Before the
First Responder Network Authority

)
Nationwide Public Safety Broadband)
Network Special Notice) No. D15PS00295
)

COMMENTS OF THE STATE OF WASHINGTON

The State of Washington ("Washington" or "State"), in cooperation with and input from the Washington OneNet ("WON") Technical Committee, submits these comments in response to the First Responder Network Authority ("FirstNet") Nationwide Public Safety Broadband Network ("NPSBN") Special Notice on cyber security.[1] These comments are prepared by Washington's Office of the Chief Information Officer ("OCIO"), which supports and staffs the Washington State Interoperability Executive Committee ("SIEC").[2]

I. INTRODUCTION

Perhaps second only to coverage, cyber security is among the most critical aspects of the NPSBN for state and local public safety practitioners. FirstNet's Cyber Notice and Draft Appendix provide a general idea of the breadth of the cyber security solution FirstNet seeks, but because FirstNet is following an "objectives-based" procurement strategy, they offer the NPSBN's future users little basis for increased confidence that the NPSBN will meet their own cyber security requirements—requirements that thus far have not been a focus of the state consultation and data collection process.

[1] First Responder Network Authority Nationwide Public Safety Broadband Network Special Notice - D15PS00295 ("Cyber Notice") (Oct. 5, 2015). FirstNet released a draft of Appendix C-10 NPSBN Cyber Security ("Draft Appendix") with the Cyber Notice, available at https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=7c77a7ef3f5b3521fd817f1e58f3c875&_cview=1.

[2] Wash. Rev. Code § 43.41A.080. Washington Governor Jay Inslee designated the SIEC and its Chair, Bill Schrier, as the FirstNet State Point of Contact ("SPoC"). Mr. Schrier recently also became the Chief Information Officer for the Seattle Police Department.

In these comments, Washington urges FirstNet to convene a workgroup of state and local participants, as well as experts from national public safety communications organizations, to help formulate an NPSBN cyber security policy that will best accommodate existing state and local requirements, such as those described in the Washington security standard provided as Appendix A to these comments. Based upon this policy, FirstNet should revise the cyber security language in its RFP to specify clear requirements for NPSBN proposals. If it cannot include specific requirements, FirstNet should at least help bidders by detailing and prioritizing its "objectives" for the NPSBN cyber security solution. It also should identify and detail the many obligations that FirstNet (and its winning bidder) must meet because of FirstNet's status as a federal agency.

FirstNet must appreciate that a solution that does not enable state and local agencies to meet their own cyber security solutions will make it very difficult for those agencies to adopt the NPSBN. To minimize that risk, FirstNet should solicit state and local input to the development of an NPSBN security policy and then should verify that the policy it adopts meets state and local requirements.

II. PUBLIC SAFETY CYBER SECURITY REQUIREMENTS

A. FirstNet Should Solicit and Confirm Public Safety Entities' Cyber Security Requirements.

Public safety entities ("PSEs") are accustomed to implementing their own cyber security protections; they are understandably reticent to delegate protection of their networks, applications, and data to entities outside their control. While FirstNet must protect the NPSBN, it is more accurate from a public safety user perspective to view NPSBN security as "layered on top of" the "jurisdictional security implementation," rather than the other way around.[3] For many PSEs, unless FirstNet pursues their individual processes for becoming a "trusted network," they will take the same precautions in using the NPSBN that they take in sending traffic over a commercial data service.

[3] Draft Appendix at 4-5.

The draft of Appendix C-10 released on October 5 is the closest FirstNet has come to describing a security policy for the NPSBN, but the Draft Appendix is intended as a procurement document, not a policy pronouncement. It states only objectives for the future network; it does not reveal the cyber security features FirstNet will require the winning bidder to implement in the NPSBN.

In keeping with their tendency toward self-reliance, many PSEs have developed their own firm cyber security requirements. As is described in more detail below, if the NPSBN prevents PSEs from meeting their own requirements—whether because the NPSBN lacks a required feature or because it obstructs PSEs from implementing actions required by their own rules—it will be difficult for those PSEs to adopt the network. As a result, in order to minimize obstacles to adoption, FirstNet should convene a work group of state and local representatives and national organizations expert in public safety communications and cyber security to draft the NPSBN security policy to minimize conflict with PSE security requirements.

B. FirstNet Should Place Satisfying User Needs Above Procurement Flexibility.

FirstNet has selected an "objectives-based" procurement strategy rather than the more traditional approach in which the purchaser specifies requirements for the solution the winning bidder must provide. The State of Washington appreciates the increased flexibility the "objectives-based" strategy provides; in a first-of-its-kind procurement such as this one, FirstNet is wants to bring vendors to the negotiating table rather than state firm requirements that could lead to the disqualification of otherwise competitive and innovative bids. From a state perspective, however, this approach is problematic. Since FirstNet first identified a timeline for the NPSBN procurement, states have been looking to the RFP as the first opportunity to confirm that the NPSBN will indeed meet public safety requirements. By adopting an objectives-based approach, however, FirstNet has postponed that confirmation until publication of the FirstNet-negotiated, final contract.

With regard to cyber security, two facts particularly contribute to state concerns. First, there has been no concerted effort by FirstNet to solicit state cyber security requirements; second, FirstNet has not disclosed its own requirements for cyber security in the NPSBN. FirstNet's procurement approach relegates public safety to the uncomfortable position of having to wait and see, hoping that FirstNet understands its cyber security needs and will be able to negotiate for a solution that meets them. Procurement flexibility is important, but it should not come at the expense of ensuring that the NPSBN meets the needs of its prospective users.

As the State explained in its most recent set of comments to FirstNet, one good way to discern public safety requirements is to understand public safety use cases.[4] The State urged FirstNet to compete the use cases it intended to include in the RFP and circulate them to states to ensure that they accurately cover the variety of state use cases.[5] The State repeats that request here: use cases would be no less useful in ensuring cyber security solution that meets states' requirements.

C. FirstNet Should Specify Firm Requirements for Cyber Security.

The Draft Appendix provides "minimum cyber security concepts … these are not requirements. Rather, they should be considered concepts that are important to the design of the NPSBN Cyber Security Solution."[6] Cyber security is too critical to leave vague; cyber security features and capabilities must be specified and required, not relegated to vendors to selection among a laundry list of broadly stated options. As noted above, many PSEs already have documented cyber security requirements; for

[4] Comments of the State of Washington, FirstNet Nationwide Public Safety Broadband Network Special Notice, No. D15PS00295 (July 27, 2015) at 5-7.

[5] *Id.* During the "State Plan / Data Collection Breakout Session" on the first day of FirstNet's SPoC Meeting in Colorado at the beginning of this month, FirstNet's Director of State Plans explained that in 2016, FirstNet intends to consult with states specifically for the purpose (among others) of ensuring its correct understanding of the data states have provided. In response to a question, the Director expressed willingness to discuss similar verification/validation of use cases with the states; Washington appreciates the offer and looks forward to the discussion.

[6] Draft Appendix at 4.

those PSEs, such rules are not subject to selective compliance. Failure to identify these requirements is a disservice not only to PSEs, but also to prospective bidders who are left with little indication of which features FirstNet considers "must haves."

1. At a Minimum, FirstNet Should Help Bidders by Detailing and Prioritizing the "Objectives."

In the absence of both requirements and prioritization of objectives, vendors lack guidance on how to ensure their bids are adequate—not only to be deemed competitive by FirstNet, but to meet the needs of public safety, the future customer. Though the Draft Appendix states that "some of the language in these concepts emphasizes their importance,"[7] such language does little to provide the necessary guidance. Descriptions of concepts and objectives are prefaced with words like "essential" "important," and "at a minimum," but these indicators cannot provide the necessary clarity for the bidders upon which FirstNet and public safety are dependent for success. What little guidance they do offer is further clouded by the use of the word "should" (as opposed to "must" or "shall") throughout the document.[8]

The State is concerned that the Draft Appendix will do more to discourage competing proposals than attract them. For a bidder to make the substantial investment to design and describe the creative, innovative, and likely one-of-a-kind solution FirstNet desires, it will require greater clarity of FirstNet's desires. Prioritizing the standards, features, and practices described in the Draft Appendix would at least enable bidders to know which of two conflicting objectives to include in their proposal. For

[7] *Id.*

[8] Notably, the Draft Appendix does include a few "must" statements. If such unambiguous language does not conflict with FirstNet's procurement strategy, FirstNet should provide similar clarity throughout the RFP. *See* Draft Appendix at 17 ("All incidents must be immediately reported, whether suspected or confirmed, involving potential risks to the confidentiality, integrity, or availability of FirstNet information or to the function of NPSBN systems operated on behalf of FirstNet."), 21 ("Applications must be compliant during development and tested in actual operation before being authorized for use on the NPSBN."), and 22 ("Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people.").

example, is it more important that bidders include push-to-talk and group calling capabilities in their solutions, or that they provide end-to-end encryption? And how should they weigh the value of robust battery life against the substantial power consumption of the encryption objective?

The State is also concerned that the absence of requirements in the Draft Appendix will extend the period required for contract negotiations, delay contract execution, and invite challenges to the eventual award. Negotiated procurement does offer the buyer greater flexibility, but because of the absence of requirements, every aspect of the proposal is open to negotiation, and bidders' uncertainty as to FirstNet's priorities will likely result in a greater number of bids "missing the mark" and therefore requiring more substantial amendment in negotiation. Even with strict adherence to federal rules for negotiated procurement, the opportunity for subjectivity and variance in evaluation of proposals may further increase the likelihood of a challenge by an unsuccessful bidder.

In addition to the above concerns regarding the "objectives" nature of the procurement, the State is also concerned that the absence of specificity in describing the desired objectives leaves too much to the bidder's own understanding of what would be best for the NPSBN's future users. For example, the Draft Appendix lists "Strong Authentication / Identity Management" among FirstNet's Cyber Security Architecture concepts. The Draft Appendix does not define "strong authentication," leaving it to the bidder to select an authentication approach and hope that it is "strong" enough for FirstNet acceptance. Instead of using such vague language, FirstNet should decide how strong it wants the authentication capabilities to be based upon known use cases, and then describe them with specificity, thus vastly improving the odds that bidders will include them in their proposals. FirstNet knows, for example, that many state and local NPSBN users will need access not only to mundane, low-risk information, but also to highly sensitive data, some of which will be owned by the federal government. Thus, FirstNet should specify that its "strong authentication" concept includes enabling not only lower-level authentication, but also authentication at the highest level of assurance (*i.e.* Level of Assurance 4)[9] at which the federal government will trust credentials issued by non-federal entities. The sole clue that the NPSBN must enable use of such credentials is found under "Cyber Security Guidance" in the suggestion that NIST Recommendations on Cybersecurity (Special Publications 800 Series), among a list of 13 other collections of standards, "should be considered and used."[10] This oblique reference appears almost designed to mask the true underlying requirement.

The unnecessary and perhaps counter-productive absence of specificity in the Draft Appendix is similarly present in the vague suggestion that applications "properly log and audit the actions by the user and appropriate information about the user who takes those actions."[11] "Properly" implies a known correct practice; FirstNet should specify that practice, rather than leaving it to the bidder to guess at the standard by which it will be judged. Likewise, FirstNet seems to have some specific definitions in mind when it refers to "actions by the user" and "appropriate information about the user;" it should reveal those definitions instead of hiding the ball.

In a further example of over-broad language, the Draft Appendix calls for "End-to-End Encryption of User Communications and Data," stating that "[t]he NPSBN Cyber Security Solution should encrypt user-plane and signaling communications everywhere possible."[12] A bidder that truly takes this language to heart may propose a solution that meets the stated goal at the expense of needlessly burdening minimally sensitive communications with excessive overhead. FirstNet should instead specify where encryption must be applied, making informed judgements on behalf of public safety, rather than

[9] Joshua Bolten, Director, Office of Management and Budget, Memorandum to the Heads of All Departments and Agencies, "E-Authentication Guidance for Federal Agencies," M-04-04 (Dec. 16, 2015) ("M-04-04") (*available at* https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf).

[10] Draft Appendix at 13-14.

[11] Draft Appendix at 10.

[12] Draft Appendix at 4.

forcing the bidder either to ignore the objective's broad language or fashion a proposal that makes little sense for public safety.

2. Washington Has Specific Cyber Security Requirements.

The explicit absence of requirements in the Draft Appendix should not be taken to suggest that public safety user agencies do not have cyber security requirements for using any network, including the NPSBN. If those agencies cannot meet such requirements when they use the NPSBN, it will be difficult for them to permit their personnel to become NPSBN subscribers.

The Washington Office of the Chief Information Officer issued Standard 141.10 specifying cyber security requirements for State agencies.[13] It is appended to these comments. The State urges FirstNet to ensure that nothing in the winning NPSBN proposal obstruct State users from being able to comply with this standard while subscribing to and using the NPSBN. Because a single national solution is unlikely to accommodate the diverse cyber security policies of every state and local agency, FirstNet should, as recommended above, convene a workgroup to develop the NPSBN cyber security policy in a way that will accommodate user agency policies to the extent possible. If FirstNet does not accept this recommendation, it should at least adopt as a baseline—and state as a requirement for bidders—the cyber security policy required by the Department of Justice for access to the Criminal Justice Information Services ("CJIS"). CJIS is widely used by law enforcement at the state and local levels; adherence to the CJIS Security Policy would be a good starting point to help ensure the NPSBN does not conflict with state and local security policies.

[13] Standard No. 141.10, Securing Information Technology Assets, Office of the Chief Information Officer, State of Washington (effective date Aug. 19, 2013) ("Standard 141.10") (attached to these comments as Appendix A).

3. Bidders Must Comply with Federal Requirements Beyond the Act; FirstNet Should Identify and Detail These Requirements.

Prior to listing the NPSBN cyber security "objectives," the Draft Appendix does explicitly state one firm requirement: "Any cyber security solution adopted by FirstNet must also comply with the provisions of the Middle Class Tax Relief and Job Creation Act of 2012 (Act)."[14] Certainly, FirstNet is subject to the Act and any winning bid must therefore comply with the Act.

Because it is a federal agency, however, FirstNet is subject to vast array of legally imposed cyber security requirements in addition to those stated in the Act. Thus, FirstNet cannot accept a proposal that does not comply with these federal agency requirements. For example, on identity authentication alone, FirstNet (and its winning vendor) must comply with a slew of executive pronouncements, including HSPD-12 (Policy for a Common Identification Standard for Federal Employees and Contractors)[15] and OMB Memoranda M-04-04 (E-Authentication Guidance for Federal Agencies) and M-11-11 (Continued Implementation of Homeland Security Presidential Directive (HSPD) 12).[16] FirstNet should specifically identify and require compliance with these and all other cyber security obligations to which it is subject as a federal agency.

III. CONCLUSION

Cyber security requirements already exist for public safety agencies at the state, local, and federal levels. For the reasons described above, FirstNet should convene a state and local work group to

[14] Draft Appendix at 3.

[15] *Available at* http://www.dhs.gov/homeland-security-presidential-directive-12.

[16] *Available at* https://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf.

ensure that the NPSBN cyber security solution does not obstruct PSE compliance with their own policies and meets any other public safety cyber security requirements.

Respectfully submitted,

___________/s/____________________
Bill Schrier
FirstNet State Point of Contact
Chair, Washington State Interoperability Executive Committee ("SIEC")
State of Washington

Washington Technology Solutions Department
1500 Jefferson Street SE
PO Box 41501
Olympia WA, 98504-1501

bill.schrier@watech.wa.gov
360.407.8700

APPENDIX A

STATE OF WASHINGTON
OFFICE OF THE CHIEF INFORMATION OFFICER
STANDARD NO. 141.10
SECURING INFORMATION TECHNOLOGY ASSETS

Office of the Chief
Information Officer (OCIO)

STANDARD NO. 141.10

Securing Information Technology Assets

Purpose: Set requirements for maintaining system and network security, data integrity, and confidentiality.

Effective Date: August 19, 2013

See Also: Appendix A: IT Security Checklist
Appendix B: IT Security Risk Threatscape
Appendix C: IT Security Non-Compliance/Deviation Form
Securing Information Technology Assets Policy (141)
Securing Information Technology Guidelines
Auditor's Procedures Engagement
Media Handling and Data Disposal Best Practices

INTRODUCTION

To implement the Information Technology (IT) Security Policy, to protect IT resources, and to enable security audits of those resources, it is required that agencies adhere to common IT security standards. Common standards will help ensure that agencies have an effective and secure environment for IT processing.

Security standards define the processes, procedures, and practices necessary for implementing an agency-specific IT security program. These IT security standards apply to all IT activities, whether they are operated by or for an agency. They include specific steps that will be taken to ensure that a secure IT environment is maintained and all agency systems provide for privacy and security of confidential information.

Such an environment is made possible through an enterprise approach to security in state government that:

(1) Recognizes an interdependent relationship among agencies, such that strengthening security for one strengthens all and conversely, weakening one weakens all.
(2) Assumes mutual distrust until proven friendly, including relationships within government, with trading partners, and with anonymous users in a least-privilege approach to access control.
(3) Supports industry standards where applicable.
(4) Implements security with a customer-centric focus.

Agencies that operate some or all of their information systems outside of this environment will still adhere to the IT security standards.

IT security planning is primarily a risk management issue. Therefore, the OCIO requires agencies to follow the IT Security policy and standards to mitigate security risks in a shared and trusted environment. Agencies will:

(1) Ensure secure interactions between and among governmental agencies take place within a shared and trusted environment.
(2) Ensure secure interactions between and among business partners, external parties, and that state agencies utilize a common authentication process, security architecture, and point of entry.
(3) Close unauthorized pathways into state networks and to the state's data.
(4) Prevent misuse of, damage to, or loss of IT hardware and software facilities.
(5) Ensure employee accountability for protection of IT assets.
(6) Ensure and oversee compliance with these IT security standards, including the annual verification of security compliance from the agency heads to OCIO.

This document contains the following IT Security Standards:

Section 1:	Agency IT Security Program Standard
Section 2 – 11:	Standards for IT security functional areas

Agencies must develop, document and implement policies and procedures for the IT security program in Section 1 and the functional areas in Sections 2 through 11. Agencies may exceed these IT security standards based on the risk and complexity of the IT environment.

SCOPE

(1) The IT security policy applies to state of Washington executive branch agencies, agencies headed by separately elected officials, and institutions of higher education.
(2) These IT security standards apply to state of Washington executive branch agencies and agencies headed by separately elected officials, referred to as "agencies" throughout this document.
(3) Institutions of higher education shall develop standards that are appropriate to their respective missions and that are consistent with the intended outcomes of the OCIO to secure data, systems and infrastructure. At a minimum, higher education institutions' security standards shall address:
   a. Appropriate levels of security and integrity for data exchange and business transactions.
   b. Effective authentication processes, security architectures(s), and trust fabric(s).
   c. Staff training.
   d. Compliance, testing, and audit provisions.

Academic and research applications and infrastructure at institutions of higher education are exempt.

STANDARDS

1. Agency IT Security Program

1.1. Documentation

The agency IT Security Program documentation must:

(1) Align with the agency's risk management strategy.

(2) Clearly identify the security objectives for agency systems.

(3) Contain policies, processes and procedures for all sections of OCIO IT security standards.

(4) Contain detail commensurate with the size, complexity, and potential business exposure based on the results of the agency's IT Risk Assessment process.

(5) Contain details of the security controls applied to agency systems.

(6) Contain details, justifications and approvals by OCIO for any deviation from the OCIO IT security standards.

(7) Contain results, logs, and records from risk and security assessments to demonstrate that the assessments performed met the intended security objectives of the agency.

(8) Identify mechanisms for receiving, documenting, and responding to reported security issues.

Agency Security Program documentation may contain information that is exempt from public disclosure as defined in RCW 42.56.420.

1.2. IT Risk Assessment

The agency must:

(1) 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.

(2) 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.

(3) 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.

(4) Identify potential threats to assets identified as within scope.

(5) Identify the vulnerabilities that might be exploited by the threats.

(6) Identify the impacts that losses of confidentiality, integrity, and availability may have on assets identified as within scope.

(7) Assess the likelihood that security failures may occur based on prevailing threats and vulnerabilities.

(8) 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.

(9) Take into account business, legal, or regulatory requirements, and contractual security obligations.

1.2.1 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.

(4) An agency project or initiative meets criteria for a Design Review as defined and documented by the agency IT security program.

Agencies are encouraged to consult with OCIO and CTS regarding any project to determine whether a design review is recommended.

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.

(4) The planned security controls and how they will be implemented.

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.

(3) Provide design recommendations as necessary for the agency to satisfy OCIO IT security standards.

Agencies may submit appeals regarding Design Review results to the OCIO.

1.3. 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. The agency must:

(1) Establish an IT Security Assessment framework and schedule to identify a sampling of agency systems, applications, and IT infrastructure to test.

(2) Conduct IT Security Assessments against the sample in the framework to verify security controls and identify weaknesses at least once every three years.

(3) 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: the addition of a new sub-network, DMZ or security perimeter device; upgrades to firewalls, switches or routers.

b. Applications have been added or significantly modified.

(4) Correct weaknesses identified with appropriate controls.

1.4. Education and Awareness

The agency must:

(1) Ensure that personnel assigned responsibilities defined in the agency IT Security Program are competent to perform the required tasks.

(2) Document the knowledge, skills, and abilities required for personnel performing work affecting the agency IT Security Program.

(3) 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.

(4) 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.

1.5. Compliance

The agency must:

(1) Ensure compliant implementation of systems and IT infrastructure funded and approved after adoption of these IT security standards.

(2) 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.

(3) 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.
   c. The IT Security Checklist is required by the agency IT security program.

(4) 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.

(5) Attain full compliance with these IT security standards by August 2012.

(6) 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.

(7) 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.
   b. The agency contracts for IT resources or services with an entity not subject to the OCIO IT security standards.

Contractor compliance may be demonstrated by mapping comparable contractor controls to these IT security standards, and by adding supplemental controls that close gaps between the two.

(8) 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.

(9) 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.

1.6. Audit

The agency must:

(1) Ensure an independent audit is performed once every three years to assess compliance with OCIO IT security standards.

(2) Ensure the audit is performed by qualified parties independent of the agency's IT organization.

(3) Submit the results of the audit to the state chief information security officer at CTS.

(4) Maintain documentation showing the results of the audit according to applicable records retention requirements.

(5) Validate that security controls are implemented appropriately based on OCIO IT security standards, the agency security program, and applicable regulatory requirements.

(6) Identify nonconformities and related causes.

(7) Track progress to correct nonconformities.

(8) Implement the corrective action needed.

1.7. Maintenance

The agency must:

(1) Conduct an annual maintenance and review of the agency IT Security Program.

(2) Identify areas to improve the effectiveness of the agency IT Security Program.

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.

Agencies must:

(1) Provide IT security orientation and supervision of employees and monitor contractors who have access to agency IT Assets.

(2) Ensure that appropriate staff conduct is achieved and maintained related to security matters.

(3) Conduct reference checks and background investigations as required by the agency IT security program and authorized by the agency.

(4) 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.

(5) Provide opportunities for IT Security support staff to obtain technical training.

(6) Impose appropriate sanctions for security violations.

(7) Establish processes for the timely removal of system access for employees and contractors when duties change or when separating from service.

(8) Include appropriate language in vendor contracts to require compliance with OCIO and agency security policies, standards, and requirements.

(9) 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.

(10) Identify, document, and implement rules for the acceptable use of IT assets consistent with rules provided by the Washington State Executive Ethics Board.

3. Physical and 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.

3.1. Facilities

Agencies must develop, document, and implement policies and procedures for the following:

(1) Location and layout of the facility.

(2) Physical security attributes for computer or telecommunications rooms.

(3) Design and enforcement of physical protection and guidelines for working in secure areas.

(4) Facility access control.

(5) Physical data storage and telecommunications controls.

(6) Off-site media storage.

(7) Physical security controls for mobile devices.

4. Data Security

Data security components outlined in this section are designed to reduce the risk associated with the unauthorized access, disclosure, or destruction of agency data.

4.1. Data Classification

Agencies must classify data into categories based on the sensitivity of the data.

Agency data classifications must translate to or include the following classification categories:

(1) Category 1 – Public Information

(2) Public information is information that can be or currently is released to the public. It does not need protection from unauthorized disclosure, but does need integrity and availability protection controls.

(3) Category 2 – Sensitive Information

(4) Sensitive information may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.

(5) Category 3 – Confidential Information

(6) Confidential information is information that is specifically protected from disclosure by law. It may include but is not limited to:

   a. Personal information about individuals, regardless of how that information is obtained.
   b. Information concerning employee personnel records.
   c. Information regarding IT infrastructure and security of computer and telecommunications systems.

(7) Category 4 – Confidential Information Requiring Special Handling

   Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which:

   a. Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements.
   b. Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

4.2. 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 the following:

(1) The data that will be shared.

(2) The specific authority for sharing the data.

(3) The classification of the data shared.

(4) Access methods for the shared data.

(5) Authorized users and operations permitted.

(6) Protection of the data in transport and at rest.

(7) Storage and disposal of data no longer required.

(8) Backup requirements for the data if applicable.

(9) Other applicable data handling requirements.

4.3. Secure Management and Encryption of Data

(1) 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).

4.4. Secure Data Transfer

Agencies must appropriately protect information transmitted electronically. The transmission of Category 3 and above information outside of the SGN requires encryption such that:

(1) All manipulations or transmissions of data during the exchange are secure.

(2) If intercepted during transmission the data cannot be deciphered.

(3) When necessary, confirmation is received when the intended recipient receives the data.

(4) Agencies must use industry standard algorithms, or cryptographic modules validated by the National Institute of Standards and Technology (NIST).

(5) For agencies not on the SGN, this standard applies when transmitting Category 3 and above information outside of the agency's secure network.

5. Network Security

Agencies must ensure the secure operation of network assets through the use of appropriate layered protections commensurate with the risk and complexity of the environment.

5.1. 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.

5.1.1 Network Devices

Agencies must:

(1) Securely segment Internet-available systems from internal networks.

(2) Disable unnecessary functionality such as scripts, drivers, features, subsystems, file systems and services.

(3) Harden devices based on industry best practice such as NIST, SANS, and vendor configuration standards.

(4) Change default or initial passwords upon installation.

(5) Display banner text conveying appropriate use at system entry points and at access points where initial user logon occurs.

(6) Disable remote communications where no business need exists.

(7) Standardize and document the device configurations deployed.

(8) Document deviations from device configuration standards along with the approval.

(9) Mask internal addresses from exposure on the Internet as necessitated by the risk and complexity of the system.

(10) Implement controls to prevent unauthorized computer connections and information flows through methods such as:

a. Authentication of routing protocols.
b. Ingress filtering at network edge locations.
c. Internal route filtering.
d. Routing protocols are enabled only on necessary interfaces.
e. Restrict routing updates on access ports.
f. Secure or disable physical network connections in public areas.

5.1.2 Firewalls

Agencies must:

(1) Securely segment DMZ interfaces, where utilized, from interfaces connected directly to the internal network.

(2) Configure network firewalls protecting production systems to:

a. Allow system administration only through secure encrypted protocols.
b. Prevent access by unauthorized source IP addresses or subnets.
c. Block ingress of internal addresses from an external interface into the DMZ or internal interface.
d. Block services, protocols, and ports not specifically allowed.
e. Allow only necessary egress communications from the internal network to the DMZ, Internet, wireless networks and SGN.
f. Allow only necessary ingress communications to the internal network from the DMZ, Internet, wireless networks and SGN.
g. Maintain comprehensive audit trails.
h. Fail in a closed state if failure occurs.
i. Operate boundary/perimeter firewalls on a platform specifically dedicated to firewalls.

(3) Document services, ports and protocols allowed through firewalls, with supporting business purposes, in the agency IT security program.

(4) Review configurations annually.

5.1.3 Device Administration

Agencies must:

(1) Use authentication processes and mechanisms commensurate with the level of risk associated with the network segment or device.

(2) 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.

5.2. 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. Restricted services include but are not limited to:

(1) Dial-in and dial-out workstation modems.
(2) Peer-to-peer sharing applications.
(3) Tunneling software designed to bypass firewalls and security controls.
(4) Auto-launching applications such as U3 that execute from a mobile device and do not require installation on a host system.
(5) Publicly managed e-mail, chat services, and video.
(6) Products that provide remote control of IT assets.
(7) Information systems audit tools.

5.3. 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.
(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.

5.4. Wireless Connections

Agencies are responsible for the secure deployment of wireless networks. Agencies must ensure:

(1) The agency IT Security Program addresses the use of wireless technologies including but not limited to:
   a. 802.11
   b. Bluetooth
(2) Wireless devices that extend their Local Area Networks (LANs):
   a. Securely segment wireless access point connections from the agency network and the SGN.
   b. Use WPA or its successor for authentication and encryption. Use WPA2 Enterprise on all new equipment purchased and existing equipment that supports the protocol.
   c. Change wireless vendor defaults including but not limited to pre-shared keys and passwords.
   d. Disable Simple Network Management Protocol (SNMP) unless there is a clear business need. If enabled, change the vendor defaults.

e. Follow wireless access security practices developed within the agency.

f. Continuously monitor for rogue wireless devices.

(3) Wireless devices that do not extend the agency's local area network or connect to the SGN:

a. Securely segment wireless access point connections from the Internet.

b. Use authentication and encryption appropriate for the environment.

c. Change wireless vendor defaults including but not limited to pre-shared keys and passwords.

d. Disable Simple Network Management Protocol (SNMP) unless there is a clear business need. If enabled, change the vendor defaults.

e. Follow wireless access security practices developed within the agency.

f. Monitor for rouge wireless devices as defined in the agency security program.

(4) 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.

If wireless networks are prohibited, the agency IT Security Program documentation must define how this is periodically verified and enforced.

5.5. 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 that at a minimum includes:

(1) Identification of the responsibilities required for patch management.

(2) Identification of the authorized software and information systems deployed in the production environment.

(3) Timely notification of patch availability.

(4) A method of categorizing the criticality of patches in route or on delivery.

(5) Testing procedures, when required, before deployment into production environments.

(6) Time-specific criteria for deploying patches as soon as reasonably possible after notification, including criteria for zero-day patches.

(7) Regular verification that available patches are managed according to the agency patch management process.

(8) A requirement for current patches on agency or non-agency remotely attached devices.

(9) A requirement for current patches on agency or non-agency devices attached to agency networks, whether on agency local area networks or wireless networks.

(10) Restrict access from devices that do not conform to the agency patch management policy.

5.6. System Vulnerabilities

Agencies must:

(1) Establish a process to identify newly discovered security vulnerabilities such as subscribing to alert services freely available on the Internet.

(2) Use processes that manage the installation and modification of system configuration settings.

(3) 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.

5.7. Protection from Malicious Software

Agencies must:

(1) Use anti-malware protection.

(2) Address malware prevention, detection, and removal.

(3) Keep malware protection current when connecting devices to the agency network or the SGN.

(4) Ensure that file transfers, e-mail, and Web browser-based traffic are examined for known viruses.

(5) Implement detection, prevention, and recovery controls to protect against malicious code.

(6) Integrate malicious software detection reporting with the Washington Computer Incident Response Center (WACIRC) incident reporting processes.

5.8. 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. At a minimum, agencies must

(1) Approve and document the use of category 3 data or above on mobile devices.

(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).

(3) Implement policies and procedures that address the use of portable data storage devices.

6. Access Security

6.1. Access Management

6.1.1 Policies

To ensure proper access controls that conform to the principle of least privilege agencies must:

(1) 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.

(2) Restrict access to data, application, and system functions by users and support personnel in accordance with the agency defined access control policy.

(3) Authentication and authorization controls must be appropriately robust for the risk of the application or systems to prevent unauthorized access to IT assets.

(4) Manage and group systems, data, and users into security domains and establish appropriate access requirements within and between each security domain.

(5) Implement appropriate technological controls to meet access requirements consistently.

(6) Restrict the use of programs or utilities capable of overriding system and application controls.

(7) Implement policies and procedures for identity proofing individuals.

6.1.2 Accounts

To ensure appropriate management of user accounts on system components agencies must:

(1) Establish a formal procedure for issuance, management and maintenance of UserIDs and passwords.

(2) Establish formal user registration and de-registration procedures for granting and revoking access to information systems and services.

(3) Identify users with a unique identifier, for their individual use only, before allowing them to access components, systems, networks, or data.

(4) Ensure that accounts are assigned access only to the services that they have been specifically authorized to use.

(5) 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.

(6) Control the addition, deletion, and modification of user IDs, credentials, and other identifier objects.

(7) Implement mechanisms to restrict and control the use of privileges.

(8) Verify user identity before performing password resets.

(9) Set first-time passwords to a unique value per user that must be changed immediately after first use.

(10) Use time of day, and day of week restrictions as appropriate.

(11) Enable accounts used by vendors for remote maintenance only during the time needed.

(12) Prohibit the use of group, shared, or generic UserIDs/passwords.

(13) Establish a maximum of five incorrect login attempts and lock the account for a minimum of 15 minutes or until reset by an administrator.

6.1.3 Sessions

To ensure appropriate management of sessions on system components agencies must:

(1) Establish procedures to shut down or reauthorize inactive sessions after a defined and reasonable period of inactivity.

(2) 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.

(3) Ensure that access to operating systems is controlled by a secure log-on procedure.

6.1.4 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.

(2) Implement mechanisms to monitor the use of privileges.

6.2. Password Requirements

Agencies must ensure:

(1) Administration of password rules must be technically or procedurally enforced.

(2) UserID/password combinations are Category 3 data and must be protected.

(3) Individuals are prohibited from submitting a new password that is the same as any of the last four passwords used by the individual.

(4) Passwords used for External Authentication Types outlined under section 6.3.1 must:

a. Be a minimum of 10 characters long and contain at least three of the following character classes: uppercase letters, lowercase letters, numerals, special characters.

b. Not contain the user's name, UserID or any form of their full name.

c. Not consist of a single complete dictionary word, but can include a passphrase.

d. Be significantly different from the previous four passwords. Passwords that increment (Password1, Password2, Password3 ...) are not considered significantly different.

(5) Passwords used for Internal Authentication Types outlined under section 6.3.2 must:

a. Be a minimum of 8 characters long and contain at least three of the following character classes: uppercase letters, lowercase letters, numerals, special characters.

b. Not contain the user's name, UserID or any form of their full name.

c. Not consist of a single complete dictionary word, but can include a passphrase.

d. Be significantly different from the previous four passwords. Passwords that increment (Password1, Password2, Password3 ...) are not considered significantly different.

(6) PIN codes used in multi-factor authentication schemes must:

a. Be a minimum of five digits in length.
b. Not be comprised of all the same digit. PINs consisting of 11111, 22222 are not acceptable.
c. Not contain more than a three consecutive digit run. PINs consisting of 12347, 98761 are not acceptable.

(7) Pass codes used to secure mobile devices must:

a. Be a minimum of six alpha numeric characters.
b. Contain at least three unique character classes. Pass codes consisting of 11111a, aaaaa4, are not acceptable.
c. Not contain more than a three consecutive character run. Pass codes consisting of 12345a, abcde1 are not acceptable.
d. Render the device unusable after 10 failed login attempts.

6.3. 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.

6.3.1 External Authentication

Six methods of authentication are defined for users accessing agency owned systems from resources outside the SGN.

6.3.1.1 Type 1 - External

Access to category 1 data, if authenticated, requires authentication via the SecureAccess® Washington infrastructure (OCIO Identity Management User Authentication Standards 7/10/2008) with the following controls:

(1) Requires UserID and hardened passwords as defined in Section 6.2.
(2) Password expiration period not to exceed 24 months.
(3) Successful authentication requires that the individual prove through a secure authentication protocol (in other words, encrypted) that the individual controls the password.
(4) Category 1 data may be accessed using type 2 or 3 authentication.

6.3.1.2 Type 2 – External

Access to category 2 data or a single category 3 record belonging to the individual requires authentication via the SecureAccess® Washington infrastructure (OCIO Identity Management User Authentication Standards 7/10/2008) with the following controls:

(1) Requires UserID and hardened passwords as defined in Section 6.2.

(2) Password expiration period not to exceed 24 months.

(3) Successful authentication requires that the individual prove through a secure authentication protocol (in other words, encrypted) that the individual controls the password.

(4) Category 2 data may be accessed using type 3 authentication.

6.3.1.3 Type 3 - External

Access to category 3 data or a single category 4 record belonging to the individual requires multi-factor authentication via the SecureAccess® Washington infrastructure (IOCIO Identity Management User Authentication Standards 7/10/2008) with the following controls:

(1) Requires multi-factor authentication supported by SecureAccess® Washington.

(2) Passwords must meet the criteria outlined in Section 6.2.

(3) Password expiration period not to exceed 13 months.

(4) Requires that the individual prove through a secure authentication protocol (in other words, encrypted) that the individual controls the password or token.

(5) Category 3 data may be accessed using type 4 authentication.

6.3.1.4 Type 4 - External

Access to category 4 information requires multi-factor authentication via the SecureAccess® Washington or Transact™ Washington infrastructure (OCIO Identity Management User Authentication Standards 7/10/2008) with the following controls:

(1) Requires multi-factor authentication using hardware or software tokens or digital certificates.

(2) Requires that the individual prove through a secure, encrypted authentication protocol that the individual controls the token by first unlocking the token with a password, PIN or biometric in a secure authentication protocol to establish two factors of authentication using a hardware or software token or digital certificate.

6.3.1.5 Type 5 - External

Employee and contractor access to agency resources or the SGN via common remote access methods outlined in Section 6.4 requires two-factor authentication with the following controls:

(1) Requires that the individual prove through a secure, encrypted authentication protocol that the individual controls a hardware or software token by first unlocking the token with a password, PIN or biometric in a secure authentication protocol to establish two factors of authentication.

6.3.1.6 Type 6 – External

Authenticated access that does not meet the criteria outlined in the OCIO Identity Management User Authentication Standards, 7/10/2008, requires the following minimum controls:

(1) Requires a hardened password as defined in Section 6.2 or stronger authentication.

(2) Password expiration not to exceed 120 days.

(3) Additional controls documented in the agency IT Security Program

6.3.2 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.

6.3.2.1 Type 7 - Internal

Access to category 4 data and below requires authentication via the Enterprise Active Directory infrastructure (OCIO Identity Management User Authentication Standards, 7/10/2008) with the following controls:

(1) Requires UserID and hardened passwords as defined in Section 6.2.

(2) Password expiration period not to exceed 120 days.

6.3.2.2 Type 8 – Internal

Access to system administration functions requires the following controls:

(1) Requires a discrete account used only for interactive system administration functions.

(2) Where passwords are employed as an authentication factor:

a. Requires a hardened password as defined in Section 6.2 with an extended password length of 16 characters.

b. Password expiration period not to exceed 60 days.

6.3.2.3 Type 9 – Internal

Accounts used for system service, daemon or application execution (service accounts) require documentation in the agency security program and the following controls:

(1) Requires a discrete account used only for the defined privileged functions, and never used by an individual.

(2) Requires a hardened password as defined in Section 6.2 with an extended password length of 20 characters.

(3) Password expiration requirements must be documented in the agency security program.

(4) The principle of least privilege must be employed when determining access requirements for the account.

6.3.2.4 Type 10 – Internal

Authenticated access that does not meet the criteria outlined in the OCIO Identity Management User Authentication Standards, 7/10/2008, requires the following minimum controls:

(1) Requires a hardened password as defined in Section 6.2 or stronger authentication.

(2) Password expiration not to exceed 120 days.

(3) Additional controls documented in the agency IT Security Program.

6.4 Remote Access

Agencies must:

(1) 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:

a. Monitoring practices for remote access sessions.

b. Requirements for remote access devices.

c. Remote access session controls that conform to the principle of least privilege.

(2) Ensure mitigation is not susceptible to end-user modification.

(3) 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.

(4) Use industry standard protocols for remote access solutions.

(5) Use the state’s common remote access services such as IPSec or SSL VPN when remotely accessing agency resources and services on the SGN.

(6) Ensure remote access solutions prompt for re-authentication or perform automated session termination after 30 minutes of inactivity.

(7) 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.

7 Application Security

7.1 Planning and Analysis

Agencies must specify security controls when developing business requirements for new or enhanced information systems including but not limited to:

(1) 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.

(2) Procedures are in place to manage the installation of software on operational systems including but not limited to servers and workstations.

(3) Access to program source code is restricted to only those individuals whose job requires such access.

(4) Include specific requirements in contracts for outsourced software development to protect the integrity and confidentiality of application source code.

(5) Implementation of changes will be managed by the use of formal change management procedures.

(6) Appropriate access and security controls; audit trails; and logs for data entry and data processing.

(7) Requirements for appropriate data protection.

7.2 Application Development

Agencies must develop software applications based on industry best practices and include information security throughout the software development life cycle, including the following:

(1) Separate development, test, and production environments.

(2) 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.

(3) 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.

(4) Removal of test data and accounts before production systems become live.

(5) Removal of custom application accounts, usernames, and passwords from production environments before applications become active or are released to customers.

(6) Review of custom code prior to release to production or customers to identify potential coding vulnerabilities as described in Section 7.4 Vulnerability Prevention.

(7) Appropriate placement of data and applications in the IT infrastructure based on the risk and complexity of the system.

(8) Use of appropriate authentication levels.

7.3 Application Maintenance

Agencies must:

(1) Review and test system changes to ensure there are no adverse impacts on agency operations or security.

(2) 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.

7.4 Vulnerability Prevention

Agencies must prevent common coding vulnerabilities in software development processes. Agencies must:

(1) Develop software and applications based on secure coding guidelines. An example is the Open Web Application Security Project guidelines. See www.owasp.org – “The Ten Most Critical Web Application Security Vulnerabilities” which include:

a. Un-validated input.
b. Weak or broken access control such as malicious use of UserIDs.
c. Broken authentication/session management such as use of account credentials and session cookies.
d. Cross-site scripting (XSS) attacks.
e. Buffer overflows.
f. Injection flaws such as SQL injection.
g. Improper error handling that creates other conditions, divulges system architecture or configuration information.
h. Insecure storage.
i. Denial of service.
j. Insecure configuration management.

(2) Review code to detect and mitigate code vulnerabilities that may have security implications when significant changes have been made to the application.

7.5 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.

(2) Agency security standards and procedures.

The operation of such applications must not jeopardize the enterprise security environment.

8 Operations Management

8.1 Change Management

Agencies must implement an effective change management process that:

(1) 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.

(2) Ensures computing environments are segmented to reduce the risks of unauthorized access or changes to the operational system.

(3) 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.

8.2 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).

8.3 Media Handling and Disposal

Agencies must:

(1) Ensure that media be disposed of securely and safely when no longer required, using formal documented procedures.

(2) 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.

  b. Destroy, securely overwrite, or make unavailable software consistent with the software licensing agreement.

(3) Ensure the safe and secure disposal of sensitive media.

(4) Ensure that system documentation is protected against unauthorized access.

(5) Ensure Media containing information is protected against unauthorized access, misuse, or corruption during transportation beyond an agency's physical boundaries.

8.4 Data and Program Backup

Agencies must:

(1) Satisfy data archival and rotational requirements for backup media based on the results of an IT Security Risk Assessment.

(2) Implement procedures for periodic tests to restore agency data from backup media.

(3) Test recovery procedures for critical systems at the frequency documented in the agency IT Security Program.

(4) Establish methods to secure their backup media.

(5) Store media back-ups in a secure location such as a designated temporary staging area, an off-site facility, or a commercial storage facility.

9 Electronic Commerce

Agencies must address the effect of using the Internet to conduct transactions for state business with other public entities, citizens, and businesses.

Agencies must:

(1) Prepare and incorporate plans for Internet-based transactional applications, including but not limited to e-commerce, into the agency's portfolio.

(2) 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.

(3) Protect information involved in on-line transactions in order to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication, or replay.

(4) Protect IT infrastructure supporting electronic commerce services from unauthorized access and use according to these IT security standards.

10 Security Monitoring and Logging

Audit logs recording user activities, exceptions, and information security events are necessary to detect and audit unauthorized information processing activities.

10.1 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:

(1) The log records including events, exceptions and user activities necessary to reconstruct unauthorized activities defined by the strategy.

(2) Procedures for periodic review and analysis of recorded logs as set forth in the agency IT Security Program.

(3) Retention periods for logs.

10.2 Logging Systems

At a minimum, logging systems must satisfy the logging strategy identified by the agency and:

(1) Protect the logging facilities and log information against tampering and unauthorized access.

(2) Synchronize with an agency approved accurate time source.

(3) 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.
   c. Initialization of the logging process.
   d. Creation and deletion of system objects.

10.3 Intrusion Detection and 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.

11 Incident Response

Agencies must:

(1) Ensure timely and effective handling of IT security incidents.

(2) 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:

   a. Escalation procedures.
   b. Designate specific personnel to respond to alerts.

c. Be prepared to implement the incident response plan and to respond immediately to a system breach.
d. Provide appropriate training to staff with security breach response responsibilities.
e. Have a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.
f. Incorporate the incident response plan in the agency IT Security Program.

(3) Test the incident response plan at least annually.

(4) 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.

(5) 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.

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.

RESPONSIBILITIES

Chief Information Officer (or designee)

(1) Interpret the policy and standards.
(2) Ensure policy and standards content is kept current.
(3) Recommend updates to the policy and related standards in response to changes in technology, service delivery, or other challenges to the security environment.
(4) Review agency projects for compliance with the security policy and standards.
(5) Develop an escalation process if an agency is not in agreement or compliance.
(6) Help agencies understand how to comply with the policy and standards.
(7) Monitor annual compliance by agencies.
(8) Approve deviations from the standard.

Technology Services Board

(1) Review and approve major policy changes.

CTS

(1) Maintain security of all CTS-managed networks such as the SGN, Intergovernmental Network (IGN), and Public Government Network (PGN).
(2) Design, establish, and maintain the shared IT infrastructure necessary to support applications and data within a trusted, state-wide environment.
(3) Review agency projects for compliance with the security policy and standards.
(4) Help agencies understand how to comply with the policy and standards.

State Auditor

(1) Develop, publish, and maintain audit standards for IT security audits.
(2) Conduct audits of state agencies according to its audit schedule.

Agency Heads

(1) Oversee the agency's information technology security program and ensure compliance with the security policy and these IT security standards.

(2) Assign responsibility for IT security to an individual or group with the appropriate training and background to administer those functions and ensure that the individual or group has proper authority to install, monitor, and enforce IT security standards and procedures.

(3) Ensure agency security policies, procedures, and other documents necessary for the security program are developed, implemented, maintained, and tested.

(4) Ensure all agency users of IT resources are trained to follow security policies, standards, and procedures.

(5) Submit an annual, signed security verification letter.

DEFINITIONS

When used in these IT security standards, the following terms are defined terms and will be proscribed the following meanings:

Access. The ability to use, modify, or affect an IT system or to gain entry to a physical area or location.

Application. A computer program or set of programs that meet a defined set of business needs. See also Application System.

Application System. An interconnected set of IT resources under the same direct management control that meets a defined set of business needs.

Attack. An attempt to bypass security controls on an IT system in order to compromise the data.

Authentication. The process of ensuring the identity of a connected user or participants exchanging electronic data.

Contractor. The firm, its employees and affiliated agents. Contractor also includes any firm, provider, organization, individual, or other entity performing the business activities of the agency. It will also include any subcontractor retained by Contractor as permitted under the terms of the Contract. Contractor and third-party are synonymous as defined within the Definitions section of this standard.

Environmental Security. Physical protection against damage from fire, flood, wind, earthquake, explosion, civil unrest and other forms of natural and man-made risk.

Extranet/VPN Connection. Network-level access originating from outside the network. Examples include SSL, IPSec, "terminal service" or Citrix-like connections.

Firewall. A combination of hardware and software designed to control the types of network connections allowed to a system or combination of systems or that enforces a boundary between 2 or more networks.

Information Technology (IT). Telecommunications, automated data processing, databases, the Internet, management information systems, and related information, equipment, goods, and services.

Information Technology (IT) Assets. The processes, procedures, systems, IT infrastructure, data, and communication capabilities that allow each agency to manage, store, and share information in pursuit of its business mission, including but not limited to:

- Applications**.**

- All data typically associated with IT systems regardless of source (agency, partner, customer, citizen, etc.).
- All data typically associated with IT systems regardless of the medium on which it resides (disc, tape, flash drive, cell phone, personal digital assistant, etc.).
- End-user authentication systems.
- Hardware (voice, video, radio transmitters and receivers, mainframes, servers, workstations, personal computers, laptops, and all end point equipment).
- Software (operating systems, application software, middleware, microcode).
- IT infrastructure (networks, connections, pathways, servers, wireless endpoints).
- Services (data processing, telecommunications, office automation, and computerized information systems).
- Telecommunications hardware, software, and networks.
- Radio frequencies.
- Data computing and telecommunications facilities.
- Intelligent control systems such as video surveillance, HVAC, and physical security.

Information Technology (IT) Infrastructure. IT infrastructure consists of the equipment, systems, software, and services used in common across an organization, regardless of mission/program/project. IT Infrastructure also serves as the foundation upon which mission/program/project-specific systems and capabilities are built. Approaches to provisioning of IT infrastructure vary across organizations, but commonly include capabilities such as Domain Name Server (DNS), Wide Area Network (WAN), and employee locator systems. Additional common capabilities examples include IT security systems, servers, routers, workstations, networked Supervisory Control and Data Acquisition (SCADA) systems, and networked printers (multifunction devices).

Information Technology (IT) Risk Assessment. Reference 1.2. Risk assessment is a process by which to determine what IT Assets exist that require protection, and to understand and document potential risks from IT security failures that may cause loss of information confidentiality, integrity, or availability. The purpose of a risk assessment is to help management create appropriate strategies and controls for stewardship of information assets. (Source: Information Resources and Communications (IR&C) at the University of California Office of the President)

Internal System or Network. An IT system or network designed and intended for use only by state of Washington employees, contractors, and business partners.

Intrusion Detection Systems (IDS). Software and/or hardware designed to detect an attack on a network or computer system. A Network IDS (NIDS) is designed to support multiple hosts, whereas a Host IDS (HIDS) is set up to detect illegal actions within the host. Most IDS programs typically use signatures of known cracker attempts to signal an alert. Others look for deviations of the normal routine as indications of an attack.

Intrusion Prevention Systems (IPS). Software and/or hardware designed to prevent an attack on a network or computer system. An IPS is a significant step beyond an IDS because it stops the attack from damaging or retrieving data. Whereas an IDS passively monitors traffic by sniffing packets off of a switch port, an IPS resides inline like a firewall, intercepting and forwarding packets. It can thus block attacks in real time.

Malicious Code. Software (such as a Trojan horse) that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a user into executing other malicious logic.

Malware. A general term coined for all forms malicious software including but limited to computer viruses, worms, trojan horses, most rootkits, spyware, dishonest adware, crimeware and other malicious and unwanted software.

Mobile Device. A small-sized computing device that may have a display screen, touch input or a keyboard, and/or data storage capability. Examples include laptops, Personal Digital Assistants (PDAs), smart phones, tablet PCs, accessible equipment, and portable data storage devices such as tape drives, zip drives, removable hard drives, USB data storage devices.

Multi-factor Authentication (MFA). A security system or mechanism in which more than one form of authentication is implemented to verify the legitimacy of a transaction. In contrast, single factor authentication involves only a UserID/password.

In 2-factor authentication, the user provides dual means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorized, such as a security code.

Additional authentication methods that can be used in MFA include biometric verification such as keyboard cadence, finger scanning, iris recognition, facial recognition and voice ID. In addition to these methods, device identification software, smart cards, and other electronic devices can be used along with the traditional user ID and password.

Network. A term that describes an approach to link together computers and their peripherals in order to communicate among them and with outside parties.

Network Device. A device available to other computers on a network. Examples include servers, firewalls, routers, switches, workstations, networked Supervisory Control and Data Acquisition (SCADA) systems, and networked printers (multifunction devices).

Password. A unique string of characters that, in conjunction with a logon ID, authenticates a user’s identity.

Penetration Test. A deliberate probe of a network or system to discover security weaknesses. The test attempts to leverage identified weaknesses to penetrate into the organization. The test exploits the vulnerabilities uncovered during a vulnerability assessment to avoid false positives often reported by automated assessment tools.

Physical Security. Physical security describes measures that prevent or deter attackers from accessing a facility, resource, or information stored on physical media in an IT facility.

RecordUnits of related data fields such as groups of data fields that can be accessed by a program and that contains information on a specific item or an individual.

Risk. The potential that an event may cause a material negative impact to an asset.

Risk Assessment. The process of identifying and evaluating risks to assess potential impact.

Risk Management. Identification and implementation of IT security controls to reduce risks to an acceptable level.

Secure Segmentation. Secure segmentation is defined as implementing methods that allow for secure communication between various levels of segmented environments. These environments typically involve 4 basic segment groups:

1. Outside (Trust no one)
2. Services (Trust limited to defined segmentation lines)
3. Internal (Trust limited to defined group)
4. External users (Trust limited to defined group)

The methods for securing these segments may include but are not limited to firewall and switch/router configurations and router/switch ACLs.

Security. The protection afforded to IT systems and data in order to preserve their availability, integrity, and confidentiality. The ability to protect:

- The integrity, availability, and confidentiality of information held by an agency.
- Information technology assets from unauthorized use or modification and from accidental or intentional damage or destruction.
- Information technology facilities and off-site data storage.
- Computing, telecommunications, and applications related services.
- Internet-related applications and connectivity.

Security Controls. The security requirements and methods applied by agencies to manage IT security risk including but not limited those defined in the OCIO IT security standards.

Security Domain. An environment or context that is defined by security policy, a security model, or security architecture to include a set of system resources and the set of system entities that have the right to access the resources.

System. Any collection of people, processes, and technology needed to deliver a service, capability, or functionality.

Tablet PC. A portable general-purpose computer contained within a single small form factor LCD display sized to approximately match that of a traditional writing paper tablet. A tablet PC utilizes a touch screen as the primary input source. Typically either wireless (802.11) or mobile (4G) networks are used for connectivity with limited physical port options.

Examples of Tablet PC's include: iPad, Motorola Xoom, HP Elitebook, Samsung Galaxy, Sony Tablet S, Toshiba Thrive, Acer Iconia, Kindle Fire, Nook tablet, etc.

Threat. Any circumstance or event (human, physical, or environmental) with the potential to cause harm to an IT system in the form of destruction, disclosure, adverse modification of data, and/or denial of service by exploiting vulnerability.

Token. A security token may be either a dedicated hardware device or software-based installation on an electronic device which is used for identity proofing in multi-factor authentication.

Trusted Agency, System or Network. An IT system or network that is recognized automatically as reliable, truthful, and accurate without continual validation or testing.

Untrusted. Characterized by absence of trusted status. Assumed to be unreliable, untruthful, and inaccurate unless proven otherwise.

Vulnerability. Relates to risk of attack. In IT terms, vulnerability describes points of risk to penetration of security barriers. Awareness of potential vulnerability is very important to designing ever more effective defenses against attack by unauthorized parties.

Vulnerability Assessment. A comprehensive analysis that attempts to define, identify, and classify the security holes (vulnerabilities) in a system, network, or communications infrastructure within the assessment scope.

REVISION HISTORY

Date	Action taken
August 19, 2013	Wording change to section 1.4(3) and addition of new section, 1.4(4). The purpose is to remove the requirement that all employees be required to be trained on OCIO Security Policy and Standard and the agency's security policies and procedures, but stipulates such requirement for personnel assigned responsibilities defined in the agency's IT Security Program.

April 10, 2012	Technical correction to clear up confusion about the meaning of 6.2.7 (b). Added the term “classes” to modify the phrase “Contain at least three unique characters.” The purpose is to clarify that the pass code must contain some combination of at least three of the following: uppercase letters, lowercase letters, numerals, and special characters.
March 28, 2012	The standards are changed to add an additional subsection (7) following Section 6.2 (6). A new definition is added for the term “Tablet PC”; and “tablet PCs” are added to the examples listed in the definition of Mobile Device.
October 2011	Standards reformatted for migration to Office of Chief Information Officer. Reflected changes in responsibilities from DIS to CTS. Highlighted sections currently under review.
August 13, 2009	The revision was designed to close the gap between the existing Standards and current industry security best practices to mitigate the breadth and sophistication of IT security threats. Many of the security controls and the organization of the updated standards are based on IT security best practice frameworks from the recognized IT standards bodies.
January 10, 2008	Added statement #9 requiring comparable security policies for entities wishing to connect to state systems.
November 2006	Revised format; revised Applies To section content; added requirement to submit audit results to the ISB in statement #7; revised annual compliance filing date to match agency’s budget submittal date in statement #8; removed language redundant with Information Technology Security Standards, Policy No. 401-S3; simplified and clarified language throughout.
April 2002	Revised format; added language to policy statement #5 on Internet applications; added language to policy statement #8 on agencies providing annual certification to the ISB.
October 6, 2000	Initial effective date.
July 14, 2000	Policy adopted.

CONTACT INFORMATION

For questions about this policy, please contact your OCIO Information Technology Consultant. For technical security questions or to request a Design Review, please contact the state Chief Information Security Officer at Consolidated Technology Services.

APPROVING AUTHORITY

Chief Information Officer Date
Chair, Technology Services Board