Office of the State Auditor

Dianne E. Ray, CPA
Acting State Auditor

MEMORANDUM

Date: May 23, 2011

To: Members of the Legislative Audit Committee

From: Dianne E. Ray, CPA
Acting State Auditor

Re: Cyber Security Performance Audit Status Report

Attached is a summary status report of the progress made by the Governor's Office of Information Technology in implementing recommendations from the Office of Cyber Security performance audit presented to the Legislative Audit Committee in December 2010. Out of a total of 47 recommendations (each subpart counted separately) included in the public report, 23 have been implemented, 16 have been partially implemented, and 8 have not been implemented.

A separate, confidential status report addressing the confidential recommendations included in the private report will be made available to the Committee during the executive session in June.

Legislative Services Building • 200 East 14th Avenue • Denver, Colorado 80203-2211
Ph. 303.869.2800 • Fax: 303.869.3060

AUDIT RECOMMENDATION STATUS REPORT

AUDIT NAME: Office of Cyber Security
AUDIT NUMBER: 2068A
DEPARTMENT/AGENCY/ENTITY: Governor's Office of Information Technology
DATE: April 20, 2011

SUMMARY INFORMATION

Recommendation Number *(e.g., 1a, 1b, 2, etc.)*	**Agency's Response** *(i.e., agree, partially agree, disagree)*	**Original Implementation Date** *(as listed in the audit report)*	**Implementation Status** *(Implemented, Partially Implemented, or Not Implemented)* * *A recommendation that is in progress should be denoted as "partially implemented."*	**Revised Implementation Date** *(Complete only if agency is revising the original implementation date.)*
1a.	Agree	July 2011	Partially Implemented	
1b.	Agree	July 2011	Implemented	
1c.	Agree	July 2011	Implemented	
1d.	Agree	July 2011	Implemented	
1e.	Agree	July 2011	Implemented	
1f.	Agree	July 2011	Implemented	
1g.	Agree	July 2011	Implemented	
1h.	Agree	July 2011	Implemented	
2a.	Agree	July 2011	Implemented	
2b.	Agree	July 2011	Partially Implemented	
2c.	Agree	July 2011	Implemented	
2d.	Agree	July 2011	Partially Implemented	
2e.	Agree	July 2011	Implemented	
2f.	Agree	July 2011	Implemented	
2g.	Agree	July 2011	Implemented	
3a.	Agree	July 2011	Implemented	

Recommendation Number *(e.g., 1a, 1b, 2, etc.)*	**Agency's Response** *(i.e., agree, partially agree, disagree)*	**Original Implementation Date** *(as listed in the audit report)*	**Implementation Status** *(Implemented, Partially Implemented, or Not Implemented)* ** A recommendation that is in progress should be denoted as "partially implemented."*	**Revised Implementation Date** *(Complete only if agency is revising the original implementation date.)*
3b.	Agree	July 2011	Implemented	
3c.	Agree	July 2011	Implemented	
4.	Agree	January 2011	Implemented	
5a.	Agree	July 2011	Partially Implemented	
5b.	Agree	July 2011	Implemented	
5c.	Agree	July 2011	Partially Implemented	
5d.	Agree	July 2011	Not Implemented	December 2011
5e.	Agree	July 2011	Not Implemented	December 2011
6a.	Agree	July 2011	Partially Implemented	
6b.	Agree	July 2011	Implemented	
6c.	Agree	July 2011	Implemented	
7a.	Agree	July 2011	Partially Implemented	
7b.	Agree	July 2011	Partially Implemented	
7c.	Agree	July 2011	Partially Implemented	
7d.	Agree	July 2011	Partially Implemented	
7e.	Agree	July 2011	Not Implemented	December 2011
7f.	Agree	July 2011	Partially Implemented	
8a.	Agree	July 2011	Partially Implemented	
8b.	Agree	July 2011	Implemented	
8c.	Agree	July 2011	Not Implemented	December 2011
8d.	Agree	July 2011	Not Implemented	December 2011
8e.	Agree	July 2011	Not Implemented	December 2011
8f.	Agree	July 2011	Partially Implemented	
8g.	Agree	July 2011	Partially Implemented	

Recommendation Number *(e.g., 1a, 1b, 2, etc.)*	**Agency's Response** *(i.e., agree, partially agree, disagree)*	**Original Implementation Date** *(as listed in the audit report)*	**Implementation Status** *(Implemented, Partially Implemented, or Not Implemented)* * *A recommendation that is in progress should be denoted as "partially implemented."*	**Revised Implementation Date** *(Complete only if agency is revising the original implementation date.)*
9a.	Agree	July 2013	Partially Implemented	
9b.	Agree	July 2013	Not Implemented	
9c.	Agree	July 2013	Implemented	
9d.	Agree	July 2013	Implemented	
9e.	Agree	July 2013	Not Implemented	
9f.	Agree	July 2013	Implemented	
9g.	Agree	July 2013	Partially Implemented	

DETAIL OF IMPLEMENTATION STATUS

Recommendation #: 1a, 1b, 1c, 1d, 1e, 1f, 1g, 1h.

Agency Addressed: Governor's Office of Information Technology (OIT) and Office of Cyber Security (OCS)

Recommendation Text in Audit Report:
The Governor's Office of Information Technology should work with the Office of Cyber Security to reevaluate and improve the Agency Cyber Security Plan development, submission, and review process by:

a. Establishing additional guidelines and procedures for the completion of the Agency Cyber Security Plan, including further guidance related to the performance and documentation of agency risk assessments and self assessments.
b. Providing training to agency information security officers on the completion and submission of the Agency Cyber Security Plans.
c. Developing and implementing a policy that requires written feedback on submitted Plans to be delivered to public agencies within a reasonable period of time—e.g., within 45 days.
d. Reviewing all Agency Cyber Security Plans submitted to the Office of Cyber Security and providing timely feedback to the agencies, including updating the agencies' Plans of Actions and Milestones to ensure that all control gaps are addressed.
e. Holding agencies accountable for the timely submission of statutorily compliant Agency Cyber Security Plans by reporting non-compliant agencies to the Governor or appropriate oversight body or executive, such as the Attorney General or the Chief Justice of the Supreme Court.
f. Ensuring that agencies' risk assessments include specific dates for remediating identified control gaps and that Plans of Actions & Milestones align with the agencies' risk assessments.
g. Incorporating the information contained in the Agency Cyber Security Plans into the Office of Cyber Security's strategic planning process.
h. Working with the Colorado Commission on Higher Education to ensure that security plans developed by institutions of higher education are being received annually and reviewed, as required by statute.

Agency's Original Response *(i.e., Agree, Partially Agree, Disagree)*: **Agree**

Agency's Written Response in Audit Report:
Implementation Date: July 2011.

The Agency Cyber Security Plan (ACSP) was never intended to be utilized as a "paper exercise" but as a strategic document to manage the agency cyber security program. The Office of Cyber Security is currently revising the management policies, procedures, training, and practices governing the requirements, development, maintenance, evaluation, and enhancement of State of Colorado ACSPs.

For example, OCS recently developed an ACSP Scorecard to provide guidance to non-consolidated agencies, Governor's Office of Information Technology, and Colorado Commission on Higher Education on areas of improvement to their ACSP. Another example is moving from having individual ACSPs for Executive branch consolidated agencies to having a single consolidated cyber security plan for the State.

To improve the ACSP submission process, OCS will develop an internal policy that requires that the ACSP Scorecard be completed and provided to the reporting agency within 90 days of the Plan's submission. Additionally, OCS will work with OIT senior leadership to hold agencies accountable for the timely submission of statutorily compliant ACSPs. OCS will also be working with the Colorado Commission on Higher Education to develop formal submission procedures for the security plans developed by institutions of higher education.

OCS has also adopted and implemented a statewide tool, called the Colorado Risk, Incident, & Security Compliance (CRISC) system; to document and manage all identified security deficiencies on state systems using a comprehensive and consistent risk management process that meets the Risk Management Framework

developed by the National Institute of Standards and Technology. Plans of Action and Milestones (POAM) are automatically generated from the tool allowing state personnel that are responsible for their agency POAM to spend their limited time on other agency mission critical tasks. This information will be used to guide the State on focusing limited resources (people, time, budget) to address the most important risks with the highest level of impact to the State.

Status of Corrective Actions (To be provided by agency):
OCS has adopted an internal policy to provide feedback to all agencies within 90 days after their ACSP submission. For the 2010 submission period, the OCS ACSP scorecard was utilized and improved for use in the 2011 ACSP submittal feedback process.

ACSP submittal requirements have been presented and reviewed at the January and February Colorado Cyber Security Council (C3) meetings. Email communication was sent to agency ISOs in May of 2011 on the upcoming ACSP submission deadline with emphasis on all ACSP submission requirements. An ACSP submittal report will be presented to the State CIO, non-Executive branch CIOs, and Executive Leadership Team for OIT at the end of July of each submittal year.

Risk assessments are being facilitated through the centrally managed Colorado Risk Incident Security Compliance (CRISC) application to include expected completion dates, remediation plans, and evidence of implementation documentation for all security control gaps. All control gaps are being mapped to the NIST 800-53 controls, which allows the State CISO to see systemic issues across each agency and the state. This information will be utilized for 2012 strategic security initiatives. Plans of Action and Milestones (POA&M) are being managed through CRISC.

Subpart a. of the recommendation is partially implemented as the OCS is still working on developing further guidance for agency ISOs related to the performance and documentation of agency risk assessments and self assessments

The State CISO has established a process with the Department of Higher Education and the Institutes of Higher Education for ACSP submission and reviews. Institutes will submit their ACSPs to the Department of Higher Education who will submit them to OCS for review and feedback.

Recommendation #: 2a, 2b, 2c, 2d, 2e, 2f, 2g.

Agency Addressed: Governor's Office of Information Technology

Original Recommendation in Audit Report:
The Governor's Office of Information Technology should improve the State's incident identification, reporting, analysis, and response processes and procedures by:

a. Ensuring that all public agencies, including the Department of Higher Education and institutions of higher education, are aware of their responsibilities to report cyber security incidents to the Office of Cyber Security.
b. Providing training to employees, information security officers, and system administrators in incident awareness, identification, documentation, response, and reporting.
c. Updating the State Incident Response Plan.
d. Ensuring that each public agency has detailed, written procedures for responding to security incidents and that agency-level procedures align with the procedures contained in the State Incident Response Plan.
e. Implementing an automated incident response reporting and tracking system and analyzing and reporting incidents to senior management within the Governor's Office of Information Technology on a periodic basis.
f. Performing incident response debriefings with appropriate staff to further improve the Office's incident response capabilities.
g. Updating incident response procedures to require that system administrators enforce password changes on accounts that are suspected of being compromised.

Agency's Response *(i.e., agree, partially agree, disagree)*: **Agree**

Agency's Written Response in Audit Report:
Implementation Date: July 2011.

The Office of Cyber Security Colorado Risk, Incident, & Security Compliance (CRISC) tool has an Incident Response (IR) module that will be used by OCS for a centralized Computer Incident Response Capability (CIRC) that meets all IR criteria as defined by NIST Guidance (SP 800-61: Computer Security Incident Handling Guide) as well as US-CERT reporting requirements. This will aid OCS and state agencies in streamlining and improving incident response processes, provide incident tracking through consistent IR workflows, enhanced incident analysis capabilities, and provide increased statewide incident visibility and IR reporting for state management. The current OCS State IR Plan is being updated to incorporate Governor's Office of Information Technology staff within other IT operational bands as part of a State Computer Security Incident Response Team (CSIRT). Training for all roles and responsibilities identified in the IR Plan will be developed and offered through the OCS state online security training system and formal debriefings will be instituted following the resolution of cyber security incidents occurring within consolidated agencies. As part of the ACSP review process, OCS will also work to ensure that agencies have sufficiently detailed incident response procedures that align with the OCS State IR Plan.

A first responder tool has been developed by OCS to be utilized by state incident first responders to collect data on suspected compromised systems that automatically sends IR data back to the Information Security Operations Center (ISOC) for analysis. This tool will increase the state IR response time and analysis throughout the State, especially at remote state offices where any state staff resource can be utilized to collect data from a system for investigation. IR reporting requirements have been incorporated into the State Security Awareness Training, which is presented during monthly OIT staff meetings, updated on the State Chief Information Security Officer (CISO) website, and distributed through security awareness posters.

OCS will also work with the Chief Technology Officer's office and agency Information Security Officers to ensure that system administrators know to enforce password changes on accounts that are suspected of being compromised following an incident. OCS will also ensure that this is a standard procedure included in agency-level IR procedures.

Status of Corrective Actions (To be provided by agency):
The State CISO has established a process with the Department of Higher Education and the Institutes of Higher Education for ACSP incident reporting. Institutes will report incidents to the Department of Higher Education who will then report them to the state CISO.

OCS has updated the state incident response (IR) plan to include roles, responsibilities, and a localized plan for agencies that have not written their own plan. Training will be provided in June of 2011 to all ISOs and relevant staff. The IR plan has been modified to match the IR workflow as designed in the Colorado Risk Incident Security Compliance (CRISC) application and conforms to the National Institute of Standards and Technology guidance on incident management.

First responder training for state desktop support staff will be offered in July of 2011. This training will cover all steps within the IR plan that are relevant to first responders and technical training on analyzing infected systems.

Beginning in Fiscal Year 2011-12, OCS will be offering brown bag sessions and awareness training for the entire state on information security and incident reporting.

Recommendation #: 3a, 3b, 3c.

Agency Addressed: Governor's Office of Information Technology and

Original Recommendation in Audit Report:

The Governor's Office of Information Technology should ensure that the Office of Cyber Security has implemented and is complying with all statutory requirements of the Colorado Cyber Security Program by:

a. Inventorying all statutory requirements that pertain to the Colorado Cyber Security Program.
b. Ensuring that the Chief Information Security Officer is aware of his or her duties and responsibilities and is knowledgeable of all statutory requirements of the Colorado Cyber Security Program.
c. Developing and executing a work plan to bring the Office of Cyber Security and public agencies into compliance with Colorado Cyber Security Program requirements.

Agency's Response *(i.e., agree, partially agree, disagree)*: **Agree**

Agency's Written Response in Audit Report:

Implementation Date: July 2011.

It is the responsibility of the Chief Information Security Officer to ensure that he fully understands the statutory requirements of the Colorado Cyber Security Program (CCSP), his or her duties and responsibilities to meet these requirements, and provide the leadership and direction for the Office of Cyber Security to ensure that these requirements are being met. Steps have already been taken to prioritize all OCS staff and activities to create, improve and consistently follow OCS processes to meet all statutory requirements and CISO strategic initiatives.

Status of Corrective Actions (To be provided by agency):

The current CISO is fully aware and active in ensuring that the Colorado Cyber Security Program is meeting the statutory requirements in all security initiatives in the state.

Recommendation #: 4.

Agency Addressed: Governor's Office of Information Technology and Office of Cyber Security

Original Recommendation in Audit Report:
The Governor's Office of Information Technology should work with the Office of Cyber Security to develop a strategic plan for the State's cyber security operations. The strategic plan should establish the Office of Cyber Security's mission, vision, goals, objectives, and short- and long-term priorities and include measurable objectives that can be used to assess the Office's progress in achieving its goals. Once finalized, the Office of Cyber Security should communicate the contents of its strategic plan to information security staff and the key stakeholders within public agencies and institutions of higher education. Finally, the Governor's Office of Information Technology should increase its oversight of the Office of Cyber Security and ensure that an effective leadership structure is in place to carry out the strategic plan and implement the Colorado Cyber Security Program.

Agency's Response *(i.e., agree, partially agree, disagree)*: **Agree**

Agency's Written Response in Audit Report:
Implementation Date: January 2011.

The Office of Cyber Security has developed a strategic plan for the State's cyber security operations. The strategic plan establishes the OCS's mission, vision, goals, objectives, and short- and long-term priorities and includes measurable objectives that can be used to assess the Office's progress in achieving its goals. Upon review and approval by the State CIO, the strategic plan will be communicated to information security staff and key stakeholders within public agencies and institutions of higher education. The Governor's Office of Information Technology has recently made strategic leadership changes within OCS and has increased its oversight of OCS operations to ensure that the Colorado Cyber Security Program is being effectively carried out. OIT senior leadership will also be closely monitoring OCS' implementation of the audit recommendations to ensure appropriate mitigation strategies are being executed.

Status of Corrective Actions (To be provided by agency):
The State CISO, through the direction of the State CIO, has clearly defined the role and responsibilities, value proposition, and key performance measures and outcomes for OCS. This was presented and communicated to staff within OCS in April of 2011. Strategic initiatives for 2012 have been developed for the Colorado Cyber Security Program and will be included in the Office of Information Technology (OIT) playbook and communicated through the OIT communication plan. Additional communication will happen through the State CISO via agency management training sessions and OCS staff meetings.

Recommendation #: 5a, 5b, 5c, 5d, 5e.

Agency Addressed: Governor's Office of Information Technology

Original Recommendation in Audit Report:

The Governor's Office of Information Technology should improve the security of the State's network and Internet-facing applications by:

a. Ensuring that the specific deficiencies identified in the confidential appendices provided under separate cover are immediately addressed.
b. Identifying and inventorying all network devices and applications with management interfaces exposed to the Internet or other publicly accessible or insecure networks.
c. Working with agency staff to reconfigure the devices and applications with Internet-exposed management interfaces so that access to the interfaces can only be gained from inside the State's network. If this is not technically possible, then IP filtering should be added to the interface to limit those systems that can reach the service.
d. Revising State Cyber Security Policies to require that administrative interfaces not be directly accessible from the Internet.
e. Implementing firewall rules at the State gateway to filter incoming traffic bound for ports running administrative interfaces.

Agency's Response *(i.e., agree, partially agree, disagree)*: **Agree**

Agency's Written Response in Audit Report:

Implementation Date: July 2011.

Due to budget and resource constraints the exercise of reconfiguring devices and reprogramming software has not been as robust as the Office of Cyber Security originally envisioned. In 2007, OCS initiated a project called the Web Application Scanning Project. The purpose of the project was to work with state agencies to reduce any unnecessary exposure of state systems on the Internet. OCS is planning a similar effort to begin in January 2011. Using the recent Office of the State Auditor penetration test results with additional OCS activities, OCS will identify all state system exposures on the Internet and work with agency staff for business justification. Any exposure that does not have a legitimate agency business purpose will be removed either at the system, agency firewall, or state network level.

Once the State Internet footprint has been reduced to a baseline, the OCS Threat and Vulnerability Management Program (TVMP) will be utilized for the identification and management of new system exposures, vulnerabilities, and configuration weaknesses. It is an industry best practice to not expose system administrative interfaces on the Internet and this will be incorporated in the State Cyber Security Policies during the next OCS policy review and change process.

Status of Corrective Actions (To be provided by agency):

OCS initiated the Colorado Internet Footprint Reduction project in February of 2011. Through this project, OCS has identified all state system exposures on the Internet and is working with agency ISO and staff for business justification for each exposure. Any exposure that does not have a legitimate agency business purpose will be removed either at the system, agency firewall, or state network level. Policy requirements for administrative interfaces will be incorporated in the 2012 OCS Policy and Governance Update initiative.

The state has been actively managing the results from the OSA penetration test with the following OCS requirements:

High Findings – Remediation in January and February – All findings remediated and tracked through the CRISC system by February 28th with remediation plans and efforts in place for any finding needing to be extended past this deadline.

Medium Findings – Remediation in March, April, and May – All findings remediated by May 31st with remediation plans and efforts in place for any finding needing to be extended past this deadline. Findings with extensions will need to be tracked through the CRISC system.

Low Findings – Remediation in June – All findings remediated by June 30th with remediation plans and efforts in place for any finding needing to be extended past this deadline. Findings with extensions will need to be tracked through the CRISC system.

Status of the remediation efforts at the time of this status report:

87% complete for HIGH-rated findings
75% complete for MEDIUM-rated findings
73% complete for LOW-rated findings

Recommendation #: 6a, 6b, 6c.

Agency Addressed: Governor's Office of Information Technology

Original Recommendation in Audit Report:
The Governor's Office of Information Technology should ensure that all state systems, especially those exposed to the Internet, use strong passwords and non-default usernames by:

a. Ensuring that the specific deficiencies identified in the confidential appendices provided under separate cover are immediately addressed.
b. Performing routine vulnerability scans of state systems and networks.
c. Requiring that all new state systems and network devices undergo the OIT approved hardening, or securing, process using the Center for Internet Security benchmarks, which include the removal of default credentials from all hardware and software prior to being placed into production.

Agency's Response *(i.e., agree, partially agree, disagree)*: **Agree**

Agency's Written Response in Audit Report:
Implementation Date: July 2011.

Beginning in 2011, the Office of Cyber Security will expand the Threat and Vulnerability Management Program by requiring agency Information Security Officers (ISOs) to perform monthly vulnerability scans within each agency environment. Pending budget approval, OCS will procure vulnerability scanning software for each of the consolidated Executive Branch agencies. OCS will provide training, standardized scanning policies, vulnerability tracking tools, and monthly reporting requirements for ISO's dedicated to each agency. Phase I of this effort will focus on mitigating high-rated vulnerabilities within each agency. Phase II of this effort will focus on the continuous management of high-rated vulnerabilities and the initiation of mitigating medium-rated vulnerabilities. Phase III will focus on the continuous monitoring and management of all vulnerabilities within each agency environment. Management of the identified vulnerabilities from the Office of the State Auditor penetration test effort will be managed through this process.

OCS has been working with the Chief Technology Officer's office with adopting, implementing, and socializing the use of the Center for Internet Security (CIS) hardening practices as the state security standard for all state systems, applications, and network devices. OCS will utilize the TVMP efforts as an assurance program to validate that the CIS standards are being met and maintained throughout the system development life cycle of each state system.

Status of Corrective Actions (To be provided by agency):
OCS purchased the Nessus vulnerability scanning software for all state agencies (Executive and Non-Executive branches). Each agency will be required to follow the Agency Vulnerability Management Program (AVMP) scanning requirements to scan their environments every quarter and manage the identified vulnerabilities and weaknesses. Scanning requirements will be changed from quarterly to monthly scanning as the state matures the management of findings through the AVMP. Any high-risk finding discovered on the same asset over three scans will require the asset to come offline until it is addressed appropriately.

OCS continues to work with OIT operational staff on the requirements of implementing and maintaining system hardening based on the Center of Internet Security (CIS) standards. OCS will utilize the TVMP/AVMP efforts as an assurance program to validate that the CIS standards are being met and maintained throughout the system development life cycle of each state system.

Recommendation #: 7a.

Agency Addressed: Governor's Office of Information Technology

Original Recommendation in Audit Report:
The Governor's Office of Information Technology should reduce the State's exposure to attacks against unnecessary and insecure ports, services, and utilities by:

a. Ensuring that the specific deficiencies identified in the confidential appendices provided under separate cover are immediately addressed.
b. Reducing the overall Internet footprint of the State through the consolidation of servers and identification and removal of unneeded IP addresses and systems.
c. Limiting the number of ingress and egress points to the State Wide Area Network and to agency-specific networks.
d. Inventorying all systems and applications (assets) that require public Internet access.
e. Defining the appropriate access rules for each inventoried asset.
f. Ensuring that all assets are protected by a monitored firewall.

Agency's Response *(i.e., agree, partially agree, disagree)*: **Agree**

Agency's Written Response in Audit Report:
Implementation Date: July 2011.

Reducing the overall Internet footprint by reducing servers and consolidating applications is the primary goal of consolidation and is complex and will take resources and some time to complete. The State's wide area network was re-bid this summer and is now known as the Colorado State Network. This new network will enable the Office of Cyber Security to provide more secure ingress and egress points as well as improve monitoring. Additionally, through consolidation, OCS is working with the Governor's Office of Information Technology to develop a comprehensive list of all state systems and applications, including those exposed to the Internet. OCS will ensure that proper access rules protect these systems through the vulnerability scans and remediation activities discussed next. Beginning in 2011, OCS will expand the Threat and Vulnerability Management Program by requiring agency Information Security Officers to perform monthly vulnerability scans within each agency environment. Pending budget approval, OCS will procure vulnerability scanning software for each of the consolidated Executive Branch agencies. OCS will provide training, standardized scanning policies, vulnerability tracking tools, and monthly reporting requirements for ISOs dedicated to each agency. Phase I of this effort will focus on mitigating high-rated vulnerabilities within each agency. Phase II of this effort will focus on the continuous management of high-rated vulnerabilities and the initiation of mitigating medium-rated vulnerabilities. Phase III will focus on the continuous monitoring and management of all vulnerabilities within each agency environment. Data collected through this effort will be consolidated for a root cause analysis (i.e., configuration management, patch management, access controls, etc.) and used to target agencies' limited resources (people, time, budget) and future OIT strategic planning. Where budget and resources permit, OCS will also work with agencies to ensure that all critical state systems are protected with a firewall that includes appropriately defined ingress and egress rules.

Status of Corrective Actions (To be provided by agency):
OCS initiated the Colorado Internet Footprint Reduction project in February of 2011. Through this project, OCS has identified all state system exposures on the Internet and is working with agency ISOs and staff for business justification for each exposure. Any exposure that does not have a legitimate agency business purpose will be removed either at the system, agency firewall, or state network level. Policy requirements for administrative interfaces will be incorporated in the 2012 OCS Policy and Governance Update initiative.

OCS has purchased an enterprise Intrusion Prevention Solution for the state that will assist in the management and protection of Internet exposed systems and applications.

Recommendation #: 8a, 8b, 8c, 8d, 8e, 8f, 8g.

Agency Addressed: Governor's Office of Information Technology

Original Recommendation in Audit Report:

The Governor's Office of Information Technology should ensure that state web applications are appropriately secured by:

a. Ensuring that the specific deficiencies identified in the confidential appendices provided under separate cover are immediately addressed.
b. Training state application developers on the fundamentals of secure coding and application design.
c. Routinely testing all existing web applications both manually and with automated application security scanners and correcting the identified deficiencies.
d. Ensuring that all newly designed web applications, whether created by the state or a vendor, are tested manually and with automated scanners.
e. Requiring the Office of Cyber Security to validate that all web applications have been sufficiently tested and properly secured before being moved into production.
f. Protecting critical web applications with web application firewalls.
g. Ensuring IT staff are routinely reviewing and monitoring web application logs and reporting suspicious activity to appropriate staff.

Agency's Response *(i.e., agree, partially agree, disagree)*: **Agree**

Agency's Written Response in Audit Report:

Implementation Date: July 2011.

The Office of Cyber Security initiated an Application Security (AppSec) program in March 2010 to begin to handling the issues of weak web applications within the State of Colorado. Due to budgetary and human resource constraints (the AppSec program currently consists of one highly skilled security application expert), the AppSec has had limited but effective success through the offering of several application security classes to state developers, reviewing and providing guidance on application security requirements for several key state projects, creating a communication mechanism to assist developers with mitigation strategies to close security holes in state web applications, aiding in the implementation of several web application firewalls for critical state applications, and developing application security checklists to be used by developers to check the security of their applications. Testing of applications will be performed through the OCS Threat & Vulnerability Management Program and all identified issues will be mitigated through the AppSec program and tracked to resolution using the OCS Colorado Risk, Incident, & Security Compliance tool. Where budget and resources permit, OCS will assist agencies in testing all new critical and major rated web applications prior to moving the applications into production and will continue providing assistance in the implementation and configuration of web application firewalls.

Guidance on the detection of anomalous and malicious activity against state web applications will be created by the AppSec program and will be integrated into the OCS detection and monitoring program where budget allows for the expansion of the centralized OCS centralized logging system.

Status of Corrective Actions (To be provided by agency):

The OCS Application Security (AppSec) program continues to be limited by budgetary and human resource constraints. Even with these constraints, the AppSec program continues to make improvements in state application security through training and by actively assisting agencies with fixing identified application issues. For example, over that last several months, the OCS AppSec program redesigned and redeveloped one of the highest rated risk applications from the OSA penetration test resulting in all security issues being fixed. The AppSec program will continue to assist all state agencies with the application issues identified during the OSA penetration test.

In fiscal year 2012, the AppSec program and TVMP will be performing a security web application assessment against the top 10 applications within the state.

Guidance on the detection of anomalous and malicious activity against state web applications will be created by the AppSec program and will be integrated into the OIT detection and monitoring program where budget allows for the expansion of the centralized OIT centralized logging system.

Recommendation #: 9a, 9b, 9c, 9d, 9e, 9f, 9g.

Agency Addressed: Governor's Office of Information Technology

Original Recommendation in Audit Report:
The Governor's Office of Information Technology should improve the security of public agencies' internal networks by:

a. Ensuring that the specific deficiencies identified in the confidential appendices provided under separate cover are immediately addressed.
b. Architecting internal networks so that they are "segmented," or broken into different zones based upon the access and security requirements of the systems in those zones. In particular, OIT and agencies should isolate servers and databases where sensitive data may be stored and limit the systems which can access them and the protocols that are allowed based on business needs.
c. Requiring information security officers to routinely perform automated vulnerability scans of internal networks to identify and remediate vulnerabilities.
d. Working with agency IT staff to ensure that proper hardening and patch management practices are being followed.
e. Providing guidance to IT staff and agency IT directors on the development and implementation of proper network segmentation.
f. Requiring that agencies utilize secure protocols when transmitting sensitive information to prevent someone who gains access to the internal network from being able to "sniff," or capture usernames and passwords.
g. Implementing intrusion detection capabilities within internal networks where feasible.

Agency's Response *(i.e., agree, partially agree, disagree)*: **Agree**

Agency's Written Response in Audit Report:
Implementation Date: July 2013.

Many of the state internal networks were created before the Office of Cyber Security policy requirements stating that "all sensitive data is to be stored and processed on a LAN segment that is separated from end users through the use of a firewall or other access control mechanism" as well as that "security protocols are [to be] used to protect user login information to State systems." Through consolidation, the Office of Information Technology has inherited these State networks that do not comply with these security requirements. Mitigating these problems will require significant budget and human resources. Through the data center consolidation effort, agency server systems will be segmented from the agency end user workstation environments and provide some of the compliance mechanisms for this policy requirement. OCS will also be working with the Chief Technology Officer's office to develop guidance for agencies on proper network segmentation practices.

OCS will be requiring monthly vulnerability scanning in agencies which will assist in the identification of all unsecure protocol issues. These issues will be managed through the OCS Colorado Risk, Incident, & Security Compliance tool. OCS will ensure that proper patching and hardening practices are implemented within each agency through the Information Security Officers annual self-assessments and through monthly scanning. Where budget and resources permit, OCS will assist agencies in the implementation and monitoring of internal intrusion detection systems.

Status of Corrective Actions (To be provided by agency):
OCS is requiring quarterly/monthly vulnerability scanning in agencies, which will assist in the identification of all unsecure protocol issues. These issues will be managed through the OCS Colorado Risk, Incident, & Security Compliance (CRISC) tool. OCS will ensure that proper patching and hardening practices are implemented within each agency through the Information Security Officers annual self-assessments and through quarterly/monthly scanning. Where budget and resources permit, OIT will assist agencies in the implementation and monitoring of internal intrusion detection systems.

OCS will continue to address the segmentation issues through OIT initiatives and non-consolidated state agency initiatives.