THE ELECTIONS GROUP

Accelerating Excellence

Cyber Navigator Resources Case Study

Published March 2023

Partnering to Share Cyber and Physical Elections Security Expertise Through the Rapid Response Election Security Cyber Unit

Colorado's RESCU Team

The security environment for state and local officials has evolved rapidly in the past several years. While states quickly developed cybersecurity programs to protect critical infrastructure from foreign threats, disinformation campaigns presented a new front. Protecting our elections now requires collaboration among cybersecurity experts, communications experts and those skilled at building alliances.

The Problem

Multiple cyberattacks in 2016 alerted many state and local election officials to the importance of election cybersecurity. Colorado became an early leader in the security field, and in 2018, The Washington Post declared Colorado "the safest state to cast a vote," citing the state's cybersecurity posture, audits and voting equipment as examples of outstanding election security.

Nevertheless, Colorado soon experienced a new kind of attack on election security: election mis- and disinformation campaigns. In Colorado, mis- and disinformation campaigns included "lies about voter fraud, mail ballots and election results to decrease confidence in elections." Election mis- or disinformation can mislead or confuse voters – or worse, disenfranchise them.

Breadth of Support Offered

	Cyber	Physical	Personal	Operations	Information
Basic	X	X			X
Intermediate	X	X			X
Intensive					X

Depth of Support

Project Features and Characteristics

Service Strategies	Assessments	Trainings/Exercises	Grant Funds	
	Collaborations	Information Sharing	Hands-On Support	
Program Creation Authority	Statutory	Regulatory / Rule-Making Authority	Discretionary Authority	
Local Participation	Statutory Mandate	Voluntary but Funding-Driven	Entirely Voluntary	
Financing	Federal Funds	State Funds	Other Funds	Mixed Financing
Staffing / Scale	Single Individual	Multiple Staff	Partnerships	Voluntary Providers
Staffing Focus	Security Subject Matter Expertise	Relationship Builders	Elections Expertise	
Partners	Federal Agencies	Other State Agencies	NGOs	
Collaboration Approach	Top - Down	Collaborative: Advisory Board; Roundtables; Working Groups		
Assessment Tools	NIST	Cybersecurity Framework	CIS Controls	Other

Officials from the Colorado Department of State (CDOS) faced many obstacles while trying to combat election mis- and disinformation. State cybersecurity experts did not necessarily have the communications experience and training to combat the particular election security threat posed by mis- and disinformation. Additionally, CDOS officials had strong relationships with local election officials, but not necessarily with county information technology and communications personnel. In some counties, there were no such full-time staff.

Similar to the counties, the state election office did not have a full-time staff member with the combination of knowledge, expertise and time to lead the effort against election mis- and disinformation.

"We didn't have enough horses," Judd Choate, Colorado's director of elections, said of the state's lack of resources focused on the problem.

The Solution

Colorado's solution was forming the Rapid Response Election Security Cyber Unit, known as RESCU. Secretary of State Jena Griswold and her leadership team developed their vision for the program. It was a solution to combat emerging threats by closing the gap between elections, cybersecurity, information technology, communications and law enforcement professionals at the state and local level.

RESCU consists of five full-time cybersecurity and communications professionals responsible for cybersecurity intelligence and response. Existing state cybersecurity staff were also detailed to assist RESCU from time to time. They primarily serve counties on two fronts:

- Communications support to combat disinformation
- Relationship building between state and local professionals

Previous security efforts focused directly on cybersecurity and voting equipment, making RESCU unique in that it branched out to communications and physical security. Secretary Griswold's team knew they needed to find an exceptional professional with the specialized background needed to lead this effort. They contacted Nathan Blumenthal, then Acting Deputy Assistant Secretary of Counter Terrorism and Threat Prevention for the United States Department of Homeland Security. An expert in foreign disinformation and counter-terrorism, Blumenthal was excited about this new program, and he agreed to take the lead in Colorado.

With Blumenthal at the helm, RESCU moved to boost the state's cybersecurity posture, establish a strategic response to mis- and disinformation campaigns, and assist counties with physical security."

Colorado's Approach

RESCU broadened and expanded Colorado's awareness and response to election security. It prioritized helping counties understand and combat disinformation while also building connections between state and local IT professionals.

Communications Support

The RESCU team established a strong portfolio of communications support. They conducted a qualitative and quantitative survey of Colorado voters to determine what messaging was getting communicated. They developed a multi-pronged approach to combating disinformation with an ad campaign: "Opinions are fun. Facts are better."

The campaign used cartoon characters expressing funny, likely unpopular opinions about the Colorado lifestyle. This helped the public easily grasp the importance of using trusted sources and thinking before sharing information they see on social media. The ads always directed readers back to the official CDOS website.

"The Opionionators" - Colorado's state symbols as cartoons

RESCU helps counties and the public understand disinformation using three simple and easily remembered steps:

1. Be aware
2. Think before you link
3. Use trusted sources

RESCU also runs a sophisticated online defense. They actively monitor the deep web, dark web and open sources to identify potential threats and share that information. They made sure that if people were searching the Internet for keywords associated with disinformation, then the state's official site would be at or near the top of the search results. Through the use of targeted advertising, RESCU could direct their advertising efforts toward general audiences, such as age groups more likely to encounter disinformation. They were mindful to ensure that ads were targeted broadly to increase effectiveness and avoid any unintentional partisan angles.

RESCU helped local officials establish a positive and authoritative presence online. They helped counties obtain verification on Twitter and provided tailored local graphics for online branding. RESCU also worked with counties to reach out to all ends of the political spectrum to highlight authoritative information sources.

Relationship Building

For years, the Secretary of State's office put considerable effort into fostering relationships between state and county officials. However, that capacity for professional networking did not always extend to local IT and cybersecurity teams.

"States are missing out if they do not know who those key people are at the county level. There is a huge opportunity gap," said Trevor Timmons, the Colorado Department of State's Chief Information Officer, adding that the state needed to "connect their geeks with our geeks."

RESCU developed strong contacts with each county's IT professionals. It was important to RESCU to establish one-on-one relationships with each county. The unit held regular – first quarterly and eventually monthly – phone calls, sharing information with counties. Through this continuous effort, RESCU team members knew the name and recognized the voice of key contacts in each county. Counties in turn were confident in the familiar, professional voice they heard when reaching out to the state.

Physical Security

RESCU provides information about threats to their federal, state and local law enforcement partners and creates situational awareness through its fusion center. The team worked with county sheriffs, creating a one-pager for sheriffs and undersheriffs that explained election laws. Larimer County Sheriff Justin Smith co-authored a piece on elections security for NBC Think.

RESCU also understood that the law enforcement community, by design, has a high bar for taking action. They wanted to make sure counties were aware of even low-level threat information so they could prepare and respond as needed. For example, some individuals participating in online harassment or threats began showing up in person at public meetings. RESCU would share that information with county officials so they were at least aware of what they were potentially walking into at public meetings.

Additional Program Efforts

The RESCU program is not limited by any program charter or statutory authority. Related program activities include:

- Proactively reaching out to counties to offer cyber and physical security assessments
- Setting up a grant program for the counties and reviewing grant application
- Working with the district attorneys' association and sheriffs' association to educate them on election laws
- Partnering with the Belfer Center at the Harvard University Kennedy School of Government to create Election Preparedness for Infrastructure and Cybersecurity (EPIC) tabletop exercises that were educational and engaging.

Infrastructure Needs

The RESCU program relies on subject matter expertise and coalition building above all. Recruiting and retaining the right people is paramount. RESCU team members have the expertise to look at search engine results and make sure the correct information is found on the first results page. They also used third-party monitoring and did not need to develop new technology or monitoring systems.

The state already had a fairly strong security policy foundation. For example, at the organizational level, the state required voter registration workstations be properly secured, patched and monitored for potential malicious activity. At the user level, the state required agreements for training, workstation configuration, multi-factor authentication and standards for use. The state had a large enough IT staff to support its existing security program.

Colorado benefits from a strong and long-standing working relationship between state and local election officials. Choate, who became director of elections in 2009, and his predecessor invested time into fostering strong working relationships with county officials.

Costs and Funding

The state used Help America Vote Act (HAVA) funds to launch and operate the RESCU program. Some efforts, such as the "Opinions Are Fun" campaign, involved securing additional funds and contracting with an advertising firm.

Startup Timeline

RESCU was deployed in July 2020 when the presidential election was just around the corner. During the first four to five months, Blumenthal onboarded his team and deployed the communications campaign.

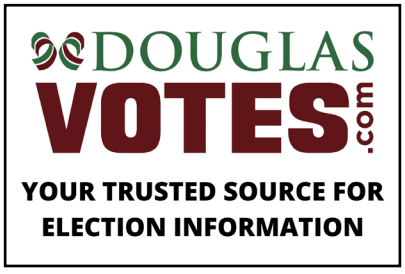
"The work was nonstop," he said.

In early 2021, the team pivoted to physical security. It took an additional six to seven months to get their staff all the resources they needed to develop processes and procedures

Impact

In October 2020, Secretary Griswold testified before the United States House of Representatives' Committee on House Administration's Subcommittee on Elections. She highlighted the initial impact of the RESCU program, noting that the team was "coordinating with partners across Colorado" and positioning the office to "rapidly respond to foreign mis- and disinformation."

Douglas County is one of many counties that sends out voter information guides prior to an election. RESCU worked with



Douglas and other counties to include a section to help voters recognize disinformation and establish county and state officials as trusted sources of election information.

The dynamic exchange of information between county, state and federal agencies greatly improved. On the cybersecurity front, after sending alerts to counties, RESCU team members would often follow up with phone calls. On those calls, they would learn if counties noticed potential security threats that the state could then share with CISA and EI-ISAC.

Obstacles

Security programs must be able to pivot and adapt to emerging threats. In Colorado, RESCU was originally going to focus on three pillars: cybersecurity, mis- and disinformation, and physical security. As the team assembled, they realized that mis- and disinformation would be their biggest threat, posing a risk to existing physical security infrastructure.

Scalability

States should be prepared to expand security and communications teams, rather than giving additional duties to an existing full-time employee with other job functions. Combating disinformation is not something an existing employee can simply add to their workload.

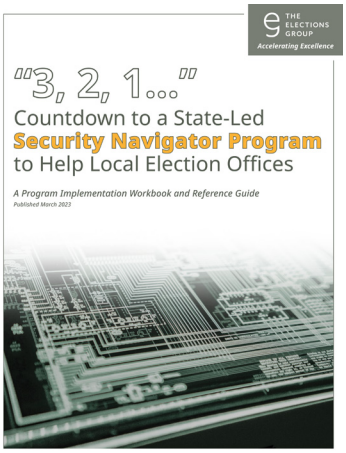
"If you're already working 80 hours a week and you encounter cyber issues, it's a non-starter," Blumenthal said.

States and counties should make a decision to dedicate resources. States can consider dedicating HAVA funds or even passing legislation to fund new positions.

Personnel should have relevant military or intelligence experience. They need someone who understands the state and local issues, but also has the communications experience to navigate social media.

Accelerating Your State's Cybersecurity Maturity

Download The Elections Group's Cyber Security Navigator Implementation Guide for a step-by-step guide to launching a security navigator program in your state.



The Elections Group provides resources such as *Writing an Elections Fact Page* and other tools and guides at our Communications Resource Desk.