Joint Technology Committee

Whole of State Cybersecurity

February 2022

Agenda

- Introductions
- Local Voices - Experiences
- National Cybersecurity Center
- Department of State
- Statewide Internet Portal Authority (SIPA)
- Office of Information Technology
- Colorado Department of Public Safety
- Next Steps

Keys To Success

1. Focus on Local Government

   The Whole of State focus has a clear goal to support local and small government entities throughout Colorado. We depend on each other and must support all levels of government as a team.

2. Cybersecurity Support and Response Team

   Colorado has a strong cybersecurity community consisting of passionate and motivated individuals who continually volunteer their time to support Colorado. We need a strong full time base of cybersecurity professionals that can support Colorado and direct our efforts in the right direction.

3. Colorado Model for Success

   Through state, local and federal partnerships we plan to make Colorado a model for cybersecurity done right.

Local Voices - Experiences

Jill Fraser, CISO - Jefferson County

- Why we started
  - We recognized what we are doing to protect our respective communities from cyber threats is neither effective nor sustainable.

- What we found
  - There are six high-level areas of expertise required to run an organization’s cybersecurity program and only the most well-resourced of us has even a single person dedicated to developing and maintaining the organization’s security program.

Jill Fraser, CISO - Jefferson County

Ensure all Colorado's local governments and special districts would have access to the resources they require to meet and maintain a minimum baseline of cybersecurity.

1. Preventative Support
2. Incident Response
3. Ease of Use
4. Stop Duplicating Efforts
5. Accountability for delivering useful services

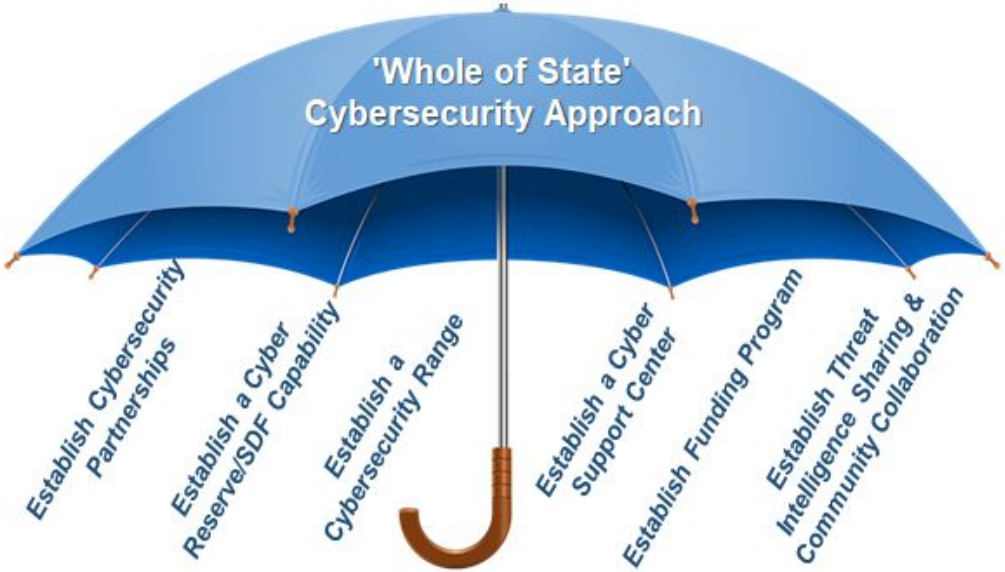
Starting the Whole of Government

Solidifying a Whole of State Approach

'Whole of State' Cybersecurity Approach

Mission: Lead a 'Whole of State' Cybersecurity Program that will raise the security posture of Colorado and beyond through training, knowledge-sharing, and delivering valuable security services

Vision: A 'Whole of State' cybersecurity program that all Colorado agencies play an active role in shaping and sustaining our state cyber resiliency



Rich Schliep, CTO - Dept. of State

The Secretary of State's Office has long had a strong partnership with election officials and county governments as a whole. We are all in this together and need to stop duplicating efforts.

- Colorado National Guard Cyber & Elections Exercises
- Ransomware Incident Support
- Policies, Standards and Guidelines
- Cybersecurity training for general staff and IT across state
- EDR Solution for all elections systems
- Colorado Threat Information Sharing (CTIS)
    - Threat Intel Sharing Platform with trusted circles

JR Noble, Senior Security Analyst - South Metro Fire Rescue

- Local Need for Statewide Support
- Experience with Whole of State
- School District Perspective
- Special District Perspective

Ben Edelen, CISO - Boulder County

- Colorado will be a leader
  - MS-ISAC model and relationship
  - OIT, CIAC, CISA

- Urgent need to support local government with accountability and responsibility

- We can and will be the most cyber-safe environment in the nation

- NCC

National Cybersecurity Center

About the NCC

CYBERSECURITY FOR STATE LEADERS

COLORADO CYBER RESOURCE CENTER

SECURE SMART CITIES

WWW.CYBER-CENTER.ORG

Mattie Gullixson
Program Director
Mattie.Gullixson@cyber-center.org
703-943-7128

[HTTPS://COLORADO-CRC.COM](https://COLORADO-CRC.COM)

SPACE ISAC

CYBER EDUCATION

Background with Whole of State

2018

*"...develop the capability to act as a **Colorado in-state center of excellence on cybersecurity advice** and national institute of standard and technologies standards"* SB18-086

2020

Began intentionally connecting with Colorado jurisdictions and state agencies on a Whole of State effort to establish more robust and connected cybersecurity advice and support of Colorado State Local Tribal and Territorials

2021

Took active support role in Whole of State Group efforts and accelerated opportunities for coordination between local governments, CISA, state agencies, MS-ISAC to accomplish the goals identified by the Whole of State

2022

Accelerating on momentum built in 2021 to deliver unique resources for local governments and overall statewide resources

Whole of State Goals

The Whole of State Working group has identified the following key objectives:

- ❏ Establish cybersecurity partnerships - enhance and leverage public and private partnerships across Colorado around WOS
- ❏ Establish a state defense force/cyber reserve - to support quicker and more affordable response support
- ❏ Establish a statewide cybersecurity range - accessible statewide range for education and upskilling purposes
- ❏ Establish a cyber support center (CSC) - a one-stop shop for cybersecurity resources and support for Colorado jurisdictions
- ❏ Establish a funding program for local governments to invest in cybersecurity resources
- ❏ Establish Colorado-specific threat intel sharing - the advance Colorado Threat Information Sharing network

Whole of State - Current State

Partnerships with industry members

MS-ISAC partnership

K-12 SIX

CISA

PISCES

MSU

Building out proposed exec committee to complement federal funding plan

Exploring models for cyber reserve that could best work for Colorado

Intent to build framework by Fall 2022

Cyber range launched

Available to K-12 students for free; Adults - $250 for year

Access to over 600 modules, 12+ learning paths

Outward-facing cyber support center launched

1-800 number to call

Offers support/resources

Key services include: PISCES, Range, & Crown Jewels Analysis

Seeking more opportunities to increase the bargaining power of local governments

Increased relationship with all-hazard regions grant coordinators

CTIS launched;

Connecting with MS-ISAC list

Whole of State - Future State

All-hands on deck

OIT to focus on private industry support

Primary lead

CIAC, with strong support from OIT and NCC

Primary Lead

NCC – coordinated with State agencies

Primary Lead

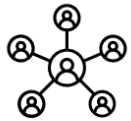
Outward-facing cyber support center – NCC in coordination with State agencies

Internally-facing cyber support center – CIAC, coordinated with other state agencies

Primary Lead

Internal state funding, DHSEM

Coordinated support for increased bargaining power, OIT



Threat info sharing

CIAC

Whole of State - Cybersecurity Council

Provides insights and options on local government needs

Whole of State Working Group Executive Committee

3 reps from small jurisdictions, with geographic diversity
1 rep from medium-size jurisdiction
1 rep from large jurisdiction
Small public critical infrastructure rep
Small school district rep
Mid-size school district rep
Tribal comm rep
Rep Secretary of State's Office
Rep DHSEM/CIAC
Rep OIT

Non-voting Executive Committee Members
Additional state agency reps who may want to participate
All-Hazards Region Coordinators rep

Phase I - Proposed Colorado Cybersecurity Council

Voting Members (*statutorily defined)*
Director, DHSEM/designee
CML representative
1 county gov (rural)
1 county gov (urban) - could be the key WoS reps from the proposed Exec. Committee
Secretary of State designee

Proposed additional members - designees from:
Lt. Gov - provides connection to policy issues, health care, Commission on Indian Affairs (Tribal rep) and aerospace & defense
Attorney General
National Guard Adjutant General
Public Utilities Commission Director - connection to public utilities/critical infrastructure
Higher Education Executive Director

Non-voting, advisory members
CISA Rep
MS-ISAC Rep
Local FBI field office rep/rep from Cybersecurity Task Force

CCC identifies strategy & resources to support local needs

Colorado
Secretary of State

Trevor Timmons, CIO - Dept. of State

- As we have seen on the elections front, cybersecurity is one of this nation's top priorities.
- The impact of a successful physical or cyberattack on a state or local entity has repercussions beyond that single entity and their ability to provide services to residents and citizens.
- An incident will be leveraged by bad actors to raise doubts about the security of any government system and structure; we are only as strong as the weakest among us.

Trevor Timmons, CIO - Dept. of State

- There is good news: federal, state and local resources have come together in Colorado to share information, strategies and resources to strengthen our community, build relationships, and rise to the serious challenges facing our public sector systems and services!

- But the bad news is that our efforts are not enough. These partners you see and hear from today have largely taken on the development of a statewide strategy as a volunteer effort on top of their daily duties.

Trevor Timmons, CIO - Dept. of State

Call to Action

- Take concrete action to support these efforts and the wide range of partners engaged in this work
  - Local Colorado cities, counties and special districts
  - Governor's Office, OIT, DHSEM, CIAC, State CISO's office, Colorado National Guard and the Department of State
  - Private sector partners like the National Cybersecurity Center (NCC) and the National Governors Association

Statewide Internet Portal Authority

Jerrod Roth, CTO - SIPA

- SIPA provides products and services to state agencies, but more so to local government
  - 84% of SIPA's customers are local government entities

- Two vendor partners provide a variety of services to local government customers:
  - Managed IT and security services
  - Security assessment, testing, training and policy development services

- Case Study: North Central All Hazards Region (Project Complete 5/2022)
  - Approached to see what services we can provide to participating governments
  - 12 government entities participated in the project
  - Variety of services performed (pen testing, vulnerability scans, health checks)

- SIPA is in the very early stages of understanding how we fit into the Whole of State initiative and how we can provide assistance

COLORADO

Governor's Office of
Information Technology

Chief Information Security Officer

- Establishes and maintains the Colorado Information Security Program (Secure Colorado) which provides guidance to public agencies.
- Promulgates statewide information security policies (Colorado Information Security Policies) and procedures to protect State of Colorado's Information Systems and related resources.
- Protects state executive branch agency systems and data.
- Solid defensive posture and responsiveness to date.

Governor's Cybersecurity Council

OIT's Office of Information Security through the State's Chief Information Security Officer is represented on the Governor's Cybersecurity Council and empowered for Whole of State as follows:

- Develop a Whole of State cybersecurity approach for the state and for local governments, including the coordination and setting of strategic statewide cybersecurity goals, roadmaps, and best practices
- Review the need to conduct risk assessments of local government systems, providing additional cybersecurity services to local governments, and proposing necessary statutory or policy changes, including the determination of ownership for these capabilities
- Make recommendations to the Governor and Colorado General Assembly on the authority and activities of the State Chief Information Security Officer with local governments by July 1, 2022

How can we make the **most impact** for agencies and Coloradans?

Tech Debt Reduction

Mitigating Risks for Colorado

Sources of attack against the State of Colorado as captured by OIT firewalls for January 2022:

- Russia: 231,752 attempts
- China: 62,738 attempts
- Iran: 2,027 attempts

In parallel to technology debt reduction, we need to increase resources focused on Security Operations and Threat Detection & Response

OIT Support for Whole of State

- Form partnerships and purchasing agreements for cybersecurity support and tools.
- Cybersecurity incident response team to support state agencies and the Colorado Information Analysis Center (CIAC) when needed.
- Work with the NCC, CIAC, MS-ISAC and EI-ISAC to support threat information sharing in support of a multi-state threat intel sharing platform (TACO).
- Work with CIAC on Security Orchestration Automation Response

COLORADO

Department of Public Safety

Colorado Information Analysis Center

- Cyber Operation Center (24-33.5-1903)
  - Fusion of cyber defense, cyber surveillance, and international and domestic intelligence and law enforcement operations
  - Training, inspections, and operational exercises
  - Establish protocols for coordinating and sharing information with state and federal law enforcement…
  - Support state and federal law enforcement agencies…
  - Ensure the coordination of cybersecurity threat information sharing among CBI, the office of prevention and security, OIT, and FBI's Cybersecurity Task Force

Colorado Information Analysis Center

- Incident response support and coordination
- Colorado Threat Information Sharing (CTIS)
- Threat Intelligence Platform (TIP) with trusted circles
  - Dark Web Monitoring
  - Intelligence Feeds
- Security Orchestration Automation Response (SOAR) with OIT
  - Network Monitoring
  - Centralized Logging
  - Endpoint Detection and Response
  - Next-generation Antivirus

CDPS Whole of State Approach

- HSAC – Cybersecurity Subcommittee
  - Whole of State
    - Partnerships
    - Cyber Reserves
    - Cyber Range
    - Cyber Support Center
    - Threat Intelligence & Community Collaboration
  - R-11

R-11 Whole of State Approach

- Collaboration to enhance the overall cybersecurity posture
  - Awareness
  - Best practices
  - Cybersecurity Assistance Group
- Focus on local and tribal governments and other critical infrastructure providers
- Develop and implement tools to prevent, mitigate, plan for, respond to, and recover from cyber security incidents
- JTC Question

Next Steps

Vision and Outcomes for Whole of State

- Infrastructure - build capacity, modernize infrastructure, increase automation
- Centralized Resources - provide incident response, operations, outreach
- Cyber Navigators - help underserved populations, municipalities, etc.
- Accountability - clarify who does what, role of the state, role of municipalities, gain efficiency of a centralized focus

Questions & Discussion