Office of Cyber Security
Governor's Office of Information Technology

Performance Audit
November 2010

PUBLIC REPORT

OFFICE OF THE STATE AUDITOR

LEGISLATIVE AUDIT COMMITTEE
2010 MEMBERS

Senator David Schultheis
Chair

Senator Lois Tochtrop
Vice-Chair

Senator Morgan Carroll
Representative Jim Kerr
Representative Joe Miklosi
Senator Shawn Mitchell
Representative Dianne Primavera
Representative Mark Waller

OFFICE OF THE STATE AUDITOR

Sally Symanski
State Auditor

Dianne Ray
Deputy State Auditor

Jonathan C. Trull
Legislative Audit Manager

Annette Argo
Julie Chickillo
Reed Larsen
Rosa Olveda
Manjula Udeshi
Legislative Auditors

Coalfire Systems
Emagined Security
Contract Auditors

The mission of the Office of the State Auditor is to improve the efficiency, effectiveness, and transparency of government for the people of Colorado by providing objective information, quality services, and solution-based recommendations.

STATE OF COLORADO

Sally Symanski, CPA
State Auditor

OFFICE OF THE STATE AUDITOR
303.869.2800
FAX 303.869.3060

Legislative Services Building
200 East 14th Avenue
Denver, Colorado 80203-2211

November 22, 2010

Members of the Legislative Audit Committee:

This report contains the results of a performance audit of the Colorado Office of Cyber Security within the Governor's Office of Information Technology. The audit was conducted pursuant to Section 2-3-103, C.R.S., which authorizes the State Auditor to conduct audits of all departments, institutions, and agencies of state government. The penetration test performed as part of this audit was conducted with the permission of the Chief Information Security Officer pursuant to Section 24-37.5-403 (2)(d), C.R.S. The report presents our findings, conclusions, and recommendations, and the responses of the Office of Cyber Security and the Governor's Office of Information Technology.

Sally Symanski

This page intentionally left blank.

TABLE OF CONTENTS

Glossary of Terms and Abbreviations

Application-level Controls - controls incorporated directly into computer applications to help ensure the validity, completeness, accuracy, and confidentiality of data during application processing and reporting.

Attack - attempt to gain unauthorized access to an information system's services, resources, or information, or the attempt to compromise an information system's integrity, availability, or confidentiality.

Colorado Cyber Security Program - an information security framework established by House Bill 06-1157 and overseen by the Governor's Office of Cyber Security.

Computer Application or Application - a computer program or set of programs that perform the processing of records for a specific function. Examples of computer applications include Microsoft Office, Microsoft Excel, COFRS, and SAP.

Defense-in-depth - a commonly accepted "best practice" for implementing computer security controls in today's networked environment. Integrates people, operations, and technology capabilities to protect information systems across multiple layers.

Denial of Service Attack - an assault on a service from a single source that floods the service with so many requests that it becomes overwhelmed and is either stopped completely or operates at a significantly reduced rate.

Firewall - a router, server, or specialized hardware device designed to restrict access to one network from another network.

FTE - Full-time equivalent. An FTE of 1.0 means that the person is equivalent to a full-time worker, while an FTE of 0.5 signals that the worker is only half-time.

General Computer Controls - controls that relate to the environment within which computer-based applications are developed, maintained, and operated. The objectives of general computer controls are to ensure the proper development and implementation of computer applications and the confidentiality, integrity, and availability of program and data files.

HTTP - Hypertext Transfer Protocol. A networking protocol commonly used to communicate over the Internet or World Wide Web.

IDS - Intrusion Detection System. An automated system that inspects network activity to identify suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

Internet - When capitalized, the term "Internet" refers to the collection of networks and gateways that use the transmission control protocol/Internet protocol suite of protocols.

Intranet - a private network that uses the infrastructure and standards of the Internet and World Wide Web, but is isolated from the public Internet by firewall barriers.

IP Address - Internet Protocol Address. A numerical label assigned to computers and devices participating in a network, such as the Internet.

ISOC - Information Security Operations Center. The group within the Governor's Office of Cyber Security responsible for detecting and responding to threats against the State.

IT - Information technology.

IT Infrastructure - all information technology assets (hardware, software, data), components, systems, applications, and resources.

Modem - short for modulator-demodulator. A device that allows digital signals to be transmitted and received over analog telephone lines. This type of device makes it possible to link a digital computer to the analog telephone system. It also determines the speed at which information can be transmitted and received.

Network - A group of computers and associated devices that are connected by communications facilities.

OIT - Governor's Office of Information Technology. The state agency within the Governor's Office that is responsible for the administration, management, and oversight of state IT operations and systems.

Patch - additional pieces of code that have been developed to address specific problems or flaws in existing software.

Penetration Test - Security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation.

PII - Personally Identifiable Information**.** Refers to any information about an individual maintained by an entity, including any information that can be used to distinguish or trace an individual's identity, such as their name, social security number, date of birth, or biometric records, and any other information which is linked or linkable to an individual.

Port - an endpoint to a logical network connection.

Public Agency - According to Section 24-37.5-402(9), C.R.S., a public agency means every state office, whether legislative, executive, or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions. "Public agency" does not include institutions of higher education or the Department of Higher Education. For our purposes, our audit did not include the Legislative Branch.

Risk - the likelihood of a threat agent taking advantage of a vulnerability and the corresponding business impact.

Threat - any potential danger to information or systems.

Service - refers to customer or product-related business functions such as file transfer protocol (FTP), hypertext transfer protocol (HTTP), and mainframe supervisor calls.

Social Engineering - a method used by hackers to obtain passwords and other sensitive information. For example, a hacker may call an authorized user of a computer system and pose as a network administrator to gain access.

URL - Uniform Resource Locator**.** The address of a web page on the Internet – e.g., www.state.co.us.

Utilities - Software used to perform system maintenance routines that are frequently required during normal processing operations. Some utilities have powerful features that will allow a user to access and view or modify data or program code.

VPN - Virtual Private Network. A protected information system link that provides the same function as a secured, dedicated line by utilizing tunneling, security controls, and end-point address translation.

Vulnerability - a software, hardware, physical, or procedural weakness that could provide an attacker with unauthorized access to an entity's networks, systems, or data.

War Dialer - software packages that sequentially dial telephone numbers, recording any numbers that answer.

Wide Area Network - a group of computers and other devices dispersed over a wide geographical area that is connected by communications links.

Web Application - an application that is accessed via the web over a network such as the Internet or an intranet.

SALLY SYMANSKI, CPA
State Auditor

Office of Cyber Security
Governor's Office of Information Technology
Performance Audit
November 2010

Purpose and Scope

Our audit reviewed the Governor's Office of Cyber Security's progress in fulfilling the requirements of the Colorado Cyber Security Program (Section 24-37.5-401 through 406, C.R.S.). As part of the audit, we reviewed State Cyber Security Policies, Agency Cyber Security Plans, and Governor's Office of Information Technology (OIT) strategic plans and budget documents; interviewed personnel; surveyed other states' chief information security officers; and analyzed the Office of Cyber Security's processes and procedures related to security incidents. In addition, we contracted with a professional computer security firm to assist our staff in performing a covert penetration test of state networks, applications, and information systems. We performed audit work from February through November 2010.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Overview

State agencies routinely collect, process, and store personally identifiable information and data, including social security numbers, taxpayer identification numbers, driver's license and ID numbers, personal health information, wage information, and criminal history records. The State, as custodian of the public's data, is responsible for safeguarding the information it receives and for ensuring the confidentiality, integrity, and availability of state systems. In 2006 the General Assembly enacted House Bill 06-1157, creating the Colorado Cyber Security Program, which forms the foundation of the State's security control structure and reflects the General Assembly's commitment to address the security risks facing public agencies.

The Colorado Cyber Security Program is overseen by the Chief Information Security Officer, who is appointed by the Governor. The Colorado Cyber Security Program requires public agencies to annually develop an information security plan utilizing the information security policies, standards, and guidelines developed by the Chief Information Security Officer. In addition to the development of information security plans, the Colorado Cyber Security Program requires the Chief Information Security Officer to direct information security audits and assessments of public agencies, establish and direct a risk management process, conduct information security awareness training, coordinate

budget requests for information security systems, and work with the Colorado Commission on Higher Education related to information security planning and incident reporting. The Office of Cyber Security, administratively located within OIT, is responsible for execution of the Colorado Cyber Security Program. For Fiscal Year 2010, the Office of Cyber Security received spending authority for approximately $2.5 million in reappropriated funds and 17 full-time equivalent positions to carry out its responsibilities.

Key Findings

Colorado Cyber Security Program

According to statute [Section 24-37.5-403, C.R.S.], the Office of Cyber Security is responsible for the implementation of the Colorado Cyber Security Program and for the day-to-day management of the State's information security operations. Overall, we concluded that the Office of Cyber Security has failed to successfully implement the Colorado Cyber Security Program, as required by statute.

- **Agency Cyber Security Plans.** We found that 12 of 20 public agencies, or 60 percent, failed to submit statutorily-required information security plans to the Office of Cyber Security by the July 15, 2010 deadline. We also found that the Commission on Higher Education is not collecting, reviewing, and submitting to the Office of Cyber Security information security plans for institutions of higher education, as required by statute. Additionally, of the eight agency plans reviewed by the Office of Cyber Security as of September 15, 2010, only one was complete. We found that the plans of agencies are often inaccurate and fail to contain detailed and meaningful information.

- **Cyber Security Incidents.** Since 2006 the Office of Cyber Security has only received 43 cyber security incident reports, none of which were reported by institutions of higher education. Additionally, we identified seven data breaches that should have been reported to the Office of Cyber Security but were not. We also found that (1) staff responsible for incident response have generally not received sufficient training, (2) the State Incident Response Plan is outdated and contains inaccurate information, (3) agencies lack sufficiently detailed agency-level procedures for responding to cyber security incidents, and (4) the Office of Cyber Security lacks an electronic incident reporting and tracking system. We also identified one agency that failed to properly respond to a social engineering attack performed as part of our penetration test.

- **Colorado Cyber Security Program Requirements.** The Office of Cyber Security has not implemented significant requirements of the Colorado Cyber Security Program, such as directing information security audits and assessments in public agencies, conducting information security awareness and training programs, and coordinating public agency budget requests related to information security systems.

- **Strategic Planning and Management Oversight.** The Office of Cyber Security lacks a strategic plan for directing its operations, lacks any meaningful measures for assessing its performance, and does not have procedures to collect and analyze meaningful cyber security information. A lack of effective leadership within the Office of Cyber Security and a lack of oversight by the Governor's Office of Information Technology led to many of the problems identified in our audit.

Penetration Test Results

We assessed the State's information security posture or preparedness and exposure to cyber attacks by performing a covert penetration test of state networks and information systems. Overall, we determined that the State is at high risk of a system compromise and/or data breach by malicious individuals, including individuals both internal and external to the State.

- **Exposed Management Interfaces.** We were able, in several cases, to gain access to exposed management interfaces by using vendor default usernames and passwords or by guessing the username and password. The State has a significant number of management interfaces for firewalls, network devices, and web applications exposed directly to the Internet.

- **Default and Easily Guessable Usernames and Passwords.** We gained unauthorized access to systems and administrative interfaces by either guessing the correct username and password or by using vendor default credentials.

- **Unnecessary and Insecure Ports, Services, and Utilities.** We identified numerous IP addresses that appeared to be unused and with ports open that were running unneeded and outdated services. The State has a large Internet presence, including more than 17,600 active Internet Protocol (IP) addresses. Many of the State's servers are running vulnerable services that provide attackers an opportunity for exploitation.

- **Unsecured Web Applications.** We identified hundreds of vulnerabilities in state web applications, including many severe vulnerabilities that led directly to the systems' compromise. In several situations, we were able to take control of the database the application was using to disclose usernames and passwords and citizen data. We also found that application-level logs are not being monitored.

- **Internal Network Security.** We found that public agencies' internal networks are not properly segmented, internal systems are not hardened or patched, insecure network protocols are used for sensitive transactions, and most public agencies lack an internal intrusion detection system.

Our recommendations and the responses from the Governor's Office of Information Technology can be found in the Recommendation Locator and in the body of this report.

This page intentionally left blank.

RECOMMENDATION LOCATOR
Agency Addressed: Governor's Office of Information Technology

Rec. No.	Page No.	Recommendation Summary	Agency Response	Implementation Date
1	31	Re-evaluate and improve the Agency Cyber Security Plan (Plan) development, submission, and review process by (a) establishing additional guidelines and procedures for Plan completion, (b) providing training to agency information security officers on Plan creation and submission, (c) developing and implementing a policy that requires timely written feedback on submitted Plans, (d) reviewing all Plans submitted to the Office of Cyber Security and providing timely feedback, (e) holding agencies accountable for the timely submission of statutorily compliant Plans, (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 Plans into the Office of Cyber Security's strategic planning process, and (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.	Agree	July 2011

RECOMMENDATION LOCATOR
Agency Addressed: Governor's Office of Information Technology

Rec. No.	Page No.	Recommendation Summary	Agency Response	Implementation Date
2	37	Improve the State's incident identification, reporting, analysis, and response processes and procedures by (a) ensuring public agencies, including the Department 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 procedures in the State Incident Response Plan; (e) implementing an automated incident response reporting and tracking system and analyzing and reporting incidents to senior management; (f) performing incident response debriefings; and (g) updating incident response procedures to require that system administrators enforce password changes on accounts that are suspected of being compromised.	Agree	July 2011
3	42	Ensure 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, and (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.	Agree	July 2011

RECOMMENDATION LOCATOR
Agency Addressed: Governor's Office of Information Technology

Rec. No.	Page No.	Recommendation Summary	Agency Response	Implementation Date
4	45	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, include measurable objectives, and be communicated to information security staff and key stakeholders. Increase oversight of the Office of Cyber Security and ensure that an effective leadership structure is in place.	Agree	January 2011
5	54	Improve the security of the State's network and Internet-facing applications by (a) ensuring that the deficiencies identified in the confidential appendices provided under separate cover are 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 is only possible from inside the State's network, (d) revising State Cyber Security Policies to require that administrative interfaces not be directly accessible from the Internet, and (e) implementing firewall rules at the State gateway to filter incoming traffic bound for ports running administrative interfaces.	Agree	July 2011

RECOMMENDATION LOCATOR
Agency Addressed: Governor's Office of Information Technology

Rec. No.	Page No.	Recommendation Summary	Agency Response	Implementation Date
6	56	Ensure that all state systems, especially those exposed to the Internet, use strong passwords and non-default usernames by (a) ensuring that the deficiencies identified in the confidential appendices provided under separate cover are addressed, (b) performing routine vulnerability scans of state systems and networks, and (c) requiring that all new systems and network devices undergo the OIT approved hardening, or secure, process using the Center for Internet Security benchmarks.	Agree	July 2011
7	58	Reduce the State's exposure to attacks against unnecessary and insecure ports, services, and utilities by (a) ensuring that the deficiencies identified in the confidential appendices provided under separate cover are addressed, (b) reducing the overall Internet footprint of the State (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 that require Internet access, (e) defining the appropriate access rules for each inventoried asset, and (f) ensuring that all assets are protected by a monitored firewall.	Agree	July 2011

RECOMMENDATION LOCATOR
Agency Addressed: Governor's Office of Information Technology

Rec. No.	Page No.	Recommendation Summary	Agency Response	Implementation Date
8	60	Ensure that state web applications are appropriately secured by (a) ensuring that the 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 and correcting identified deficiencies, (d) ensuring that all newly designed web applications 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, and (g) ensuring IT staff are routinely reviewing and monitoring web application logs and reporting suspicious activity to appropriate staff.	Agree	July 2011
9	63	Improve the security of public agencies' internal networks by (a) ensuring that the deficiencies identified in the confidential appendices and provided under separate cover are addressed, (b) architecting internal networks so that they are "segmented" based upon access and security requirements, (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, and (g) implementing intrusion detection capabilities within internal networks where feasible.	Agree	July 2013

This page intentionally left blank.

Overview of the Colorado Cyber Security Program

Chapter 1

The State of Colorado's information systems and the information they contain and process represent significant assets and are critical to the State's ability to conduct business and achieve its mission of serving Colorado's citizens. State agencies routinely collect, process, and store personally identifiable information and data, including social security numbers, taxpayer identification numbers, driver's license and ID numbers, personal health information, wage information, and criminal history records. Colorado's citizens and those doing business with the State expect that the data they provide will be protected and only used for official purposes. Because of the potential monetary value of these data and their appeal to potential hackers for purposes such as identity theft or other illegal acts, the State is often the target of directed cyber security attacks by both trusted insiders (e.g., government employees and contractors) and groups and individuals external to the State.

The State, as custodian of the public's data, is responsible for safeguarding the information it receives and for ensuring the confidentiality, integrity, and availability of its systems. Understanding the threats facing Colorado's information systems and the State's responsibility to protect the public's data, the General Assembly enacted House Bill 06-1157 during the 2006 Legislative Session. The legislation, better known as the Colorado Cyber Security Program, was signed into law by the Governor in June 2006 and was codified in Part 4 of Article 37.5, Title 24 of the Colorado Revised Statutes. Most of the law's requirements apply only to public agencies. The law defines a "public agency" as "every state office, whether legislative, executive, or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions;" however, the Legislative Branch was not included within the scope of this audit. The law's definition of "public agency" does not include the Colorado Commission on Higher Education, Department of Higher Education, or institutions of higher education. We discuss the provisions of this law in the next section.

Colorado Cyber Security Program

The goal of the Colorado Cyber Security Program is to improve Colorado's information security posture by establishing a statewide information security

framework and governance model. The Colorado Cyber Security Program forms the foundation of the State's security control structure and reflects the General Assembly's commitment to address the security risks facing public agencies using a coordinated and risk-based approach. According to the legislation, the Colorado Cyber Security Program is overseen by the Chief Information Security Officer, who is appointed by the Governor. As specified in House Bill 06-1157, the strategic objectives for the Colorado Cyber Security Program are to:

- Protect the State's communication and information resources against unauthorized access, disclosure, use, and modification or destruction, whether accidental or deliberate, as well as ensure the confidentiality, integrity, and availability of information.

- Ensure that the information the public has entrusted to public agencies is safe, secure, and protected from unauthorized access, unauthorized use, or destruction.

- Secure the State's communication and information resources through a coordinated and shared effort from all departments, agencies, and political subdivisions of the State and a long-term commitment to providing state funding that ensures the success of such efforts.

- Promulgate and implement information security standards, policies, and guidelines throughout public agencies to ensure the development and maintenance of minimum information security controls to protect communication and information resources that support the operations and assets of those agencies.

The law requires public agencies to develop an information security plan utilizing the information security policies, standards, and guidelines developed by the Chief Information Security Officer. The first information security plan for each agency was to be created by July 1, 2007 and submitted to the Chief Information Security Officer on or before July 15, 2007. According to statute, the plans must include:

- Periodic assessments of the risk and magnitude of the harm that could result from a security incident.

- A process for providing adequate information security for the agency's information resources and communications.

- Regular security awareness training for employees and users of agency information resources.

- Periodic testing and evaluation of the effectiveness of information security for the agency, which shall be performed not less than annually.

- A process for detecting, reporting, and responding to security incidents consistent with the information security standards, policies, and guidelines issued by the Chief Information Security Officer.

- Plans and procedures to ensure the continuity of operations for information resources that support the operations and assets of the public agency in the event of a security incident.

The law allowed public agencies to establish a phase-in period to fully comply with the provisions of House Bill 06-1157. Specifically, all public agencies were required to be fully compliant with the provisions of the law, including implementation of all State Cyber Security Policies subsequently issued by the Chief Information Security Officer, by July 1, 2009.

Each year on or before July 15, the executive director or head of each public agency is to report to the Chief Information Security Officer on the development, implementation, and if applicable, compliance with the phase-in schedule of the public agency's information security plan.

Office of Cyber Security

The Office of the Chief Information Security Officer, better known as the Office of Cyber Security, is tasked with statewide information technology-related cyber security functions, including assessment, monitoring, process implementation, and execution of the Colorado Cyber Security Program. The Office of Cyber Security is designated as the single state source for cyber security readiness and awareness. Working closely with federal, state, local, and private sector partners, the Office of Cyber Security actively gathers and analyzes information on cyber threats and vulnerabilities that present risk to the State's information systems, networks, and applications or the critical information managed within them.

The Office of Cyber Security (Office) is located administratively within the Governor's Office of Information Technology (OIT) and led by the governor-appointed Chief Information Security Officer. The Office was formally established in 2006 and is responsible for administering the Colorado Cyber Security Program. For Fiscal Year 2007, the Office's first year of operation, a total of $4.2 million in federal funds and one full-time equivalent (FTE) position, the Chief Information Security Officer, was set aside for the Colorado Cyber Security Program. With the assistance of contractors, the Office of Cyber Security used the funds to upgrade the State's information security infrastructure and establish Colorado's first cyber security policies and standards. These funds

were also used to support security categorization and department-level risk assessments of critical systems, establish a compliance framework, and provide key security control mechanisms. Statewide cyber security training and a multi-agency cyber security incident response program were also developed.

As shown in the table below, for Fiscal Year 2010 the Office of Cyber Security received an appropriation for two FTE, including the Chief Information Security Officer and Deputy Chief Information Security Officer positions, and approximately $2.5 million in reappropriated funds. However, the Office of Cyber Security does not have a dedicated funding source and is required to charge public agencies for its activities in administering the Colorado Cyber Security Program or use other available funds, such as grant funds and federal dollars. Therefore, as seen in the bottom half of the table below, the Office of Cyber Security's annual expenditures are often much less than that year's appropriation.

Colorado Office of Cyber Security
Appropriations, Expenditures, and Full Time Equivalents (FTE)
Fiscal Years 2007 - 2010

	Fiscal Year 2007		Fiscal Year 2008		Fiscal Year 2009		Fiscal Year 2010	
Funding Source	**Approp.**	**FTE**	**Approp.**	**FTE**	**Approp.**	**FTE**	**Approp.**	**FTE**
General Fund	$0	1.0	$0	2.0	$350,000	2.0	$0	2.0
Reappropriated funds[1]	4,200,000		2,450,000		2,455,000		2,459,000	
Total	$4,200,000		$2,450,000		$2,805,000		$2,459,000	

	Fiscal Year 2007	Fiscal Year 2008	Fiscal Year 2009	Fiscal Year 2010
Expenditures	$2,968,000	$1,202,000	$950,000	$429,000
Expenditures as a Percentage of Appropriation	71%	49%	34%	17%

Source: OSA analysis of State of Colorado budget documents and appropriation bills.
[1]Cash exempt funds were reclassified as reappropriated funds as of Fiscal Year 2009.

Senate Bill 08-155 requires that all IT-related functions, systems, and staff within the Executive Branch be consolidated within OIT. As part of the consolidation of state IT, the Office of Cyber Security received management authority for 15 FTE for Fiscal Year 2011 through the transfer of security staff from public agencies. These additional positions will be funded through the Network Services group within the OIT appropriation. The Network Services group plans, coordinates, integrates, and provides telecommunication capabilities and network solutions for state agencies and local governments. Within OIT, IT security staff represent approximately 3 percent of all Executive Branch IT staff.

Organization and Reporting Structure

Prior to July 2010, the Office of Cyber Security implemented the requirements of the Colorado Cyber Security Program through a federated or decentralized model. Agency personnel serving as information security officers did not work for or report to the Chief Information Security Officer. Agency information security officers continued to report to their agencies' management teams and carried out their duties with little oversight from the Office of Cyber Security. With the passage of Senate Bill 08-155, however, that reporting structure has changed significantly. As of July 1, 2010, Executive Branch information security officers and other Executive Branch staff performing security functions within their agencies were transferred to the Office of Cyber Security and now report directly to the Chief Information Security Officer. For Fiscal Year 2011, the Office of Cyber Security is now comprised of 17 FTE, including the vacant Deputy Chief Information Security Officer position. Senate Bill 08-155 also changed the reporting structure for the Chief Information Security Officer. Instead of reporting to the Governor, the Chief Information Security Officer now reports to the State Chief Information Officer (State CIO), the administrative head of OIT.

It also important to point out that the consolidation of state IT only affected Executive Branch agencies. However, the Colorado Cyber Security Program and the Chief Information Security Officer's responsibilities apply to public agencies as defined in Section 24-37.5-402(9), C.R.S., including the Judicial and Legislative Branches, Secretary of State, and Offices of the State Treasurer and Attorney General, and excluding institutions of higher education and the Department of Higher Education. Although these public agencies' systems are not under the Chief Information Security Officer's direct control, the Chief Information Security Officer can remove public agencies' systems from the state network under certain conditions, such as identification of severe vulnerabilities or a compromise that could impact other state systems. Additionally, the Colorado Commission on Higher Education has certain reporting requirements to the Chief Information Security Officer.

The organizational chart on page 17 shows the current structure of the Colorado Office of Cyber Security, including relevant lines of authority. The Office of Cyber Security is divided into three functional groups, each overseen by a supervisory staff person who reports to the Chief Information Security Officer. The three groups, including their responsibilities, are:

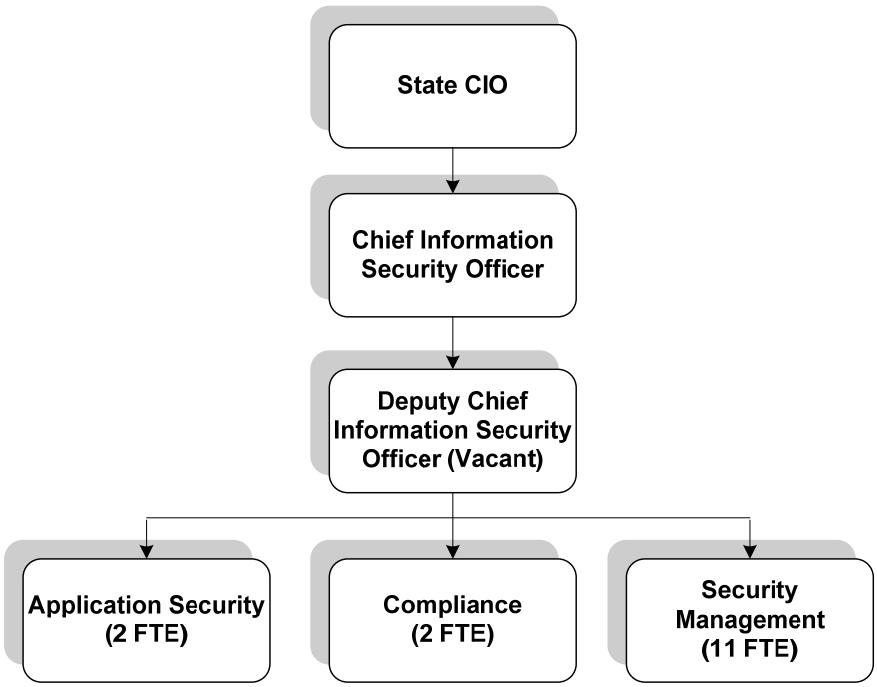
- **Compliance**. The compliance group contains two FTE and is responsible for assisting public agencies in achieving compliance with Colorado Cyber Security Policies and other applicable government and industry regulations, such as the Health Insurance Portability and Accountability Act's Security Policy or the Payment Card Industry's security requirements. The compliance group also tracks all IT audit and

compliance review findings identified by federal auditors and the Office of the State Auditor, and it works with the appropriate staff to ensure that remediation occurs in a timely manner. The compliance group does not perform IT audits or compliance reviews.

- **Security Management.** The security management group is the largest component of the Office of Cyber Security, totaling 11 FTE. The security management group includes the Colorado Information Security Operations Center (ISOC), which is responsible for detecting and responding to threats against the State's wide area network, and the information security officers assigned to handle the security requirements of all Executive Branch agencies. Through the ISOC, the security management group is responsible for network logging and monitoring related to the State's wide area network, uniform resource locator (URL) filtering, virtual private network (VPN) access provisioning, security architecture design and support, and incident identification and response.

- **Application Security.** The application security group is comprised of two staff who are responsible for ensuring that the State's web applications are securely designed. This group trains application developers on the principles of secure coding, reviews the development of state applications for compliance with secure coding principles, and is in the process of mapping and categorizing all state web applications.

Colorado Office of Cyber Security
As of October 2010



Source: Office of Cyber Security.

History and Milestones

Since its creation in 2006, the Office of Cyber Security has undergone significant organizational and leadership changes, including changes related to the consolidation of Executive Branch IT resources and staff. The bullets below identify the major organizational changes impacting the Office of Cyber Security.

- **June 2006**. Colorado Cyber Security Program is established with the enactment of House Bill 06-1157.

- **July 2006**. Office of Cyber Security is created within the Governor's Office. State's first Chief Information Security Officer is appointed by the Governor and reports directly to the Governor.

- **2006—2008**. Contract staff are hired to assist the Chief Information Security Officer in implementing the Colorado Cyber Security Program. The ISOC (including all staff) is transferred from the

Division of Information Technologies within the Department of Personnel & Administration to the Office of Cyber Security.

- **May 2008.** Resignation of the Chief Information Security Officer; duties assigned to contractors.

- **July 2008.** Senate Bill 08-155 moves the Office of Cyber Security under OIT, and the Chief Information Security Officer reports to the State CIO.

- **November 2008.** Appointment of new Chief Information Security Officer by the Governor.

- **June 2010**. Chief Information Security Officer resigns; duties assumed by the Deputy Chief Information Security Officer.

- **July 2010.** Executive Branch IT staff are consolidated under OIT. 15 FTE are transferred from state agencies to the Office of Cyber Security.

Cyber Security Threats and Trends

Research and data collected from information security research institutes and data privacy clearinghouses indicate that the number and sophistication of attacks against state government systems are increasing. According to a recent study conducted by Deloitte & Touche, LLP, on behalf of the National Association of State Chief Information Officers, more than one-fifth of reported data breaches in 2009 occurred in the state and local government sectors. Additionally, a recent study published by HP TippingPoint DVLabs and Qualys, which are computer security organizations that analyze vulnerabilities and develop appropriate countermeasures, showed that the government sector is the most targeted industry for several types of devastating attacks, including malicious Javascript and PHP "file include" attacks. Javascript attacks occur when an attacker induces a user, usually through a link in an email, to launch or run malicious Javascript-computer code on the user's computer. Based on the code run, the attacker may gain control of the user's browser or computer or obtain direct access to the user's login credentials. PHP file include attacks occur when attackers upload malicious PHP code onto a server. The uploaded PHP code is then automatically run by the web server and typically provides the attacker with complete control of the server or with access to databases and sensitive configuration files.

Attackers know that public agencies possess a significant amount of valuable data, and evidence shows that they are focused on obtaining it. The National Governors Association recently issued the following statement regarding the cyber security threat faced by state governments:

> One of our critical infrastructure assets, our state networks, are attacked on a daily basis. The failure to secure these networks has serious implications for national security, including continuity of government, the operations of critical infrastructure and the health, safety, and general welfare of citizens. Cyber attacks have disrupted state government networks, systems and operations, and potentially could impact first-responder communications during an attack on our homeland.

To understand the complexities involved in securing state systems and networks, it is first important to understand the threats that states confront and where those threats originate. A typical data breach originates from more than one type of vulnerability, and several kinds of attacks are used. For example, social tactics, such as eavesdropping on a conversation, may have been used to learn the operating system of a critical server. This valuable information could then be used by the attacker to build custom malware that avoids detection by anti-virus software, latches onto the vulnerable server, and proceeds to collect and transmit thousands of records back to the attacker.

The 2010 Verizon Data Breach Investigations Report provides helpful information for understanding the origination and responsible parties for data breaches. The analysis contained in the 2010 Verizon Data Breach Investigations Report consists of all confirmed data breaches investigated by Verizon and the United States Secret Service during 2009, including cases occurring both in the United States and internationally and both within government and private sector agencies. As the table on the following page indicates, this report found that the most common attack that resulted in a data breach was privilege misuse. Privilege misuse occurs when a trusted insider or former employee improperly uses his or her access to obtain confidential information for personal gain. Several of the data breaches noted in the study occurred when former system administrators or employees used known credentials to log into company systems and steal information they no longer had permission to view or obtain. Privilege misuse was the primary method used by a former Colorado Department of Revenue tax examiner to steal more than $10 million from the State. While employed at the Department, the employee misused the system credentials of other staff to perpetrate the fraud.

After privilege misuse, hacking and malware-based attacks are responsible for a significant number of data breaches and for the largest number of records compromised per breach. These attacks are typically coordinated and carried out by individuals or groups external to the agency attacked. The table below shows the most common types of attacks or threats that led to successful data breaches in 2009, according to investigations conducted throughout the world by Verizon and the United States Secret Service.

Origination of Data Breaches Investigated Throughout the World by Verizon and the United States Secret Service in 2009	
Origin of Breach	**Percentage of Total Breaches[1]**
Privilege Misuse	48
Hacking	40
Malware	38
Social Tactics	28
Physical Attacks	15

Source: Verizon 2010 Data Breach Investigations Report conducted by Verizon in coordination with the United States Secret Service.

[1]Percentages do not total 100 percent because there can be multiple reasons for a data breach.

One of the common misperceptions about information security is that an organization only needs to protect itself from outsiders or individuals external to its business. This concept is wrong for several reasons and could prove disastrous if used to build a perimeter-based security program—a program focused only on securing an organization's external network through firewalls and other networking equipment. First, as the table below demonstrates and as Colorado has experienced, insiders represent a significant threat to information security. In data breaches investigated by Verizon and the United States Secret Service in 2009, 48 percent resulted from actions by an insider, and another 11 percent were due to the actions of a business partner or contractor.

Responsible Parties for Data Breaches Investigated Throughout the World by Verizon and the United States Secret Service in 2009	
Responsible Party	**Percentage of Total Breaches[1]**
External Agents	70
Insiders (Employees)	48
Business Partners/Contractors	11
Multiple Parties	27

Source: Verizon 2010 Data Breach Investigations Report conducted by Verizon in coordination with the United States Secret Service.

[1]Percentages do not total 100 percent because multiple answers could apply to each breach.

Another reason to protect IT resources from both external and internal threats is that many of today's client-based attacks (attacks against client software such as Internet Explorer, Mozilla Firefox, and Adobe Acrobat) allow external parties to

gain access to an agency's internal network. Basically, with these types of attacks, the outsider becomes a trusted insider. All it takes for these client-side attacks to succeed is for an employee to make a poor decision and browse to a malicious website. Once the attacker latches onto or takes control of the employee's web browser, the attacker can then scan and attack the internal network just as if he or she were sitting inside the agency. Perimeter-based defenses such as firewalls are ineffective against these types of attacks.

In addition to these trends, the study published by HP TippingPoint DVLabs and Qualys identified the following common threats to IT systems in 2010:

- Web applications continue to be highly attractive targets and are constantly scanned and persistently attacked.
- Attackers have become more organized, sophisticated, and persistent.
- Increased use of social media and free software by employees has created new avenues for attack.
- Evolving technology and business processes like cloud computing, virtualization, and outsourcing bring new challenges to information security, including many that are not yet known.
- Legacy attacks such as viruses, phishing and pharming, zombie networks, SQL injection, and operating system-level vulnerabilities continue to be exploited quickly if proper security mechanisms are not followed.

Because of the diversity, nature, and source of the threats, information security touches on all aspects of a business or government organization, including not only technological controls but also controls related to personnel, physical security, contracting, and vendor management. To be effective, information security must not only involve technical tools such as firewalls and scanners but also focus on process improvement, training, and awareness. Finally, in today's risk environment, a security program must account for both internal and external threats and implement a layered or defense-in-depth security framework. A defense-in-depth security framework involves hardening (i.e., securing) not only the perimeter of an agency's network but also the internal network, including user computers, client software, intranets, and internal applications.

Audit Scope

This audit reviewed the Governor's Office of Cyber Security's progress in fulfilling the requirements of the Colorado Cyber Security Program (Section 24-37.5-401 through 406, C.R.S.). As part of the audit, we reviewed State Cyber

Security Policies, Agency Cyber Security Plans, and OIT strategic plans and budget documents; interviewed appropriate management, supervisory, and state information security staff; and surveyed other states' chief information security officers. Additionally, we performed a detailed analysis of the Office of Cyber Security's incident identification, reporting, and handling processes and procedures.

In conjunction with our review of the Office of Cyber Security, we contracted with a professional computer security firm to assist our staff in performing a covert penetration test of state networks, applications, and information systems. Penetration testing is a form of security testing in which evaluators attempt to circumvent the security features of systems to gain unauthorized access to data and systems. Our testing was authorized by Colorado's Chief Information Security Officer and management officials within the Governor's Office, Judicial Branch, Secretary of State's Office, Office of the State Treasurer, and Attorney General's Office.

Our testing was focused on Internet protocol (IP) addresses and systems owned and operated by a public agency, defined in Section 24-37.5-402(9), C.R.S. as "every state office, whether legislative, executive, or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions." The Legislative Branch was not included in the scope of this audit. A public agency as defined in this section does not include institutions of higher education or the Department of Higher Education. Some of the specific information systems tested included:

- Colorado Financial Reporting System (COFRS)
- Colorado Personnel and Payroll System (CPPS)
- GenTax (the Department of Revenue's tax system)
- Colorado Unemployment Benefits System (CUBS)
- Colorado Automated Tax System (CATS)
- Colorado Benefits Management System (CBMS)
- County Financial Management System (CFMS)
- Colorado Electronic Benefit Transfer System
- Veteran's Nursing Home Information System

- Medicaid Management Information System (MMIS)
- Colorado Crime Information Center (CCIC)

Because under House Bill 10-1401 the Office of the State Auditor does not have authority until August 2011 to audit the Statewide Internet Portal Authority (Authority), which is responsible for the management of the *colorado.gov* portal, no state applications hosted or housed by the Authority (such as the Colorado Online Tax Payment System) were included within the testing.

The remainder of our report is divided into two chapters. In Chapter 2 we discuss the steps the Office of Cyber Security should take to fully implement the Colorado Cyber Security Program and better secure state systems and data from unauthorized access. In Chapter 3 we provide the high-level, summarized results of the covert penetration test we performed against state systems and networks. That chapter also contains broad findings and recommendations that apply to most public agencies we tested. Due to the sensitive nature of the specific findings identified during testing, only summarized findings and recommendations are included in Chapter 3. The detailed, technical findings and recommendations are included in the appendices to this report that have been provided to the Office of Cyber Security, the Office of Information Technology, and affected public agencies. These appendices are confidential and not available to the public as authorized by the Open Meetings Law in Section 24-6-402(3)(a)(IV), C.R.S., and Public Records Law in Section 24-72-204(2)(a)(VIII), C.R.S. (2010).

This page intentionally left blank.

Colorado Cyber Security Program

Chapter 2

As previously discussed, the Colorado Cyber Security Program was established by the General Assembly in 2006 to ensure the confidentiality, integrity, and availability of state computer systems and protect the public's information entrusted to public agencies. The establishment of a single organization to coordinate and manage information security throughout the state government was key to the effective implementation of the Colorado Cyber Security Program. According to statute [Section 24-37.5-403, C.R.S.], the Office of Cyber Security is responsible for the implementation of the Colorado Cyber Security Program and for the day-to-day management of the State's information security operations.

As discussed in Chapter 3, we conducted a penetration test of public agencies and found significant vulnerabilities throughout state government that allowed the assessment team to compromise thousands of records containing individuals' confidential information, such as social security numbers, birth dates, and income levels. The assessment team also compromised several state networks and systems and identified hundreds of vulnerabilities in state systems. Based on the results of our penetration test, prior information technology audits, and our review of the implementation of the Colorado Cyber Security Program during this audit, we concluded that the Office of Cyber Security has failed to successfully implement the Colorado Cyber Security Program, as specified by statute. As such, the State and the information it receives from the public is at considerable risk of compromise unless significant changes are made.

In the following sections, we discuss specific areas where improvements are necessary to implement the State's Cyber Security Program.

Agency Cyber Security Plans

State statute [Section 24-37.5-404, C.R.S.] requires that all public agencies develop an information security plan, known as an Agency Cyber Security Plan (Plan), based on policies, standards, and guidelines established by the Chief Information Security Officer. The Plans are designed to help public agencies control the risks associated with access, use, storage, and sharing of sensitive information from the public and state electronic information and provide a mechanism for the Office of Cyber Security to use in determining an agency's compliance with the Colorado Cyber Security Program requirements. According to rules promulgated by the Chief Information Security Officer, each public

agency must submit a completed Plan to the Office of Cyber Security by July 15 of each year.

Pursuant to the rules promulgated by the Chief Information Security Officer, each public agency is to submit annually a Plan that contains the following components:

- **Cover letter requesting Plan approval**. An assertion signed by the Executive Director that either states that the agency is compliant with the Colorado Cyber Security Program or that the agency's Plan of Actions and Milestones, a corrective action plan, contains active initiatives that will bring the agency into compliance.

- **Agency Cyber Security Plan**. The agency's detailed Plan for implementing the Colorado Cyber Security Program and complying with State Cyber Security Policies.

- **Agency-Wide Risk Assessment**. An assessment that determines the extent of the potential threats and risks associated with an agency's information technology environment.

- **Agency Disaster Recovery Plan Summary**. An executive-level summary of the agency's detailed disaster recovery plan.

- **Agency Disaster Recovery Plan Test Results**. Results of the most recent disaster recovery tests performed by the agency.

- **Agency Self-Assessment Results**. Results from an annual self-assessment, which is designed to validate the security controls identified in the Agency Cyber Security Plan. The self-assessment should include vulnerability assessments, penetration tests, agency policy gap analysis, and security awareness training statistics.

- **Agency Cyber Security Plan of Action and Milestones**. A high-level plan that describes the cyber security initiatives underway to bring the agency into compliance with the Colorado Cyber Security Program.

The Chief Information Security Officer is responsible for reviewing the Plans to determine if they adhere to State Cyber Security Policies and to assess the agencies' progress in implementing the Colorado Cyber Security Program. Upon completion of his or her review, the Chief Information Security Officer is to issue one of three responses to the public agency:

- The Plan is <u>approved</u> with no changes necessary.

- The Plan is conditionally approved, with the requirement to implement, continue, or complete the initiatives in the Agency Plan of Actions and Milestones. Additionally, the Chief Information Security Officer may add additional requirements to the Plan of Actions and Milestones.

- The Plan is denied approval. If disapproved, the Chief Information Security Officer has the authority pursuant to Section 24-37.5-404(4), C.R.S., to remove the agency's connection to the State's wide area network, thereby removing the agency's ability to conduct business over the Internet.

We reviewed the Plan submission and review process for the July 15, 2010, reporting cycle and analyzed each public agency's Plan, if submitted. As shown in the table below, of the 20 public agencies required to submit plans to the Office of Cyber Security, we found that 12, or about 60 percent, had failed to submit the Plans by July 15, 2010. As of November 1, 2010, eight agencies had still not submitted Plans to the Office of Cyber Security.

Evaluation of Agency Cyber Security Plans
Public Agencies that Failed to Submit Plans by July 15, 2010

Public Agencies	Date Plan Submitted to the Office of Cyber Security
Department of Agriculture	July 27, 2010
Department of Healthcare Policy and Financing	November 9, 2010
Department of Labor and Employment	July 20, 2010
Department of Law	Not submitted
Department of Natural Resources	November 9, 2010
Department of Personnel & Administration	Not submitted
Department of Public Safety	July 23, 2010
Department of Regulatory Agencies	Not submitted
Department of Revenue[1]	September 21, 2010
Department of Treasury	Not submitted
Judicial Branch	Not submitted
Office of the Governor	Not submitted

Source: Office of the State Auditor analysis of information provided by the Office of Cyber Security.

[1] The Department of Revenue's Plan did not include information pertaining to the Colorado Lottery, which is located administratively within the Department.

Additionally, of the eight agencies whose Plans had been reviewed by the Office of Cyber Security as of September 15, 2010, only one agency's Plan, the Department of Human Services, contained all of the required components. Each component of the Plan is important, as one area supports another. For example, an agency should complete a thorough self-assessment to identify areas that need to be included in its annual risk assessment. Both the self-assessment and risk

assessment must be completed to prepare an accurate Plan of Actions and Milestones.

In the following table, for the eight agencies whose Cyber Security Plans were reviewed by the Office of Cyber Security as of September 15, 2010, we identified the number and percentage of the seven required components that were not submitted by each agency. As the table shows, the Departments of Labor and Employment and Local Affairs submitted Plans that were missing five of the seven required components, or were 71 percent incomplete. The Departments of Corrections, State, and Transportation submitted Plans that were missing three of the seven required components, or were 43 percent incomplete. Of the eight plans reviewed by the Office of Cyber Security, all contained the actual security Plan and Plan of Actions and Milestones. However, the majority of submitted plans failed to include a cover letter signed by the agency's Executive Director, a disaster recovery plan summary, and the most recent results from the agency's disaster recovery tests and self-assessments.

Evaluation of Agency Cyber Security Plans
Reviewed for Fiscal Year 2011
As of September 15, 2010

Public Agency	Number of Required Components Not Submitted[1]	Percentage of Required Components Not Submitted
Department of Corrections	3	43%
Department of Education	2	29
Department of Human Services	0	0
Department of Labor and Employment	5	71
Department of Local Affairs	5	71
Department of Public Health and Environment	2	29
Department of State	3	43
Department of Transportation	3	43

Source: Office of the State Auditor analysis of information provided by the Office of Cyber Security.

[1] Plan requirements are based on rules promulgated by the Chief Information Security Officer and include (1) Signed Cover Letter, (2) Updated Security Plan, (3) Updated Risk Assessment, (4) Disaster Recovery Plan Summary, (5) Disaster Recovery Plan Test Results, (6) Updated Self-Assessment Results, and (7) Plan of Actions and Milestones.

In addition to the lack of timely and complete submissions, we found that the Plans of agencies are often incomplete, inaccurate, and lacking in detailed and meaningful information. Specifically, we found that the Plans we reviewed were missing information on critical information systems and were so general as to be

meaningless. Additionally, we found that control gaps agencies noted in the risk assessments lacked specific remediation dates, and items agencies noted in the Plan of Actions and Milestones documents did not appear to have direct correlations to these control gaps. The Plan of Action and Milestones should include all control gaps noted in an agency's risk assessment to ensure that agency management is aware of the deficiencies and that a plan is in place to remediate the problems.

We also found that the Office of Cyber Security has not effectively utilized the information contained in the agency Plans for strategic planning purposes. To obtain greater value from the Plans, it is important that the information be used for strategic planning and budgeting purposes. For example, if most agencies report that they lack an effective intrusion detection system, then it may be appropriate for the Office of Cyber Security to make the procurement of an integrated intrusion detection system a strategic priority. Additionally, the Office of Cyber Security should consider developing a plan for implementing compensating controls until a system can be procured and implemented. We address the lack of strategic planning later in this chapter.

We met with agency information security officers, Office of Cyber Security management staff, and other IT personnel to determine the cause for the problems we identified with agency Plans. Through these discussions, we learned that many agency staff consider the Agency Cyber Security Plan development and submission process to be an unfunded mandate, confusing, and overly time consuming. Others also suggested that the Plan provides very little assurance that an agency is complying with the Colorado Cyber Security Program and takes time that would be better spent actually securing state systems and networks. Agency staff expressed frustration with the fact that the Office of Cyber Security has not established sufficient guidelines for completing each of the Plan's components, fails to provide feedback to agencies once the Plan is submitted, and does not take enforcement action against those agencies that fail to submit complete Plans. As such, many of those we spoke with indicated that the Plan development and submission process is not taken seriously and is simply seen as a "box that needs to be checked."

Our audit confirmed many of the issues identified by agency staff. For example, the Office of Cyber Security has not issued guidance on the completion of Agency Cyber Security Plans, risk assessments, self-assessments, Plans of Actions and Milestones, and disaster recovery planning. Also, until this year, the Office of Cyber Security had not established a process for reviewing and scoring submitted Plans for compliance with Colorado Cyber Security Policies. Additionally, the Office of Cyber Security has not provided formal feedback or responded to agencies on the submission of their Plans since 2007. Finally, the Office of Cyber Security has not taken enforcement action against any of the agencies that have either failed to submit Plans or continue to submit incomplete Plans.

Higher Education

As noted earlier, neither the Department of Higher Education nor institutions of higher education are defined as public agencies by the Colorado Cyber Security Program and are therefore not required to adhere to the policies, standards, and guidelines established by the Chief Information Security Officer. However, statute [Section 24-37.5-404.5, C.R.S.] requires that the Department of Higher Education and each institution of higher education, in coordination with the Colorado Commission on Higher Education (Commission), develop an information security plan. Similar to public agencies, the institutions' plans can contain a phase-in period not to exceed three years. The plans are to be submitted to the Commission by July 1 of each year for review and comment. The Commission is then required to submit the plans to the Chief Information Security Officer and report on the development, implementation, and, if applicable, compliance with the phase-in schedule of the information security plan for each institution.

We found that with the exception of the Colorado Historical Society, the Department of Higher Education has never submitted a Plan. Additionally, we met with officials from the Department of Higher Education and Office of Cyber Security and found that the information security plans for institutions of higher education are not being consistently collected, reviewed, and shared with the Office of Cyber Security. Of the 24 public institutions of higher education in Colorado, the Department of Higher Education had not received any security plans for 2010 as of October 15, 2010. According to Department of Higher Education officials, the Department has never submitted information security plans for these institutions to the Office of Cyber Security, nor has it been contacted by the Office of Cyber Security to do so. Neither the Department nor the Office of Cyber Security has developed the necessary processes and procedures to comply with this component of the Colorado Cyber Security Program.

Improvements

To ensure that Agency Cyber Security Plans are prepared and submitted according to statutory requirements, the Governor's Office of Information Technology needs to work with the Office of Cyber Security to make several improvements. First, the Office of Cyber Security needs to establish additional guidelines and procedures for the completion of the Agency Cyber Security Plan. Once the guidelines and procedures are finalized, the Office of Cyber Security should provide training to information security officers and relevant agency staff on the proper development and submission of the Plan. Second, the Office of Cyber Security needs to develop the necessary processes to ensure that Agency Cyber Security Plans are reviewed in a timely manner. As part of the review process, Office staff need to ensure that all control gaps listed in the agencies' risk

assessments are included in the Plans of Actions and Milestones. If necessary, the Office of Cyber Security should add actions and work steps to agencies' Plans of Actions and Milestones to ensure all control gaps are being addressed.

Third, at the conclusion of the review process, the Office of Cyber Security should provide written feedback on its evaluation of the Plans to state agency executive management. To ensure adjustments to Plans can be made in a timely manner, the Office of Cyber Security should establish a policy that requires written feedback to be delivered to public agencies within a reasonable period of time—e.g., within 45 days. Additionally, the Office of Cyber Security should clearly communicate the changes that are necessary to bring the Plan into compliance with State Cyber Security Policies. Fourth, the Office of Cyber Security should work with the State Chief Information Officer to hold agencies and information security officers accountable for the timely submission of Agency Cyber Security Plans. Fifth, the Office of Cyber Security should use the agencies' Cyber Security Plans as input for its strategic planning process. Finally, the Office of Cyber Security needs to work with the Commission on Higher Education to ensure that the security plans developed by institutions of higher education are received and reviewed annually.

Recommendation No. 1:

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.

Governor's Office of Information Technology Response:

Agree. 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 (OCS) 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 (OIT), 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.

Cyber Security Incidents

The timely identification and reporting of cyber security incidents is a critical component of an effective cyber security program. Research shows that the longer an incident goes undetected or unreported, the greater the damage is to information resources and the more significant the loss of data. State statute [Section 24-37.5-405 and Section 24-37.5-404.5(2)(e), C.R.S.] and State Cyber Security Policies require public agencies and institutions of higher education to report all cyber security incidents to the Office of Cyber Security. A cyber security incident is defined as an accidental or deliberate event that results in or constitutes an imminent threat of unauthorized access, loss, disclosure, modification, disruption, or destruction of communications and information resources. Examples of cyber security incidents include malicious code found on agency servers, viruses, missing or stolen computer equipment, and the unintentional disclosure of protected information to unauthorized persons through email, fax, or phone.

The Office of Cyber Security depends on the timely and accurate reporting of incidents for several reasons. First, the Office of Cyber Security is charged by statute with directing and managing appropriate responses to cyber security incidents that affect state information systems. The Office of Cyber Security has access to trained staff and contractors who can be deployed based on the type and severity of the incident. Additionally, the Office of Cyber Security has experience and training for properly handling all phases of an incident. Second, the Office of Cyber Security needs to be aware of all incidents occurring within state systems to determine if a coordinated attack against state government is underway. Although an agency may believe that an incident it identified is isolated, it may actually be the first phase of a more sophisticated attack against other public agencies. Finally, incident reports provide information needed by the Office of Cyber Security to accurately assess the threats facing state government so that proper mitigation strategies can be devised and implemented.

Incident Reporting

To determine if the Office of Cyber Security is receiving reports of all incidents identified, we analyzed the incidents reported to the Office of Cyber Security between October 2006 and September 2010, interviewed state IT staff, and monitored the number of reports generated from our penetration testing activities. Overall, we concluded that the Office of Cyber Security is not receiving reports of all cyber security incidents that are affecting state government and public institutions of higher education. First, as indicated by the table below, the Office of Cyber Security has received reports of 43 incidents in the last four years. The majority of these reports occurred in 2007 and 2008. Based on our knowledge of state operations, industry trends and statistics, and discussions with Office of Cyber Security staff, 43 reported incidents in four years is low and likely does not include all incidents occurring and detected within state information systems.

Cyber Security Incident Reports Reported by Pubic Agencies 2006 -2010[1]

Year[1]	Number of Agencies Reporting	Number of Reported Incidents
2006	1	1
2007	9	9
2008	13	26
2009	3	3
2010	4	4
Total Incidents Reported		43

Source: Office of the State Auditor analysis of Office of Cyber Security incident data.
[1] Data available for October 2006 through September 2010.

Second, of the 43 incidents reported to the Office of Cyber Security, none was reported by institutions of higher education. It is improbable that institutions of higher education have not had a cyber security incident in the last four years; therefore, such incidents are likely occurring but not being reported to the Office of Cyber Security, as required by statute. Third, we estimate that our penetration testing activities should have generated approximately 40 to 60 incident reports over the last six months. The Office of Cyber Security, however, only received four reports unrelated to our penetration testing over the six month period of April through September 2010. Additionally, during testing we became aware of an existing and ongoing incident at one agency that had never been reported to the Office of Cyber Security. Finally, we analyzed the data breaches reported in the media and on the Privacy Rights Clearinghouse website, a clearinghouse for collecting information on known data breaches, and compared those breaches involving public agencies and institutions of higher education to the incidents reported to the Office of Cyber Security. We identified seven data breaches that

should have been reported to the Office of Cyber Security but were not. Some of these breaches resulted in the exposure of personal information.

We identified the following reasons for the low number of security incidents reported to the Office of Cyber Security:

- Some agency staff reported that they do not believe it is necessary or important to report commonly occurring or "routine" incidents, such as viruses and unsuccessful attacks—e.g., multiple failed attempts to log on to a server or network device.

- The Office of Cyber Security has not established the necessary processes, procedures, and working relationships with the Department of Higher Education and public institutions of higher education to obtain incidents occurring within those environments.

- Agencies outside of the Executive Branch are reluctant to submit incidents to the Office of Cyber Security. These agencies believe sharing such information is an infringement on the separation of powers principle of state government.

- The State's intrusion detection capabilities are not sufficient for detecting many types of cyber security incidents. Due to the sensitive nature of these deficiencies, we included the details within the confidential appendices of this report.

Incident Response and Analysis

Once an incident is detected and reported, it is important that a coordinated and professional response occur. Failure to properly respond to an incident can result in increased system damage and downtime, as well as the inability to prosecute the attacker due to inadequate and inadmissible information or evidence. Proper incident response requires knowledgeable and trained staff and updated and detailed procedures and plans. Additionally, cyber security incidents should be tracked and analyzed to determine the most common targets and types of attacks launched against the State.

Statute [Section 24-37.5-405, C.R.S.] provides the Chief Information Security Officer with the authority to coordinate the State's response to cyber security incidents, including, if necessary, entering into contracts with private persons or entities to assist state staff in resolving incidents. The Chief Information Security Officer also has the authority to temporarily discontinue or suspend the operation of a public agency's communication and information resources in order to isolate the source of a security incident. We reviewed the Office of Cyber Security's

incident response processes and procedures, including the State Cyber Security Incident Response Plan, and identified the following specific problems:

- **Inadequate training**. We found that agency staff with responsibilities for incident response have generally not received sufficient training to effectively recognize, respond to, and report cyber security incidents. Although the Office of Cyber Security has provided some informal training to information security officers related to incident response, the training has not been comprehensive or realistic and has not included other key staff, such as system and network administrators. Additionally, the Office of Cyber Security does not routinely conduct debriefings or "lessons-learned meetings" following the investigation and handling of a security incident. Debriefings are an excellent way for staff to learn from their mistakes and improve their skills.

- **Outdated State Incident Response Plan**. In accordance with its duties and responsibilities within Section 24-37.5-405, C.R.S., the Office of Cyber Security developed a State Incident Response Plan for directing the State's response to cyber security incidents. We reviewed the State Incident Response Plan and found that it was outdated and contained inaccurate information. For example, key staff listed as responsible for carrying out portions of the State's Incident Response Plan no longer work for the State. Other staff listed in the plan have been moved into other, unrelated positions.

- **Lack of detailed and cohesive agency-level procedures**. State Cyber Security Policies require that agencies develop agency-level procedures for responding to cyber security incidents. We found that most agencies have not developed procedures in sufficient detail to appropriately direct staff during the handling of an incident. Additionally, we found that agency staff are unclear as to which incident response plan to use, the State Incident Response Plan or the agency-level incident response procedures. We also found that agency level procedures conflict with procedures contained in the State Incident Response Plan.

- **Lack of an electronic incident reporting and tracking system.** The Office of Cyber Security lacks an electronic incident reporting and tracking system. Incidents are reported via phone, email, or fax, and reports are maintained in hardcopy format. The lack of an automated electronic reporting and tracking system makes it difficult for the management staff within the Office of Cyber Security to track and analyze the timing and nature of cyber security incidents.

As part of the penetration test, we also identified a weakness in one agency's response to our social engineering attack (see Chapter 3 for a definition of this

type of attack). Instead of forcing password changes on compromised accounts, the system administrators within this agency left it up to the individual users to change their account passwords. Because individual users did not change their passwords timely, the assessment team was able to retain access to this agency's internal network and information systems for an additional six weeks following the initial identification of the breach.

The Office of Cyber Security has failed to ensure that the State has the processes, procedures, and technology necessary to identify, respond to, and analyze cyber security incidents occurring within computer systems of the State and institutions of higher education. Several changes need to occur to ensure that the State is prepared for cyber security incidents. These changes include communicating with agencies and institutions of higher education about their responsibilities to report security incidents; increasing the training for incident responders, system users, and system administrators; updating and coordinating agency and state incident response procedures; implementing an electronic incident response reporting, tracking, and analysis system; utilizing incident response debriefings; and revising incident response procedures to require that system administrators enforce password changes on user accounts suspected of being compromised.

Recommendation No. 2:

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.

Governor's Office of Information Technology Response:

Agree. Implementation Date: July 2011.

The Office of Cyber Security (OCS) 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 (OIT) 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.

Colorado Cyber Security Program Requirements

In addition to the areas of overseeing agency security plans and responding to security incidents, we reviewed other requirements contained in statutes related to the Office of Cyber Security. Statutes [Sections 24-37.5-403 through 406, C.R.S.] stipulate the requirements of the Colorado Cyber Security Program and specify the duties and responsibilities of the Chief Information Security Officer. The requirements contained in statute are based on information security best practices and represent Colorado's cyber security framework, or philosophy for securing the data and systems maintained by state government. The Chief Information Security Officer and public agencies are required to be knowledgeable of and compliant with these statutory provisions.

We reviewed the statutory requirements of the Colorado Cyber Security Program and evaluated whether the Office of Cyber Security had developed processes and procedures for complying with these provisions. Based on our review, we determined that the Office of Cyber Security has not implemented a significant number of the requirements of the Colorado Cyber Security Program, as specified by statute. We list the specific areas of compliance and non-compliance in the following table.

Evaluation of the Office of Cyber Security's Compliance with the Statutory Requirements of the Colorado Cyber Security Program

Statute	Requirement	Audit Finding
24-37.5-403(2)(a)	Develop and update information security policies, standards, and guidelines for public agencies.	Compliant. In 2006, the Office of Cyber Security developed the Colorado State Cyber Security Policies. Non-compliant. The Office of Cyber Security has not routinely reviewed and updated cyber security policies, standards, and guidelines. Most policies have not been updated since they were first created in 2006.

Evaluation of the Office of Cyber Security's Compliance with the Statutory Requirements of the Colorado Cyber Security Program		
Statute	**Requirement**	**Audit Finding**
24-37.5-403(2)(b)	Promulgate rules pursuant to the Colorado Cyber Security Program containing information security policies, standards, and guidelines for public agencies on or before December 31, 2006.	Compliant. The Office of Cyber Security promulgated rules for public agencies to follow on or before December 31, 2006 (8 CCR 1501-5).
24-37.5-403(2)(c)	Ensure the incorporation of and compliance with information security policies, standards, and guidelines in the information security plans developed by public agencies.	Non-compliant. The Office of Cyber Security has not ensured that public agencies are submitting security plans that comply with State Cyber Security Policies.
24-37.5-403(2)(d)	Direct information security audits and assessments in public agencies in order to ensure program compliance and adjustments.	Non-compliant. The Office of Cyber Security has not conducted or directed security audits and assessments in public agencies to ensure compliance with State Cyber Security Policies.
24-37.5-403(2)(e)	Establish and direct a risk management process to identify information security risks in public agencies and deploy risk mitigation strategies, processes, and procedures.	Non-compliant. Although risk assessments are being completed by some public agencies, the Office of Cyber Security has not used the assessments to deploy risk mitigation strategies, processes, and procedures throughout the State. Additionally, the risk assessments performed by public agencies are oftentimes incomplete and not reflective of the agencies' operating environment.
24-37.5-403(2)(f)	Approve or disapprove and review annually the information security plans of public agencies.	Non-compliant. The Office of Cyber Security has not consistently reviewed the security plans submitted by public agencies and has failed to communicate the results of its reviews to public agencies.
24-37.5-403(2)(g)	Conduct information security awareness and training programs.	Non-Compliant. The Office of Cyber Security has not

Evaluation of the Office of Cyber Security's Compliance with the Statutory Requirements of the Colorado Cyber Security Program		
Statute	**Requirement**	**Audit Finding**
		developed an effective information security awareness and training program. Most state employees have not received cyber security awareness training in the last three years.
24-37.5-403(2)(h)	In coordination and consultation with the Office of State Planning and Budgeting and the Chief Information Officer, review public agency budget requests related to information security systems and approve such budget requests for state agencies other than the Legislative Department.	Non-compliant. The Office of Cyber Security has not established a formal process for reviewing public agency budget requests related to information security systems. Additionally, the Office of Cyber Security has not developed a formal process for identifying the information security needs of public agencies, prioritizing needs based on risk, and developing and submitting consolidated cyber security budget requests to OIT, the Office of State Planning and Budgeting, and the Joint Budget Committee.
24-37.5-403(2)(i)	Coordinate with the Colorado Commission on Higher Education for purposes of reviewing and commenting on information security plans adopted by institutions of higher education that are submitted pursuant to Section 24-37.5-404.5(3), C.R.S.	Non-compliant. The Office of Cyber Security has not developed a process with the Colorado Commission on Higher Education for the annual review of security plans adopted by institutions of higher education. Since established in 2006, the Office of Cyber Security has not received or reviewed the security plans adopted by institutions of higher education.
24-37.5-406	The Chief Information Security Officer is to report to the Governor quarterly on the implementation of the Colorado Cyber Security Program.	Non-compliant. At the time of our review, the Office of Cyber Security had not established performance measures or metrics for assessing the

Evaluation of the Office of Cyber Security's Compliance with the Statutory Requirements of the Colorado Cyber Security Program		
Statute	**Requirement**	**Audit Finding**
		implementation of the Colorado Cyber Security Program. Additionally, the Chief Information Security Officer has not been making quarterly reports to the Governor.
Source: Office of the State Auditor evaluation of the Office of Cyber Security's compliance with the statutory requirements of the Colorado Cyber Security Program.		

The Office of Cyber Security's failure to comply with and enforce the statutory requirements of the Colorado Cyber Security Program puts the State at greater risk of a data breach or system compromise. We found that the Office of Cyber Security has failed to comply with the above-mentioned statutory provisions for numerous reasons, including leadership's lack of knowledge and understanding of all statutory requirements, undefined priorities by the Office of Cyber Security leadership, and poor project management and oversight. To ensure that the Colorado Cyber Security Program is a success, the Governor's Office of Information Technology needs to increase its oversight of the Office of Cyber Security and take the steps outlined in the recommendation below.

Recommendation No. 3:

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.

Governor's Office of Information Technology Response:

Agree. Implementation Date: July 2011.

It is the responsibility of the Chief Information Security Officer (CISO) 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 (OCS) 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.

Strategic Planning and Management Oversight

The strategic planning process is one of the fundamental ways in which an organization creates its unique sense of identity and purpose. Through defining its mission, goals, and methods of measuring success, an organization develops the foundation for making policy decisions and prioritizing the use of limited resources. The exercise of strategic planning is critical for the Office of Cyber Security because of the numerous and competing demands placed upon its staff and limited budget.

The Office of Cyber Security lacks a strategic plan for directing its operations. This lack of planning has resulted in many of the problems identified throughout our report. Additionally, the information security and agency business staff continually expressed concerns about the Office of Cyber Security's overall lack of vision and direction, including management's failure to establish and communicate priorities to its staff and stakeholders. We also found that the Office of Cyber Security lacks any meaningful metrics or measures for assessing its performance and does not have the processes and procedures in place to collect and analyze meaningful cyber security information. For example, during the audit we requested but were unable to obtain information related to:

- The number of public agencies that have fully implemented the Colorado Cyber Security Program.

- The number of high- and medium-level vulnerabilities identified by information security officers as part of their agencies' annual self-assessments, including the number of vulnerabilities remediated.

- The total number of security assessments and security awareness trainings completed by the Office of Cyber Security and agency information security officers in the last year.

- The number and types of cyber security attacks launched against state systems in the last year, including the Office of Cyber Security's activities to mitigate these threats.

To ensure that the Office of Cyber Security is addressing the right issues, complying with statutory requirements, using its resources and staff wisely, and meeting the intent expressed by the General Assembly in House Bill 06-1157, the Office of Cyber Security should work with the Governor's Office of Information Technology to develop a comprehensive strategic plan. The plan should include the Office of Cyber Security's mission, vision, goals, objectives, and short- and long-term priorities. The Office of Cyber Security should also identify performance targets that, if reached, indicate that the Office is on track to achieving its goals and meeting its mission. The plan should be reviewed and updated regularly and whenever major changes occur in the State's information security environment. The plan should be communicated to the Office of Cyber Security's staff, Governor's Office of Information Technology management, and stakeholders within public agencies and institutions of higher education.

Management Oversight and Leadership

As demonstrated throughout our report, we found that the Governor's Office of Information Technology's oversight of the Office of Cyber Security needs to be improved. During the four years since the enactment of House Bill 06-1157, the Colorado Cyber Security Program has still not been implemented, as required by statute. Statutory requirements have not been met, and as demonstrated in Chapter 3, significant vulnerabilities persist in state information systems and networks. We found that a lack of effective leadership within the Office of Cyber Security and lack of oversight by the Governor's Office of Information Technology led to many of the problems identified in our audit, including the Office of Cyber Security's failure to:

- Implement the Colorado Cyber Security Program and comply with statutory requirements.

- Provide timely feedback to agencies concerning their submission of the statutorily required Agency Cyber Security Plans.

- Communicate the requirements of the Colorado Cyber Security Program to key stakeholders, including public agencies, institutions of higher education, and the Department of Higher Education.

- Hold public agencies and state staff accountable for their responsibilities with regard to implementing the Colorado Cyber Security Program and complying with State Cyber Security Policies.

- Implement an effective compliance program to ensure that State Cyber Security Policies and standards are being uniformly applied.

- Remediate known and existing vulnerabilities in a timely manner.

- Develop and implement a comprehensive information security training program for those tasked with information security responsibilities.

The Governor's Office of Information Technology should take immediate steps to strengthen its oversight of the Office of Cyber Security, including the establishment of effective leadership within the Office of Cyber Security to reduce the State's level of exposure to cyber security attacks.

Recommendation No. 4:

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.

Governor's Office of Information Technology Response:

Agree. Implementation Date: January 2011.

The Office of Cyber Security (OCS) 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 (OIT) 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.

Penetration Test Results

Chapter 3

As stated earlier, the State collects and maintains a considerable amount of sensitive data and is responsible for protecting it. As part of our audit, we assessed the State's information security posture or preparedness and exposure to cyber attacks by performing a covert penetration test of state networks and information systems. A penetration test is a method for evaluating the security of networks and computer systems by simulating attacks from malicious sources. The purpose of a penetration test is to both assess an organization's risk of being compromised by a malicious attacker and to identify and recommend steps for preventing such attacks. The scope of our testing included all networks, systems, modems, wireless network devices, and Internet Protocol addresses (IP addresses) owned and operated by public agencies. Our audit did not include tests of any systems hosted or housed on the *colorado.gov* domain, as explained in Chapter 1.

The penetration testing was performed by a team composed of staff from a professional computer security firm under contract with the Office of the State Auditor (OSA), as well as staff from the OSA. Throughout Chapter 3 this team is referred to as the "assessment team" or "team." Team members had expertise in areas associated with malicious computer and system attacks, including social engineering, which involves the act of manipulating people to perform a specific action or divulge confidential information; network and web application security testing; wireless device assessments; and exploit development and execution, which is the process of writing and launching customized computer code to take control of computer systems. To simulate real attacks against state systems, the team was authorized by executive-level staff from the Governor's Office to use all available attack types and techniques to gain unauthorized access to state systems and data, including social engineering and physical-based attacks—i.e., gaining unauthorized physical access to network devices and systems. The team was provided with no advance information about the systems or networks to be tested, just as a real attacker would have no such information. In order to test the State's ability to detect and respond to an attack, state IT staff, including agency information security officers, were not notified in advance of the testing. Active testing was conducted between March 30, 2010, and September 30, 2010.

Test Objectives

The initial scope of the penetration test encompassed more than 67,000 IP addresses (computer systems and network devices), 15 key state agency

applications (e.g., the Colorado Benefits Management System, Colorado Financial Reporting System, Colorado Personnel and Payroll System, GenTax, County Financial Management System, Medicaid Management Information System), 18 physical sites or state buildings, all state-owned wireless network devices identified during testing activities, and 10,760 phone numbers. Due to the size of the State's information technology footprint and the time allotted for testing, we performed preliminary analysis and identified the following areas on which to focus our testing:

- State systems collecting, processing, and storing sensitive and confidential data such as tax records, social security numbers, criminal histories, and personal health information.

- Systems and facilities considered to be the State's most vulnerable in terms of IT security risks.

- Systems where an attacker could make a significant impact, such as high-profile websites at risk for defacement.

Additionally, the Governor's Office of Information Technology provided the names of 15 applications that are critical to state operations and should be tested. Other than the names of the applications, no other information was provided to the team, such as IP address or operating system version.

In cooperation with the Office of Cyber Security, the assessment team identified two objectives that, if achieved, would indicate a successful compromise or data breach:

- Breach the security of the State of Colorado's network and gain access to personally identifiable, sensitive, and/or confidential information.

- Identify security weaknesses in systems or web applications that, if exploited, would provide an attacker with significant visibility, confidential data, or the ability to attack the site's users—Colorado's citizens and businesses.

To ensure adequate coverage of state systems, testing was discontinued on a network or system if both objectives were achieved. As such, not all vulnerabilities that exist within an application or network may have been discovered or validated as part of this engagement.

Penetration Test Results

Overall, the results of the penetration test demonstrate that the State is at high risk of a system compromise and/or data breach by malicious individuals, including individuals both internal and external to the State. We identified a significant number of serious vulnerabilities in the State's networks and applications that would likely provide a malicious attacker with unauthorized access to the public's data or with the ability to directly target Colorado's citizens. In the following sections, we provide summarized information about the number and types of vulnerabilities identified by the assessment team for each component of the State's information resources or architecture. This information provides a high-level overview of the State's current information security posture, including the risk of being compromised by a malicious individual.

We were able to compromise several state government networks and systems and gain unauthorized access to thousands of individuals' records, including state employees' records, containing confidential data such as social security numbers, income levels, birth dates, and contact information—i.e., phone numbers and physical addresses. We also compromised or gained access to usernames and passwords belonging to state employees and other individuals. Based on national averages, a data breach of this magnitude by a malicious individual would have cost the State between $7 and $15 million to remediate. This estimate does not include the cost to individual citizens whose data would have been stolen.

In assessing the threat to State systems, the assessment team utilized the U.S. Department of Homeland Security's National Vulnerability Database (NVD) Common Vulnerability Scoring System (CVSS) to rate the vulnerabilities identified during preliminary testing. Vulnerabilities are weaknesses in information systems, system security procedures, internal controls, or implementation that could be exploited or triggered by an attacker. Vulnerabilities listed in the NVD receive a CVSS score between 0 and 10, with 0 indicating a low-risk vulnerability and 10 indicating a high-risk vulnerability. For our purposes, we utilized the following scale to rate the vulnerabilities identified:

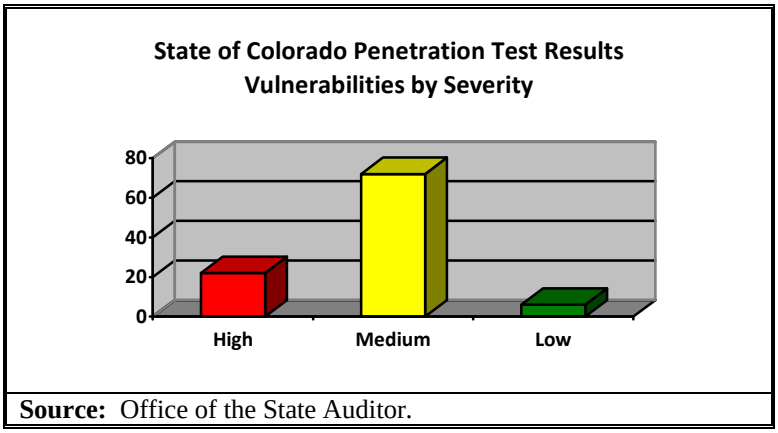
- **High.** High-risk vulnerabilities are considered to be severe security issues that can easily be exploited to immediately impact a system or network. Vulnerabilities with a CVSS base score of 7.0–10.0 are rated as "High." Additionally, regardless of the CVSS base score, the vulnerability was rated as "High" if it directly contributed to the assessment team's success in compromising confidential data.

- **Medium.** Medium-risk vulnerabilities are moderate security issues that require some effort to exploit to successfully impact a system or network. Vulnerabilities rated as "Medium" have a base CVSS score of 4.0–6.9.

- **Low.** Low-risk vulnerabilities have limited or marginal impact to systems and networks. Vulnerabilities are labeled "Low" severity if they have a CVSS base score of 0–3.9.

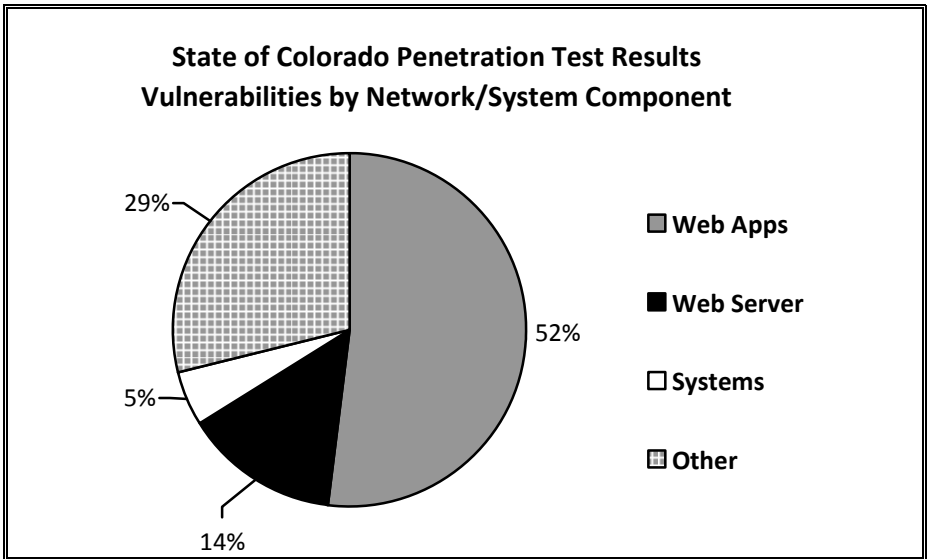
The NVD's listing of known vulnerabilities, including their CVSS base scores, can be found at http://web.nvd.nist.gov/view/vuln/search.

In total, we identified hundreds of vulnerabilities in state systems and networks. As shown in the following chart, of the total vulnerabilities identified 22 percent were high-risk, 72 percent were medium-risk, and 6 percent were low-risk vulnerabilities.



Source: Office of the State Auditor.

In addition to total vulnerabilities, we also analyzed which components of the State's information technology infrastructure contained the greatest percentage and severity of vulnerabilities. As seen in the following chart, 52 percent of all vulnerabilities were identified in web applications, with another 14 percent found in the servers hosting the web applications. This is important information because, as discussed in Chapter 1, most attackers are focused on exploiting web applications and servers, the areas of the State with the greatest number of vulnerabilities.



Source: Office of the State Auditor.

In the following table, we provide the risk ranking related to the specific components of the State's networks and systems tested. The risk ranking represents the likelihood that the confidentiality, integrity, and availability of State networks, systems, and information will be impacted based on known threats, identified vulnerabilities, and the effectiveness of the State's information system controls. As such, a risk ranking of "HIGH" means that it is extremely likely, based on current threats and system controls, that the confidentiality, integrity, and availability of the specified system component could be impacted. To protect the State, the details that led us to each risk ranking are provided to OIT, the Office of Cyber Security, and appropriate agencies in confidential appendices under separate cover.

State of Colorado Penetration Test Results Risk Ranking by Network/System Component		
Network/System Component Tested	**Description of Testing**	**Risk Ranking**
External Network Testing	Scanning the State's wide area network and publicly accessible IP addresses, or IP addresses associated with computers and other devices that are connected to and accessible through the Internet. Scanning results were then used to attempt to bypass security controls and gain unauthorized and privileged access to agency systems and internal networks.	HIGH
Physical Security Testing	Identifying and attempting to bypass physical security barriers or controls to gain access to the agency's internal network, computer hardware, or documents containing confidential information.	HIGH
Internal Network Testing	For those agencies at which the assessment team was able to bypass perimeter security controls—meaning controls within computer systems, such as firewalls, that are accessible through the Internet—or physical security controls, testing to identify and attempting to exploit systems located on the agencies' internal networks.	HIGH
Web Application Testing	Identifying all web applications exposed to the Internet, scanning identified web applications for vulnerabilities, and attempting to exploit those vulnerabilities, whether part of the web server or the application itself.	HIGH
Social Engineering	Attempting to obtain confidential information directly or to obtain information that can be used to further an attack. Testing included launching a directed "phishing" attack against state employees and other social engineering tactics.	HIGH
Modem Testing	A modem is a device that allows digital signals to be transmitted and received over analog telephone lines. Testing included "war dialing," which involves automatically dialing large blocks of phone numbers, in an attempt to find and exploit misconfigured dial-up modems.	LOW
Wireless Network Testing	A wireless network is a network that uses a wireless access point and radio waves for the transmission of data instead of network cables. Testing included identifying state-owned wireless networks and attempting to exploit the wireless access point and break the security encryption used to secure the radio transmissions.	LOW
Source: Office of the State Auditor penetration test results.		

Findings and Recommendations

In the next sections, we provide our high-level findings and recommendations that generally apply to all agencies and require a concerted and coordinated effort by the Office of Cyber Security. As stated earlier, the detailed technical findings and recommendations are being provided to OIT, the Office of Cyber Security, and appropriate agencies in confidential appendices under separate cover. The Office of the State Auditor will track OIT's, the Office of Cyber Security's, and agencies' implementation of the recommendations contained both in the public and confidential sections of this report.

The most significant vulnerabilities that allowed the assessment team to compromise state systems and networks and gain access to state data were:

- Management interfaces exposed to the Internet with default or easily guessable usernames and passwords enabled.
- Web applications, servers, and network devices accessible through the Internet with default or easily guessable usernames and passwords enabled. Many of these accounts provided the assessment team with privileged or administrative-level access to the system.
- Unnecessary ports, services, and utilities exposed to the Internet, including services with known and exploitable vulnerabilities.
- Unsecured or misconfigured web applications susceptible to SQL injection, remote file inclusion—an attack in which the attacker uploads inappropriate files onto a web server—and other well-known attacks.
- Poorly secured internal networks.
- Poor physical security that allowed testers to gain unlimited access to public agencies' internal networks and information assets.
- Lack of security awareness by employees, resulting in the successful execution of phishing attacks that allowed testers to harvest system credentials and access state systems and data.

Exposed Management Interfaces

Management or administrative interfaces to applications and network devices allow system administrators to perform privileged operations, such as adding or removing routes to other networks; reading, adding, or deleting databases; and

adding, removing, or modifying users. Oftentimes, the only barrier between an attacker and full access to an administrative interface is a username and password. Industry best practices recommend that access to administrative interfaces be limited to computers located on an entity's internal network. Access to management or administrative interfaces should not be directly accessible from the Internet because of the higher exposure to potential attacks.

During our testing, we found that the State has a significant number of administrative interfaces for firewalls, network devices, and web applications exposed directly to the Internet. This means that anyone with access to the Internet can attempt to gain access to these interfaces. In several cases, the assessment team was able to gain access to these interfaces by using vendor default usernames and passwords or by guessing the username and password. These techniques would have been impossible if the State followed industry best practices and limited access to management interfaces to only internal IP addresses. We make several recommendations to the Governor's Office of Information Technology below, including requiring the Office of Cyber Security to update State Cyber Security Policies to match industry best practices.

(Classification of Finding: Material Weakness – See Appendix A)

Recommendation No. 5:

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.

Governor's Office of Information Technology Response:

Agree. 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 (OCS) 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 (OSA) 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.

Default and Easily Guessable Usernames and Passwords

State Cyber Security Policies and industry best practices recommend the use of strong passwords. Specifically, State Cyber Security Policies require that passwords be at least eight characters in length and be complex, which means passwords should include a combination of lower and uppercase letters, numbers, and special characters. In addition to strong passwords, State Cyber Security Policies and industry best practices recommend changing vendor default usernames and passwords. These default usernames and passwords are well known by attackers and are readily available on the Internet.

Throughout our testing, we gained unauthorized access to systems and administrative interfaces by either guessing the correct username and password or by using vendor default credentials. Failure to use strong passwords or change vendor default passwords, especially for systems and applications accessible through the Internet, places the State at extreme risk of compromise. Several of the specific vulnerabilities we identified would have been discovered by the Office of Cyber Security or agency staff through routine vulnerability scans. However, we learned that the Office of Cyber Security and public agencies are not routinely performing vulnerability scans of state systems. Additionally, in one instance, a firewall we compromised had recently been moved into production without undergoing the OIT-approved hardening, or securing, process. If the state agency would have followed the hardening process required by State Cyber Security Policies, the default username and password the assessment team used to gain control of the firewall would have been disabled, removed, or changed. In the following recommendation, we provide several steps the Governor's Office of Information Technology should take to guard against the use of default and easily guessable usernames and passwords.

(Classification of Finding: Material Weakness – See Appendix A)

Recommendation No. 6:

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.

Governor's Office of Information Technology Response:

Agree. Implementation Date: July 2011.

Beginning in 2011, the Office of Cyber Security (OCS) will expand the Threat and Vulnerability Management Program (TVMP) 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 (OSA) 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.

Unnecessary and Insecure Ports, Services, and Utilities

Ports provide a gateway to services and utilities that are running on a server. State Cyber Security Policies, industry best practices, and the Center for Internet Security hardening standards specify that only those ports, services, and utilities necessary to conduct business should be open and running. Unneeded ports, services, and utilities provide an unnecessary avenue for attackers to exploit and should be closed or disabled. Additionally, some ports and services are known to be insecure. Whenever possible, insecure services and utilities should be discontinued and replaced with secure ones.

From our testing, we found that the State has a large Internet presence, including more than 17,600 active IP addresses. Of these, we identified numerous IP addresses that appeared to be unused and that had ports open that were running unneeded and outdated services. Additionally, we identified a file upload utility on one agency's web server that allowed us to upload malicious code and take full control of the server. It was later determined that the file upload utility was unnecessary and should have been removed. As part of our assessment, we also found that many of the State's servers are running vulnerable services that provide

attackers an opportunity for exploitation. During our assessment, it also became clear that the Office of Cyber Security did not have an accurate inventory of all state systems requiring public Internet access, including a list of the ports, services, utilities, and access rules required for each system. Without an accurate inventory, the Office of Cyber Security cannot take the appropriate steps necessary to limit the State's exposure to Internet-based attacks. Additionally, many of the systems and applications we exploited either did not have a functioning firewall in place or had a firewall that was not being monitored by agency staff. The lack of a monitored firewall allowed the assessment team to continuously attack and exploit Internet-facing systems without being detected.

We have provided the specific details of the vulnerabilities we identified to the Office of Cyber Security in the confidential appendices. The Governor's Office of Information Technology should take immediate steps to reduce the State's exposure to attack, including reducing the State's overall Internet footprint. We provide additional recommendations below.

(Classification of Finding: Material Weakness – See Appendix A)

Recommendation No. 7:

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.

Governor's Office of Information Technology Response:

Agree. 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 (CSN). This new network will enable the Office of Cyber Security (OCS) 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 (OIT) 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 (TVMP) 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 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.

Unsecured Web Applications

As previously discussed, web applications are becoming the primary target of malicious individuals. To ensure that web applications are attack-resilient, security controls must be implemented throughout each tier or layer of the

application's architecture, including the network within which the application resides, the server the application is running on, the application itself, and the database the application uses. Vulnerabilities or misconfigurations in any component of the application's architecture can result in a successful attack. Industry best practices recommend that web applications be secured by incorporating security within the design and initial build of the application, routinely testing applications for vulnerabilities, and using web application firewalls for the most critical applications.

As part of the penetration test, we identified hundreds of vulnerabilities in state web applications, including many severe vulnerabilities that led directly to the systems' compromise. In several situations, we were able to take control of the database the application was using to disclose usernames and passwords and citizen data. In many instances, we were also able to abuse the application's functionality to disclose usernames and bypass application controls to gain access to portions of the website normally restricted from the public. In one instance where we identified a state intranet application that was exposed to the Internet, we were able to exploit the site's poorly designed authentication mechanism to gain access to the site and download information that provided useful information for further attacks against the State. Finally, we found that system administrators do not appear to be routinely monitoring application-level logs. As part of our testing, we launched thousands of attacks against state web applications; many of these attacks would have generated tens of thousands of anomalous or suspicious log entries. Except for one agency, none of our attacks was reported to the Office of Cyber Security.

Securing the State's websites will be a large undertaking and will require, at times, the Office of Cyber Security to work with the vendors that originally developed the applications. We have provided the details of the specific deficiencies we identified to the Office of Cyber Security for remediation in the confidential appendices. Additionally, as discussed in the recommendation below, we recommend that the Governor's Office of Information Technology implement a web application security program that includes routine and pre-deployment testing, training, log monitoring, and the deployment of web application firewalls where appropriate.

(Classification of Finding: Material Weakness – See Appendix A)

Recommendation No. 8:

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.

Governor's Office of Information Technology Response:

Agree. Implementation Date: July 2011.

The Office of Cyber Security (OCS) 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 (TVMP) 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.

Internal Network Security

An agency's internal network is the portion of its network that is considered private and not accessible to the general public. The internal network typically includes user computers and applications, internal network shares, and the servers and databases that support the agency's operations. State Cyber Security Policies and industry best practices recommend a layered or defense-in-depth approach to security. A layered defensive approach means that security controls will be included or built in each layer of the agency's infrastructure, including the internal network. Common security controls include network segmentation, internal system hardening, use of secure network protocols, and intrusion detection.

Once the assessment team gained access to an agency's internal network, the team identified problems in each of these areas, including:

- **Network segmentation.** Network segmentation is the process of dividing a network into different segments or zones based upon access and security requirements of the systems in those zones. Agency internal networks were generally flat, meaning all computers and servers were included within the same network. This made it easy for the assessment team to directly reach all internal computer assets, including sensitive servers and databases. Furthermore, the assessment team found that access to administrative interfaces and utilities on internal servers was not filtered. As such, the team was able to gain administrative access to firewalls and databases as a common user.

- **System hardening.** System hardening includes removing or changing all guest accounts and default passwords, disabling nonessential services, setting system parameters to mitigate potential attacks, and patching systems from known vulnerabilities. We identified numerous systems that were not properly hardened and patched. For example, we gained

administrative access to one system within an agency's internal network by exploiting a well-known operating system vulnerability that has had an available patch since 2008. This specific vulnerability is targeted by one of the most damaging Internet worms in history.

- **Insecure network protocols.** Many common network protocols transmit information between computers in cleartext, such as the Hypertext Transfer Protocol (HTTP). Although appropriate for some uses, these types of protocols should not be used to transmit sensitive information, such as usernames and passwords. The assessment team was able to sniff, or monitor network traffic, once internal access was gained. Through network monitoring, the assessment team was able to capture usernames and passwords and default strings for network devices and internal applications, many of which contained sensitive information about state employees.

- **Intrusion detection.** With the exception of one agency, our internal testing was not detected by system administrators. From prior audit engagements and our interviews with information security officers, we determined that most public agencies lack an internal intrusion detection capability.

Failure to properly secure the internal network makes it more likely that attackers will gain access to confidential or sensitive data if external controls are bypassed or fail. We recommend that the Governor's Office of Information Technology work with public agencies to further harden or secure their internal networks by taking the steps listed below.

(Classification of Finding: Material Weakness – See Appendix A)

Recommendation No. 9:

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.

Governor's Office of Information Technology Response:

Agree. Implementation Date: July 2013.

Many of the state internal networks were created before the Office of Cyber Security (OCS) 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 (OIT) 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 (CRISC) tool. OCS will ensure that proper patching

and hardening practices are implemented within each agency through the Information Security Officers (ISO) 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.

Poor Physical Security Over Information Systems

Due to the sensitive nature of the information contained within this finding, it is reported in the confidential appendices provided under separate cover.

(Classification of Finding: Material Weakness – See Appendix A)

Lack of Employee Security Awareness

Due to the sensitive nature of the information contained within this finding, it is reported in the confidential appendices provided under separate cover.

(Classification of Finding: Material Weakness – See Appendix A)

This page intentionally left blank.

Appendix

This page intentionally left blank.

Public Appendix A

Report Findings by Classification of Finding

Definition of Finding Classifications	
Classification	**Description**
Material Weakness	A material weakness produces an immediate risk directly impacting the confidentiality, integrity, and availability of information systems and data. For IT projects, a material weakness represents an immediate threat to the overall success of the project. This would be considered a high risk finding.
Significant Deficiency	Significant deficiencies do not alone produce an immediate risk, but could affect the confidentiality, integrity, or availability of systems in conjunction with other factors. For IT projects, significant deficiencies do not represent an immediate threat to the overall success of the project but could result in project delays, cost overruns, or incomplete deliverables. This would be considered a moderate risk finding.
Control Deficiency	Control deficiencies do not present an immediate risk but could be indicative of operating deficiencies and/or have the potential to adversely affect the confidentiality, integrity, or availability of systems over an extended period of time. For IT projects, control deficiencies may not represent an immediate threat to the overall success of the project but could, over an extended period of time and in conjunction with other deficiencies, result in project delays, cost overruns, or incomplete deliverables. This would be considered a low risk finding.

Rec. No.	Page No.	Audit Finding	Classification of Findings		
			Material Weakness	Sig. Deficiency	Control Deficiency
1	31	Re-evaluate and improve the Agency Cyber Security Plan development, submission, and review process.	X		
2	37	Improve the State's cyber security incident identification, reporting, and response processes and procedures.	X		
3	42	Implement and comply with all statutory requirements of the Colorado Cyber Security Program.	X		
4	45	Develop a strategic plan for the Office of Cyber Security, hold cyber security leadership accountable, and increase the Governor's Office of Information Technology's oversight of the Colorado Cyber Security Program.	X		
5	54	Secure exposed management interfaces.	X		
6	56	Ensure that all state systems are using strong passwords and that vendor default usernames and passwords are changed.	X		
7	58	Inventory all Internet-facing systems and close and/or disable all unnecessary and insecure ports, services, and utilities.	X		
8	60	Secure state web applications.	X		
9	63	Improve the security of public agencies' internal networks.	X		
CONFIDENTIAL RECOMMENDATIONS					
1	N/A	Poor Physical Security Over Information Systems	X		
2	N/A	Lack of Employee Security Awareness	X		

The electronic version of this report is available on the website of the
Office of the State Auditor
www.state.co.us/auditor

A bound report may be obtained by calling the
Office of the State Auditor
303.869.2800

Please refer to the Report Control Number below when requesting this report.

Report Control Number 2068A

Report Control Number 2068A