Executive Summary

The Colorado Information Security Act ("ISA") or Colorado Revised Statute (C.R.S.) 24-37.5-401 through 406 was enacted by the legislature (House Bill 06-1157) and signed into law by the Governor on June 6, 2006. The Colorado ISA recognized the importance of information security to the economic and security interests of the State of Colorado. In accordance with the Colorado ISA, the State Chief Information Security Officer (CISO) has been appointed and given the responsibility to publish policies, standards and guidelines for the development of Agency Cyber Security Plans (ACSP) that secure State communication and information resources and to enforce the provisions of the Colorado ISA.

In order to achieve this lofty objective, Mark Weatherford, state CISO, has put together the Colorado Cyber Security Program, a state-wide security team that aims to establish a common risk management approach to cyber security and to centralize and standardize security controls in the state's highly distributed Information Technology environment. This is an ongoing effort, and has been supported by numerous technical and non-technical security initiatives. This paper serves to describe two of the key initiatives that his organization completed.

Establishing a security framework across 24 disparate state public agencies requires two key data points: the identification of assets that are critical to each agency ("Critical Systems Inventory"), and the current level of security program performance to accepted standards ("Risk Based Gap Analysis"). It is imperative to lay this groundwork to measure improvements in the program over time, yet when Mr. Weatherford was appointed as CISO, this information had not been collected, nor was there any ambition to undertake such an effort.

This groundwork was laid through the instantiation of the Colorado Cyber Security Program which set out to enumerate and categorize the most critical systems in the state, followed by an assessment of the security posture of each state public agency. This was undertaken through two separate projects that are being submitted as one project for consideration of NASCIO for award in the category of Information Security and Privacy.

Nomination Justification

Title: Colorado Cyber Security Program

Problem Statement:

Establishing a security framework across 24 disparate state public agencies requires two key data points: the identification of assets that are critical to each agency ("Critical Systems Inventory"), and the current level of security program performance to accepted standards ("Risk Based Gap Analysis"). It is imperative to lay this groundwork to measure improvements in the program over time, yet when Mr. Weatherford was appointed as CISO, this information had not been collected, nor was there any ambition to undertake such an effort.

Detailed descriptions of the Critical Systems Inventory and Risk Based Gap Analysis follow:

Colorado Cyber Security Program, Critical Systems Inventory

The identification of assets was addressed by Mark Weatherford through leveraging existing projects and resources to gather and consolidate the required information. Piggy-backing on an existing contract kept the costs of the study to less than 25% of the original estimate versus if it was performed on its own accord. The project provided the CISO and the Governor's Office a view of state resources that had never before been available.

Project Objective

The objective of this project was to identify the most critical systems used to deliver State services through a major system inventory and characterization in accordance with National Institute of Standards and Technology SP 800-30 and FIPS 199 guidelines, as adapted to the environment at the state.

Project Approach

The Critical Systems Inventory was managed and funded by the CISO from September through November of 2006. It was staffed through leveraging and augmenting an existing effort already underway to identify and enumerate disaster recovery requirement state-wide, thereby reducing overall project cost by over 50%. The approach to the existing project employed by the contractor was enhanced to not only collect the information to support disaster recovery efforts, but also to include gathering information that lent itself to achieving the goals of this project. These goals included:

1. Identify all Major Systems used by departments to achieve its mission and deliver services to the Citizens of Colorado.
2. Characterize each major system including the criticality of each of the major systems used within the state.
3. Identify the most critical systems in each department. At least three major systems in each department should be characterized.

Project Accomplishments

This project successfully met all three goals across all state public agencies. It concluded in November of 2006

- The project was completed "On Time" and "Within Budget"

- 295 major systems were identified
- All systems identified were catalogued in a critical systems database for reference during agency security risk analysis
- The state is now positioned to begin a risk analysis at each public agency (see Risk Based Gap Analysis, below)

Project Summary

This comprehensive study had never before been attempted across all public agencies in the state. The insight gained by this project not only set the stage for quantifying risk levels at each public agency, it also provided each agency an objective view of how security program goals should be structured.

Colorado Cyber Security Program, Risk Based Gap Analysis

Measuring the current level of performance at each public agency to a set of draft policies and requirements was a much bigger task. Mr. Weatherford stood up teams of security professionals to act as consultants with each of the state public agencies to identify their current state of compliance with his proposed security policies, identify a path forward at each agency for upcoming budget cycles to close gaps in compliance, and to assist each public agency in establishing a comprehensive Agency Cyber Security Plan (ACSP) that provides vision and direction to each agency's security initiatives.

Project Objective

The objective of the RBGA program was to facilitate the development of initial draft Agency Cyber Security Plans to accelerate the planning process and to improve the likelihood that security plans will comply with the Colorado Information Security Act (C.R.S. 24-37.5 part 4).

The CISO conducted a statewide Risk Based Gap Analysis (RBGA) program from December 15, 2006 to April 28, 2007 to help agencies determine relative compliance with new cyber security policies. The analysis resulted in the development of DRAFT Agency Cyber Security Plans (ACSP) and development of a Plan of Action and Milestones (POAM) to close gaps in compliance with Cyber Security Policies as well as mitigate known risks to critical State systems. Agencies are required to submit the initial ACSP and POAM to the CISO by July 15, 2007 and the RBGA program helped "jump start" the security planning process.

Project Approach

The RBGA project was funded by the CISO in an effort to provide the skills and resources necessary to develop first year enterprise security plans. The RBGA included five (5) senior security specialists that were assigned up to 6 agencies to provide security planning input and guidance. In addition to individually assigned advisors, the RBGA project included a series of workshops where the CISO office provided templates and guidelines for completing initial plans. The draft analysis and planning documents were collected and reviewed through a Cyber security portal managed by the CISO office.

While the final project deliverables remained the responsibility of each agency, the RBGA team was assigned a role to ensure agencies could meet their obligations.

Project Accomplishments

The project was successful. Every agency participated in the program and the vast majority successfully developed draft ACSP and POAM prior to the end of the project. The project included the following accomplishments:

- The project was completed "On Time" and "Within Budget"
- Cyber security awareness at the agency level is at an all time high. Accordingly, the content in security plans reviewed by RBGA advisors is solid.
- Agency technology teams are now intimately aware of their risks and vulnerabilities.
- Many agencies had previously identified risks to critical State systems and sensitive citizen data. These agencies had already begun developing security plans and were implementing enhanced cyber security at project launch.
- The enthusiasm to develop and implement cyber security plans throughout the majority of agencies has been transferred to agency staff.
- Over 70% of agencies participated in each workshop.
- All participants came to concur that the Colorado Cyber Security Policies represent justified controls that should be deployed for sensitive state systems and private citizen data.
- A handful of agencies have already made substantial investment in security programs.

Project Summary

It is likely that all agencies will meet the July 2007 deadline for submitting initial ACSP and POAM documents to the CISO. The planning process identified substantial gaps in compliance to the new Cyber Security Policies. As a result, additional resources will be requested to fully implement the Colorado Cyber Security Program by the designated compliance date, July 2009.