COLORADO
Information Security
Governor's Office of Information Technology

Secure Colorado

Colorado's Strategy for Information Security and Risk Management

Fiscal Years 2020-2022

Table of Contents

SECTION I: Introduction & Background

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

Incorporating Lessons Learned Into Our Go-Forward Strategy...

In February of 2018, the Colorado Department of Transportation (CDOT) suffered a malware event that took its business operations offline for four weeks while our team worked to contain and eradicate the malware, and then to restore services.

Having a security program in place, while it didn't make us immune to the attack, did assist significantly with recovery. Having completed an enterprise backup strategy only a few years earlier, meant that we didn't have to consider paying the ransom, as we were completely confident that all data associated with all of CDOT's production servers was safely backed up, offline, and available for a successful restore. This was proven accurate. Additionally, a network segmentation strategy ensured that the malware did not infect CDOTs Traffic Operations, nor did it infect the rest of the state agencies. Lastly, having practiced our combined incident response with the Colorado National Guard twice a year since 2014, prepared us for our combined response to this event.

In partnership with CDOT, the Office of Emergency Management, and the Colorado National Guard, we created an After Action Report, which can be found here: https://www.colorado.gov/pacific/cobeoc/news/after-action-report-released-cdot-cyber-incident

With the help and guidance of the Colorado Information Security Advisory Board, our state had the right security activities already underway. Had these been completed, they would have prevented or significantly lessened the impact of the attack. It became very clear that, having a good strategy underway, *but not completed*, doesn't provide the necessary mitigation coverage, during an attack. We realized we needed to accelerate the implementation of these efforts, to reduce the likelihood of a successful future attack.

Lessons learned during the CDOT ransomware event were incorporated into our FY20 security strategy. Therefore, during FY20, we will complete efforts that were already in progress, such as:

- Completing a Role Based Access Control strategy to ensure access is right-sized to only what is needed to perform the job
- Upgrading agency firewalls to our enterprise standard best-of-breed firewall

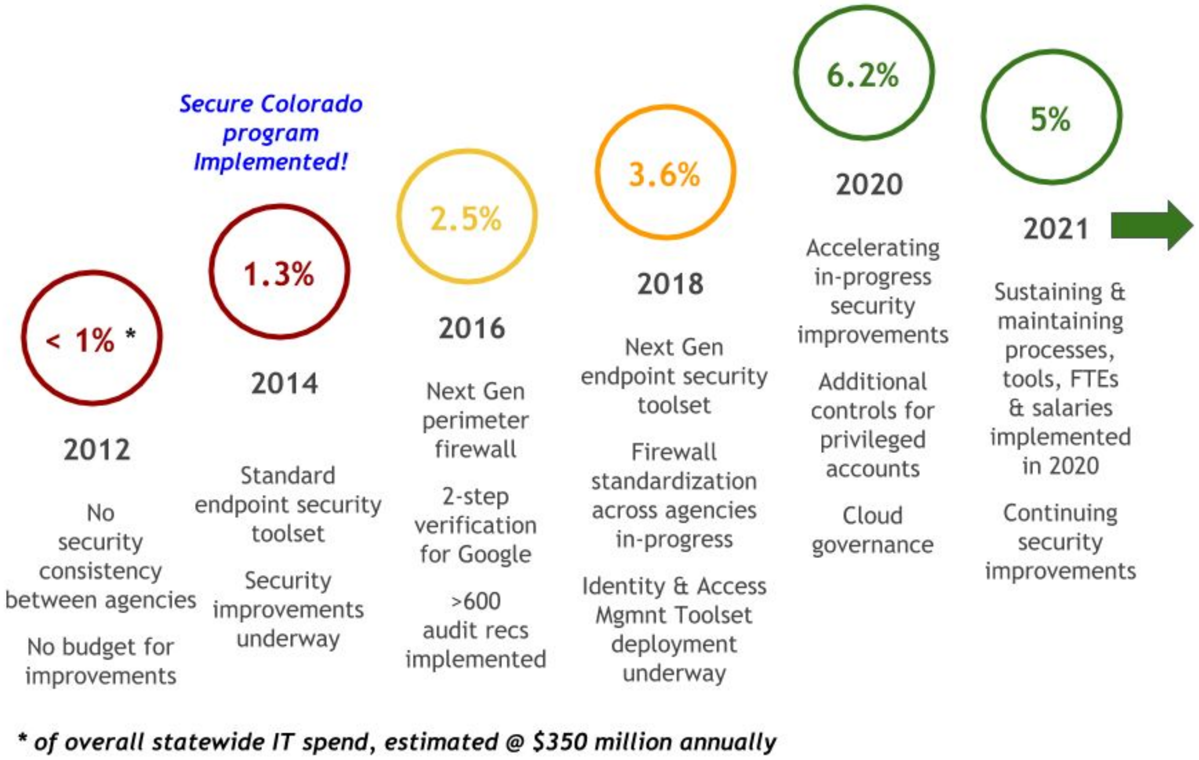
- Implementing our Identity and Access Management toolset and Privileged Access Management across the enterprise
- Broadening our use of two-factor authentication
- Improving visibility and correlation of security logs throughout the state
- Strengthening our patching capabilities, including for third-party software

Additionally, FY20 has brought new funding enabling us to:

- Create an expertly skilled cloud governance team
- Focus on the documentation of operational procedures and security standards
- Create security champions within infrastructure operations
- Perform a salary study, and adjust salaries for underpaid security analysts in hard-to-retain roles

In FY21 and FY22 we will mature these controls, as we continue to implement security best practices.

Below is a historical depiction of the budgetary growth success of the Secure Colorado Program since its inception.



Secure Colorado program Implemented!
< 1% *
2012
No security consistency between agencies
No budget for improvements
1.3%
2014
Standard endpoint security toolset
Security improvements underway
2.5%
2016
Next Gen perimeter firewall
2-step verification for Google
>600 audit recs implemented
3.6%
2018
Next Gen endpoint security toolset
Firewall standardization across agencies in-progress
Identity & Access Mgmnt Toolset deployment underway
6.2%
2020
Accelerating in-progress security improvements
Additional controls for privileged accounts
Cloud governance
5%
2021
Sustaining & maintaining processes, tools, FTEs & salaries implemented in 2020
Continuing security improvements

*** of overall statewide IT spend, estimated @ $350 million annually***

The Colorado Information Security Advisory Board continues to play an important role in validating our ongoing security strategy. In 2018, the Board last met, providing 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 include: information security governance, security architecture, risk and compliance management, identity and access management, network and endpoint security administration, threat and vulnerability management, security event monitoring, incident response, and computer forensics.

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.

Increase OIT's organizational efficiency, transparency, and customer satisfaction.

Ensure a Secure Colorado by evaluating and improving statewide cybersecurity practices.

Expand virtual access to government services anytime and anywhere.

Mission

Together we enhance the lives of all Coloradans.

Vision

Be the best public service technology organization innovating today for tomorrow.

Our goal is to delight customers in all of their interactions with OIT. This includes agency customers, strategic partners, vendors, employees, and ultimately all Coloradans. We want to ensure that customer needs are met in a timely, cost-effective manner while finding ways to prove our value and exceed expectations. We strive to be easy to work with while keeping systems, information, projects, and programs running smoothly and securely. We want to remove obstacles to create a low-effort customer experience, minimize confusion to ensure mutual understanding, streamline processes to meet customer needs faster, improve transparency of our operations and billing to prove our value, and quickly handle issues to get customers back to work delivering programs to Coloradans. In turn, we want our customers to say good things about OIT.

To achieve these outcomes, we will establish satisfaction-related metrics and listen to customers to ensure we understand what they truly need. Expected outcomes from these strategic partnerships include:

- Clarified roles and responsibilities for agency-led decision-making.
- Prioritized strategic technology direction for Colorado initiatives, enhancing the ability for agencies and OIT to plan.
- Improved IT standards and satisfaction, and thereby customer delight.
- Ensured widespread adoption of standards and best practices.

FY20 Wildly Important Goals

WIG 1: Increase OIT's organizational efficiency, transparency, and customer satisfaction
WIG 2: Ensure a Secure Colorado by evaluating and improving statewide cybersecurity practices
WIG 3: Expand virtual access to government services anytime and anywhere

OIT's Playbook can be found here: http://www.oit.state.co.us/about/playbook

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 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	98%	Monthly	Percentage of total state systems actively managed and protected (in near real-time).
% of Agencies Complying with Minimum Threshold for CIS Benchmarks	85%	Monthly	This represents the percentage of agencies with systems configured to meet a minimum threshold of compliance with CIS Benchmarks. https://www.cisecurity.org/cis-benchmarks/
Mean Time from Incident Detection to Containment and Restoration	Tracking Only Reduce over Time	Quarterly	Measures the average length of time necessary to contain a security incident and restore impacted services.
Percentage of Employees Completing Security Training	95%	Quarterly	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.
Develop expertise in Emerging Technologies and Securing Emerging Technologies	1	Annual	Represents the number of training classes per person, designed to equip the security team with the necessary training to ensure innovation at the state is including appropriate skilled security oversight.

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 / Product Evaluations / Teaching Presentations Shared with Partners	Tracking Only	Annual	Number of cybersecurity product evaluations, thought papers, and teaching presentations shared with partners.
Goal 4: Comply with applicable information security and data privacy laws and regulations			
Number of Managed Security Audit Findings	Tracking Only	Monthly	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	Tracking Only Reduce over Time	Annual	The average number of new security-related audit findings per external party audit.
Number of Security Assessments, Solution Assessments, and Vendor Assessments	17	Quarterly	Tracks the number of Security Assessments, Solution Risk Assessments, and Vendor assessments conducted each quarter.

APPENDIX A: Colorado Information Security Advisory Board

Chad Alvarado Supervisory Special Agent Federal Bureau of Investigation	**Eric Bergman** Policy and Research Supervisor Colorado Counties, Inc.
Gail Coury Chief Information Security Officer, Cloud Oracle	**Stephen Coury** Chief Information Security Officer City and County of Denver
Markie Davis Risk Management Colorado Department of Public Administration	**Andrea Day** Budgeting Analyst Governor's Office of State Planning & Budgeting
Everette Denney Security Solutions Director Optiv	**Steve Fulton** Director, Center for Information Assurance Studies Regis University
Tim Gama Program Coordinator Pueblo Community College	**Kent Glassman** Glassman and Associates
Jeff Goodwin Director Public Sector Cyber Risk Services Deloitte	**Christopher Haas** Google Cloud Customer Engineer Google
Dan Jones Assistant Vice President and CISO University of Colorado System	**Corey Kispert** Information Security Officer Colorado Department of Education
Kevin Klein Director, CO Division of Homeland Security & Emergency Management	**Drew Labbo** Chief Information Security Officer Rocky Mountain HIPAA Guru
Sue Lapierre Vice President, Information Security Officer Prologis	**Colonel Isaac Martinez** Chief Information Officer Colorado Army National Guard
Ted Mink Deputy Director Colorado Bureau of Investigation	**Kevin Ransom** Cyber Security Specialist Cisco
Dan Santangelo Deputy Chief Technology Officer Governor's Office of Information Technology	**Rich Schliep** Chief Information Security Officer Colorado Department of State
Bryan Sparling Chief Executive Officer Victory 6 Consulting	**Trevor Timmons** Chief Information Officer Colorado Department of State
Jonathan Trull Principal Chief Security Advisor & Strategist Microsoft	**Mike Whatley** Chief Technology Officer Statewide Internet Portal Authority

STATE · OF · COLORADO

UNION AND CONSTITUTION

NIL SINE NUMINE

1876