



*State of West Virginia
Executive Branch*

INFORMATION SECURITY Strategic Plan

*This plan was prepared by the Office of Information Security and Controls
Jim Richards, Chief Information Security Officer*



(This page intentionally blank)

TABLE OF CONTENTS

- Information Security Program.....4
- Security Policy Development.....5
- Privacy Partnership6
- Risk Management7
- Business Continuity Plans.....9
- Disaster Recovery (DR) Plans10
- Security Operations Center (SOC).....11
- Training and Culture.....12
- Information Security Management Emphasis.....14
- Audit Program15
- Certification and Accreditation (C&A)17
- Incident Management and Computer Forensics.....18
- Staffing Levels and Team Development.....19
- Funding20
- Information Security Metrics21
- Outreach22
- Office of Technology Partners.....23
- WV Information Security Principles25

INFORMATION SECURITY PROGRAM

Introduction

A documented statewide program for Information Security is part of an architecture for the protection of systems and information that is entrusted to Executive Branch agencies. This state-collected and stored information enables government operations, and the endeavor to provide significant services to State citizens. The intent of this Strategic Plan is to describe and document the key elements of the West Virginia Executive Branch security program, and outline the initiatives that support each element.

The West Virginia Office of Technology (WVOT) develops Executive Branch security standards, policies, and procedures for use by Executive organizations, and provides best-practice guidelines for all other state and local public sector organizations. With these policies as a framework for what needs to be accomplished, procedures offer detail about how the policies are implemented. Other policies that address IT or Information Security issues, pre-existing or developed by Executive Branch agencies, may be more (but not less) stringent than those issued by the State Chief Technology Officer (CTO), and must be approved by the WVOT.

West Virginia must maintain compliance with legal and regulatory requirements. It is essential that the WVOT implement practical measures to protect the State's information systems (and the associated data) from compromise. Best practices must be followed in order to safeguard **all** forms of information.

The discipline of Information Security supports the three essential requirements of confidentiality, integrity and availability.

An enterprise-wide approach to Information Security enables WV State Government's Executive Branch to advance in a coordinated and effective progression toward reduced risk. Risk can never be eliminated, but it can always be reduced.

The concept of "layered security" involves the use of controls and protections at every opportunity in the information system landscape. Some of the layers in an effective information security program include:

Administrative Controls, such as policies, management emphasis on risk reduction behaviors (e.g. not clicking on unpredictable Internet links), awareness training (fostering cultural change in the form of supportive behaviors in the user community, such as locking unattended workstations; creating and protecting strong passwords; storing, using, and conveying sensitive information with safeguards commensurate with its sensitivity and criticality, etc.), as well as minimum necessary privileges and access rights to systems and data, segregation of duties, auditing for policy and regulatory compliance; Technical Controls, such as firewalls, access control lists in network equipment, anti-virus, spam filtering, WEB site blocking, encryption, event monitoring, vulnerability scanning, configuration and patch management, etc.; and adequate Physical Security standards and compliance.

The WVOT has utilized the International Standards Organization (*ISO*) and National Institute of Standards and Technology (*NIST*) Information Security Standards in defining West Virginia's Information Security objectives.

SECURITY POLICY DEVELOPMENT

Policy is the foundation upon which all successful information security programs are built, and through which the vision for an effective information security program is communicated. Policy development is most meaningful as a collaborative venture, and benefits from the input of key stakeholders. The WVOT strives to elicit input from these key stakeholders, such as the Governor's Information Security Team (GEIST)), a group comprised of representatives, known as Information Security Administrators, who have been appointed by Cabinet Secretaries from all Executive Branch department-level organizations, with appropriate staff support, management, and leadership roles.

The WVOT has created a general security policy, as well as other security-related policies and procedures, for the Executive Branch of West Virginia government. Agencies may establish more stringent policy supplements, but duplication of content should be avoided. Each agency developing a security policy supplement must submit it to the WVOT for review/approval.

If necessary, procedures must be developed to specify how each policy is implemented. While policies are typically published for general consumption, procedures are frequently maintained as internal documents, as they often provide operational detail(s) that should not be revealed, for security reasons, to the general public.

POLICY INITIATIVES

- Initiative 1.** Periodically update the existing Executive Branch security policies and procedures
- Initiative 2.** Create additional targeted policies and procedures
- Initiative 3.** Review agency Information Security policies to ensure consistency, elimination of duplication, and compliance with the Executive Branch security standards
- Initiative 4.** Maintain copies of all adopted policies online for WEB (Internet) access
- Initiative 5.** Develop an effective awareness training strategy for policies, and implement this strategy across the Executive Branch. Involve stakeholders from the GEIST in this policy deployment strategy development
- Initiative 6.** Maintain a comprehensive, targeted, set of policies that specifically address the expectations held for employees with critical technical roles, in view of their elevated privileges and the inherent threat potential (e.g. non-malicious accidents) that elevated privileges provide to the holder.

PRIVACY PARTNERSHIP

The Information Office of Security and Compliance (OISC) works closely with the West Virginia Privacy Office so that privacy concerns are properly addressed as they relate to technical and administrative security controls. It is essential that privacy and security be viewed as related challenges for the State, and that the policies and standards set forth by these Offices are complimentary, and become integrated into all business processes within the Executive Branch. Executive Order 6-06 effectively solidifies the linkage between Information Security and Privacy.

PRIVACY SUPPORT INITIATIVES

- Initiative 1.** Provide security expertise to the Privacy Management Team and State Privacy Officers
- Initiative 2.** Collaborate with the Chief Privacy Officer on security and privacy concerns, such as incident prevention, preparedness, and response
- Initiative 3.** Collaborate with the Privacy Office to achieve compliance with privacy mandates, laws, and best practices



RISK MANAGEMENT

In all enterprise environments, there are numerous risks to Information Technology (IT) systems and the data residing on them. Risks can be both internally and externally sourced.

Constantly changing vulnerabilities and threats require risk assessments that are ongoing and thorough, in continuously repeating cycles, identifying emergent risks, and requiring the implementation of necessary risk mitigation actions.

Risk is a relationship between *value, threats, and vulnerabilities*. In the absence of any value, threat, or vulnerability, no risk exists. Value of data tends to increase in most organizations over time (because quantity increases, environmental complexity increases, and investment in data analysis, and resultant information, increases). Since the complete elimination of threats and/or vulnerabilities is impossible, risk will always exist, and the increase in value raises the stakes proportionately over time. The reduction of externally-based threats is virtually impossible, although many threats can be blocked, once they are identified. Focus of skills and resources must therefore be directed primarily at the reduction of vulnerabilities, especially around the highest value (potential) targets. Threats must be identified and analyzed, so the targets of these threats – the vulnerabilities – can be reduced, and the threats that **can** be blocked, **are** blocked.

A very real threat is actually generated within a culture that is not well educated in security awareness, or fails to adhere to policy and best practices to which they actually have been oriented. Put another way, for the sake of highlighting the work that needs to be done “internally,” ***failure to reduce identified vulnerabilities is an invitation to any threat-vector targeting the known vulnerability.*** For example: If a parent allows a toddler to cross a busy highway alone, that parent is a threat to the child’s well-being, even if the threat-agent that would do the actual harm is the traffic. If a user makes a mistake, or intentionally violates policy, this user becomes a threat. This user-threat is, statistically, more likely to cause an incident than most external threat agents, such as hackers. These internal user-threats must be addressed with training, disciplinary action, and elevated cultural expectations.

Resources available for the reduction of vulnerabilities are limited, so available resources should be allocated first to the vulnerabilities associated with highest value targets. Risk management provides understanding of what it is that has greatest value to the organization, e.g. the State’s most critical applications, and the data that these applications process. The approach we are taking is to classify systems and data.

In order to properly manage IT risks, the WVOT utilizes a repeating-activity management approach. The cycle is as follows:

- Risk Assessment
- Risk Mitigation
- Evaluation and re-assessment

Risk assessment is the initial phase in the risk management life-cycle. Risk assessment is used to determine each system’s criticality to the entity (Department, agency, etc.), and to identify potential threats to each system. The output of this process seeks to identify appropriate controls for reducing risk during the risk mitigation process. To determine the likelihood of a future adverse event, system threats must be analyzed in conjunction with potential vulnerabilities and other relevant factors. System/data classification is critical to this phase.

The second phase is risk mitigation. This involves evaluating, prioritizing, resourcing, and implementing the appropriate and accomplishable risk-reducing controls/countermeasures to address the risks identified during the risk assessment process.

Components of most computer systems inevitably are upgraded or replaced, and software applications may be updated with newer versions, or replaced. These changes often introduce new vulnerabilities, and previously mitigated risks can re-emerge, or new risks can materialize. Thus, the risk management process is ongoing and iterative, creating a repeating cycle of evaluation and re-assessment, followed by appropriate mitigation.

RISK MANAGEMENT INITIATIVES

- Initiative 1.** Review and update documentation of system characterizations: purpose, scope, criticality, sensitivity, platform, age, version, support capability, complexity, etc.
- Initiative 2.** Identify existing relevant threats and vulnerabilities
- Initiative 3.** Analyze existing controls to reduce risk
- Initiative 4.** Determine likelihood and impact of adverse event
- Initiative 5.** Create a qualitative risk matrix: High, Medium, Low
- Initiative 6.** Conduct a cost-benefit analysis on risk reduction strategies
- Initiative 7.** Select a risk mitigation strategy based upon risk and cost-benefit analysis
- Initiative 8.** Recommend changes in controls/countermeasures
- Initiative 9.** Complete selected mitigation activities. Test effectiveness of mitigation effort
- Initiative 10.** Monitor system for changes and repeat process at appropriate intervals (go to: Initiative 1)



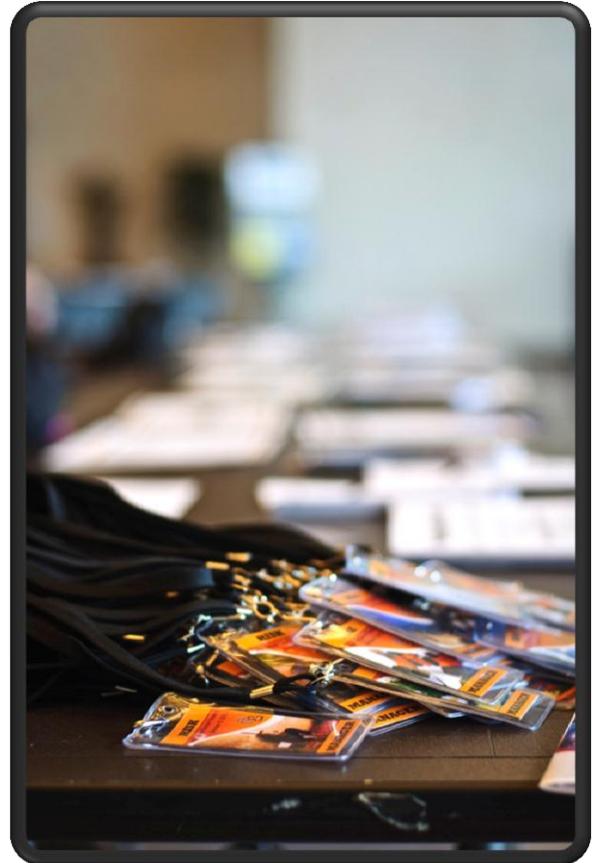
BUSINESS CONTINUITY PLANS *

Each agency is required to maintain **business continuity and / or Continuity of Operations (COOP)** plan for identified critical business functions. Each plan must specify how the agency will continue to sustain its critical business functions and provide services to constituent consumers until disrupted operations can be fully restored. Continuity plans must be tested and updated by the business units, in collaboration with the Office of Technology (to ensure technical feasibility of plans).

() Note: The fact that Business Continuity Planning is included in this Strategic planning document does not in any way mean to suggest that this plan creation and maintenance can be accomplished by the WVOT or the OISC. "Business Continuity Plans" is included in this document because this planning is a necessary prerequisite to the disaster planning process that is performed by the IT organization (WVOT, etc.), and cannot be performed intelligently without Business Continuity plans that identify critical systems, and prioritizes the order of system recoveries. Business Continuity planning must be performed by the business units, whose staff must, in addition to address prioritization with respect to system restoration, have alternate working arrangements pre-planned in order to sustain operations during a situation that renders the normal workplace unusable.*

INITIATIVES

- Initiative 1.** Support activity of agency data and system classification, to ensure adequate classification and identification of most critical business systems
- Initiative 2.** Support enforced alignment between business continuity and disaster recovery plans
- Initiative 3.** Support periodic testing of business continuity plans, in conjunction with the associated disaster recovery plan



DISASTER RECOVERY (DR) PLANS

Disaster recovery plans may be developed with the mistaken thought that they will be useful only in the aftermath of explosions or natural disasters, but reliance upon sound disaster plans can be just as necessary when an event, such as airborne asbestos, is detected and causes a business location to become unusable. When an event occurs that disrupts a normal business function, rapid resolution is usually desired and expected, and for most critical functions, this resolution must necessarily be appropriately expedited. Disaster recovery addresses the requirement for restoring adequate IT functions when a significant, or protracted, interruption in service occurs. In some cases, the DR activity may be limited to a redirection of connectivity to an alternate business continuity location specified by an affected agency.

Major disaster recovery activity would be associated with the physical destruction, or functional disruption, of a State data center or critical server or storage location, such as those located at Building 6, DHHR, DEP, TAX, and DoT.

Disaster recovery plans are simply technology services-resumption plans. They address emergency equipment acquisition and installation, and/or switching operations to alternate sites where computing equipment has been pre-positioned. The process can include activating additional alternate locations for equipment, including servers, storage, support staff, communications, power, cooling, etc. DR plans require specific instructions for application and data restoration, account login restoration, network and voice communications and other services restoration, expertise deployment, and coordination of efforts to restore most critical services first.

Because there must be an organized and appropriate order of events in the restoration of services, providing the restoration of most critical systems and services first, disaster recovery plan priorities are derived from business continuity plans. This linkage ensures that restoration of a technology function is accomplished according to the pre-defined business need(s).

The recovery of IT functionality to meet the business needs is the responsibility of the WVOT operational units. For this reason, disaster recovery requires a swift, coordinated effort undertaken by staff who may not typically work together under conditions of great urgency. Successful and efficient recovery can, therefore, best be executed when the DR plan has been tested. The WVOT OISC is responsible for validating the completion, viability, and testing of these disaster recovery plans.

The WVOT Client Services, Networking and Enterprise Applications organizations all play a key role in the development of a viable DR plan and, ultimately, the recovery of IT services after a disruptive event.

Coordination between these groups will be essential for the DR planning process, and the orderly restoration of critical WVOT services should an event occur.

INITIATIVES

- Initiative 1.** Verify that disaster recovery plans are completed for each critical business function, and aligned with the associated business continuity plan
- Initiative 2.** Verify that the plan for adequate periodic testing and validation of disaster recovery plans is completed and documented, along with indicated revisions

SECURITY OPERATIONS CENTER (SOC)

To assist in the reduction of risk, a dynamic view of the traffic and “events” that take place in the State computing environment, including the network and the server/storage areas, must be maintained. The WVOT-OISC SOC utilizes a set of tools that view events, correlate events that have known malicious signatures, or anomalous characteristics, and intervene when traffic or events suggest that some violation or malicious activity is taking place in the State network environment. When a problem is suspected, recorded logs can be used to analyze event history, and the cause can be identified to a point in time and often to a source location. The primary system used is referred to as a System Event and Incident Management (SEIM) tool.

Security Operations includes the SOC activities, as well as vulnerability scanning of State systems, validating patch levels, configuration hardening, WEB monitoring/site blocking, and other system safeguards.

INITIATIVES

- Initiative 1.** Maintain the full functionality needed in the SOC, including traffic analysis, event correlation and log analysis, threshold alerts, etc.
- Initiative 2.** Maintain 24x7x365 security surveillance of network traffic and system events for all critical infrastructure components combining threat analysis and alerts to State technicians when any anomalies are detected, correlated, and/or quarantined
- Initiative 3.** Maintain a regular schedule of vulnerability scanning within the State technical environment
- Initiative 4.** Maintain comprehensive WEB activity monitoring and selective site blocking based upon customer requirements
- Initiative 5.** Develop a state-of-the-art situational watch room, combining analyst, management, and executive-level dashboards, giving the agency real-time business security intelligence
- Initiative 6.** Focus upon the insider threat, and network violation management through the use of effective policy monitoring, reporting and agency enforcement
- Initiative 7.** Support the WVOT – OISC Audit function
- Initiative 8.** Maintain and support the analysis of cyber-security counter-intelligence
- Initiative 9.** Establish WV-ISAC as the the Security Operations Center's brand name for Information/Cyber Security information sharing, analysis, and alerting, for West Virginia public sector entities.

TRAINING AND CULTURE

People are generally recognized as being the weakest link in securing systems. Even the best technological and physical controls can be defeated easily if the human factor is weak. It is imperative that all State employees be part of the human defense system developed in the State. We ask that all State employees become “human firewalls.”

The “human firewall” component can only be achieved with proper training and education that creates an elevated awareness of the threats, human vulnerabilities, and risk reduction techniques. To that end, the WVOT OISC deploys online Information Security awareness training. Topics include, but are not limited to, the following:

- Social Engineering – how to avoid being victimized by malicious manipulation techniques
- Password Management – creating, securing, and periodically changing strong, unshared passwords
- Physical Security – supporting controls in place to protect spaces, such as door controls
- Acceptable Use – avoiding unsafe or unethical use of State equipment
- Workplace Security – using precautions to prevent unauthorized access to systems/data
- Internet Security – web use and misuse issues; web filtering and malware challenges



The federal government enacted the *Computer Security Act of 1987* in response to Internet crime and cyber terrorism. This act requires periodic security awareness training for all federal employees who are involved in the management, use, or operation of a computer system. Our State has no less need for information security awareness to be solidified throughout its employee body.

Making staff aware of threats has proven to be a very cost-effective countermeasure against security violations and/or mishaps. **Gartner analysts Ouellet, Proctor, and Witty (2006) estimated that there is a 0.8 (80%) probability of 25% productivity savings in Information Security due to the workforce awareness of threats, risks, and controls, which reduces the number of security incidents.** Staff trained in a security awareness program will have the knowledge to prevent common incidents and/or to reduce the damage done when an incident does occur.

All of the work involved in creating a set of technological system security controls (such as firewalls, anti-virus, encryption, etc.) is severely diminished in the absence of an informed community of computer users, brought to this status by a comprehensive awareness training program for all State employees.

TRAINING AND CULTURE INITIATIVES

- Initiative 1.** Provide all Executive Branch employees with security awareness training.
- Initiative 2.** Establish an annual refresher training program for all employees.
- Initiative 3.** Establish a process to audit for, and assure, completion of training and refresher sessions by all employees, with proper documentation of completion. This will also include new employees, contractors, and any other individuals using state computer systems
- Initiative 4.** For the subsets of State employees listed below, establish minimum training standards, and assist with curriculum development that addresses the unique and/or elevated responsibilities and requirement for expertise, commensurate with the role:
- Executive/ Management / Supervisory
 - Technician
 - Help Desk
 - Mobile or Portable Device User
- Initiative 5.** Offer WEB-based Information Security awareness training to local governments
- Initiative 6.** Conduct an annual “October is Cyber and Information Security Awareness Month” event
- Involve the Governor and other State Executives in reinforcement of the message when possible, including event attendance
 - Support the request that the Governor issue a Proclamation, naming October as Cyber and Information Security Awareness month
 - Publicize the event to the greatest extent possible
 - Record the event, if financially feasible, and make available online, on-demand
 - Broadcast the event live, online, if financially feasible.

INFORMATION SECURITY MANAGEMENT EMPHASIS

Under the authority established by Senate Bill 653, effective July 1, 2006, and the Governor's Executive Order 06-06, signed August 16, 2006, and following the mandate of these documents, a high-level Information Security Team, known as the Governor's Executive Information Security Team (GEIST) has been organized to assist with the implementation of Information Security initiatives throughout the Governor's Executive Branch of West Virginia State government.

The membership of this team includes the Information Security Administrators (ISA) appointed by the Cabinet Secretaries of each Department or agency. These ISAs provides leadership or oversight in the following areas:

- **Business Continuity planning**
- **Training completion tracking and documentation**
- **Risk management**
- **Data classification**
- **Plan testing**
 - Business continuity and disaster recovery
- **Audits**
 - Facilitate Information Security audits performed by the WVOT OISC
- **Policy implementation**
 - Policy recommendations to the Office of Information Security and Controls
 - Policy draft reviews, comments and proposed revisions
 - Monitoring for compliance
 - Arranging emphasis or disciplinary action as needed
 - Policy deployment strategy development
- **Supplemental policy facilitation**
 - Recommending policy additions, changes, or drafting agency supplements to WVOT-issued policy
- **GEIST team membership and mandatory meeting attendance (or substitute attendance)**
 - ISAs may form teams of support staff for their organizations, and invite them to attend quarterly GEIST meetings, and be added to GEIST Listserv for all notifications.



INITIATIVES

- Initiative 1.** Maintain an informed and engaged GEIST through quarterly meetings, information advisories, and adhoc meetings, as needed
- Initiative 2.** Elevate the visibility of the GEIST throughout West Virginia State government.
- Initiative 3.** Periodically review the GEIST Charter for relevance and suitability

AUDIT PROGRAM

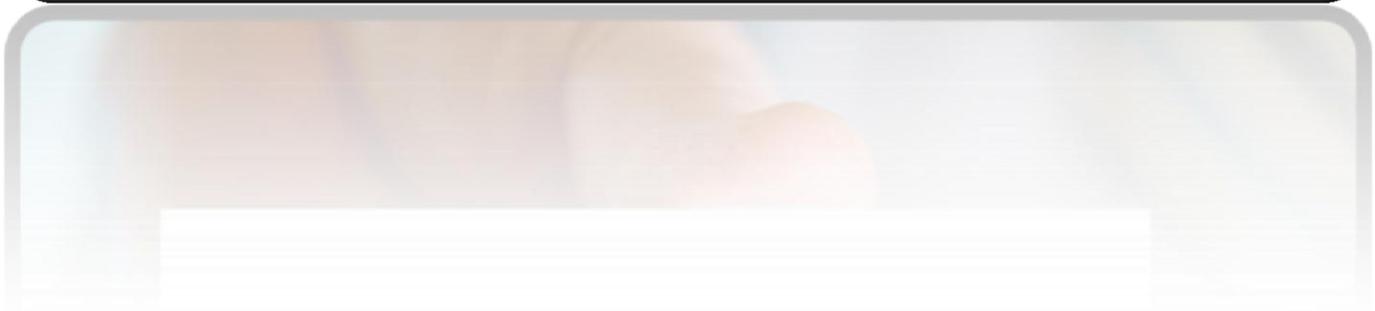
Under the authority established by Senate Bill 653, effective June 11, 2006, and the Governor's Executive Order 06-06, the WVOT is charged with establishing an audit function to review compliance with all policy provisions that are issued concerning the use of technology, and the security practices governing that use. The WVOT OISC has committed to this audit function with the establishment of an IT Internal Audit Program.

Audit efforts are focused on those areas presenting the highest degree of risk, as well as those areas where risk mitigation will provide the greatest potential benefit to the Executive Branch. In addition to performing both random and targeted audits in State agencies - examining, evaluating, and reporting on: IT applications, related systems, operations, processes, and practices - the Audit Program will review internal controls within the WVOT operations, and will conduct audits of selected 3rd party providers at their off-site locations.

INITIATIVES

- Initiative 1.** Conduct audits in agencies for compliance with Executive Branch IT policy, including the following:
- User adherence to desktop practices of logging off workstations when leaving unattended, protecting passwords from use by others, and absence of confidential material left in plain view in the desktop area
 - Absence of password sharing
 - Adequate controls at building entrances and exits
 - Documented completion of mandatory Information Security training
 - Annual certification of working knowledge of policy governing Information Security practices
 - Annual signoff on reading and agreeing to adhere to the requirements of a suitable Confidentiality Agreement
 - Completion (and testing) of business continuity plan(s).
- Initiative 2.** Conduct audits of technical environments, with emphasis on the WVOT, for compliance with policy and best practices related to the following:
- Segregation of duties
 - Effective end user account management processes and compliance with policy/procedure
 - Normal user
 - Elevated privileges user
 - Contractor user
 - System (automated) user
 - Effective Architecture, and Engineering design (may utilize 3rd party reviewers as needed)
 - Unique administrative accounts for each technician with direct responsibility for a system function(s)
 - Use of administrative accounts for administrative duties only
 - Maintaining current patch levels
 - Using standardized, policy-compliant configurations (no default configurations in any device)
 - Maintaining "least privilege" access rights for all users and technicians
 - Using strong password enforcement controls on all systems
 - Disaster Recovery Plan completion and testing.
 - Maintaining WEB sites free from publically accessible, legally protected information
- Initiative 3.** Formal reporting of findings to all levels of relevant management with recommendation for corrective action to mitigate identified risk(s)

- Initiative 4.** Conduct vulnerability scans, and perform penetration testing as needed to verify required system hardening, or conduct these scans by proxy utilizing skills and tools from the SOC
- Initiative 5.** Contract for 3rd party auditing services to augment internal audit resources or to perform specialized audit services
- Initiative 6.** Conduct audits of 3rd party provider agreements and services, including at off-site locations, to ensure adequate security controls. Assure that all 3rd party contracts allow this audit



CERTIFICATION AND ACCREDITATION (C&A)

In the implementation phase of new software applications, or the configuration phase of deployment of new hardware (servers, personal computers, wireless access points, etc.), it is critically important that the product being brought into production is correctly created and/or hardened. Certification is a comprehensive validation and verification of the viability of software or hardware, using rigorous testing to ensure that security requirements have been met prior to introduction into the production environment. Accreditation is the approval and authorization to initiate any change in the technology environment, within the scope of C & A.

The C & A discipline is applied throughout the technology life-cycle to confirm that security controls are implemented correctly, and are effective in their implementation. While not all technology falls under the C & A umbrella, risk analysis should be applied to each technology being considered for deployment, to determine if this discipline is applicable.



Ultimately, the CTO should authorize, by specific signoff, the introduction of a piece, or system (including software systems) of technology into the production environment, based upon its having met the applicable C & A standard(s) for that technology.

INITIATIVES

- Initiative 1.** Identify responsibility and resources for the development of a C & A program.
- Initiative 2.** Establish the framework (processes, practices, and procedures) for Certification and Accreditation, through an exercise of collaboration within the Office of Technology and between the WVOT and its State agency partners.
- Initiative 3.** Define Certification and Accreditation criteria and scope, meaning: what kinds of technologies must undergo C & A before being moved into production, and what are the standards that must be met at each milestone.
- Initiative 4.** Plan, develop and deliver C & A training to all affected practitioners to foster the required cultural change, and provide necessary understanding about how to plan Accredited product and service rollouts within the C & A framework.
- Initiative 5.** Map C & A activities to the technology, and project-management life-cycle.

INCIDENT MANAGEMENT AND COMPUTER FORENSICS

Incidents are inevitable, and the ongoing occurrences of incidents range in seriousness from mild, to severe. With the frequency of reported incidents steadily increasing, the WVOT and OISC must be proactive in efforts to protect information and information systems from disruption, and maintain a readiness to recover from the effects of critical information security incidents. A proven (tested and/or utilized) incident management plan is recognized as the best preparation for the unexpected event.



The WVOT OISC developed policies, standards, and procedures to establish a framework specific to incident response. The OISC has established a central point of contact for reporting incidents (incident@wv.gov), and an automated notification system to contact key responders. The OISC also offers consulting services and support during the analysis, recovery, and post-mortem phases of incident handling, to any subscribed State organization that is affected by a computer related incident, with a security implication or impact.

Computer forensics capabilities are required to determine what has transpired in systems at a user level, within a server or network component layer, or on a system-wide level - after the fact. Forensics tools and skills may be employed to analyze logs, investigate computer abuse, detect and isolate an automated malware infestation or attack, or interrupt and block a targeted attack against any system.

INITIATIVES

- Initiative 1.** Maintain a Computer Security Incident Response Team (CSIRT)
- Maintain appropriate policies and procedures for notification, response, and recovery from computer security incidents
 - Maintain a central point of contact for reporting computer security incidents
 - Maintain a service to provide alerts and notification of newly discovered computer vulnerabilities and threats to State, county and local government agencies
 - Test the plan on a periodic basis; include testing of all the methods of establishing communications with critical responders
- Initiative 2.** Maintain adequate forensics skills to accomplish needed investigations professionally, timely, and suitably documented as needed to provide evidence in a court of law

STAFFING LEVELS AND TEAM DEVELOPMENT

Staffing levels and building expertise with targeted training must be adequate to support the mission of the OISC, even as this mission grows, and the ongoing requirements of both the technical and administrative components of the OISC grow. While specialization and depth of skill levels is desirable, Information Security staff will be required to assume multiple roles, as they will at times participate in the audit program, policy development, training development and deployment, system security monitoring, WEB use monitoring and filtering, forensics, incident response, and research and testing functions, to name a few.



Each staff person will ideally be cross-trained, and acquire multiple skill-sets. We will collaborate as a team, and create time and task-defined “virtual teams” to complete specific projects, and to meet both short and long-term objectives.

A startup team consists of 8 staff, plus the Director, for a total of 8.5 full-time Information Security staff in the OISC. A requirement exists for an additional FTE at this time in the SOC area of security monitoring, and there currently is no DR oversight capacity.

▪ Management:	2	FTE
▪ Technical Security (SOC):	3	FTE
▪ Audit Staff:	1	FTE
▪ Policy/Training Specialist:	1	FTE
▪ Privacy/Spec. Prj./Forensics:	1	FTE

TEAM DEVELOPMENT INITIATIVES:

- Initiative 1.** Develop Job Classification Series that closely describes the work of an Information Security professional - Completed
- Initiative 2.** Obtain resources needed to accomplish the goals of the OISC, and the initiatives set forth in this plan
- Initiative 3.** Train and cross-train staff to a multi-disciplinary model as much as possible. Develop staff skills, professionalism, and business awareness. Keep career progression and succession planning in the skills development strategy

FUNDING

The practice of Information Security and Compliance in the Executive Branch of West Virginia is an endeavor to prevent problems that are more costly than the expense of instituting preventative controls, including the cost of supporting the OISC's set of functions. For the most part, the OISC does not generate revenue, however there are exceptions. For this reason, operational cost must be borne by all Agencies in proportion to their use of information technology services. A 2008 Ponemon Study showed that the cost of information security initiatives are increasing in organizations at a rate projected at 26% for 2009, with actual increases over the prior 3 years at 18%, 20%, and 19% respectively (2006-2008).

Investment in Information Security in the Executive Branch of West Virginia has historically been minimal. Pre-centralization of the Information Security and Compliance function within the WVOT, agencies had varying levels of financial commitment in this area, funded and focused proportionately to the perceived need of agency leadership, and available dollars. There was not a correlation between data value (criticality) and investment in safeguards.

Staffing levels in the WVOT OISC should continue to increase somewhat over the coming years, through the consolidation of infrastructure into the WVOT, and by limited hiring into newly allocated positions. Increasing the mission of the OISC may require additional personnel resources above the levels portrayed in this document. Investment in appropriate tools, and maintenance of existing tools, to adequately perform policy development and maintenance, monitoring and auditing services, training, forensics, etc., will continue at an appropriate level of spend, if possible.



In 2009, a \$3/user/month fee was initiated to fund information security. The fee was increased in 2010 to \$4/user/month. This fee does not yet cover the cost of providing adequate information security services to the Executive Branch. Funding at the \$5 or \$6 level per user per month is a more realistic level, so staffing and toolsets are more adequately resourced.

FUNDING INITIATIVES

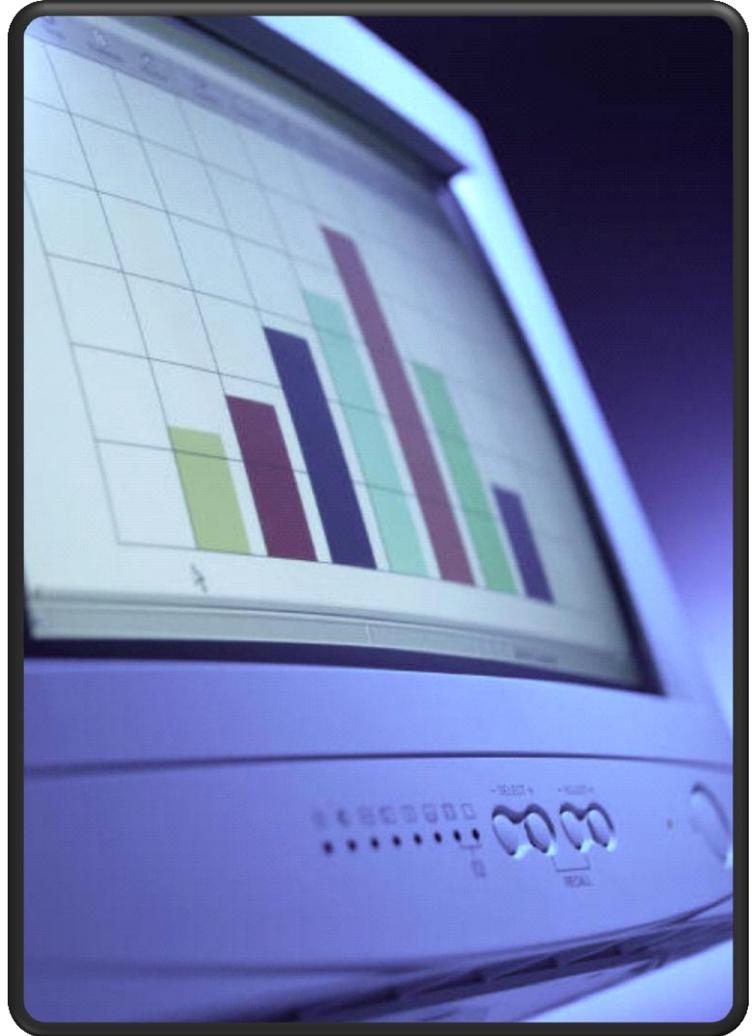
Initiative 1. Establish an adequate per seat per user fee for security services that will fund a viable Information Security and Compliance program as described in this document

INFORMATION SECURITY METRICS

In order to measure our work, and to be able to represent “accomplishments” to stakeholders, we need to refine a system of capturing and reporting metrics. The types of metrics needed will vary by the audience for whom they are developed. The audience should ideally have a role in prescribing the metrics that are most useful to them.

INITIATIVES

- Initiative 1.** Work with a representation of partners to develop a set of metrics to be identified and tracked. Determine the interval, frequency, and format for reporting on these metrics to the various stakeholder groups
- Initiative 2.** Determine how to derive the metric, and most efficiently capture and report the metric at the specified interval
- Initiative 3.** Automate the metrics reporting function wherever possible
- Initiative 4.** Continue to evaluate the effectiveness of the metrics strategy



OUTREACH

Public Sector Partners

The OISC is the leader in providing necessary Information Security services in West Virginia's Public Sector. It is therefore essential that we share the resources and talent developed within our organization to assist all of the West Virginia governmental entities in any effort they undertake to realize more effective Information Security practices. We are committed to be supportive of our fellow public sector partners, including local governments and law enforcement.

Physical Security Partners

Physical Security is the front line of defense in the practice of Information Security. If individuals with malicious intent are permitted to enter a target facility, their ability to do harm is significantly enhanced. The use of security badges, door ingress controls, surveillance, and other physical controls is essential to effective physical security management. Under the current organizational structure in the Executive Branch, physical security is coordinated out of the West Virginia Department of Military Affairs and Public Safety (WV DMAPS). For this reason, it is highly desirable for the WVOT OISC to maintain a strong working relationship with our physical security partners, such as the Division of Protective Services.

Other Security Partners

A critical aspect of maintaining an effective Information Security program is the exchange of intelligence and expertise among practitioners. The WVOT OISC is actively involved with multiple national organizations, and maintains relationships with other West Virginia State experts including those within the WV Fusion Center and WV Critical Infrastructure Protection Task Force. The WVOT OISC acts as a conduit for Information Security alerts and advisories, and as an analytical resource, having recently initiated the WV-Information Sharing and Analysis Center (WV-ISAC) as described in the section on the Security Operations Center

INITIATIVES

- Initiative 1.** Share expertise, assistance, and training materials with other public sector organizations
- Initiative 2.** Promote discussions that will enhance the security work of all public sector partners in West Virginia, including organizations such as the WV Department of Military Affairs and Public Safety, the State Treasurer's Office, the Secretary of State, the State Auditor, and other State offices not within the Governor's span of authority, as well as counties and municipalities.
- Initiative 3.** Maintain active participation with the Multi State – Information Sharing Analysis Center (MS-ISAC), including focus committee participation (currently Training and Awareness, Outreach and Operations)
 - Continue to update the State alert level
 - Continue to relay all advisories out to partners and constituents
 - Maintain the membership list of members of the State of WV, WV-ISAC Portal (derivative of the MS-ISAC Portal)
- Initiative 4.** Maintain active participation in the National Association of State CIOs (NASCIO) Privacy and Security workgroup, and other relevant organizations
- Initiative 5.** Maintain a working relationship with Legislative Commission on Special Investigations

OFFICE OF TECHNOLOGY PARTNERS

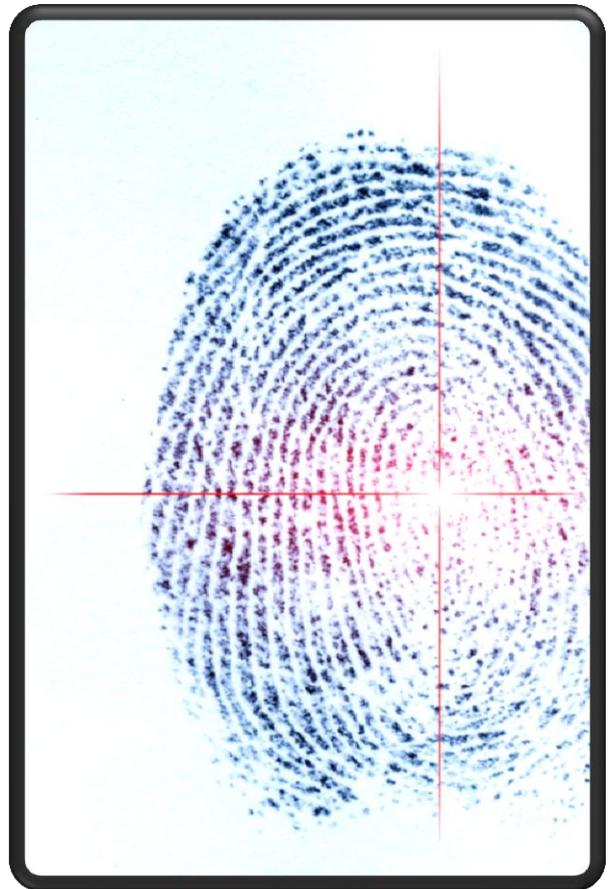
Looking from a security perspective at the State's technical landscape, it is certain that no organization needs greater security self-discipline than the WVOT itself. Our staff

hold the "keys to the kingdom(s)," and have access to virtually every aspect of the computing environment in West Virginia State government. With these elevated access privileges come equally elevated responsibilities, as well as the need for accountability, throughout the WVOT technical organization.

It is important that all organizational units in the WVOT work closely together, and particularly closely with Information Security, to ensure that we are creating and using standards in naming conventions, configurations, settings, documentation, and process creation and implementation. All of our initiatives and projects must have security objectives embedded within the architecture and design, and incorporated into the setup configuration and deployment routine for all system components. Information Security should be involved as a partner in every design project, and should be an involved participant in regular, technically focused meetings with Client Services, Enterprise Applications, and Networking, and State agencies.

Each organization with a role in the technical setup and administration of system components should align their operational activities with the following **fundamental security concepts**:

- **Least Privilege** – No assignment of privilege to anyone without a need for access
- **Segregation of Duties** – Separation of responsibilities to ensure no conflict of interest, and to ensure accountability
- **Documentation of all critical operational processes, procedures, and security activities** – Diligence is not verifiable without documentation
- **Cross training** to provide redundant skills in critical functional areas – Eliminate skills vulnerabilities created by lack of skills breadth and depth
- **Documentation of all configurations and system setup procedures** - In the event of a failure or "disaster," restoration and recovery operations may need to be completed by someone other than the primary technician assigned to the customary system support function. Thorough documentation reduces dependence on single or specific individuals, especially important during critical situations.
- **Elimination of Single Points of Failure, and Vulnerability to Internal Sabotage** – Strategies which reduce the chance that critical functions can be adversely impacted by the absence, mistakes, or deliberate actions of a single individual can include rotation of responsibilities and implementation of requirements for multiple individuals to perform and document the processes supporting all aspects of key functions, on a regular basis.



OFFICE OF TECHNOLOGY PARTNERS INITIATIVES

- Initiative 1.** Review all procurements processed by or through the WVOT having any technical, physical, or administrative security implications, for consistency and compatibility with overall security architecture, designs, technologies, and strategies
- Initiative 2.** Maintain active participation in all substantive planning sessions within the WVOT and the Executive Branch, or specifically elect Initiatives Continued (Office of Technology Partners) to waive participation, documenting the reason(s) for non-participation.
- Initiative 3.** Monitor all security-related operational activities for compliance with best practices, policies, procedures, and standards, particularly in the six fundamental security concept areas listed above.
- Initiative 4.** Maintain a comprehensive set of policies, which specifically address the expectations held for employees with critical technical roles in view of their elevated privileges, and the inherent threat potential (e.g. non-malicious accidents) that elevated privileges provide to the holder.
- Initiative 5.** Develop specialized training for technicians addressing responsibilities and accountability practices, emphasizing the policies and procedures developed solely for their roles, and to assure their compliance with best practices, as privileged-access users within the State's technical infrastructure.
- Initiative 6.** Promote the development of an Accreditation and Certification Program requiring compliance with all applicable standards including, but not limited to security standards, documented, with signoff by an authorized authority (CTO or designee) prior to putting any system (hardware or software) into production within the Executive Branch (CTO's span of control). This applies to Servers, Personal Computers, PDA's, Thumb Drives, Applications, Networking components, phones, and other devices that require setup or customization to work properly in the State environment, with appropriate security settings enabled.

WV INFORMATION SECURITY PRINCIPLES

- **Security Awareness** – All employees should understand the elements of their role in the protection of information systems and the data that these systems contain.
- **Individual Responsibility** – All employees should be responsible for their actions in the use of information systems, in order to support Information Security.
- **Incident Prevention/Reporting** – Employees should strive at all times to prevent security incidents, and report suspected incidents in a timely manner.
- **Ethical Practices** – All employees should adhere to the ethical standards established for public employees in their use of information systems.
- **Respect** – Employees should recognize the sensitivity of data maintained about citizens, and respect the confidentiality needs and rights of all individuals.
- **Risk Awareness** – As part of the larger risk awareness / risk management process, each employee should review and report any and all risks (threats or vulnerabilities) that may uniquely impact their specific work with information systems.
- **Culture of Security** – Employees should incorporate secure practices into all of their work activities, handling of information, and use of information systems.
- **Security Leadership** – All levels of leadership in West Virginia State government should support sound security practices, and respond constructively and comprehensively to all security initiatives.
- **Process Improvement** - Ongoing analysis and re-evaluation of risks, threats and vulnerabilities should foster continuous improvements in the security posture, and associated controls.