Colorado Civilian Cyber Reserve

JTC Presentation – January 18, 2024

Jonah Wisch, Program Director

Background

"Whole of State" Cybersecurity

Colorado has done an excellent job bringing together relevant agencies to improve information sharing, collaboration, risk assessment and identification

COLORADO
Governor's Office of Information Technology

HOMELAND SECURITY EMERGENCY MANAGEMENT
PREVENTION ★ PROTECTION ★ MITIGATION ★ RESPONSE ★ RECOVERY

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Colorado Secretary of State

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

NCC
NATIONAL CYBERSECURITY CENTER

- Department of Homeland Security and Emergency Management
- Governor's Office of Information Technology
- Secretary of State – Office of the CIO / CISO
- CISA
- MS-ISAC
- Regional Homeland Security Coordinators
- National Cybersecurity Center

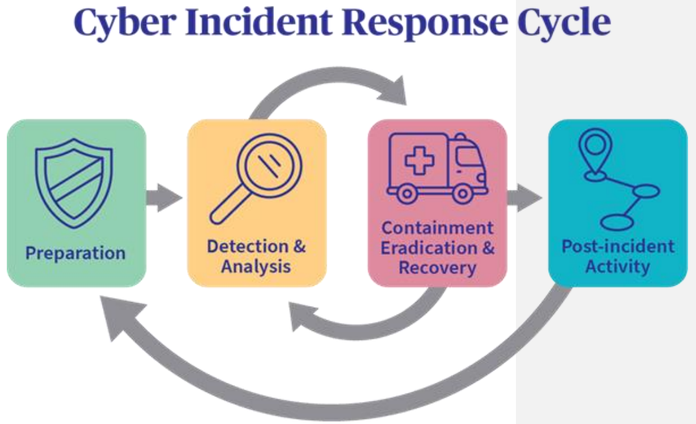
NCC

Local Governments DO NOT have access to cost-effective hands-on support in a proactive or reactive capacity, despite all of the state and federal resources available

The Solution

Civilian Cyber Reserve

1. A group of volunteer cybersecurity professionals that are capable and have the authority to effectively respond to cybersecurity incidents and mitigate vulnerabilities



Michigan Cyber Civilian Corps Act of 2017: "Cybersecurity incident includes, but is not limited to, the existence of a **vulnerability** in an information system, system security procedures, internal controls, or implementation that is subject to exploitation"

Local Government Testimony

IT / Cyber Professionals:

- Jesse Dubin, City of Wheat Ridge
- JR Noble, South Metro Fire and Rescue

Jesse Dubin – Wheat Ridge

IT Director

In August 2022, City of Wheat Ridge experienced an attack from the BlackCat ransomware gang

Problems with response:

- At the time, we were totally unprepared. We had no idea who to call, where to go, how to recover, or what our obligations were
- We needed our friends to help
- Managing resources is difficult and it's hard to know who to trust
- Budget and time are strong constraints
- Insurance may not be there to help

With a Cyber Reserve, we could have tackled these challenges!

1. Faster response time and strong technical resources
2. Allows local governments to be more proactive

JR Noble – South Metro Fire & Rescue

Senior Systems and Security Analyst

Experience with Special District, K12, and Higher Education Cybersecurity

Small Agency and EDU Challenges

- Often inherit insecure configurations
- Security impacts mission
- Replace tech vs hire new teachers
- Securing student data
- Use of DHS/CISA resources can help, but only with identification

With a Cyber Reserve, we could tackle these challenges!

1. Allows organizations to focus on their core missions
2. Solves the perpetual need for more technical staff

Homeland Security Coordinator Testimony

North Central Region: Scott Kellar

Northeast Region: Nicole Cantrell

Scott Kellar – North Central Region

A cyber equivalent to mutual aid for kinetic events DOES NOT exist

Resources and Gaps

- Most agencies, regardless of size, are not staffed to keep up with identified gap areas
- Efficiently funding cyber projects is difficult because each agency does not have the resources to fix identified vulnerabilities
- Response is important, but prevention has more of an impact

With a Cyber Reserve, we could tackle these challenges!

1. Provide trained professionals to the right place at the right time
2. IT/Cyber teams can keep up with documented vulnerabilities

Nicole Cantrell – Northeast Region

Cybersecurity is consistently identified as a top threat or hazard

Federal Resources and Gaps

- Limited due to staffing and lack on individualized support
- CIAC team is limited in size and scope
- Targeted attacks on critical infrastructure and government agencies are increasing
- Lack of sustainable funding mechanism to solve ongoing problems
- NEAH has already committed funds to help stand up cyber reserve

With a Cyber Reserve, we could tackle these challenges!

1. Hands on support, especially for rural jurisdictions
2. Solves the problem of year to year grant funds

Program Details

Focus of Colorado Cyber Reserve

The Colorado Cyber Reserve will **initially** focus on:

1. **Not having the budget or resources to fix known vulnerabilities in your cybersecurity program**
2. *Provide resources that can aid in the response to and recovery from a confirmed cyber attack on your network and systems.*

Reserve Member Lifecycle

Volunteer signs up to become a Colorado Cyber Reserve member through an application process

Members will sign a contract that denotes their liability, protections, and rules of engagement

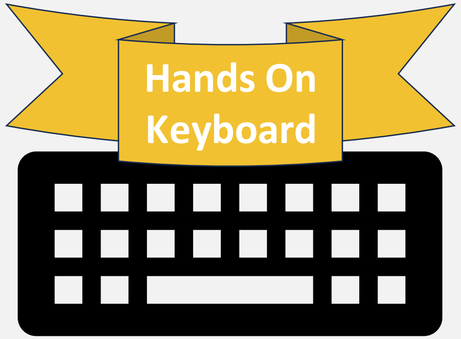
As an incentive, volunteers will be given team based, hands-on training that is normally very expensive unless your company (or military) performs exercises regularly

Volunteer → Vetting → Sign Member Contract → Training → Deployment

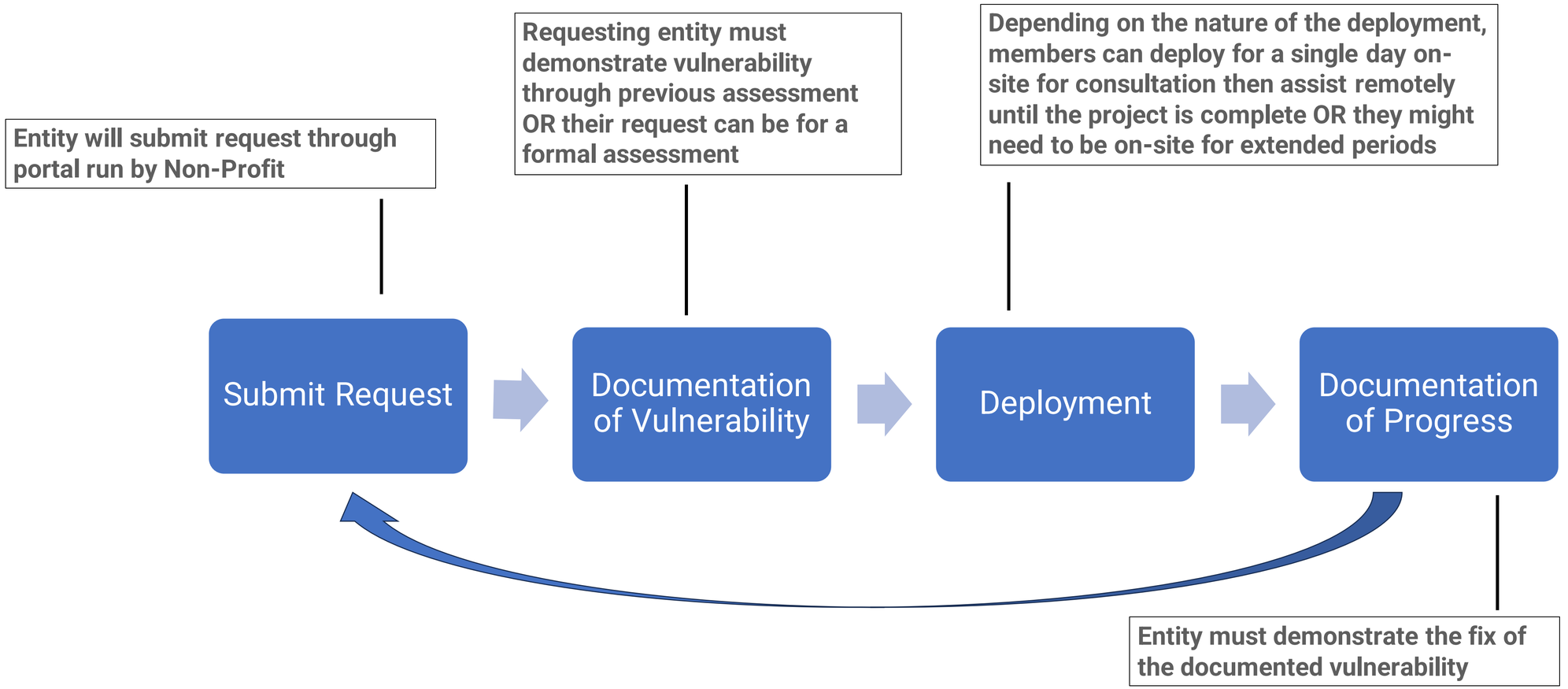
Member must meet criteria to join the reserve:

- 3 years of experience within a specialty in the cybersecurity industry
- Security + Certification
- Pass state and federal background checks
- American Citizen
- Pass a cybersecurity skill-based exam

Members will have a minimum deployment requirement to maintain member status



Request for Assistance



Similar to the Colorado Rangers Police Reserve, the State will hold the liability and insurance responsibilities unless there is demonstrated gross negligence

Types of Proactive Projects

Policy Development

- Work with IT staff or vendor to develop policies and procedures for incident response, vulnerability management, acceptable use policies, etc.

Fix a Vulnerability

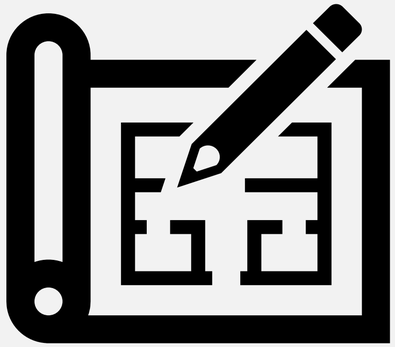
- After an assessment shows a vulnerability that needs **hands-on-keyboard work**, a cyber reserve member can deploy instead of needing to call your vendor

Virtual CIO / CISO

- Some entities just need guidance on what steps to take next in the development of their cybersecurity program. Experienced CIOs and CISOs reserve members will be there to help

Ownership

Structure and Leadership



Create the Colorado Cyber Reserve (CCCR) as a parallel to the Colorado Rangers Police Reserve (CRRR)

- Local governments enter into an intergovernmental agreement (IGA), creating the Authority which grants immunity and liability protections
- State can then fund the Department of Public Safety to administer the program with oversight from the IGA BoD

CCCR: NCC ; CRRR: Colorado Mountain Rangers

Funding Request

"Rolls Royce" Option

Staffing

- 1 Director, 1 Manager, 1 Coordinator
- Perform outreach, recruitment, vetting training of members
- Coordinate deployments for proactive and incident response
- Capacity: 150 members, unlimited proactive deployments, 2 simultaneous incidents

Training

- 2 x Year Team-Based Hands-on, In-Person training exercises for Incident Response
- Asynchronous training platform to develop skills

Pay

- Reserve members give "reserve pay" similar to Army Reserve
- Reimbursement for expenses related to incident (travel, lodging, food, etc)

$1,000,000

"Tesla" Option

Staffing

- 1 Director and 1 Manager
- Perform outreach, recruitment, vetting, and training of members
- Coordinate deployments for proactive and incident response
- Capacity: 100 members, unlimited proactive deployments, 1 simultaneous incident

Training

- 1 x Year Team Based, Hands-On training exercises for Incident Response
- Asynchronous training platform to develop skills

Pay

- Reimbursement for expenses related to incident (travel, lodging, food, etc).

$500,000

"Toyota" Option

Staffing

- 1 Director and 1 Coordinator
- Perform outreach, recruitment, vetting, and training of members
- Coordinate deployments for proactive and incident response
- Capacity: 50 members, limited proactive deployments, 1 simultaneous incident

Training

- 1 x Year Team Based, Hands-On training exercises for Incident Response

Pay

- None

$250,000

Future Vision

Initial Growth Period (Y1)

- Focus on proactive engagements and grow to 50 members while performing bi-annual exercises

Grow and Develop (Y2-3)

- Continue proactive focus while developing IR capabilities and grow to 100 members

Mature Stage (Y4+)

- Grow to 150 members and increase utilization rate of proactive response and IR

Cost Analysis

Costs include:

- Overtime
- Meals
- Equipment
- Vendors
- New security features

Cost of an Incident

Colorado Department of Transportation
$1.7 million

City of Wheat Ridge
$500,000

Fremont County
$250,000

Cost of Proactivity

Variables:

- Cybersecurity vendor hourly rate: $100 - $500
- Vendor usage per year (for 1 agency): 50 – 250 hours
- *Agencies utilizing vendors: 30 counties + 90 cities + 150 school districts = 270 agencies

Estimated cost range per year:

High - $500 * 250 * 270 = $33,750,000

Medium – $300 * 150 * 270 = $12,150,000

Low - $100 * 50 * 270 = $1,350,000

*Counties, cities, school districts based on % of jurisdictions that use vendor vs internal staff

Return on Investment – Low Usage

<u>If Colorado Civilian Cyber Reserve responds to just 1 incident and proactively assists 15 jurisdictions per year…</u>

$300 / hour * 150 hours * 15 jurisdictions = $675,000
Medium jurisdiction (50% of incident cost) = $250,000
Total: $925,000

Return on Investment – High Usage

<u>If Colorado Civilian Cyber Reserve responds to just 1 incident and proactively assists 50 jurisdictions per year…</u>

$300 / hour * 150 hours * 50 jurisdictions = $2,250,000
2 x Medium jurisdiction (50% of incident cost) = $500,000
Total: $2,750,000

Conclusion

Investing in a Colorado Civilian Cyber Reserve will...

1. Increase the cybersecurity posture of local governments and critical infrastructure across the state
2. Save millions of dollars in proactive and cyber-attack clean-up costs
3. Create a simple, sustainable solution to a complex problem

Contact Information

Email: jonah.wisch@cyber-center.org
Phone: 215-680-4187


NCC
NATIONAL
CYBERSECURITY
CENTER