SECURANCE CONSULTING

Information Security Assessment

LEGISLATIVE AUDIT COMMITTEE

Senator Lucia Guzman - Chair

Senator David Balmer
Senator Kevin Grantham
Representative Dan Nordberg
Representative Dianne Primavera

Representative Su Ryden
Representative Jerry Sonnenberg
Senator Lois Tochtrop

OFFICE OF THE STATE AUDITOR

Dianne E. Ray	State Auditor
Matt Devlin	Deputy State Auditor
Reed Larsen	Contract Monitor
Securance Consulting	Contractor

AN ELECTRONIC VERSION OF THIS REPORT IS AVAILABLE AT
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 REPORT NUMBER 1404P WHEN REQUESTING THIS REPORT

S|C SECURANCE CONSULTING

the advantage of insight

November 20, 2014

Members of the Legislative Audit Committee:

This report contains the results of our current information system security evaluation of the Governor’s Office of Information Technology and the Judicial Branch. The audit was conducted pursuant to Section 2-3-103, C.R.S., which authorizes the State Auditor to assess, confirm, and report on the security practices of all departments, institutions, and agencies of state government. The report presents our findings, conclusions, and recommendations, and the responses of the Governor’s Office of Information Technology and the Judicial Branch.

Sincerely,

Paul Ashe
President of Securance Consulting

TABLE OF CONTENTS

IT SECURITY THROUGHOUT STATE GOVERNMENT

Report Highlights

Governor's Office of Information Technology
Judicial Branch

EVALUATION CONCERN

The Governor's Office of Information Technology and the Judicial Branch have technical security vulnerabilities that should be remediated. Additionally, there are areas for improvement on the governance side of information security.

KEY FACTS AND FINDINGS

- The **Governor's Office of Information Technology** (OIT) is responsible for oversight and governance of information security for all Executive Branch agencies.
- Our work identified 243 technical security vulnerabilities that should be remediated. Vulnerabilities are categorized according to nationally recognized Common Vulnerability Scoring System Version 2 (CVSS V2) methodology. The classifications in this system, from most severe to least severe are Urgent, Critical, High, Medium, Low, and Advisory.
    - We found zero Urgent vulnerabilities.
    - We found 27 Critical vulnerabilities.
    - We found 74 High vulnerabilities.
    - We found 142 Medium vulnerabilities.
    - We do not report on Low and Advisory vulnerabilities.
- Disaster recovery plans do not exist for the two critical enterprise applications we reviewed.
- We found areas for improvement of logical access controls.

- The **Judicial Branch** is responsible for oversight and governance of its own information security.
- Our work identified 9 technical security vulnerabilities that should be remediated.
    - We found zero Urgent vulnerabilities.
    - We found zero Critical vulnerabilities.
    - We found 3 High vulnerabilities.
    - We found 6 Medium vulnerabilities.
    - We do not report on Low and Advisory vulnerabilities.
- Disaster recovery plans do not exist for the one critical enterprise application we reviewed.
- We found areas for improvement of logical access controls.

BACKGROUND

Governor's Office of Information Technology:

- Was established in 2008.
- Centralized the management of Executive Branch information technology resources, including IT staff.
- Is responsible for securing networks, servers, databases, and web applications across Executive Branch agencies.

Judicial Branch:

- Manages its own IT services through the Judicial Business Integrated with Technology Services division.
- Is responsible for securing its own networks, hardware, databases, enterprise applications, and web applications.

KEY RECOMMENDATIONS

The Governor's Office of Information Technology should:

- Improve IT security by continuing the consolidation of IT services and processes, update policies, and train staff to follow prescribed policies.
- Work with business owners to develop, test, and update disaster recovery plans for the critical IT systems reviewed.
- Improve controls over logical access to critical IT systems reviewed.

The Judicial Branch should:

- Develop IT security policies in those areas that have a gap, including configuration and patch management.
- Develop, test, and update disaster recovery plans for the critical IT system reviewed.
- Improve controls over logical access to critical IT system reviewed.

RECOMMENDATION LOCATOR

REC. NO.	PAGE NO.	RECOMMENDATION SUMMARY	AGENCY ADDRESSED	AGENCY RESPONSE	IMPLEMENTATION DATE
1	17	Improve IT security governance by (a) continuing consolidation efforts of IT services, including updating outdated operating systems and reconfiguring systems that are using default passwords; (b) holding vendors and OIT staff accountable for best practices, including industry hardening standards, in administering OIT systems; (c) updating IT security policies on a regular basis including the removal of conflicting language and timely communicating these updates to all OIT staff; and (d) implementing a comprehensive internal training program to ensure that OIT staff are adequately trained on current policies and procedures.	OIT	**A) AGREE** **B) AGREE** **C) AGREE** **D) AGREE**	A) DECEMBER 2015 B) DECEMBER 2015 C) JULY 2015 D) JULY 2015
2	21	Improve the ability to manage interruption of the two enterprise applications by (a) working with the business owners of the application to develop a comprehensive disaster recovery plan for each enterprise application, (b) developing comprehensive recovery testing strategies and performing recovery testing on a regular basis, and (c) updating the disaster recovery plan based on feedback and analysis of the testing done in subpart B.	OIT	**A) AGREE** **B) AGREE** **C) AGREE**	A) DECEMBER 2015 B) DECEMBER 2015 C) DECEMBER 2015

REC. NO.	PAGE NO.	RECOMMENDATION SUMMARY	AGENCY ADDRESSED	AGENCY RESPONSE	IMPLEMENTATION DATE
3	23	Improve the ability to manage interruption of the one enterprise applications by (a) developing a comprehensive disaster recovery plan for the one enterprise application, (b) developing comprehensive recovery testing strategies and performing recovery testing on a regular basis, and (c) updating the disaster recovery plan based on feedback and analysis of the testing done in subpart B.	Judicial	**A) AGREE** **B) AGREE** **C) AGREE**	A) JUNE 2016 B) JUNE 2016 C) JUNE 2016
4	27	Improve logical access controls for the two enterprise applications reviewed by (a) working with the business owners of the two enterprise applications to review all active production user accounts to ensure they are assigned to current employees and to assess the appropriateness of access granted; (b) ensuring passwords for administrative for the one critical application are consistent with State Information Security Policies, and ensuring that administrative access is adequately logged and monitored; and (c) developing a segregation of duties matrix for the one critical application identified.	OIT	**A) AGREE** **B) AGREE** **C) AGREE**	A) JULY 2015 B) SEPTEMBER 2015 C) JULY 2015
5	29	Improve logical access controls for the one enterprise application reviewed by (a) reviewing all active production user accounts to ensure they are assigned to current users and to assess the appropriateness of access granted; (b) ensuring that administrative access is adequately logged and monitored; and (c) developing segregation of duties matrix for the one critical application identified.	Judicial	**A) AGREE** **B) AGREE** **C) PARTIAL AGREE**	A) JUNE 2016 B) JUNE 2016 C) NOVEMBER 2015

IT Security Throughout State Government

State agencies routinely collect, process, and store personally identifiable information and data, including social security numbers, tax identification numbers, driver's license information and ID numbers, personal health information, and criminal history records. Colorado's citizens and those organizations that conduct business with the State expect that the data will be protected. Overall, 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 and the information contained in those systems.

IT ORGANIZATION

Until 2008, each department within the Executive Branch had its own IT division headed by a chief information officer who reported to the department's Executive Director. Individual departments made IT budgeting, procurement, and operational decisions with limited interaction or planning across the Executive Branch. Such a fragmented infrastructure was shown to increase the difficulty of achieving economies of scale, improving operational efficiency, lowering costs, and optimizing service delivery and resource utilization.

To address these concerns, in January 2007 Governor Bill Ritter, Jr. announced a multiyear IT consolidation plan to bring the decentralized IT operations, which were spread across 16 Executive Branch departments, under the Governor's Office of Information Technology (OIT). The "IT Consolidation Bill" (Senate Bill 08-155) was enacted during the 2008 Legislative Session. Senate Bill 08-155 took effect July 1, 2008.

OIT's operational domain is the State's IT infrastructure, including data centers, servers, mainframe operations, personal computers, data storage, operating systems, local and wide area networks, and communications.

On July 1, 2010, OIT took the first step to further consolidate the State's fragmented IT operations by bringing all IT personnel and the accompanying appropriations for full-time-equivalent (FTE) staff positions under one agency, as required by Senate Bill 08-155. While the IT functions for a majority of departments under the Executive Branch were consolidated under OIT, several departments and the legislative and judicial branches of government remained outside of OIT's oversight. The following exhibit shows the 17 Executive Branch departments currently under OIT oversight and the agencies and branches that currently fall outside of OIT oversight.

GOVERNOR’S OFFICE OF INFORMATION TECHNOLOGY OVERSIGHT	
AGENCIES WITHIN OIT’S OVERSIGHT	
Department of Agriculture	Department of Natural Resources
Department of Corrections	Department of Personnel and Administration
Department of Education	Department of Public Health and Environment
Department of Health Care Policy and Financing	Department of Public Safety
Department of Higher Education	Department of Regulatory Agencies
Department of Human Services	Department of Revenue
Department of Labor and Employment	Department of Transportation
Department of Local Affairs	Governor’s Office
Department of Military and Veteran Affairs	
AGENCIES OUTSIDE OIT’S OVERSIGHT	
Department of Law (Attorney General)	Institutions of Higher Education
Department of State (Secretary of State)	Judicial Branch
Department of Treasury (State Treasurer)	Legislative Branch

SOURCE: Analysis of details in Colorado stature - Sections 24-37.5-102 through 105 C.R.S.

For the departments and branches of state government that remain outside of OIT’s oversight, below is a brief description of the way in which they handle their IT operations.

- **Department of Law (Attorney General)**: The Department of Law’s Information Technology division handles the department’s computer-related needs, including maintenance, training, and operation of the Attorney General’s website.

- **Department of State (Secretary of State)**: The Department of State’s Information Technology division supports the information system needs of the entire Secretary of State's office. The division maintains the department’s IT infrastructure consisting of multiple servers, personal computers, networking equipment, firewall, telephone system, and other IT equipment to support data and imaging needs. The division also supports the Web presence of the Secretary of State.

- **Department of Treasury (State Treasury)**: Although otherwise outside of OIT oversight, the department contracts with OIT for server and desktop support.

- **Institutions of Higher Education**: Each of the 28 public higher education institutions maintains its own IT department, which supports the IT needs of the campus, faculty, staff, and students.

- **Judicial Branch**: The Information Technology Services (ITS) division manages the Judicial Branch’s IT needs and is overseen by the branch’s Chief Information Officer. ITS provides the five following services: executive services, application development services, court services, e-filing services, and technical services.

- **Legislative Branch**: Legislative Information Services (LIS) is under the Colorado

Legislative Council and manages IT services for the Legislative Branch. LIS provides IT support and services for all legislators and their staff, the Office of Legislative Legal Services, Colorado Legislative Council, the Joint Budget Committee staff, and the Office of the State Auditor.

INFORMATION SECURITY

The governance structure over information security in Colorado state government is slightly different and more expansive than the structure in place for other types of IT funding and operations. Specifically, the General Assembly enacted House Bill 06-1157, better known as the Colorado Cyber Security Program, during the 2006 Legislative Session. The legislation was codified in Sections 24-37.5-401 through 406, C.R.S. The law also created the position of State Chief Information Security Officer (CISO) to oversee the Colorado Cyber Security Program. The program, which is now referred to as the Colorado Information Security Program, is responsible for governance, risk management, and compliance. Most of the law's requirements apply to public agencies, which are defined in the law as "every state office, whether executive or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions." In addition to Executive and Judicial Branch agencies, the institutions of higher education and the General Assembly, although not directly accountable for the Colorado Information Security Program requirements, have specific reporting and coordination requirements.

Information security is no longer just an IT problem, it is an enterprise business issue. Every agency uses information and most are dependent on it. Information is an asset and, like other important State assets, is essential to the State of Colorado and consequently needs to be protected. This is especially important in the increasingly interconnected government environment, where information is now exposed to a growing number and a wider variety of threats and vulnerabilities. According to a 2014 study conducted by Deloitte & Touche, LLP, on behalf of the National Association of State Chief Information Officers, states are subject to a growing number of sophisticated cyber attacks that range from data breaches to the political protests of hacktivists – individuals who break into computer networks to promote their political agendas. The 2014 study reports that 60 percent of Chief Information Security Officers (CISOs) have seen an increase in the sophistication of cyber attacks, and that these increasingly sophisticated attacks are a major threat to securing state IT networks and IT assets. In terms of support from executive leadership, 65 percent of CISOs reported that their senior executives are committed to IT security, but IT security funding is not sufficient to meet the growing number of sophisticated attacks. Within just the past few years a number of high-profile attacks on states have resulted in the loss of Personally Identifiable Information (PII) of millions of citizens, including social security numbers, payment card records, dates of birth, driver's license numbers, and tax data. These incidents have cost states millions of dollars in clean-up costs, as well as loss of both revenue and public trust.

The goal of the Colorado Information Security Program is to improve Colorado's information security posture by establishing a statewide information security framework and governance model. The program forms the foundation of the State's information security control structure and reflects the General Assembly's commitment to address the information security risks facing public agencies with a coordinated and risk-based approach.

FUNDING

Annually, OIT must request an appropriation of funds for direct and indirect OIT costs of services including materials, labor, and administrative overhead. The appropriated funds come from fees collected from other Executive Branch agencies for payments to OIT for the agencies' share of information technology staff payroll costs, including centrally appropriated items, and personal services expenses that have been deposited in OIT's Information Technology Revolving Fund. The annual appropriations of funds are identified in the General Appropriations Act Long Bill. The Fiscal Year 2015 appropriations include central administration, IT infrastructure, network, information security, applications, and end-user services. In the Exhibit below, we provide a high-level overview of the appropriations and total full time employees (FTEs) for FY2012 through FY2015.

EXHIBIT 2 - OFFICE OF INFORMATION TECHNOLOGY EXPENDITURES AND FTE FOR FISCAL YEARS 2012 THROUGH 2015

DESCRIPTION	FY 2012	FY 2013	FY 2014	FY 2015	PERCENT CHANGE FROM FY2012-FY2015
Appropriation (Millions)	$125.7	$136.3	$151.4	$186.4	48.3%
FTE	902.8	897.5	920	925.9	2.6%

SOURCE: HB14-1336 Long Appropriation Bill

PRIOR ENGAGEMENTS

During November 2010, the Office of the State Auditor conducted an assessment of the Cyber Security Program. As part of this audit the State's information security posture or preparedness and exposure to cyber attacks were assessed by performing a covert penetration test of state networks and information systems. The key findings from the performance audit were (1) the state was at a high risk of system compromise and/or data breach by malicious individuals, including individuals both internal and external to the State, and (2) the Office of Cyber Security failed to successfully implement the Colorado Cyber Security Program. The November 2010 engagement produced 228 recommendations to help improve the security posture of the State's IT systems.

2014 EVALUATION PURPOSE, SCOPE AND METHODOLOGY

This report includes the results of our current information system security evaluation. We conducted the evaluation pursuant to Section 2-3-103, C.R.S., which authorizes the State Auditor to assess, confirm, and report on the security practices of all departments, institutions and agencies of state government. Our work was performed from April 2014 to August 2014, and our opinions of the security posture of the environment are as of July 10, 2014. We noted certain other matters that are not included in this audit report that we reported to Judicial Branch management in a separate letter dated November 21, 2014.

The key objectives of the evaluation were to assess the current state of information system security across key components of the technology environment and to gain an understanding of the root causes of identified information system security weaknesses.

To achieve the objectives the OSA contracted with a security firm specializing in vulnerability assessment, penetration testing, and technical security assessments. This contractor conducted the engagement and performed test procedures utilizing its proven methodology.

The scope of the assessment focused on areas identified by the Office of the State Auditor and included an assessment of six main areas. The following describes the high-level tasks performed for each component of the project.

EXTERNAL AND INTERNAL NETWORK VULNERABILITY TESTING: During this phase, we performed step-by-step discovery and vulnerability assessment procedures aimed at identifying weaknesses in Internet Protocol (IP) network services. We assessed 89,614 external IP addresses and also reviewed the internal IP networks for three executive branch agencies.

NETWORK DEVICE TESTING (E.G., FIREWALLS): During this phase, we performed a configuration analysis against the in-scope network devices (firewalls). OIT manages about 180 firewalls, and we selected a sample of 10 firewalls to analyze. We obtained the most current configuration file for the 10 selected firewalls and used a commercially licensed software program coupled with our analysis to perform a comprehensive analysis of the Firewall's configuration.

ENTERPRISE APPLICATION TESTING: During this phase, we assessed a sample of three critical enterprise applications. Two of these enterprise applications are managed by OIT for executive branch agencies, and the third application is managed by ITS for the judicial branch. We performed the following activities while analyzing these three enterprise applications:

- Interviews with key Information Technology and Business personnel;
- Reviews of system configuration settings;
- Tests of database security;
- Tests of operating system security/vulnerability; and
- Reviews of the following supporting processes:
  - Change | Patch Management
  - User Administration
  - Database Access Administration
  - Production Access
  - Monitoring and Logging
  - Datacenter Physical Security and Environmental Controls
  - Remote Access
  - Virus Protection Strategy

WEB APPLICATION TESTING: During this phase we assessed a sample of six web-based applications to determine their susceptibility to vulnerabilities in several common attack categories including SQL injections, cross-site scripting, remote execution, and web server attacks. Five of the six web applications are managed by OIT for executive branch agencies and the remaining one web application is managed by ITS for the judicial branch.

SOCIAL ENGINEERING ASSESSMENT: During this phase we designed a social engineering campaign to test the effectiveness of internal user security awareness training. The campaign included eMail Phishing – a technique in which a perpetrator sends out a legitimate-looking email in an attempt to solicit the recipient to respond with confidential and often sensitive data (i.e., username, password, social security number, etc.).

In addition, we reviewed policies and procedures, reviewed various configurations and interviewed numerous OIT management and staff.

Overall, we determined that the evidence we obtained provides a reasonable basis for our findings and conclusion based on our objectives.

SECURITY VULNERABILITIES WITHIN EXECUTIVE BRANCH SYSTEMS

WHAT AUDIT WORK WAS PERFORMED AND WHAT WAS THE PURPOSE?

The purpose of the audit was to perform a focused vulnerability assessment, penetration test, and technical information security evaluation of state networks, applications, and information systems from April 2014 through August 2014. We applied a risk-based approach and selected networks, applications and systems for testing based on their criticality to the State. In addition, we identified five different IT infrastructure areas managed by OIT for our review. Specifically, we performed vulnerability and penetration assessment procedures and reviewed information security controls over the State's (1) external network, (2) a sample of three departmental internal networks, (3) a sample of ten network firewalls (both external and internal-facing), (4) a sample of two enterprise applications and their supporting databases, and (5) a sample of five web-applications. Our procedures included the use of commercial tools to identify risks to these specific technologies and interviews of key OIT management and staff.

In addition, we conducted a social engineering exercise to determine whether state employees were sufficiently aware of information security threats to state networks and systems and were able to detect and avoid illegitimate attempts to gain user access credentials to state systems. We performed the social engineering test by distributing phishing emails to 499 State employees across 15 Executive Branch agencies.

Lastly, we performed a root cause analysis as part of the vulnerability assessment and penetration test, to determine the reasons why the vulnerabilities we found existed. The finding listed below relates to this root cause analysis.

HOW WERE THE RESULTS OF THE AUDIT WORK MEASURED?

We applied the following criteria when evaluating the sufficiency of information security processes and controls within state networks, applications, and information systems:

- **OIT MUST CREATE POLICIES, STANDARDS, SPECIFICATIONS, AND GUIDELINES FOR INFORMATION SECURITY.** As part of the Chief Information Officer's duties and responsibilities in overseeing OIT, statute [Section 24-37.5-106, C.R.S.] requires OIT to develop policies, standards, specifications, and guidelines for information technology and related procedures to effectively manage IT.

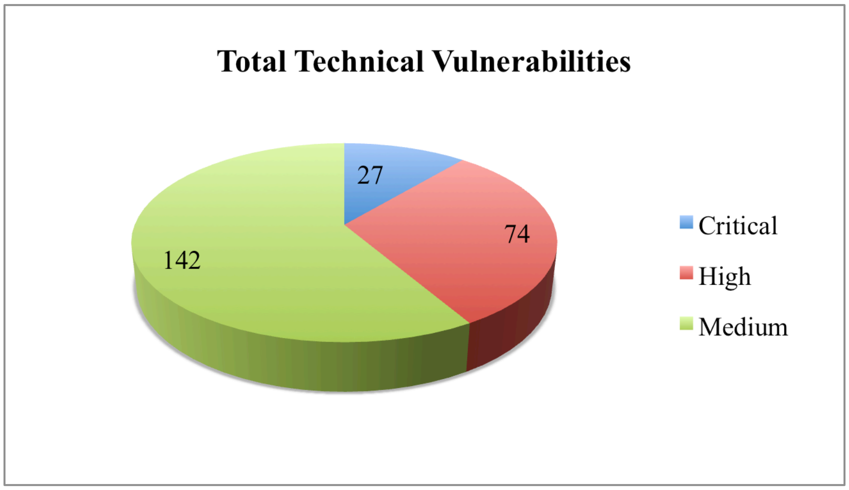
- **THE CHIEF INFORMATION SECURITY OFFICER (CISO) IS REQUIRED TO DEVELOP AND UPDATE POLICIES THAT ADDRESS INFORMATION SECURITY AND ENSURE COMPLIANCE.** Statute requires the CISO to develop and update information security policies, standards, and guidelines (Section 24-37.5-403, C.R.S.). Statute further requires the CISO to ensure the compliance with these policies. The CISO and the Office of Information Security (an office within OIT) have developed and published the Colorado Information Security Policies (CISPs). These policies outline security standards and practices that should be followed by Executive Branch agencies, as well as the Judicial Branch.

- **SYSTEM CONFIGURATIONS MUST CONFORM WITH INDUSTRY BEST PRACTICES.** During this engagement, the CISO reported that all OIT staff are directed to configure systems to benchmark standards outlined by industry leading organizations. The CISO's policies create the initial standard and point to these industry best practices. Where the CISO's policies are not specific, internal OIT policies are intended to provide additional guidance. Specifically, OIT's Configuration and Patch Management policy (Cyber-POL-101) states, "All current and future servers, desktops, and network devices deployed and/or operated by OIT will be configured to meet industry best practices." Industry best practices include configuration standards for firewalls, databases, operating systems, servers, and web servers. When a system is configured to a specific standard it decreases the likelihood the system will be targeted for exploitation by those with malicious intent or misuse by an internal employee.

- **IDENTIFIED VULNERABILITIES SHOULD BE ADDRESSED BASED ON RISK AS IDENTIFIED IN THE COMMON VULNERABILITY SCORING SYSTEM VERSION 2 (CVSS V2)**. CVSS is a globally recognized standard for assigning severity levels to technical IT vulnerabilities. When evaluating the severity of a technical vulnerability, we relied on this risk scoring system. Organizations can prioritize fixing vulnerabilities based on the risk scoring or ranking system. The risk rankings are identified from most serious to least serious. A risk ranking of "Urgent" means a remote intruder can gain Administrative privileges to a system and these items should be remediated immediately; a risk ranking of "Critical" means an intruder can gain standard privileges to a system and these items should be remediated as soon as possible; a risk ranking of "High" means an intruder can gain access to specific information stored on a system and these items should be remediated within 90 days; and a risk ranking of "Medium" means some sensitive information may be exposed and these items should be remediated within 180 days.

WHAT PROBLEMS DID THE AUDIT WORK IDENTIFY?

MULTIPLE SECURITY VULNERABILITIES EXIST WITHIN THE STATE'S NETWORKS AND SYSTEMS. Throughout the engagement we identified multiple IT security vulnerabilities within state networks and systems. In total, we identified 243 vulnerabilities in Executive Branch networks and systems. We classified these 243 vulnerabilities according to the CVSS V2 scoring system. As shown in the following chart, of the total number of vulnerabilities identified, 11% percent were critical, 31% percent were high, and 58% percent were medium. There were no urgent vulnerabilities identified.



For a more detailed explanation of the vulnerabilities identified, including an overall risk ranking by area, please see the confidential reports.

SYSTEM CONFIGURATIONS DO NOT MEET INDUSTRY BEST STANDARDS.

- **SERVER CONFIGURATIONS.** The configuration of several of the external and internal network servers we assessed was inconsistent with the various hardening standards. Relative to the external network, we identified 25 servers that are exposed to the Internet and are running operating systems that are outdated. This means they are at significant risk of breach, as the vendor is no longer developing patches to address known security vulnerabilities. Relative to the internal network for one agency, we identified four systems that are configured with a default password for the 'root' (e.g., administrator) account. The 'root' account is an account that has full permission on a system and can be used to compromise a system.

- **DATABASE CONFIGURATIONS.** The configuration of the database that supports one enterprise application is inconsistent with industry hardening standards. We acknowledge that a third party vendor manages the database. However, it is ultimately the responsibility of OIT to ensure that the vendor is adhering to specified hardening standards.

OIT STAFF ARE NOT FAMILIAR WITH OIT'S GOVERNANCE FRAMEWORK. We found that OIT staff are not knowledgeable of the current IT security governance framework including its supporting policies, procedures, standards, and guidelines. As a result, they manage the technologies they are responsible for to the best of their ability and/or based on their experience, which we found is inconsistent with OIT's IT security governance framework.

WHY DID THE PROBLEMS OCCUR?

The security vulnerabilities we identified exist or have occurred due to the following reasons:

- **CONSOLIDATION OF IT SERVICES IS NOT COMPLETE.** We found that OIT's centralization of common technologies remains incomplete. For example, we found several different firewall technologies, including those that are considered industry leaders and those that are considered non-enterprise. Another example is the wide variety of platforms being supported. OIT manages several different operating systems, along with various versions of the operating system. Traditional centralization looks to streamline technology offerings so that the shared services organization in maintaining a defined number of platforms, instead of a wide variety of technologies. In addition, as part of the consolidation, OIT has not held vendors accountable for best practices in administering IT security within systems.

- **IT SECURITY POLICIES AND STANDARDS ARE OUT OF DATE.** We found that OIT's IT security policies and standards are not consistently updated. The most current Colorado Information Security Policies (P-CISPs) were last revised August 2011.

- **OIT SECURITY POLICIES AND STANDARDS CONFLICT.** We found that OIT's information security policies (P-CISP-001 – P-CISP-019) direct agencies to develop agency-level IT policies as opposed to providing specific detail. For example, OIT's Change Control policy (P-CISP-009 3.0) states that "all Agencies and their business partners shall develop, disseminate, implement, and periodically review a formal documented Configuration Management and Change Control Program." However, OIT has developed its own configuration and patch management policy that OIT staff are to adhere to when deploying a system. These two distinctly divergent messages leave OIT staff unclear on how to perform and document changes to production systems. OIT management is aware of this conflict. During discussions with the OIT Enterprise Manager responsible for change management, we learned that an enterprise change control program is currently being redesigned and is anticipated for rollout in March 2015. However, until this new enterprise change control program is released and current information security policies are updated and released, OIT policies and standards will continue to conflict.

- **LACK OF AN EFFECTIVE COMMUNICATION OF OIT POLICIES.** OIT lacks an effective mechanism to ensure all OIT staff receive and fully comprehend

OIT management's IT security policies and procedures. For example, OIT staff responsible for patching systems reported that they were not aware of the current patch management policy or any supporting procedures and/or tools that OIT has provided to support patch management. OIT management has selected a specific solution as the enterprise patch management solution. However, OIT staff that support IT services at one agency were unaware of this solution and are instead using a different, or second, solution. While there is nothing inherently wrong with the second solution, when an organization is using multiple patch management solutions, it increases the difficulty in administrating patch management across the entire enterprise, and increases the chances that critical patches will not be applied in a timely manner.

- **OIT DOES NOT HOLD STAFF ACCOUNTABLE FOR FOLLOWING POLICIES**. The current method used by OIT to manage IT policy changes does not include a component of accountability and/or monitoring to ensure each OIT staff is properly trained and adhering to the OIT management approved policy. For example, the firewalls for one executive branch agency (Agency A) are not under the central control and administration of OIT's Network Services Security Operations Manager. While the administrator of Agency A's firewalls is an OIT employee, they are not operating or reporting directly to OIT's Network Services Security Operations Manager. Instead, this OIT employee acts semi-autonomously and is not held accountable to adhering to the practices of OIT's Security Operations Manager. Another example is OIT's change management process. According to OIT's Change Control policy (P-CISP-009, 7.3), system vulnerabilities should immediately be remediated. OIT management has provided a dashboard, available to OIT staff, that shows system vulnerabilities but there is no follow-up or effective monitoring process to ensure system vulnerabilities are remediated in a timely manner.

- **OIT'S STRATEGIC VISION NOT SHARED WITH OIT STAFF.** We found that OIT management has not effectively communicated its overall strategic vision related to IT security governance. While OIT maintains a strategic planning document known as the "OIT Playbook," we found that staff were not familiar with this planning document. During interviews with OIT staff, we found that OIT staff in charge of day-to-day operations were unclear on the OITs IT security strategy and as a result they are not sure on the direction of the organization or its governance in the area of IT security.

WHY DO THESE FINDINGS MATTER?

The problems noted above are important because individually they each contribute to a weaker network and system security posture. When combined they create an environment ripe for a network or system breach. For example, the current set of IT security policies do not address the current IT security trend of Advanced Persistent Threats (APTs). APTs are continuous, methodical attempts to penetrate and exploit an organization's network and information. Attackers could leverage multiple vulnerabilities within a system to install malware in order to gain control of IT assets. Attackers could then move slowly through the network to capture and extract sensitive information. This represents a weakness in the State's security posture. Lack of actively monitoring compliance with policies and standards leads to inconsistent systems and device configuration and unapplied security patches. This results in a technology environment ripe for breach by an external attacker or an internal employee. Depending on the type of attack executed and how successful the attack is, systems could be rendered unresponsive, citizen or employee data could be compromised, or the network could be used to breach other trusted systems. In addition, if a breach occurs and become public knowledge the organization could suffer negative will due to media exposure.

RECOMMENDATION NO. 1:

The Governor's Office of Information Technology (OIT) should improve IT security governance by:

a. Continuing the consolidation efforts of IT services, including updating outdated operating systems and reconfiguring systems that are using default passwords.

b. Holding vendors and OIT staff accountable for best practices, including industry hardening standards, in administering OIT systems.

c. Updating its IT security policies, including the Colorado Information Security Policies (CISPs), on a regular basis including the removal of conflicting language and timely communicating these updates to all OIT staff.

d. Implementing a comprehensive internal training program that will ensure all OIT staff are adequately trained on the current IT policies and procedures, and informed on the current strategic plan and its goals and objectives. The program should include accountability and consequences for non-adherence components. Further, implementation of the program should include defined monitoring periods.

Governor's Office of Information Technology Response:

A. AGREE. IMPLEMENTATION DATE: DECEMBER 2015.

OIT's infrastructure encompasses different technologies and varied interdependent infrastructure. Fixing one system or one configuration can sometimes adversely impact another system in another area. OIT will remediate this finding at an enterprise level and will need until December 2015 to fully remediate this finding due to the complexity of the environment. At a minimum OIT will have to identify those systems that have default passwords, implement a validation plan before changing the default passwords to ensure that all systems including peripheral are still operational before changing the password, schedule relevant downtimes, identify relevant network infrastructure components and identify internal resources who are subject matter experts to ensure that default passwords can be changed in most effective and efficient manner. As OIT moves towards consolidating and standardizing the environment, several system vulnerabilities, such as the one identified here, will systematically be remediated. OIT's consolidation efforts are ongoing.

B. AGREE. IMPLEMENTATION DATE: DECEMBER 2015.

OIT agrees that systems should be hardened as required by OIT standards that are based on industry best practices. OIT's policies and standards are in the process of being revised and submitted to the Executive Leadership team for approval. Once approved, these policies and standards will be published and made available to all OIT personnel, state agencies and vendors. OIT will implement an annual operational review for all relevant OIT staff and vendors to strengthen accountability and ensure compliance with established policies and procedures.

C. AGREE. IMPLEMENTATION DATE: JULY 2015.

OIT agrees that a process for reviewing, updating, and communicating policies is critical to the business. The Colorado Information Security Policies are being revised and will be submitted for approval to executive leadership team for approval. Once approved, these policies will be published and made available to all OIT personnel and state agencies. Currently any new policies that are approved by the executive leadership team are communicated to all OIT staff through email and also published on OIT's internal website. OIT will enhance its policy communication effort by creating a quarterly update with OIT staff.

D. AGREE. IMPLEMENTATION DATE: JULY 2015.

OIT agrees that a comprehensive internal training is needed to ensure that all relevant staff are trained on the current IT policies and procedures. The Colorado Information Security Policies are being revised and will be submitted to executive leadership team. Once approved, these policies will be published and made available to all OIT personnel and state agencies. Any new policies are communicated to employees via email as well as published on OIT's internal website. OIT's policy communication effort will be enhanced with quarterly updates to OIT staff. OIT will provide annual training for all OIT employees to make them aware of policies and procedures relevant to their area.

OIT informs all OIT staff on its current strategic plans, goals and objectives through annual playbook initiatives. The CIO and Executive Leadership Team conduct quarterly meetings ("All-Hands", "Open-Mic", "All-Managers") to reinforce them across the organization. OIT leaders work diligently to operationalize strategic goals and objectives. Progress of OIT's goals is tracked and managed by the Executive Leadership Team and also included in performance plans. OIT leadership believes employees are now aware of playbook initiatives and considers this part of the recommendation implemented.

DISASTER RECOVERY PLANNING

Enterprise applications are IT applications that provide a comprehensive solution in a specific business area. For example, a software solution that manages all of the accounts receivables, accounts payable, and other financial tools would be combined into one enterprise solution. Enterprise applications that are critical to conducting state business, including those applications used heavily by the public, should have comprehensive disaster recovery plans. These plans are to be developed with the business owners of the applications, to ensure that applications can be restored in a timely manner in the event of a failure or disaster. These disaster recovery plans should be tested on a regular basis. The tests should help IT organizations and the business owners refine and improve the disaster recovery plans.

WHAT AUDIT WORK WAS PERFORMED AND WHAT WAS THE PURPOSE?

The purpose of audit work was to determine if there are disaster recovery plans, and if those plans have been tested, for the three enterprise applications we tested at OIT and the Judicial Branch.

HOW WERE THE RESULTS OF THE AUDIT WORK MEASURED?

We applied the following criteria when evaluating the sufficiency of disaster recovery plans for the enterprise systems we tested:

The Office of Information Security's Disaster Recovery policy (P-CISP-004, 7) requires agencies to develop disaster recovery plans in order to reduce the impact of key business functions and processes. This policy applies to all executive branch agencies, as well as the Judicial Branch. Each agency is required to maintain a plan, training staff on it, and test against it on a regular basis.

WHAT PROBLEMS DID THE AUDIT WORK IDENTIFY?

As part of our assessment, we inquired with both OIT and the Judicial Branch about disaster recovery plans and testing for the enterprise systems we tested. We noted that disaster recovery measures and the development of a written disaster recovery plan have not been implemented, as we were unable to obtain documentation or evidence of a business continuity or disaster recovery plan.

WHY DID THE PROBLEMS OCCUR?

We determined than neither OIT nor the Judicial Branch has prioritized resources to plan and develop disaster recovery plans for these critical applications.

WHY DO THESE FINDINGS MATTER?

When a disaster strikes, the normal operations of the enterprise are suspended and replaced with operations spelled out in the disaster recovery plan. The risk associated with the failure to maintain a comprehensive tested disaster recovery plan varies based on the nature of the unplanned business disruption. Generally, without a disaster recovery plan, the organization may be unable to perform day-to-day tasks in a timeframe acceptable to its customers, in this case, the public. As a result, the organization may suffer significant downtime to enterprise applications used by both state employees to conduct critical business or in some cases by citizens to conduct necessary business.

RECOMMENDATION NO. 2:

The Governor's Office of Information Technology should improve their ability to manage an interruption of the two enterprise applications by:

a. Working with the business owners of the enterprise application to develop a comprehensive disaster recovery plan for each enterprise application.

b. Developing comprehensive recovery testing strategies and performing recovery testing on a regular basis.

c. Updating the disaster recovery plan based on feedback and analysis of the testing done in subpart B.

Governor's Office of Information Technology Response:

A. AGREE. IMPLEMENTATION DATE: DECEMBER 2015.

OIT agrees that a comprehensive disaster recovery plan is critical. OIT is already working on documenting the disaster recovery plan for one of the two applications identified and will create a testing strategy and implement a schedule for regular disaster recovery plan maintenance by September 2015. For the other application, OIT has already initiated the process of identifying business requirements with the agency for disaster recovery. If funding is needed, OIT will work with the agency to secure funding and resources. While it is hard to ascertain a firm implementation date for this application due to several unknowns, OIT will strive to fully implement this recommendation by December 2015.

B. AGREE. IMPLEMENTATION DATE: DECEMBER 2015.

Once business needs are formalized, OIT will work with the agency to document disaster recovery plan including procuring the needed infrastructure and resources, identifying testing strategies, conducting the disaster recovery test and ensuring that the plan is updated on a regular basis. If funding is needed, OIT will work with the agency to secure funding and resources. While it is hard to ascertain a firm implementation date for this application due to several unknowns, OIT will strive to fully implement this recommendation by December 2015.

C. AGREE. IMPLEMENTATION DATE: DECEMBER 2015.

Once OIT is able to test the disaster recovery plans, OIT will ensure that the plan is updated on a regular basis by December 2015.

RECOMMENDATION NO. 3:

The Judicial Branch should improve their ability to manage an interruption of the one enterprise application by:

a. Developing a comprehensive disaster recovery plan for the one enterprise application.

b. Developing comprehensive recovery testing strategies and performing recovery testing on a regular basis.

c. Updating the disaster recovery plan based on feedback and analysis of the testing done in subpart B.

Judicial Branch Response:

A. AGREE. IMPLEMENTATION DATE: JUNE 2016.

The Department believes that a comprehensive Disaster Recovery Plan (DRP) is an important element of our overall IT policies and procedures. The Department has developed and implemented various aspects of a DRP including two data centers, redundant servers and network equipment, as well as data replication for our enterprise applications. Furthermore, the Department has requested in Fiscal Year (FY) 2016 additional funding to engage IT consultant services to help develop a viable and actionable DRP.

B. AGREE. IMPLEMENTATION DATE: JUNE 2016.

The Department agrees to develop a comprehensive recovery testing strategy as part of our disaster recovery plan and will perform recovery tests on a regular basis.

C. AGREE. IMPLEMENTATION DATE: JUNE 2016.

The Department agrees to update the recovery plan addressed in this recommendation based on feedback and analysis of the testing completed in subpart B.

LOGICAL ACCESS CONTROLS FOR ENTERPRISE APPLICATIONS

IT systems, such as enterprise applications, are usually secured with user names and passwords. The rules and controls surrounding access to IT systems are called logical access controls. The Office of Information Security has developed rules surrounding logical access, and all Executive Branch agencies and the Judicial Branch are required to follow these rules. These rules including logging and monitoring access to systems, configuring password expiration dates, developing system roles and segregated duties within the system, and conducting periodic user access reviews.

WHAT AUDIT WORK WAS PERFORMED AND WHAT WAS THE PURPOSE?

The purpose of audit work was to determine if logical access controls for the three enterprise applications reviewed were in compliance with Colorado Information Security Policies (P-CISPs).

HOW WERE THE RESULTS OF THE AUDIT WORK MEASURED?

We applied the following criteria when evaluating the sufficiency of logical access controls for the enterprise systems we tested:

- **THE CHIEF INFORMATION SECURITY OFFICER (CISO)** is required to develop and update policies that address logical access and ensure compliance. Statute requires the CISO to develop and update information security policies, standards, and guidelines (Section 24-37.5-403, C.R.S.). This includes the development of policies related to logical access. Statute further requires the CISO to ensure the compliance with these policies.

- **AGENCIES ARE TO CONDUCT PERIODIC USER ACCESS REVIEWS.** According to the Office of Information Security's Access Control Policy (P-CISP-008, 7.2.1.3), agencies are to develop procedures to ensure lists of terminated staff are reconciled with user accounts on systems, so that all access credentials are revoked, retrieved, changed, or otherwise become inaccessible to the terminated staff member. A regularly scheduled user access review of all user accounts is a key control that should be utilized by the organization to ensure that all access to the production system is current and authorized, and that adequate segregation of duties remains in place.

- **IT SYSTEMS SHOULD HAVE ROLE-BASED ACCESS AND ACCOUNTS**. The Office of Information Security's Access Control policy (P-CISP-008, 3) requires agencies to create role-based access, establishing varying levels of access so that users have the appropriate level of access to perform job duties (P-CISP-008, 7.2.9.1).

- **SYSTEM ACCESS IS TO BE LOGGED**. The Office of Information Security's Access Control policy (P-CISP-007, 7.6) also requires agencies to monitor anomalous system activity. Logging should be enabled for critical systems in accordance with Access Control Policy P-CISP-008. Furthermore, agencies are required to maintain the logs for at least one (1) year.

- **PASSWORDS MUST BE CHANGED EVERY 90 DAYS.** The Office of Information Security's Access Control policy (P-CISP-008, 7.2.6.4) states that passwords are to be changed at least every 90 days. The same policy also requires agencies to log all successful and failed access attempts (P-CISP-008, 7.2.7.1).

WHAT PROBLEMS DID THE AUDIT WORK IDENTIFY?

USER ACCESS REVIEWS ARE NOT OCCURRING. We tested user access provisioning for the three enterprise applications at the Executive Branch and Judicial Branch, and verified that appropriate documentation was available and processed by the appropriate persons, in accordance with organization policy and procedure. However, we noted that a regularly scheduled user access review of all user accounts for the three systems reviewed has not been formalized or has not been conducted on frequent basis. For example, for one enterprise application at the Executive Branch, a user access review is only conducted once every three years. The other Executive Branch enterprise application we found that a regularly scheduled user access review of all user accounts has not been formalized and is currently not in place. For the Judicial Branch, we found that a regularly scheduled user access review of all user accounts has not been formalized and is currently not in place.

A regularly scheduled user access review of all user accounts is a key control that should be utilized by the organization to ensure that all access to the production system is current and authorized, and that adequate segregation of duties remains in place.

ENTERPRISE APPLICATION SEGREGATION OF DUTIES MATRICES DO NOT EXIST. As part of our testing of the enterprise applications, we assessed the type of access granted to users. This testing is typically based on pre-defined roles that have been developed to eliminate violations of segregation of duties. However, we were informed that segregation of duties matrices do not exist for the applications in scope. The most effective method to ensure segregation occurs is to develop a management-approved segregation of duties matrix and provide it to the application administrator (i.e., person(s) responsible for user setup).

APPLICATION LEVEL LOGGING OF ADMINISTRATIVE ACCOUNTS. For the Judicial Branch application, we identified ten accounts with full administrative access to the Judicial application. Based on inquiry, we determined that none of the administrative access is logged or monitored at the application level.

We also found one Executive Branch enterprise application that did not log or monitor administrative access at the application level.

ADMINISTRATIVE ACCOUNTS WITHOUT PASSWORD EXPIRATIONS. For one Executive Branch application, we found three accounts with administrative access that have passwords that do not expire.

WHY DID THE PROBLEMS OCCUR?

We determined that these problems occurred for three main reasons. First, OIT and the Judicial Branch have not created a formal process to review all production-level user accounts on a regular basis.

Second, we determined that passwords and comprehensive logging controls for one of the two Executive Branch enterprise applications reviewed have not been reviewed and adjusted according to Information Security Policies. For the Judicial Branch, we determined that they have not been reviewed and adjusted according to Information Security Policies.

Third, we determined that proper segregation of duties matrices for the two Executive Branch applications and the one Judicial Branch application have not been developed.

WHY DO THESE FINDINGS MATTER?

Without an annual review of all production users, there is an increased likelihood that production systems will have active accounts that were initially assigned to a former employee. Depending on the privilege level of the account, the account may be used by current employees to gain access to sensitive information or information that they do not need to perform their job responsibilities. In worst-case scenarios, an attacker may breach a production system and obtain sensitive and/or confidential information.

The lack of segregation of duties matrices, combined with the complexity of the application technologies deployed, creates a ripe environment where fraudulent transactions or the misuse of sensitive information can occur and be undetected for an extended period of time.

Administrative privileges allow a user to perform any function within the application. Permitting accounts to have non-expiring passwords greatly increases the risk of the account password becoming known by someone other than the account owner, and, as such, fraudulent transactions or the misuse of sensitive information may occur. Password expiration is one of several methods used to reduce the likelihood of the password for an account becoming known to anyone other than the account owner. Keeping the password safe is a key factor in the overall security of an individual's digital identity, and consequently the services and resources to which that identity has been granted access. Additionally, without logging successful and failed attempts to access a system, it is nearly impossible for IT security staff to conduct forensics reviews in the event of an incident.

RECOMMENDATION NO. 4:

The Governor's Office of Information Technology should improve logical access controls for the two enterprise application(s) reviewed by:

a. Working with the business owners of the two enterprise applications to review all active production user accounts to ensure they are assigned to current employees and to assess the appropriateness of access granted.

b. Ensuring that passwords for administrative accounts for the one critical application, identified and communicated under separate cover, are consistent with the State Information Security Policies, and ensuring that administrative access is adequately logged and monitored.

c. Developing a segregation of duties matrix for the one critical application identified and communicated under separate cover.

Governor's Office of Information Technology Response:

A. AGREE. IMPLEMENTATION DATE: JULY 2015.

OIT agrees that application user access should be assigned to current employees and that access is commensurate with job responsibilities. OIT will work with the agency to help review the application users.

B. AGREE. IMPLEMENTATION DATE: SEPTEMBER 2015.

OIT will evaluate the administrative accounts identified and will ensure that the passwords for these accounts are consistent with state security policies. OIT will implement this part of the recommendation by January, 2015. OIT will work with relevant stakeholder to evaluate the need for new tools, technology, system and resources requirements for implementing logging and monitoring of users with administrative access. Without a firm solution carved out and all variables assessed it is hard to ascertain a firm implementation date for this part of the recommendation. Based on initial analysis, OIT will strive to fully implement this part of the recommendation by September 2015.

C. AGREE. IMPLEMENTATION DATE: JULY 2015.

Establishing a segregation of duties matrix is a joint responsibility shared between OIT and business users/agency. We are aware of the need to improve in this area and have already started evaluating existing profile earlier this year. We have already completed part of this recommendation and are now preparing to launch a new configuration application by July 2015, with which, we expect to fully implement this recommendation.

RECOMMENDATION NO. 5:

The Judicial Branch should improve logical access controls for the one enterprise application reviewed by:

a. Reviewing all active production user accounts to ensure they are assigned to current users and to assess the appropriateness of access granted.

b. Ensuring that administrative access is adequately logged and monitored.

c. Developing a segregation of duties matrix for the one critical application identified and communicated under separate cover.

Judicial Branch Response:

A. AGREE. IMPLEMENTATION DATE: JUNE 2016

The Department will work with our IT advisory committee and stakeholders to implement ongoing procedures necessary for reviewing all ICCES accounts and ensure all active user access is appropriate.

B. AGREE. IMPLEMENTATION DATE: JUNE 2016

The Department agrees that it would be advantageous to log and monitor activity associated with the administrative accounts and will plan to incorporate such changes to the system.

C. PARTIALLY AGREE. IMPLEMENTATION DATE: NOVEMBER 2015

The Department's IT Department has created a Responsible, Accountable, Support, Consulted, and Informed (RASCI) chart for all systems and applications. With one IT staff dedicated to the Department's information security systems, the Department will find it very difficult to implement a true segregation of duties matrix given that multiple IT staff take on many different roles, which is in direct conflict with the Information Systems Audit and Control Association (ISACA) recommendation that no one employee should have responsibility to complete two or more major responsibilities. With a relatively small IT department who work in an agile environment, the Department's IT staff must take on multiple responsibilities in order to work efficiently and implement technical solutions to the business requirements in a timely manner.

Auditor's Addendum:

The Office of Information Security's Access Control policy (P-CISP-008, 3) requires agencies to create role-based access, establishing varying levels of access so that users have the appropriate level of access to perform job duties (P-

CISP-008, 7.2.9.1). If the *Department is experiencing resource constraints a compensating controls such as monitoring would be appropriate.*

S|C

the advantage of insight

6922 W. Linebaugh Ave., Suite 101
Tampa, FL 33625
877.578.0215
www.securanceconsulting.com