systems deployed in the production environment.	
NIST CM-8:Information System Component Inventory	Y
NIST PM-5:Information System Inventory	Y
5.5(3)-Network Security-Security Patch Management-At a minimum, this process must include: Timely notification of patch availability.	
NIST SI-2:Flaw Remediation	Y
5.5(4)-Network Security-Security Patch Management-At a minimum, this process must include: A method of categorizing the criticality of patches in route or on delivery.	
NIST RA-3:Risk Assessment	Y
5.5(5)-Network Security-Security Patch Management-At a minimum, this process must include: Testing procedures, when required, before deployment into production environments.	
NIST SI-2:Flaw Remediation	Y
5.5(6)-Network Security-Security Patch Management-At a minimum, this process must include: Time-specific criteria for deploying patches as soon as reasonably possible after notification, including criteria for zero-day patches.	
NIST SI-2:Flaw Remediation	Y
5.5(7)-Network Security-Security Patch Management-At a minimum, this process must include: Regular verification that available patches are managed according to the agency patch management process.	
NIST CA-7:Continuous Monitoring	Y
5.5(8)-Network Security-Security Patch Management-At a minimum, this process must include: A requirement for current patches on agency or non-agency remotely attached devices.	
NIST SI-2:Flaw Remediation	Y
5.5(9)-Network Security-Security Patch Management-At a minimum, this process must include: A requirement for current patches on agency or non-agency devices attached to agency networks, whether on agency local area networks or wireless networks.	
NIST SI-2:Flaw Remediation	Y

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
5.5(10)-Network Security-Security Patch Management-At a minimum, this process must include: Restrict access from devices that do not conform to the agency patch management policy.	
NIST CM-9:Configuration Management Plan	Y
5.6-Network Security-System Vulnerabilities	
ISO 12.6.1, Operations Security:Management of technical vulnerabilities	Y
NIST CA-8:Penetration Testing	Y
NIST RA-5:Vulnerability Scanning	Y
NIST RA-6:Technical Surveillance Countermeasures Survey	Y
NIST SC-30:Concealment and Misdirection	Y
5.6(1)-Network Security-System Vulnerabilities-Agencies must: Establish a process to identify newly discovered security vulnerabilities such as subscribing to alert services freely available on the Internet.	
ISO 6.1.4, Organization of IS:Contact with special interest groups	Y
NIST SI-5:Security Alerts, Advisories, and Directives	Y
5.6(2)-Network Security-System Vulnerabilities-Agencies must: Use processes that manage the installation and modification of system configuration settings.	
ISO 12.6.1, Operations Security:Management of technical vulnerabilities	Y
NIST CM-1:Configuration Management Policy and Procedures	Y
NIST CM-3:Configuration Change Control	Y
5.6(3)-Network Security-System Vulnerabilities-Agencies must: Harden systems before deployment using hardening standards that meet or exceed current best practices and manufacturer recommendations at the time of system deployment and throughout the lifecycle.	
ISO 12.6.1, Operations Security:Management of technical vulnerabilities	Y
NIST CM-2:Baseline Configuration	N
NIST CM-6:Configuration Settings	N
5.7(1)-Network Security-Protection from Malicious Software-Agencies must: Use anti-malware protection.	
ISO 12.2.1, Operations Security:Controls against malware	Y
ISO 12.6.2, Operations Security:Restrictions on software installation	Y
ISO 6.1.3, Organization of IS:Contact with authorities	Y
NIST SI-16:Memory Protection	Y
NIST SI-8:Spam Protection	Y
NIST SI-3:Malicious Code Protection	Y
NIST SI-7:Software, Firmware, and Information Integrity	Y

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
5.7(2)-Network Security-Protection from Malicious Software-Agencies must: Address malware prevention, detection, and removal.	
NIST SI-3:Malicious Code Protection	Y
NIST SI-4:Information System Monitoring	Y
NIST SI-7:Software, Firmware, and Information Integrity	Y
5.7(3)-Network Security-Protection from Malicious Software-Agencies must: Keep malware protection current when connecting devices to the agency network or the SGN.	
NIST SI-3:Malicious Code Protection	Y
5.7(4)-Network Security-Protection from Malicious Software-Agencies must: Ensure that file transfers, e-mail, and Web browser-based traffic are examined for known viruses.	
NIST SI-3:Malicious Code Protection	Y
5.7(5)-Network Security-Protection from Malicious Software-Agencies must: Implement detection, prevention, and recovery controls to protect against malicious code.	
NIST SI-3:Malicious Code Protection	Y
NIST SI-4:Information System Monitoring	Y
NIST SI-7:Software, Firmware, and Information Integrity	Y
5.7(6)-Network Security-Protection from Malicious Software-Agencies must: Integrate malicious software detection reporting with the Washington Computer Incident Response Center (WACIRC) incident reporting processes.	
NIST IR-6:Incident Reporting	Y
5.8-Network Security-Mobile Computing-Examples of mobile devices include laptops, smart phones, Personal Digital Assistants (PDAs), accessible equipment, and portable data storage devices such as tape drives, zip drives, removable hard drives, and USB data storage devices. Agencies must implement policies and procedures controlling the use of Category 3 and above data on mobile devices.	
ISO 6.2.1, Organization of IS:Mobile device policy	N
ISO 6.2.2, Organization of IS:Teleworking	N
NIST AC-19:Access Control for Mobile Devices	N
5.8(1)-Network Security-Mobile Computing-At a minimum, agencies must: Approve and document the use of category 3 data or above on mobile devices.	
NIST AC-19:Access Control for Mobile Devices	Y
5.8(2)-Network Security-Mobile Computing-At a minimum, agencies must:(2) Encrypt Category 3 data or above on mobile devices using industry standard algorithms or cryptographic modules validated by the National Institute of Standards and Technology (NIST).	
NIST IA-7:Cryptographic Module Authentication	Y

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
NIST SC-13:Cryptographic Protection	Y
5.8(3)-Network Security-Mobile Computing-At a minimum, agencies must:(3) Implement policies and procedures that address the use of portable data storage devices.	
NIST MP-2:Media Access	Y
NIST MP-4:Media Storage	Y
Standard 6 - Access Security	
6.1.1-Access Security-Access Management-Policies	
ISO 9.1.1, Access Control:Access control policy	Y
NIST AC-14:Permitted Actions without Identification or Authentication	N
6.1.1(1)-Access Security-Access Management-Policies-To ensure proper access controls that conform to the principle of least privilege agencies must: Implement policies and procedures that address access security controls for mainframe, client/server, wireless LANs, and stand-alone workstation-based systems that are consistent with the agency's classification of the data processed.	
ISO 9.1.1, Access Control:Access control policy	Y
NIST AC-1:Access Control Policy and Procedures	Y
6.1.1(2)-Access Security-Access Management-Policies-To ensure proper access controls that conform to the principle of least privilege agencies must: Restrict access to data, application, and system functions by users and support personnel in accordance with the agency defined access control policy.	
ISO 6.1.2, Organization of IS:Segregation of duties	Y
NIST AC-1:Access Control Policy and Procedures	Y
NIST AC-6:Least Privilege	Y
NIST CM-7:Least Functionality	Y
6.1.1(3)-Access Security-Access Management-Policies-To ensure proper access controls that conform to the principle of least privilege agencies must: Authentication and authorization controls must be appropriately robust for the risk of the application or systems to prevent unauthorized access to IT assets.	
ISO 9.1.1, Access Control:Access control policy	Y
NIST IA-1:Identification and Authentication Policy and Procedures	Y
NIST RA-3:Risk Assessment	Y
6.1.1(4)-Access Security-Access Management-Policies-To ensure proper access controls that conform to the principle of least privilege agencies must: Manage and group systems, data, and users into security domains and establish appropriate access requirements within and between each security domain.	
ISO 9.1.1, Access Control:Access control policy	Y
NIST AC-3:Access Enforcement	Y

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
NIST RA-2:Security Categorization	Y
NIST SC-5:Denial of Service Protection	Y
NIST SC-7:Boundary Protection	Y
6.1.1(5)-Access Security-Access Management-Policies-To ensure proper access controls that conform to the principle of least privilege agencies must: Implement appropriate technological controls to meet access requirements consistently.	
ISO 9.1.1, Access Control:Access control policy	Y
NIST AC-24:Access Control Decisions	Y
NIST AC-3:Access Enforcement	Y
6.1.1(6)-Access Security-Access Management-Policies-To ensure proper access controls that conform to the principle of least privilege agencies must: Restrict the use of programs or utilities capable of overriding system and application controls.	
ISO 9.1.1, Access Control:Access control policy	Y
NIST CM-7:Least Functionality	Y
6.1.1(7)-Access Security-Access Management-Policies-To ensure proper access controls that conform to the principle of least privilege agencies must: Implement policies and procedures for identity proofing individuals.	
ISO 9.1.1, Access Control:Access control policy	Y
NIST AC-2:Account Management	Y
NIST IA-4:Identifier Management	Y
6.1.2-Access Security-Access Management-Accounts	
NIST AC-9:Previous Logon (Access) Notification	N
NIST IA-6:Authenticator Feedback	N
6.1.2(1)-Access Security-Access Management-Accounts-To ensure appropriate management of user accounts on system components agencies must: Establish a formal procedure for issuance, management and maintenance of UserIDs and passwords.	
ISO 9.2.2, Access Control:User access provisioning	Y
NIST AC-2:Account Management	Y
NIST IA-4:Identifier Management	Y
6.1.2(2)-Access Security-Access Management-Accounts-To ensure appropriate management of user accounts on system components agencies must: Establish formal user registration and de-registration procedures for granting and revoking access to information systems and services.	
ISO 9.2.1, Access Control:User registration and de-registration	Y
NIST AC-2:Account Management	Y

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
NIST IA-4:Identifier Management	Y
6.1.2(3)-Access Security-Access Management-Accounts-To ensure appropriate management of user accounts on system components agencies must: Identify users with a unique identifier, for their individual use only, before allowing them to access components, systems, networks, or data.	
ISO 9.2.1, Access Control:User registration and de-registration	Y
NIST IA-2:Identification and Authentication (Organizational Users)	Y
NIST IA-4:Identifier Management	Y
6.1.2(4)-Access Security-Access Management-Accounts-To ensure appropriate management of user accounts on system components agencies must: Ensure that accounts are assigned access only to the services that they have been specifically authorized to use.	
ISO 9.2.2, Access Control:User access provisioning	Y
NIST AC-2:Account Management	Y
NIST AC-6:Least Privilege	Y
6.1.2(5)-Access Security-Access Management-Accounts-To ensure appropriate management of user accounts on system components agencies must: Ensure the access rights of users to information and information processing facilities are removed upon suspected compromise, termination of their employment or contract, or are adjusted upon change in status.	
ISO 9.2.6, Access Control:Removal or adjustment of access rights	Y
NIST AC-2:Account Management	Y
NIST IA-4:Identifier Management	Y
6.1.2(6)-Access Security-Access Management-Accounts-To ensure appropriate management of user accounts on system components agencies must: Control the addition, deletion, and modification of user IDs, credentials, and other identifier objects.	
ISO 9.2.1, Access Control:User registration and de-registration	Y
NIST IA-5:Authenticator Management	Y
6.1.2(7)-Access Security-Access Management-Accounts-To ensure appropriate management of user accounts on system components agencies must: Implement mechanisms to restrict and control the use of privileges.	
ISO 9.2.3, Access Control:Management of privileged access rights	Y
NIST AC-2:Account Management	Y
NIST AC-6:Least Privilege	Y
NIST IA-4:Identifier Management	Y
6.1.2(8)-Access Security-Access Management-Accounts-To ensure appropriate management of user accounts on system components agencies must: Verify user identity before performing password resets.	

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
ISO 9.2.2, Access Control:User access provisioning	Y
NIST AC-2:Account Management	Y
NIST IA-4:Identifier Management	Y
6.1.2(9)-Access Security-Access Management-Accounts-To ensure appropriate management of user accounts on system components agencies must: Set first-time passwords to a unique value per user that must be changed immediately after first use.	
ISO 9.4.3, Access Control:Password management system	Y
NIST IA-5:Authenticator Management	Y
6.1.2(10)-Access Security-Access Management-Accounts-To ensure appropriate management of user accounts on system components agencies must: Use time of day, and day of week restrictions as appropriate.	
ISO 9.4.2, Access Control:Secure log-on procedures	Y
NIST AC-6:Least Privilege	Y
6.1.2(11)-Access Security-Access Management-Accounts-To ensure appropriate management of user accounts on system components agencies must: Enable accounts used by vendors for remote maintenance only during the time needed.	
ISO 9.4.2, Access Control:Secure log-on procedures	Y
NIST AC-17:Remote Access	Y
NIST MA-4:Nonlocal Maintenance	Y
6.1.2(12)-Access Security-Access Management-Accounts-To ensure appropriate management of user accounts on system components agencies must: Prohibit the use of group, shared, or generic UserIDs/passwords.	
ISO 9.3.1, Access Control:Use of secret authentication information	Y
NIST AC-2:Account Management	Y
NIST IA-4:Identifier Management	Y
6.1.2(13)-Access Security-Access Management-Accounts-To ensure appropriate management of user accounts on system components agencies must: Establish a maximum of five incorrect login attempts and lock the account for a minimum of 15 minutes or until reset by an administrator.	
ISO 9.4.2, Access Control:Secure log-on procedures	Y
NIST AC-7:Unsuccessful Logon Attempts	Y
6.1.3-Access Security-Access Management-Sessions	
ISO 11.2.8, Physical & Environmental Security:Unattended user equipment	Y
ISO 9.4.2, Access Control:Secure log-on procedures	Y
NIST AC-10:Concurrent Session Control	N
NIST AU-14:Session Audit	Y

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
NIST SC-23:Session Authenticity	Y
6.1.3(1)-Access Security-Access Management-Sessions-To ensure appropriate management of sessions on system components agencies must: Establish procedures to shut down or reauthorize inactive sessions after a defined and reasonable period of inactivity.	
NIST AC-11:Session Lock	Y
NIST AC-12:Session Termination	Y
NIST SC-10:Network Disconnect	Y
6.1.3(2)-Access Security-Access Management-Sessions-To ensure appropriate management of sessions on system components agencies must: Restrict user access to shared systems, especially those extending across the agency's boundaries, in accordance with the access control policy and requirements of the business applications.	
NIST AC-1:Access Control Policy and Procedures	Y
NIST AC-6:Least Privilege	Y
6.1.3(3)-Access Security-Access Management-Sessions-To ensure appropriate management of sessions on system components agencies must: Ensure that access to operating systems is controlled by a secure log-on procedure.	
NIST IA-7:Cryptographic Module Authentication	Y
6.1.4-Access Security-Access Management-Auditing-To ensure system controls are effectively enforcing access policies agencies must:(1) Periodically review user access rights based on the risk to the data, application, or system using a formal process, and (2) Implement mechanisms to monitor the use of privileges.	
ISO 9.2.5, Access Control:Review of user access rights	Y
NIST AU-1:Audit and Accountability Policy and Procedures	Y
NIST AU-10:Non-repudiation	N
NIST AU-11:Audit Record Retention	N
NIST AU-12:Audit Generation	N
NIST AU-13:Monitoring for Information Disclosure	Y
NIST AU-15:Alternate Audit Capability	Y
NIST AU-16:Cross-Organizational Auditing	Y
NIST AU-2:Audit Events	N
NIST AU-3:Content of Audit Records	N
NIST AU-4:Audit Storage Capacity	N
NIST AU-5:Response to Audit Processing Failures	Y
NIST AU-6:Audit Review, Analysis, and Reporting	N
NIST AU-7:Audit Reduction and Report Generation	N
NIST AU-8:Time Stamps	N

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
NIST AU-9:Protection of Audit Information	N
6.2-Access Security-Password Requirements	
ISO 9.3.1, Access Control:Use of secret authentication information	Y
NIST AC-7:Unsuccessful Logon Attempts	Y
NIST IA-5:Authenticator Management	Y
6.3-Access Security-Authentication-Authentication is used to validate the identity of users performing functions on systems. Selecting the appropriate authentication method is based on risks to data.	
NIST IA-1:Identification and Authentication Policy and Procedures	N
NIST IA-2:Identification and Authentication (Organizational Users)	Y
NIST IA-3:Device Identification and Authentication	Y
NIST IA-7:Cryptographic Module Authentication	Y
NIST IA-8:Identification and Authentication (Non-Organizational Users)	Y
NIST IA-9:Service Identification and Authentication	Y
NIST SC-12:Cryptographic Key Establishment and Management	Y
NIST SC-13:Cryptographic Protection	Y
NIST SC-17:Public Key Infrastructure Certificates	Y
6.3.1-Access Security-External Authentication-Six methods of authentication are defined for users accessing agency owned systems from resources outside the SGN.	
NIST IA-5:Authenticator Management	Y
6.3.1.1-Access Security-External Authentication-Type 1	
ISO 9.3.1, Access Control:Use of secret authentication information	Y
NIST IA-5:Authenticator Management	Y
6.3.1.2-Access Security-External Authentication-Type 2	
ISO 9.3.1, Access Control:Use of secret authentication information	Y
NIST IA-5:Authenticator Management	Y
6.3.1.3-Access Security-External Authentication-Type 3	
ISO 9.3.1, Access Control:Use of secret authentication information	Y
NIST IA-5:Authenticator Management	Y
6.3.1.4-Access Security-External Authentication-Type 4	
ISO 9.3.1, Access Control:Use of secret authentication information	Y
NIST IA-5:Authenticator Management	Y
6.3.1.5-Access Security-External Authentication-Type 5	
ISO 9.3.1, Access Control:Use of secret authentication information	Y

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
NIST IA-5:Authenticator Management	Y
6.3.1.6-Access Security-External Authentication-Type 6	
ISO 9.3.1, Access Control:Use of secret authentication information	Y
NIST IA-5:Authenticator Management	Y
6.3.2-Access Security-Internal Authentication-Four methods of authentication are defined for users accessing agency owned systems from resources inside the agency network, SGN or already authenticated via common remote access methods outlined in Section 6.4.	
NIST IA-5:Authenticator Management	Y
6.3.2.1-Access Security-Internal Authentication-Type 7	
ISO 9.3.1, Access Control:Use of secret authentication information	Y
NIST IA-5:Authenticator Management	Y
6.3.2.2-Access Security-Internal Authentication-Type 8	
ISO 9.3.1, Access Control:Use of secret authentication information	Y
NIST IA-5:Authenticator Management	Y
6.3.2.3-Access Security-Internal Authentication-Type 9	
ISO 9.3.1, Access Control:Use of secret authentication information	Y
NIST IA-5:Authenticator Management	Y
6.3.2.4-Access Security-Internal Authentication-Type 10	
ISO 9.3.1, Access Control:Use of secret authentication information	Y
NIST IA-5:Authenticator Management	Y
6.4-Access Security-Remote Access	
NIST AC-2:Account Management	Y
NIST IA-4:Identifier Management	Y
6.4(1)-Access Security-Remote Access-Agencies must: Implement policies and procedures for remote access that mitigate the threat or risk posed by users or devices authorized to connect remotely to the agency network or the SGN.	
NIST AC-17:Remote Access	Y
6.4(1)(a)-Access Security-Remote Access-Agencies must: Implement policies and procedures for remote access that mitigate the threat or risk posed by users or devices authorized to connect remotely to the agency network or the SGN including but not limited to: Monitoring practices for remote access sessions.	
NIST AC-17:Remote Access	Y

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
6.4(1)(b)-Access Security-Remote Access-Agencies must: Implement policies and procedures for remote access that mitigate the threat or risk posed by users or devices authorized to connect remotely to the agency network or the SGN including but not limited to: Requirements for remote access devices.	
NIST IA-3:Device Identification and Authentication	Y
6.4(1)(c)-Access Security-Remote Access-Agencies must: Implement policies and procedures for remote access that mitigate the threat or risk posed by users or devices authorized to connect remotely to the agency network or the SGN including but not limited to: Remote access session controls that conform to the principle of least privilege.	
NIST AC-6:Least Privilege	Y
6.4(2)-Access Security-Remote Access-Agencies must: Ensure mitigation is not susceptible to end-user modification.	
NIST AC-17:Remote Access	Y
6.4(3)-Access Security-Remote Access-Agencies must: Prohibit the use of dial-up unless there is no other way to satisfy a business need. Dial-up access, if used, must be approved by management and documented in the Agency IT Security Program.	
NIST AC-17:Remote Access	Y
NIST CM-7:Least Functionality	Y
6.4(4)-Access Security-Remote Access-Agencies must: Use industry standard protocols for remote access solutions.	
NIST AC-17:Remote Access	Y
6.4(5)-Access Security-Remote Access-Agencies must: Use the state's common remote access services such as IPSec or SSL VPN when remotely accessing agency resources and services on the SGN.	
NIST AC-17:Remote Access	Y
6.4(6)-Access Security-Remote Access-Agencies must: Ensure remote access solutions prompt for re-authentication or perform automated session termination after 30 minutes of inactivity.	
NIST AC-12:Session Termination	Y
NIST IA-11:Re-authentication	Y
6.4(7)-Access Security-Remote Access-Agencies must: Ensure that agency operated remote access solutions, not connected to the agency network or the SGN, use equivalent technologies that require multi-factor authentication and include documentation of the configuration in the agency IT Security Program.	
NIST IA-10:Adaptive Identification and Authentication	Y
Standard 7 - Application Security	
7.1-Application Security-Planning & Analysis-Agencies must specify security controls when developing business requirements for new or enhanced information systems.	
ISO 14.1.1, System Acquisition, Development & Maintenance:IS requirements analysis and specification	Y
NIST PL-2:System Security Plan	N

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
NIST PL-8:IS Architecture	N
NIST PM-8:Critical Infrastructure Plan	Y
NIST SA-12:Supply Chain Protection	Y
NIST SA-14:Criticality Analysis	Y
7.1(1)-Application Security-Planning & Analysis-Controls may include but are not limited to: Ensure applications provide for data input validation to ensure the data is correct and appropriate and cannot be used to compromise security of the application, IT infrastructure, or data.	
NIST SI-10:Information Input Validation	Y
7.1(2)-Application Security-Planning & Analysis-Controls may include but are not limited to: Procedures are in place to manage the installation of software on operational systems including but not limited to servers and workstations.	
NIST CM-1:Configuration Management Policy and Procedures	Y
7.1(3)-Application Security-Planning & Analysis-Controls may include but are not limited to: Access to program source code is restricted to only those individuals whose job requires such access.	
NIST AC-5:Separation of Duties	Y
NIST AC-6:Least Privilege	Y
NIST SC-2:Application Partitioning	Y
7.1(4)-Application Security-Planning & Analysis-Controls may include but are not limited to: Include specific requirements in contracts for outsourced software development to protect the integrity and confidentiality of application source code.	
NIST SA-4:Acquisition Process	Y
7.1(5)-Application Security-Planning & Analysis-Controls may include but are not limited to: Implementation of changes will be managed by the use of formal change management procedures.	
NIST CM-1:Configuration Management Policy and Procedures	Y
NIST CM-3:Configuration Change Control	Y
7.1(6)-Application Security-Planning & Analysis-Controls may include but are not limited to: Appropriate access and security controls; audit trails; and logs for data entry and data processing.	
NIST AU-2:Audit Events	Y
7.1(7)-Application Security-Planning & Analysis-Controls may include but are not limited to: Requirements for appropriate data protection.	
See practices addressed in OCIO Standard 4	
7.2-Application Security-Application Development-Agencies must develop software applications based on industry best practices and include information security throughout the software development life cycle.	
ISO 14.2.1, System Acquisition, Development & Maintenance:Secure development policy	Y

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
NIST SA-10:Developer Configuration Management	Y
NIST SA-15:Development Process, Standards, and Tools	Y
NIST SA-17:Developer Security Architecture and Design	N
NIST SA-3:System Development Life Cycle	Y
NIST SA-5:Information System Documentation	N
NIST SA-8:Security Engineering Principles	N
NIST SC-38:Operations Security	N
NIST SI-11:Error Handling	Y
7.2(1)-Application Security-Application Development-Requirements include the following: Separate development, test, and production environments.	
ISO 12.1.4, Operations Security:Separation of development, testing, and operational environments	Y
NIST SC-7:Boundary Protection	Y
7.2(2)-Application Security-Application Development-Requirements include the following: Implement separation of duties or other security controls between development, test and production environments. The controls must reduce the risk of unauthorized activity or changes to production systems or data including but not limited to the data accessible by a single individual.	
ISO 14.2.6, System Acquisition, Development & Maintenance:Secure development environment	Y
NIST AC-5:Separation of Duties	Y
NIST AC-6:Least Privilege	Y
NIST SA-21:Developer Screening	Y
7.2(3)-Application Security-Application Development-Requirements include the following: Production data used for development testing must not compromise privacy or confidentiality. Prohibit the use of Category 3 data or higher in development environments unless specifically authorized by the IT security program. Production data in any environment must meet or exceed the level of protection required by its data classification.	
ISO 14.3.1, System Acquisition, Development & Maintenance:Protection of test data	N
NIST SA-15:Development Process, Standards, and Tools	Y
7.2(4)-Application Security-Application Development-Requirements include the following: Removal of test data and accounts before production systems become live.	
ISO 14.3.1, System Acquisition, Development & Maintenance:Protection of test data	N
NIST SA-15:Development Process, Standards, and Tools	Y
7.2(5)-Application Security-Application Development-Requirements include the following: Removal of custom application accounts, usernames, and passwords from production environments before applications become active or are released to customers.	

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
ISO 14.3.1, System Acquisition, Development & Maintenance:Protection of test data	N
NIST SA-15:Development Process, Standards, and Tools	Y
7.2(6)-Application Security-Application Development-Requirements include the following: Review of custom code prior to release to production or customers to identify potential coding vulnerabilities as described in Section 7.4 Vulnerability Prevention.	
ISO 14.2.3, System Acquisition, Development & Maintenance:Technical review of applications after operating platform changes	Y
NIST SA-11:Developer Security Testing and Evaluation	N
7.2(7)-Application Security-Application Development-Requirements include the following: Appropriate placement of data and applications in the IT infrastructure based on the risk and complexity of the system.	
ISO 14.2.1, System Acquisition, Development & Maintenance:Secure development policy	Y
NIST SA-17:Developer Security Architecture and Design	Y
7.2(8)-Application Security-Application Development-Requirements include the following: Use of appropriate authentication levels.	
ISO 14.2.1, System Acquisition, Development & Maintenance:Secure development policy	Y
NIST IA-5:Authenticator Management	Y
7.3(1)-Application Security-Application Maintenance-Agencies must: Review and test system changes to ensure there are no adverse impacts on agency operations or security.	
ISO 14.2.4, System Acquisition, Development & Maintenance:Restrictions on changes to software packages	Y
ISO 14.2.8, System Acquisition, Development & Maintenance:System acceptance testing	Y
NIST CM-3:Configuration Change Control	Y
NIST SI-2:Flaw Remediation	Y
7.3(2)-Application Security-Application Maintenance-Agencies must: Obtain timely information about technical vulnerabilities of information systems being used, evaluate the agency's exposure to such vulnerabilities, and take appropriate measures to address the associated risk.	
ISO 14.2.2, System Acquisition, Development & Maintenance:System change control procedures	Y
NIST RA-5:Vulnerability Scanning	Y
NIST SI-2:Flaw Remediation	Y
NIST SI-5:Security Alerts, Advisories, and Directives	Y
7.4(1)-Application Security-Vulnerability Protection-Agencies must: Develop software and applications based on secure coding guidelines	
ISO 14.2.5, System Acquisition, Development & Maintenance:Secure system engineering principles	Y
NIST RA-5:Vulnerability Scanning	Y

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
NIST SA-15:Development Process, Standards, and Tools	Y
NIST SA-3:System Development Life Cycle	Y
7.4(2)-Application Security-Vulnerability Protection-Agencies must: Review code to detect and mitigate code vulnerabilities that may have security implications when significant changes have been made to the application.	
ISO 14.2.9, System Acquisition, Development & Maintenance:System acceptance testing	Y
NIST RA-5:Vulnerability Scanning	Y
NIST SA-11:Developer Security Testing and Evaluation	Y
7.5-Application Security-Application Service Providers-Applications hosted by an Applications Service Provider or other third party outside of the shared, trusted environment must comply with:(1)The OCIO IT Security Policy and Standard as described in Section 1.5 and (2)Agency security standards and procedures.	
ISO 15.2.1, Supplier Relationships:Monitoring and review of supplier services	Y
NIST AC-20:Use of External Information Systems	Y
NIST CA-3:System Interconnections	Y
NIST SA-1:System and Services Acquisition Policy and Procedures	Y
NIST SA-4:Acquisition Process	N
NIST SA-9:External Information System Services	N
Standard 8 - Operations Management	
8.1-Operations Management-Change Management	
ISO 12.1.2, Operations Security:Change management	N
NIST CA-5:Plan of Action and Milestones	N
NIST CM-1:Configuration Management Policy and Procedures	N
NIST CM-2:Baseline Configuration	N
NIST CM-9:Configuration Management Plan	N
NIST MA-1:System Maintenance Policy and Procedures	N
NIST MA-3:Maintenance Tools	N
NIST MA-5:Maintenance Personnel	N
NIST MA-6:Timely Maintenance	N
8.1(1)-Operations Management-Change Management-Agencies must implement an effective change management process that: Ensures that duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the agency's IT assets.	
NIST AC-5:Separation of Duties	Y

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
8.1(2)-Operations Management-Change Management-Agencies must implement an effective change management process that: Ensures computing environments are segmented to reduce the risks of unauthorized access or changes to the operational system.	
NIST CM-5:Access Restrictions for Change	Y
NIST SC-7:Boundary Protection	Y
8.1(3)-Operations Management-Change Management-Agencies must implement an effective change management process that: Includes acceptance criteria for new information systems, upgrades, and new versions and ensure that suitable tests of the system(s) are carried out during development and prior to acceptance.	
NIST CM-3:Configuration Change Control	N
NIST CM-4:Security Impact Analysis	Y
NIST SI-2:Flaw Remediation	N
8.2-Operations Management-Asset Management-Agencies must:(1)Clearly identify and maintain an inventory of major components in the IT environment, (2) Ensure that information and assets associated with information processing be assigned to or 'owned' by designated parts of the agency. The term 'owner' identifies an individual or entity that has management responsibility for authorizing the collection, use, modification, protection and disposal of the information and asset(s).	
ISO 11.2.5, Physical & Environmental Security:Removal of assets	Y
ISO 8.1.1, Asset Management:Inventory of assets	N
ISO 8.1.2, Asset Management:Ownership of assets	Y
ISO 8.1.4, Asset Management:Return of Assets	Y
NIST CM-8:Information System Component Inventory	Y
NIST PE-16:Delivery and Removal	Y
NIST PM-5:Information System Inventory	Y
8.3-Operations Management-Media Handling & Disposal	
NIST MP-1:Media Protection Policy and Procedures	Y
NIST MP-3:Media Marking	Y
NIST MP-4:Media Storage	Y
NIST MP-8:Media Downgrading	Y
NIST SI-12:Information Handling and Retention	Y
8.3(1)-Operations Management-Media Handling & Disposal-Agencies must: Ensure that media be disposed of securely and safely when no longer required, using formal documented procedures.	
ISO 11.2.7, Physical & Environmental Security:Secure disposal or re-use of equipment	N
ISO 8.3.2, Asset Management:Disposal of media	N

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
NIST MP-7:Media Use	Y
8.3(2)-Operations Management-Media Handling & Disposal-Agencies must: Sanitize equipment containing storage media prior to disposal (reference best practices such as NIST SP 800-88 Guidelines for Media Sanitation or equipment disposal procedures documented in the IT security program) and:(a)Destroy, securely overwrite, or make unavailable agency identifiable data, and (b)Sanitize equipment containing storage media prior to disposal (reference best practices such as NIST SP 800-88 Guidelines for Media Sanitation or equipment disposal procedures documented in the IT security program) and: Destroy, securely overwrite, or make unavailable software consistent with the software licensing agreement.	
ISO 8.3.1, Asset Management:Management of removable media	Y
NIST MP-6:Media Sanitization	N
8.3(3)-Operations Management-Media Handling & Disposal-Agencies must: Ensure the safe and secure disposal of sensitive media.	
ISO 8.3.2, Asset Management:Disposal of media	Y
NIST MP-6:Media Sanitization	Y
8.3(4)-Operations Management-Media Handling & Disposal-Agencies must: Ensure that system documentation is protected against unauthorized access.	
ISO 9.4.5, Access Control:Access control to program source code	Y
NIST MP-2:Media Access	Y
8.3(5)-Operations Management-Media Handling & Disposal-Agencies must: Ensure Media containing information is protected against unauthorized access, misuse, or corruption during transportation beyond an agency's physical boundaries.	
ISO 8.3.3 (ISO/IEC 27005:2011), IS Risk Assessment:Assessment of incident likelihood	Y
NIST MP-5:Media Transport	Y
8.4-Operations Management-Data & Program Backup	
ISO 12.3.1, Operations Security:Information backup	N
NIST CP-1:Contingency Planning Policy and Procedures	Y
NIST CP-10:Information System Recovery and Reconstitution	Y
NIST CP-2:Contingency Plan	Y
8.4(1)-Operations Management-Data & Program Backup-Agencies must: Satisfy data archival and rotational requirements for backup media based on the results of an IT Security Risk Assessment.	
NIST CA-1:Security Assessment and Authorization Policies and Procedures	Y
NIST CA-2:Security Assessments	Y
NIST RA-3:Risk Assessment	Y

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
NIST SA-14:Criticality Analysis	Y
8.4(2)-Operations Management-Data & Program Backup-Agencies must: Implement procedures for periodic tests to restore agency data from backup media.	
NIST CP-4:Contingency Plan Testing	Y
8.4(4)-Operations Management-Data & Program Backup-Agencies must: Establish methods to secure their backup media.	
NIST CP-9:Information System Backup	Y
8.4(5)-Operations Management-Data & Program Backup-Agencies must: Store media back-ups in a secure location such as a designated temporary staging area, an off-site facility, or a commercial storage facility.	
NIST CP-6:Alternate Storage Site	Y
Standard 9 - Electronic Commerce	
9(1)-Electronic Commerce-Agencies must: Prepare and incorporate plans for Internet-based transactional applications, including but not limited to e-commerce, into the agency's portfolio.	
ISO 13.2.1, Communications Security:Information transfer policies and procedures	Y
NIST SC-1:System and Communications Protection Policy and Procedures	Y
9(2)-Electronic Commerce-Agencies must: Protect information involved in electronic commerce passing over public networks from fraudulent activity, contract dispute, and unauthorized disclosure and modifications required by these IT security standards.	
ISO 14.1.2, System Acquisition, Development & Maintenance:Securing application services on public networks	Y
NIST SC-8:Transmission Confidentiality and Integrity	Y
9(3)-Electronic Commerce-Agencies must: Protect information involved in on-line transactions in order to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication, or replay.	
ISO 14.1.3, System Acquisition, Development & Maintenance:Protecting application services transactions	Y
NIST SC-13:Cryptographic Protection	Y
9(4)-Electronic Commerce-Agencies must: Protect IT infrastructure supporting electronic commerce services from unauthorized access and use according to these IT security standards.	
ISO 18.1.1, Compliance:Identification of applicable legislation and contractual requirements	Y
NIST SC-7:Boundary Protection	Y
Standard 10 - Security Monitoring & Logging	
10.1-Security Monitoring & Logging-Logging Policies-Agencies must develop and document a logging strategy that addresses each system based on the risk and complexity of the system.	
ISO 12.4.1, Operations Security:Event Logging	Y

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
ISO 16.1.7, IS Incident Management:Collection of evidence	Y
NIST AU-1:Audit and Accountability Policy and Procedures	Y
10.1(1)-Security Monitoring & Logging-Logging Policies-Agencies must develop and document a logging strategy that addresses each system based on the risk and complexity of the system. At a minimum the logging strategy must address the following: The log records including events, exceptions and user activities necessary to reconstruct unauthorized activities defined by the strategy.	
NIST AU-2:Audit Events	Y
NIST AU-3:Content of Audit Records	Y
10.1(2)-Security Monitoring & Logging-Logging Policies-Agencies must develop and document a logging strategy that addresses each system based on the risk and complexity of the system. At a minimum the logging strategy must address the following: Procedures for periodic review and analysis of recorded logs as set forth in the agency IT Security Program.	
NIST AU-6:Audit Review, Analysis, and Reporting	Y
10.1(3)-Security Monitoring & Logging-Logging Policies-Agencies must develop and document a logging strategy that addresses each system based on the risk and complexity of the system. At a minimum the logging strategy must address the following: Retention periods for logs.	
NIST AU-11:Audit Record Retention	Y
10.2(1)-Security Monitoring & Logging-Logging Systems-At a minimum, logging systems must satisfy the logging strategy identified by the agency and: Protect the logging facilities and log information against tampering and unauthorized access.	
ISO 12.4.2, Operations Security:Protection of log information	Y
NIST AU-9:Protection of Audit Information	Y
10.2(2)-Security Monitoring & Logging-Logging Systems-At a minimum, logging systems must satisfy the logging strategy identified by the agency and: Synchronize with an agency approved accurate time source.	
ISO 12.4.4, Operations Security:Clock synchronization	Y
NIST AU-8:Time Stamps	Y
10.2(3)-Security Monitoring & Logging-Logging Systems-At a minimum, logging systems must satisfy the logging strategy identified by the agency and: Provide automated recording to allow for reconstruction of the following events:(a)Actions taken by individuals with root or administrative privileges,(b)Invalid logical access attempts, and (c)Creation and deletion of system objects.	
ISO 12.4.3, Operations Security:Administrator and operator logs	Y
NIST AU-10:Non-repudiation	Y

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
10.3-Security Monitoring & Logging-Intrusion Detection & Prevention-CTS will monitor state networks with Intrusion Detection and Prevention systems at critical junctures. Agencies that deploy Intrusion Detection and Prevention systems must ensure the systems are configured to log information continuously and the logs are reviewed periodically as set forth in the agency IT Security Program.	
ISO 12.4.1, Operations Security:Event Logging	Y
NIST AU-16:Cross-Organizational Auditing	Y
Standard 11 - Incident Response	
11-Incident Response	
ISO 16.1.5, IS Incident Management:Response to IS incidents	Y
ISO 18.1.3, Compliance:Protection of records	Y
ISO 6.1.3, Organization of IS:Contact with authorities	Y
11(1)-Incident Response-Agencies must: Ensure timely and effective handling of IT security incidents.	
ISO 16.1.2, IS Incident Management:Reporting IS events	Y
NIST IR-1 :Incident Policy and Procedures	Y
11(2)-Incident Response-Agencies must: Establish, document, and distribute an incident response plan to be used in the event of system compromise.	
ISO 16.1.1, IS Incident Management:Responsibilities and procedures	Y
NIST IR-4:Incident Handling	Y
NIST IR-5:Incident Monitoring	Y
NIST IR-8:Incident Response Plan	Y
NIST SI-6:Security Function Verification	Y
11(2)(a)-Incident Response-Agencies must: Establish, document, and distribute an incident response plan to be used in the event of system compromise. At a minimum, the plan must address specific incident response procedures, recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies in addition to the following: Escalation procedures.	
ISO 16.1.1, IS Incident Management:Responsibilities and procedures	Y
NIST IR-6:Incident Reporting	Y
11(2)(b)-Incident Response-Agencies must: Establish, document, and distribute an incident response plan to be used in the event of system compromise. At a minimum, the plan must address specific incident response procedures, recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies in addition to the following: Designate specific personnel to respond to alerts.	
ISO 16.1.1, IS Incident Management:Responsibilities and procedures	Y
NIST IR-10:Integrated IS Analysis Team	Y

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
11(2)(c)-Incident Response-Agencies must: Establish, document, and distribute an incident response plan to be used in the event of system compromise. At a minimum, the plan must address specific incident response procedures, recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies in addition to the following: Be prepared to implement the incident response plan and to respond immediately to a system breach.	
ISO 16.1.1, IS Incident Management:Responsibilities and procedures	Y
NIST IR-4:Incident Handling	Y
11(2)(d)-Incident Response-Agencies must: Establish, document, and distribute an incident response plan to be used in the event of system compromise. At a minimum, the plan must address specific incident response procedures, recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies in addition to the following: Provide appropriate training to staff with security breach response responsibilities.	
ISO 16.1.1, IS Incident Management:Responsibilities and procedures	Y
ISO 16.1.4, IS Incident Management:Assessment of and decision on IS events	Y
NIST IR-2:Incident Response Training	Y
11(2)(e)-Incident Response-Agencies must: Establish, document, and distribute an incident response plan to be used in the event of system compromise. At a minimum, the plan must address specific incident response procedures, recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies in addition to the following: Have a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	
ISO 16.1.6, IS Incident Management:Learning from IS incidents	Y
NIST IR-4:Incident Handling	Y
11(2)(f)-Incident Response-Agencies must: Establish, document, and distribute an incident response plan to be used in the event of system compromise. At a minimum, the plan must address specific incident response procedures, recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies in addition to the following: Incorporate the incident response plan in the agency IT Security Program.	
ISO 16.1.6, IS Incident Management:Learning from IS incidents	Y
NIST IR-8:Incident Response Plan	Y
11(3)-Incident Response-Agencies must: Test the incident response plan at least annually.	
NIST IR-3:Incident Response Testing	Y

OCIO Standard No. 141.10 - Securing Information Technology Assets	Standard incorporates leading practice(s) (Y/N)
11(4)-Incident Response-Agencies must: Leverage the statewide incident response capabilities such as the WACIRC and the CTS Computer Security Incident Response Team to satisfy these response standards. Agencies are also encouraged to participate in appropriate security alert response organizations at the state and regional levels.	
ISO 16.1.3, IS Incident Management:Reporting IS weaknesses	Y
NIST IR-4:Incident Handling	Y
NIST IR-7:Incident Response Assistance	Y
11(5)-Incident Response-Agencies must: Develop and maintain a managed process for system availability throughout the agency that addresses the information security requirements needed for the agency's business operations.	
ISO 17.2.1, IS Business Continuity:Availability of information processing facilities	Y
NIST IR-4:Incident Handling	Y
11.1-Incident Response-Agencies must: Comply with the WACIRC incident reporting process(es). In the event of an incident involving the release of Category 3 data and above, agencies must comply, as appropriate, with the state breach notification statute, RCW 42.56.590 Personal Information.	
ISO 16.1.5, IS Incident Management:Response to IS incidents	Y
ISO 18.1.3, Compliance:Protection of records	Y
NIST IR-9:Information Spillage Response	Y