

Schedule 13
Funding Request for the 2014-15 Budget Cycle

Department: Governor's Office of Information Technology

Request Title: Secure Colorado Phase II

Priority Number: R-2

Dept. Approval by: David B. King 11/1/2013
 Date

- Decision Item FY 2014-15
 Base Reduction Item FY 2014-15
 Supplemental FY 2013-14
 Budget Amendment FY 2014-15

OSPB Approval by: Erin M. Baker 10/24/13
 Date

Line Item Information		FY 2013-14		FY 2014-15		FY 2015-16
		1	2	3	4	5
Fund		Appropriation FY 2013-14	Supplemental Request FY 2013-14	Base Request FY 2014-15	Funding Change Request FY 2014-15	Continuation Amount FY 2015-16
Total of All Line Items	Total	1,075,700	-	1,075,700	4,100,000	4,100,000
	FTE	-	-	-	-	-
	GF	-	-	-	-	-
	GFE	-	-	-	-	-
	CF	-	-	-	-	-
	RF	1,075,700	-	1,075,700	4,100,000	4,100,000
	FF	-	-	-	-	-
(5) Office of Information Technology, (A) Management and Administration of OIT, Information Technology Security Program	Total	1,075,700	-	1,075,700	4,100,000	4,100,000
	FTE	-	-	-	-	-
	GF	-	-	-	-	-
	GFE	-	-	-	-	-
	CF	-	-	-	-	-
	RF	1,075,700	-	1,075,700	4,100,000	4,100,000
	FF	-	-	-	-	-

Letternote Text Revision Required? Yes: No: If yes, describe the Letternote Text Revision:

Cash or Federal Fund Name and COFRS Fund Number: COFRS Fund 613

Reappropriated Funds Source, by Department and Line Item Name: User Changes

Approval by OIT? Yes: No: Not Required:

Schedule 13s from Affected Departments:

Other Information: The request requires corresponding schedule 13s from departments

This page intentionally left blank.



Cost and FTE

- The Office of Information Technology requests \$4.1 million Reappropriated spending authority beginning in 2014-15 for the Information Technology Security Program.

Current Program

- This budget request directly supports Secure Colorado Phase II, the second of the State's three-year information security and risk management strategic plan. This program supports the State's enterprise cyber security program and protecting the State's collection of data.
- The Office of Information Security Program is the single state source for cyber security awareness, monitoring, and defense. This program supports the State's enterprise cyber security program and protecting the State's collection of data. The mission of the OIS is to safeguard the state's information assets and citizen information against unauthorized use, disclosure, modification, damage, or loss.

Problem or Opportunity

- Key security equipment has reached end-of-life and needs to be replaced. / The current IT infrastructure, tools, and resources are not sufficient to protect the State from the more than 600,000 daily attacks currently hitting systems and are no longer sufficient for new, more advanced attacks.
- Funding for information security has not been sufficient to implement industry recommended critical security controls, meet state and federal regulatory requirements, or maintain an appropriate level of risk.

Consequences of Problem

- Failure to refresh the State's core security infrastructure and implement critical security controls will result in increased network and system downtime, data loss, and potential fraud and abuse.
- Funding is required to achieve the goals contained in Secure Colorado, the State's three-year strategic plan for addressing the evolving cyber threat and reducing risk, fraud, and abuse.

Proposed Solution

- Continued funding of the Secure Colorado Program will provide for new hardware to refresh/upgrade firewalls; refresh/upgrade the State's domain name servers; and procure network traffic analyzers, access control appliances, and incident detection and response tools.
- New software – application layer monitoring and defensive software to identify and stop layer 7 attacks and outages (a more sophisticated and less identifiable type of attack). Cyber threats to Colorado include attacks or threats to data, applications, host servers/network, internal networks, perimeter, physical attacks, and policies/procedures/awareness.
- Procure managed security services (contractors) to install, tune, and monitor security infrastructure.

This page intentionally left blank.



COLORADO

Office of Information Technology

FY 2014-15 Funding Request | November 1, 2013

John W. Hickenlooper
Governor

Kristin D. Russell
Secretary of Technology and
Chief Information Officer

Department Priority: R-2
Request Detail: Secure Colorado Phase II

Summary of Incremental Funding Change for FY 2014-15	Total Funds	General Fund
Office of Information Security Program	\$4,1000,000	\$4,100,000

Problem or Opportunity:

Information security continues to be a significant risk area for state government. The recent Colorado State Auditor Report titled "Information Technology in Colorado State Government August 2013", identified information security as its primary risk area. The risk includes the vulnerability of state information to attacks, and citizen information held by various state entities.

Protection of state and citizen data requires a layered defense that protects against the range of security challenges facing government institutions today. The layered defense needs to address the users (internal and external), infrastructure and applications that maintain state and citizen data.

Cyber threat to Colorado

Colorado state networks and systems are continuously under attack. These attacks are increasing in volume and sophistication and are quickly overwhelming existing staff, network and cyber security equipment. During FY 2012-13, the State was hit with an average of over 600,000 cyber security attacks per day. Of these attacks, 25 percent were malware, Trojans and worms; 50 percent were web attacks (including SQL injection), scamming/phishing attacks, and denial of service attacks; and 25 percent were composed of advanced persistent threats that combine multiple and sophisticated attack methods. Of this total, approximately 33 percent of the attacks were considered high or medium severity.

Colorado state government continues to be at high risk of a system compromise and/or data breach by malicious individuals, both internal and external to the State. In 2010, contractors, on behalf of the Office of the State Auditor, performing a comprehensive penetration test of state systems were able to compromise thousands of citizen records. If the test had been an actual breach, the compromise would have cost the State between \$7.0 and \$15.0 million to remediate. The calculation does not include the cost to Colorado citizens and taxpayers that would have been impacted by the breach.

The Governor's Office of Information Security (OIS), located within the Office of Information Technology (OIT), is responsible for statewide cyber security, and has responded to and mitigated nearly 55 security incidents per month over the past two years. OIS works hard to remediate known

vulnerabilities, improve controls and implement training. HB06-1157 – IT Security in Public Agencies established the directives for cyber security but was unfunded and removed from the long bill in FY21012-13. Last year was the first time a direct appropriation was made to support enterprise information security initiatives. The \$1,075,000 appropriation represents the base appropriation for the program but represents less than one percent of total IT expenditures or approximately \$41 per state employee. As this request demonstrates, additional appropriations are necessary to ensure sufficient security countermeasures are implemented to meet cyber security threats, and that Phase II of Secure Colorado, the State’s three-year Information Security and Risk Management Strategic Plan, is successful.

Proposed Solution:

In late 2012, OIS created the Colorado Information Security Advisory Board (CISAB) comprised of industry leaders, educators and experts in the cyber security field to provide guidance on how to address known and future threats. Throughout 2012 and early 2013, the OIS held several meetings with the CISAB and performed several enterprise-wide risk assessments. Based on the CISAB’s guidance and output from the OIS risk assessments, the State’s Chief Information Security Officer (CISO) released Secure Colorado in June 2013, the State’s three-year Information Security and Risk Management Strategic Plan. The goal of Secure Colorado is to significantly reduce the State’s exposure to data breaches and other related cyber attacks over a three-year period, beginning with Fiscal Year 2013.

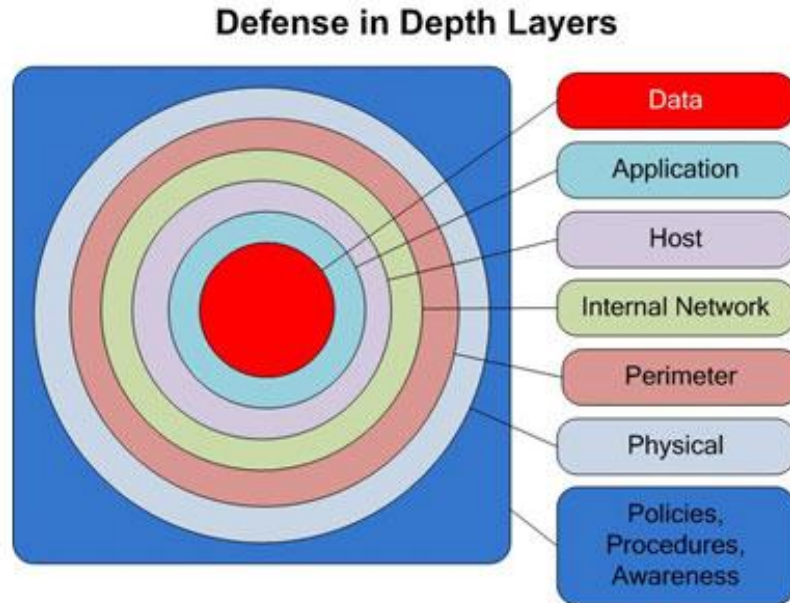
Secure Colorado is based on industry-validated information security frameworks, specifically the SANS Critical Security Controls (see Exhibit B) that have been proven to significantly reduce information security risks within an organization.

Secure Colorado Phase II is the second part of a three-year phased implementation plan focusing on those critical security controls that have been proven by industry experts and federal agencies to prevent and/or detect and contain 90 to 95 percent of known cyber security threats.

The specific types of tools and estimated expenses necessary to make Secure Colorado a success are listed in the Assumptions and Calculations section. Additionally, Exhibit A identifies how the proposed baseline cyber security program aligns with cyber security defense principles and industry best practice critical security controls.

Secure Colorado is also based on a defensive, in-depth or layered security approach as illustrated in the following exhibit.

Table 1.
7 LAYER DEFENSE MODEL



Secure Colorado is focused on deploying the critical controls listed in Exhibit B as follows:

- FY 2013-14 – Perimeter and Internal Network Layer – Phase I
- FY 2014-15 – Host and Application Layer – Phase II
- FY 2015-16 – Data Layer – Phase III

OIS has already addressed policies, procedures, and awareness and does not control physical security.

Anticipated Outcomes:

Secure Colorado contains 12 metrics that are being used to measure the outcomes achieved through this and subsequent and future funding requests. These metrics are:

Metric	Target
Percentage of State Systems Actively Managed by Security	100%
Composite Information Security Risk Index	<10
Mean Time From Incident Detection to Containment	< 60 min.
Percentage of Employees Completing Security Training	95%
Percentage of IT Expenditures Spent on Information Security	5%
Number of Emerging Cyber Security Product Evaluations. Completed	3
Mean Time from Identified Need to Recommended Solution	< 12 days
Number of Active Information Sharing Agreements	Tracking Only
Number of Security Thought/Evaluation. Products Shared with Partners	3
Number of Managed Security Audit Findings	Tracking Only
Percentage of Overdue Security Audit Findings	5%
Average Number of New Security Audit Findings Per Ext. Audit/Inspection	< 8

Based on these metrics, OIS is working toward:

- A 10% reduction in overall risk to state systems each year for the next three years;
- All new systems (100%) are compliant with state cyber security policies and contain the industry recommended critical security controls; and
- A 25% increase in the number of systems evaluated/monitored in near real-time each year for the next three years.

The continued funding will allow the program to be successful.

Assumptions and Calculations:

The costs for this request were derived from previous and current estimates, requests for information, and request for proposals. In addition, the cost estimates were validated by contacting industry experts such as Gartner and the SANS Institute and by analyzing similar deployments in other states and at the federal level. All cost estimates were based on actual FY 2012-13 levels (e.g., number of state employees, number of endpoints, network traffic) plus estimated growth rates over the next 12 months.

The detailed cost estimates and calculations include:

Item	Estimated Cost	Description
Core Security Infrastructure Upgrade	\$1,100,000	These funds will be used to upgrade existing, core security infrastructure that has reached end of life or is no longer sufficient to handle existing bandwidth and/or cyber threats, including firewalls, domain name servers, IP address and firewall rule sets management/audit tools, network forensics (deep packet inspection) appliances and licenses, secure password management vaults, and enterprise incident identification, response, and reporting toolsets.
Application Firewalls / Monitoring	\$750,000	This includes deploying application firewalls to protect OIT’s list of Internet-facing critical and essential web applications. In addition, these funds will be used to implement a continuous application monitoring system so that OIT’s critical and essential applications can be monitored in real-time, attacks can be automatically stopped, and incident response teams, if necessary, know where and how to quickly respond to stop/contain successful attacks.
Identity and Automated Access Control	\$1,500,000	These funds will be used to procure and implement the necessary software and hardware to identify all systems connecting to state networks as trusted or un-trusted and then to automatically apply network, application, and host-based rules to control what types of data and network resources these systems can access and what the systems can do with this data. This is one of the most critical

Item	Estimated Cost	Description
		components of Secure Colorado and is essential for ensuring both state-owned and BYOD and/or mobile devices of any kind are properly identified and controlled.
Managed Security Services	\$750,000	These funds will be utilized to procure the necessary professional services to architect, deploy, and operationalize the items listed above. In addition, these funds will support a managed service to provide 24x7x365 monitoring of state systems, including threat and vulnerability identification, attack identification, and incident response.
Total	\$4,100,000	

Agency Allocations

The costs associated with this consolidation are anticipated to be included in the IT Security rate structure. As such, the existing IT Security rate structure is allocated to departments based on their number of FTE. The table below outlines the allocated cost per department.

Department	FY15 Allocation	FY16 Est Allocation
Agriculture	\$40,664	\$40,664
Corrections	\$863,408	\$863,408
Education	\$79,892	\$79,892
Governor's Office	\$150,137	\$150,137
Healthcare Policy and Finance	\$48,982	\$48,982
Higher Education	\$18,296	\$18,296
Human Services	\$687,493	\$687,493
Judicial	\$597,218	\$597,218
Labor and Employment	\$157,454	\$157,454
Law	\$59,217	\$59,217
Local Affairs	\$20,298	\$20,298
Military and Veterans Affairs	\$20,290	\$20,290
Natural Resources	\$202,848	\$202,848
Personnel and Administration	\$51,408	\$51,408
Public Health and Environment	\$181,176	\$181,176
Public Safety	\$220,594	\$220,594
Regulatory Agencies	\$78,627	\$78,627
Revenue	\$170,410	\$170,410
State	\$16,090	\$16,090
Transportation	\$431,427	\$431,427
Treasurer	\$4,071	\$4,071
Total	\$4,100,000	\$4,100,000

Exhibit A



Colorado's Strategy for Information Security and Risk Management

Fiscal Years 2014 - 2016



Secure Colorado

Governor's Office of Information Technology



June 1, 2013

Table of Contents

Section I – Introduction and Background	2
A Call to Action	2
Information Security Governance	3
Section II – Strategic Priorities.....	6
Protection.....	7
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.....	7
Research and Development.....	8
Goal # 2 – Research, develop, and employ innovative and sustainable information security solutions to address Colorado's cyber security challenges	8
Partnerships.....	9
Goal # 3 – Develop and foster key partnerships to improve information sharing, reduce information security risk, and promote innovation and collaboration	9
Compliance	10
Goal # 4 – Comply with applicable information security and data privacy laws and regulations	10
Section III –Strategic Success Measures	11
Appendix A – Colorado Information Security Advisory Board.....	13

Section I - Introduction and Background

A Call to Action

The need to manage cyber security is an increasingly strategic tenant of any mature enterprise. In addition, to be successful, security must incorporate the right mix of technology, people, and processes and properly balance risk against the overarching need to accomplish the State's mission of providing efficient, elegant, and effective services to Coloradans.

Although we are not alone in our need to protect ourselves, governments are uniquely being targeted. In fact, the State of Colorado's networks, systems, employees, and endpoints are continuously under attack. As of December 2012, state systems are being hit by approximately 600,000 malicious events per day. In addition, our enemies' attacks are becoming more sophisticated, persistent, and targeted. In the last six months, the State has been hit by advanced persistent threats and malware that was highly customized and targeted to avoid the State's defenses and create maximum damage.

While the volume and sophistication of attacks are increasing, the most recent economic downturn has had a serious, detrimental impact on cyber security protective resources and measures deployed throughout state government.

The time has come to take action in order to proactively and preemptively protect the residents of Colorado!

This strategic plan, known as **Secure Colorado**, is a three-year initiative focused on making 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.

Respectfully,

Jonathan C. Trull

Jonathan C. Trull
Chief Information Security Officer

600,000

Number of cyber attacks
launched against the state
each day

680%

Increase in significant cyber
security threats against U.S.
government systems
2006 – 2011

94 Million

Number of Americans' files
in which personal
information has been
exposed to potential identity
theft through data breaches
at government agencies since
2009

Information Security Governance

The Colorado Information Security Program was created through legislation in 2006. According to Colorado law (Part 4 of Section 24, Article 37.5 of the Colorado Revised Statutes), 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 administratively to the Chief Technology Officer (CTO) who reports to the CIO. Information security duties and responsibilities for executive branch agencies are administratively divided between OIT’s CTO and Chief Operations Officer (COO). While the CISO maintains responsibility for information security governance, architecture, risk, and compliance, the COO 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 and Priorities

It's important that **Secure Colorado** aligns with OIT's mission and priorities, which in turn are aligned with the Governor's strategic plan. Protecting residents' data is required to meet OIT's value proposition to enable the effective, efficient and elegant delivery of government services through trusted partnerships and technology. OIT is committed to a set of core priorities, one of which is specifically focused on information security:

- Customer Success
- People
- Innovation
- Service Excellence
- Trusted Partnerships
- **Information Security** –ensuring the security, integrity, privacy and availability of information and systems

<p>CUSTOMER SUCCESS</p> <p>We will enable our customers, the state agencies and departments who serve all Coloradans, to be national leaders. We will honor our commitments, provide reliable, consistent and high quality services, communicate openly and be a trusted advisor in helping our customers solve their toughest problems.</p>  <p>PEOPLE</p> <p>People are the foundation of our success. We will attract, develop and retain the best talent for OIT by fostering a culture of empowerment, high performance and mutual respect.</p>	<p>INNOVATION</p> <p>We will provide strategic, sustainable solutions using emerging technologies that align with the business needs and deliver both short- and long-term value for the state and all Coloradans.</p>  <p>SERVICE EXCELLENCE</p> <p>We will deliver timely, secure, agile, cost effective, sustainable, high quality IT services that meet and exceed business requirements.</p>	<p>INFORMATION SECURITY</p> <p>We will protect the confidentiality, integrity and availability of state and citizen information. We will be compliant with all federal and state policies and requirements.</p>  <p>TRUSTED PARTNERSHIPS</p> <p>We will cultivate and strengthen existing partner relationships and develop new partnerships necessary for successful service delivery.</p>
---	--	--

Colorado Information Security Program Vision and 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 residents' 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 and 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

Every soldier must know, before he goes into battle, how the little battle he is to fight fits into the larger picture, and how the success of his fighting will influence the battle as a whole.

-- Bernard Law Montgomery

Secure Colorado establishes a roadmap for improving cyber security in Colorado over the next three years. This plan was developed in cooperation with the Colorado Information Security Advisory Board (Board) – see Appendix A for Board Membership. 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.

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 – www.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 Colorado Information Security Advisory Board and OIT 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 cyber security 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 CTO’s strategy, known as “The Compass: Enterprise Architecture 2011-2014,” (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 and Development

Goal # 2 - Research, develop, and employ innovative and sustainable information security solutions to address Colorado's cyber security challenges

STRATEGIC INITIATIVES

Initiative # 2.1 – Actively leverage federal government, private sector, and academic research and development of advanced cyber security 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.

Initiative # 2.4 – Use data and information to research and analyze cyber security trends.

Partnerships

Goal # 3 - Develop and foster key partnerships to improve information sharing, reduce information security risk, and promote innovation and collaboration

STRATEGIC INITIATIVES

Initiative # 3.1 - Develop and formalize new partnerships with academic institutions, the private sector, and Colorado 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 CIOs (NASCIO) Privacy and Security Committee, Multi-State Information Sharing Analysis Center (MS-ISAC), Colorado Government Association of Information Technology, National Institute of Standards and Technology, the SANS Institute, and other relevant organizations.

Initiative # 3.3 – Promote discussions and cooperative engagements that will enhance cyber security for all Colorado residents including partnering with the Colorado Department of Public Safety, Federal Department of Homeland Security, and the Colorado National Guard in achieving the cyber security objectives of the Colorado homeland security 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 non-compliance with State Cyber Security Policies and applicable federal laws and regulations.

Initiative # 4.3 – Partner with executive branch agencies and other public 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) by the Colorado security team.
Composite Information Security Risk Index	< 10	Quarterly	Overall, enterprise-level cyber security risk rating - based on current threats, asset value, and implemented security controls, ranked on a scale from 1 to 100 with 100 being extreme risk and 0 being no risk.
Mean Time from Incident Detection to Containment	< 60 min.	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, annual 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 Cyber Security Product Evaluations Completed	3	Annual	Represents the number of emerging security product reviews completed annually to address emerging cyber security challenges.
Mean Time from Identified Need to Recommended Solution	< 12 days	Annual	The average number of days elapsed between the identification of a cyber security 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 / Evaluation Products Shared with Partners	3	Annual	Number of written cyber security 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	5%	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

Colorado Information Security Advisory Board 2012-2013	
Alan Paller, Co-Chair Founder and Director of Research SANS Institute	Rick Dakin, Co-Chair Co-Founder and CEO Coalfire Systems
Kent Lambert, Member State Senator, District 9	Paul Underwood, Managing Partner and COO Emagined Security
Dan Jones, Assistant Vice President and CISO University of Colorado System	Brian Tillet, Chief Security Strategist Symantec
Tim Erlin, Director, Product Management, Security, and IT Risk Strategist, nCircle	Robert Rudolff, Assistant Vice Chancellor and CISO University of Denver
John Conley, Executive Director Statewide Internet Portal Authority	Steve White, Director, Cybersecurity Practice, Enterprise Services, Microsoft Corp.
Eran Feigenbaum, Director of Security Google	Mark Lewis, Security Engineer McAfee
Sheryl Rose, Vice President, CISO Catholic Health Initiatives	Trevor Timmons, CIO Colorado Secretary of State's Office
Colonel Gregory A. Miller, Deputy Chief of Staff Colorado Army National Guard	Jeff Franklin, CISO State of Iowa
Eric Bergman, Policy and Research Supervisor Colorado Counties, Inc.	Randall J. Romes, Principal CliftonLarsenAllen, LLP
Tim Gama, Program Coordinator Pueblo Community College	Len Meyer, Director of Infrastructure Services Governor's Office of Information Technology
Alfritch Anderson, Security Operations Manager Governor's Office of Information Technology	Craig Fuller, IT Asset Manager Governor's Office of Information Technology
Rick Matsumoto Director of Enterprise Applications Governor's Office of Information Technology	Barbara Gilmore Deskside Support Services Manager Governor's Office of Information Technology
Heather Copp, Deputy Director Colorado Department of Revenue	Erika Bohl, Chief Privacy Officer Department of Health Care Policy and Financing
Kathleen Foo, Chief Privacy Officer Colorado Department of Human Services	Dan Krug, Analyst Governor's Office of State Planning and Budgeting
Stephanie Donner, Deputy Legal Counsel Office of the Governor	Brandon Rattiner, Denver Metro Regional Director Office of Senator Mark Udall
Dana Reynolds, Director of Preparedness Colorado Department of Public Safety	Karl Wilmes, Deputy Director Colorado Bureau of Investigation

Exhibit B

The Center for Strategic & International Studies (CSIS) identified twenty critical security controls that have been widely adopted for security programs in large enterprises and public sector entities as guiding principles for effective cyber defense. These controls are intended to direct spending on cyber security on the controls that most effectively address cyber threats and vulnerabilities enterprise wide. The goal of the controls is to enhance the effectiveness of an organization's security program and to efficiently protect critical infrastructure and technology assets. A general consensus indicates that implementing these controls can result in 90-95% reduction in information security risk. The twenty controls are listed below, and this request primarily addresses critical control #s 1, 6, 7, 10, 15, 16, and 18.

20 Critical Security Controls -

- Critical Control 1 – Inventory of Authorized and Unauthorized Devices
 - Critical Control 2 – Inventory of Authorized and Unauthorized Software
 - Critical Control 3 – Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
 - Critical Control 4 – Continuous Vulnerability Assessment and Remediation
 - Critical Control 5 – Malware Defenses
 - Critical Control 6 – Application Software Security
 - Critical Control 7 – Wireless Device Control
 - Critical Control 8 – Data Recovery Capability
 - Critical Control 9 – Security Skills Assessment and Appropriate Training to Fill Gaps
 - Critical Control 10 – Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
 - Critical Control 11 – Limitation and Control of Network Ports, Protocols, and Services
 - Critical Control 12 – Controlled Use of Administrative Privileges
 - Critical Control 13 – Boundary Defense
 - Critical Control 14 – Maintenance, Monitoring, and Analysis of Audit Logs
 - Critical Control 15 – Controlled Access Based on the Need to Know
 - Critical Control 16 – Account Monitoring and Control
 - Critical Control 17 – Data Loss Prevention
 - Critical Control 18 – Incident Response and Management
 - Critical Control 19 – Secure Network Engineering
 - Critical Control 20 – Penetration Tests and Red Team Exercises
-
-