COLORADO
Information Security
Governor's Office of Information Technology

Secure Colorado

Colorado's Strategy for Information Security and Risk Management

Fiscal Years 2017-2019

Table of Contents

SECTION I: Introduction & Background

Progress and Still More Work to Be Done...

This strategic plan, known as Secure Colorado, set the stage for ongoing security improvements, creating a budget and enabling strategic decisions and investments to protect the data Coloradans have entrusted to state government. Secure Colorado outlines the strategic goals and initiatives of the Colorado Information Security Program to safeguard the state's information assets and assure the confidentiality, integrity, and availability of the information vital to achieve the State of Colorado's mission.

Secure Colorado has been operational for more than three years now, and it's my great privilege to be able to highlight some of the program accomplishments.

- Measuring enterprise risk, using a Risk Index, we have reduced risk across the state by 48% over the past two years. In fiscal year 2016, we were successful in reducing the risk for all executive branch agencies below our enterprise risk index goal. For the five agencies with the highest risk scores, this represented a 20%-56% improvement in a two-month timeframe.
- We created Agency Risk Report Cards to demonstrate how well we are managing risk for each agency. Metrics reported include the following: agency risk index, the level of agency systems compliance with our hardening standards, how many open audit findings exist for each agency, how well our tools are automatically remediating threats in the agency environment, how effective we are at patching the agency systems, and agency completion of security awareness training.
- We switched from annual to quarterly Cybersecurity Awareness training to ensure that security remains top-of-mind for all state employees.
- We participated in and led multiple simulated cybersecurity incident response activities in partnership with the Colorado National Guard, Regis University, and other state and local responders. These exercises have helped us to uncover and remediate gaps in our incident response plan, and have helped to create familiarity so that in an actual incident, teams know immediately what to do and how to get started on investigating, containing and recovering from a cyber incident. Additionally, through the use of partners, we are able to practice our combined response which helps us to understand each other's capabilities and strengths and prepares us for good partnership during an actual event.
- We implemented an identity and access management toolset for OIT. We are now ready to introduce this as an enterprise-wide toolset. This will reduce the time it takes our team to provision employee access for each agency and improves the thoroughness in which employee access is deprovisioned.
- Secure Colorado was chosen as a model for the National Governor's Association policy academy to help states who are less mature in their cybersecurity programs to develop a sustainable cybersecurity strategy.
- The implementation of a secure coding assessment tool enabled software developers to find and fix more than 4,000 otherwise unknown application security vulnerabilities. The implementation and use of this tool ensures that developed applications do not contain vulnerabilities that would put sensitive agency data at risk.
- As part of our cybersecurity community outreach, we provided Internet Safety presentations to more than 900 students in grades 6-8.

Even with these successes, there still remains much to do. While we have components of all of the 20 Critical Security Controls implemented, ad-hoc processes need to be formalized and manual processes need to be automated to ensure consistency in performance. Implementing additional sub-controls, fine tuning of existing controls and maturation of the program will be ongoing activities. Additionally, we are looking forward to deploying security analytics capability this year, improving our ability to detect and respond to anomalous activities in our network.

This important work is not done in a vacuum. In 2015 and again in 2016, the Colorado Information Security Advisory Board reconvened to receive an update on our progress and to reevaluate Secure Colorado. The Board provided valuable input and recommendations, while continuing to affirm that the direction and program priorities are relevant, appropriate, and sound. The work of this team continues to guide program relevancy to ensure continued cybersecurity investment will provide maximum benefit to the agencies we serve and all Colorado residents.

Sincerely,

Deborah M. Blyth
Chief Information Security Officer

Information Security Governance

The Colorado Information Security Program was created through legislation in 2006. According to Colorado law (C.R.S. § 24 -37.5-4xx), the Colorado Information Security Program is overseen by the Chief Information Security Officer (CISO) and applies to "public agencies." A public agency is defined as: "… every state office, whether executive or judicial, and all its respective offices, departments, divisions, commissions, boards, bureaus, and institutions. "Public agency" does not include institutions of higher education or the general assembly."

According to statute, the CISO shall:

- Develop and update information security policies, standards, and guidelines for public agencies.
- Promulgate rules containing information security policies, standards, and guidelines.
- Ensure the incorporation of and compliance with information security policies, standards, and guidelines in the information security plans developed by public agencies.
- Direct and respond to information security audits and assessments in public agencies in order to ensure program compliance and adjustments.
- Establish and direct a risk management process to identify information security risks in public agencies and deploy risk mitigation strategies, processes, and procedures.
- Approve or disapprove and review annually the information security plans of public agencies.
- Conduct information security awareness and training programs.
- In coordination and consultation with the Office of State Planning and Budgeting and the Chief Information Officer (CIO), review public agency budget requests related to information security systems and approve such budget requests for state agencies other than the legislative branch.
- Coordinate with the Colorado Commission on Higher Education for purposes of reviewing and commenting on information security plans adopted by Institutions of Higher Education.
- Oversee incident response activities as well as the investigation of security breaches, and assist with the disciplinary and legal matters associated with such breaches as necessary and maintain authority to direct discontinuation of services from unsafe systems.
- Maintain relationships with local, state and federal partners and other related private and government agencies.

Within the Governor's Office of Information Technology (OIT), the CISO reports to the CIO. Information security duties and responsibilities for executive branch agencies are administratively divided between the CISO and the Chief Technology Officer (CTO). While the CISO maintains responsibility for information security governance, architecture, risk, and compliance, the CTO is responsible for overseeing day-to-day security operations, including access provisioning, network and endpoint security monitoring and administration, threat and vulnerability management, and computer forensics and incident response.

OIT Mission, Vision & Goals

It is important that Secure Colorado aligns with OIT's mission and goals, which in turn are aligned with the Governor's strategic plan. Protecting Coloradans' data is required to align to OIT's mission.

Mission

To securely enable the effective, efficient and elegant delivery of government services through trusted partnerships and technology.

Vision

Enriching the citizen experience at every digital touchpoint

Every interaction Coloradans have with the state is a critical touchpoint and each touchpoint should be positive. Though it is our customers who directly serve the public, OIT is the IT service delivery partner that enables them to do so. Today, we are building the foundation for a seamless end-to-end user experience. We are propelling broadband coverage across the state, leading the way for enterprise solutions enabling agencies to more effectively collaborate, streamlining processes for more efficient service, and enhancing security to keep public data and systems safe.

We envision a future where the entire journey of a citizen receiving state services is simple and fast no matter how many agencies or applications are involved on the back-end; customers get the services they need, when they need it, wherever they are.

Goals

Since FY15, OIT has kept a steady focus on four major areas: service excellence, information security, employee engagement, and IT economic development. In FY17, we will continue to center on these areas to drive positive behavioral changes throughout the organization.

I. Delivering effective solutions and reliable customer service
II. Securing Colorado Through Innovation
III. Advancing a culture of employee support and collaboration
IV. Strengthening Colorado's Technology Landscape

Colorado Information Security Program Vision & Mission

The following are the vision and mission for the Colorado Information Security Program, including a description of our philosophy for tackling the state's information security challenges and assuring the confidentiality, integrity, and availability of state networks, systems, and data.

Vision

Cost-effectively preserving the confidentiality, integrity, and availability of state and Coloradans' data through the innovative use of the right people, processes, and technology.

Mission

Enable the State of Colorado to achieve its business objectives by maintaining an appropriate level of information security risk that promotes innovation, the effective use and adoption of information and information technologies, and fosters citizen engagement and e-commerce.

Team Slogan

Together, enabling state government operations through the efficient, effective, and elegant application of information security.

Philosophy Toward Information Security & Risk Management

Our philosophy describes how we approach the development of solutions for securing Colorado's information and systems. The Colorado Information Security Program will perform its work according to the following principles:

1. Offense must inform defense
2. Security must be built into business processes and IT systems from the start
3. Cyber threats are mitigated through the right combination of people, processes, and technology
4. Our security efforts must first be focused on our high value targets
5. Complexity is the enemy of security
6. Automated controls are superior to manual controls
7. Security drives compliance and not vice versa
8. Security must be efficient - only those security resources necessary to achieve our mission are acquired and deployed
9. Security must be effective - security must be results-oriented and anticipated outcomes measured, tracked, and compared to the resources expended
10. Security must be elegant – the most effective controls and security solutions are those that are transparent to the business and end user and seamlessly integrate with the state's business processes and existing technology

SECTION II: Strategic Priorities

Secure Colorado establishes a roadmap for improving cybersecurity in Colorado. This plan was developed in cooperation with the Colorado Information Security Advisory Board (Board). The Board was formed by the CISO in 2012 to assist in the development of strategic and tactical plans aimed at reducing the State of Colorado's risk levels and improving the confidentiality, integrity, and availability of the information entrusted to the state. The Board has met annually since 2015, with almost half of the original members returning alongside with some new members. These individuals represent public and private sectors, along with higher education, and include security, privacy, and business professionals. See Appendix A for 2016 Board Membership.

Secure Colorado includes four strategic goals supported by 18 strategic initiatives. These goals and initiatives are based on foundational information security principles that are designed to be relevant for years to come. Supporting operational initiatives will be developed annually and included in the OIT Playbook, which can be found on the OIT's website (colorado.gov/oit). These operational-level initiatives will be the Colorado Information Security Program's primary focus for that specific fiscal year, and will be aligned with one or more of Secure Colorado's strategic goals and initiatives.
To maintain its relevancy, Secure Colorado will be reviewed annually by the CISO in conjunction with the Board and OIT's Executive Leadership Team.

Protection

Goal 1: Protect State of Colorado information and information systems to assure that the confidentiality, integrity, and availability of all information is commensurate with mission needs, information value, and associated threats

Strategic Initiatives

Initiative 1.1 - Design, build, and operate resilient and self-healing systems and networks that are capable of resisting current and emerging cybersecurity threats.
Initiative 1.2 – Recruit, develop, and retain a motivated, professional, and knowledgeable information security workforce.
Initiative 1.3 - Design, build, and operate the necessary tools, techniques, and procedures to maintain 24/7 information security situational awareness of all state networks, systems, and data.
Initiative 1.4 - Develop and maintain information security policies, standards, and guidelines that are relevant, adaptable, and cost-effective.
Initiative 1.5 - Promote the understanding and acceptance of information security concepts and practices throughout state government.
Initiative 1.6 - Equip state information technology professionals with the tools, knowledge, and skills to design, build, and operate secure applications and systems.

Initiative 1.7 – Develop, document, and socialize an information security architecture that (1) aligns with the technology strategy, (2) transparently integrates security processes into next-generation state networks and systems, and (3) anticipates and addresses future threats.
Initiative 1.8 – Develop and maintain a statewide incident response and computer forensic capability that is able to (1) quickly identify and isolate security incidents, (2) recover impacted systems and business processes, and (3) when feasible, identify and prosecute those attacking state systems.
Initiative 1.9 – Develop, document, and implement a standardized risk management framework for accurately and uniformly assessing and managing the risk to the confidentiality, integrity, and availability of state systems and networks.

Research & Development

Goal 2: Research, develop, and employ innovative and sustainable information security solutions to address Colorado's cybersecurity challenges

Strategic Initiatives

Initiative 2.1 - Actively leverage federal government, private sector, academic research, and development of advanced cybersecurity tools and capabilities to assure the confidentiality, integrity, and availability of state systems and data.
Initiative 2.2 - Rapidly evaluate, build, and deploy cutting-edge information security technologies to outpace emerging threats.
Initiative 2.3 – Identify, evaluate, and share information on the threats and vulnerabilities impacting state government to support future research and development efforts.

Partnerships

Goal 3: Develop and foster key partnerships to improve information sharing, reduce information security risks, and to promote innovation and collaboration

Strategic Initiatives

Initiative 3.1 – Develop and formalize new partnerships with academic institutions, the private sector, and Colorado's state and local governments to share information security threat intelligence, research and development efforts, and best practices.
Initiative 3.2 – Maintain active participation with the relevant organizations such as the National Association of State Chief Information Officers (NASCIO) Privacy and Security Committee, Multi-State Information Sharing Analysis Center (MS-ISAC), and the SANS Institute.

Initiative 3.3 – Promote discussions and cooperative engagements that will enhance cybersecurity for all Colorado residents including partnering with the Colorado Department of Public Safety in achieving the cybersecurity objectives of the Colorado Division of Homeland Security and Emergency Management strategy.

Compliance

Goal 4: Comply with applicable information security and data privacy laws and regulations

Strategic Initiatives

Initiative 4.1 - Continuously assess and evaluate state systems and networks.
Initiative 4.2 – Conduct targeted, technical audits to identify and correct noncompliance with Colorado Information Security Policies (CISPs) and applicable federal laws and regulations.
Initiative 4.3 – Partner with executive branch agencies to assist them in preparing for and responding to information security-related audits.

SECTION III: Strategic Success Measures

Metric Name	Target	Reporting Frequency	Description
Goal 1: Protect State of Colorado information and information systems to assure that the confidentiality, integrity, and availability of all information is commensurate with mission needs, information value, and associated threats			
Percentage of State Systems Actively Managed by Security	100%	Monthly	Percentage of total state systems actively managed and protected (in near real-time).
Composite Information Security Risk Index	Low	Quarterly	Overall, enterprise-level cyber security risk rating based on current threats, asset value, and implemented security controls.
Mean Time from Incident Detection to Containment and Restoration	< 4 hours	Quarterly	Measures the average length of time necessary to contain a security incident and restore impacted services.
Percentage of Employees Completing Security Training	95%	Monthly	Percentage of state employees completing security training, including new employee training, refresher training, and technical security training.
Goal 2: Research, develop, and employ innovative and sustainable information security solutions to address Colorado cyber security challenges			
Percentage of State IT Expenditures Spent on Information Security	5%	Annual	Measures the percentage of IT expenditures utilized to design, build, and implement innovative and sustainable information security solutions.
Number of Emerging Cybersecurity Product Evaluations Completed	3	Annual	Represents the number of emerging security product reviews completed annually to address emerging cybersecurity challenges.
Mean Time from Product Evaluation and Selection to Deployment	< 120 days	Annual	The average number of days elapsed between the completion of an emerging cybersecurity need to a recommended solution.
Goal 3: Develop and foster key partnerships to improve information sharing, reduce information security risk, and promote innovation and collaboration			

Number of Active Information Sharing Agreements	Tracking Only	Annual	Tracks the number of partners for which the security program shares threat and vulnerability information.
Number of Security Thought Papers / Evaluation Products Shared with Partners	>4	Annual	Number of written cybersecurity product evaluations and thought papers shared with partners.
Goal 4: Comply with applicable information security and data privacy laws and regulations			
Number of Managed Security Audit Findings	Tracking Only	Quarterly	Tracks the total number of security-related audit findings actively being managed by the security team.
Percentage of Overdue Security Audit Findings	10%	Quarterly	Percentage of security-related audit findings that are not implemented and are past their agreed-to implementation date.
Average Number of New Security Audit Findings Per External Audit/ Inspection	< 8	Annual	The average number of new security-related audit findings per external party audit.

APPENDIX A: Colorado Information Security Advisory Board

Chad Alvarado Supervisory Special Agent Federal Bureau of Investigation	**Corey Kispert** Information Security Officer Colorado Department of Education
Alfritch Anderson Security Operations Manager Governor's Office of Information Technology	**Kevin Klein** Director Colorado Division of Homeland Security and Emergency Management
Jack Arrowsmith Executive Director Statewide Internet Portal Authority	**Drew Labbo** Chief Information Security Officer Denver Health
Dr. Beth Bean Chief Research Officer Department of Higher Education	**Mark Lewis** Manager,Western Region Engineers McAfee
Eric Bergman Policy and Research Supervisor Colorado Counties, Inc.	**Jory Maes** CO Infrastructure Protection Program Manager Colorado Department of Public Safety, Division of Homeland Security & Emergency Management
Casey Carlson Enterprise Architect Governor's Office of Information Technology	**LTC Isaac Martinez** Deputy Chief of Staff Colorado Army National Guard
Stephen Coury Chief Information Security Officer City and County of Denver	**Ted Mink** Deputy Director Colorado Bureau of Investigation
Andrea Day OSPB Analyst Governor's Office of State Planning & Budgeting	**Robert Ochoa** Account Manager Security Cisco
Everette Denney Security Solutions Director Optiv	**Chris Payne** Sr. Security Engineer McAfee
Marty Esquibel Privacy and Security Officer Colorado Department of Human Services	**Shari Plantz-Masters** Academic Dean College of Computer & Information Sciences Regis University
Nicole Frazier Denver Metro Regional Director Office of Senator Cory Gardner	**Fred Sargeson** General Manager Colorado Interactive
Ralph Gagliardi Agent-in-Charge, Identity Theft Advocacy Network	**Rich Schliep** CISO Colorado Department of State

Colorado Bureau of Investigation	
Tim Gama Program Coordinator Pueblo Community College	**Trevor Timmons** CIO Colorado Department of State
Kent Glassman Glassman and Associates	**Jonathan Trull** Principal Chief Security Advisor & Strategist Microsoft
Jon Gottsegen Chief Data Officer Governor's Office of Information Technology	**Jane Wilson** Privacy Officer Department of Health Care Policy and Financing
John Huber Sr. Director of Enterprise Applications Governor's Office of Information Technology	**Don Wisdom** Director, Infrastructure Operations Governor's Office of Information Technology
Dan Jones Assistant Vice President and CISO University of Colorado System	**Michael Wyatt** Director Public Sector Cyber Risk Services Deloitte
Ian Kelly Director of Security Google	


STATE · OF · COLORADO
UNION
AND
CONSTITUTION
NIL SINE NUMINE
1876