2018 NASS IDEAS Award Application
State of Colorado

Nominating State Office:
Secretary of State Wayne W. Williams
1700 Broadway, Suite 200
Denver, CO 80290
303-894-2200

Project Lead and Staff Contact for Questions:
Judd Choate, Elections Director
judd.choate@sos.state.co.us – 303-869-4927
Trevor Timmons, CIO
trevor.timmons@sos.state.co.us – 303-860-6946

Program Title:
Cybersecurity Protects Election Integrity initiative

Program Description:
The 2016 General Election cybersecurity revelations were a real eye-opener for the news media, the public and, apparently, many in the federal government. But hacking efforts were not a surprise to election professionals, who have long prepared for just these kinds of intrusion attempts. Technology has provided extraordinary advances in election management, increasing voter choice and convenience, while enhancing operational efficiencies for election administrators. But these benefits come at the cost of greater exposure to cybersecurity threats. Banking, online commerce, and sectors covered by the critical infrastructure designation employ ever-more-advanced security measures. But elections have been slower to adopt these best practices. Colorado's "Cybersecurity Protects Election Integrity" initiative has employed these cutting-edge ideas to protect elections.

General Subject Area:
Election Cybersecurity

Executive Summary

History and Significance

The use of technology in election management has increased voter choice and convenience, while enhancing operational efficiencies for election administrators. But these benefits are inversely proportional to the security posture of election systems. While state and local election administrators were largely prepared for external attempts to infiltrate election systems in 2016, these will not be the last such efforts. Election administrators are still building their toolkit of digital protections analogous to chain of custody logs and ballot box seals. In order to maintain election integrity, officials must match advances in one area—voter choice and administrative efficiency—with advances in the other—election cybersecurity.

Outside actors' attempts to influence the 2016 General Election heightened the public's attention to and expectations of election administrators to secure election systems and, ultimately, ensure the integrity of election outcomes.

> *"State and local autonomy over elections is our greatest asset against malicious cyberattacks and manipulation."*
>
> *NASS statement, Jan. 9, 2017*

And the U.S. Department of Homeland Security's January 2017 decision to designate election systems as critical infrastructure further heightened the urgency with which state election officials must take a leadership position in election cybersecurity.

State chief election officials play a unique and critical role in creating and implementing standards and best practices while also coordinating resources among a number of interested parties to ensure election integrity. Colorado has worked to implement one of the most voter-friendly election systems in the country, including no-excuse absentee ballots (1992), in-person early voting (1996), vote centers (2003), online voter registration (2010), secure electronic ballot delivery (2012) and return (2016) for military and overseas voters, all-mail ballot elections (2013), and same-day voter registration (2013). But each technology that increases voter choice and administrative efficiency also increases the risk of cyber intrusion. So Colorado's advancements in voter convenience have necessitated commensurate cybersecurity efforts, including implementing standards, enforcing best practices, and coordinating resources that secure election systems and protect election integrity.

Other industries have led the way on cybersecurity, including online commerce, banking, and others. Colorado utilizes a variety of security measures, and has led with an effort to employ not just existing elections best practices but security practices seen as state-of-the-art in all industries with a cyber footprint. Three specific efforts highlight Colorado's "Cybersecurity Protects Election Integrity" initiative.

1. Securing the statewide voter registration system

The Colorado Secretary of State operates the **S**tatewide **CO**lorado voter **R**egistration and **E**lection management system (SCORE) and the ePollbook application (webSCORE). Together, these leverage technological infrastructure to provide voters with incredible choice and convenience. Active Colorado voters receive a mail ballot or they can choose to vote at any Voter Service and Polling Center (VSPC) in their county during early voting or on Election Day. Voters can also register at a VSPC up to and including Election Day and cast a "real" ballot in that election. This means all county election staff must have access to a real-time statewide voter registration system and poll book. This requirement increases

opportunities for cyber intrusions. So Colorado has implemented cybersecurity best practices that apply to all state and county-level users of the SCORE system, including multi-factor authentication and security awareness training.

Multi-factor authentication improves Colorado's security posture.

Beginning in 2013, the Colorado Secretary of State's office required all state and county-level SCORE users to login with **multi-factor authentication**. Users must each use not only a unique username and password, but also a numeric sequence (unique to each user), provided on a physical card distributed by the Secretary of State. This provides a significant security improvement to thwart password-stealing spyware, brute force password attacks, password guessing, and the sharing of user credentials.

Security awareness training helps "secure the human" element of cybersecurity.

Security awareness training is the formal process the Secretary of State implemented to educate users about computer security, departmental policies and procedures, and the three goals that are the basis of all security programs: protect the confidentiality of data, preserve the integrity of data, and promote the availability of data for authorized use.

Also beginning in 2013, all active SCORE and webSCORE county users were required to take the *Securing the Human* security awareness training program from the SANS Institute. Everyone, including full-time, part-time, and temporary state and county staff, who accesses the SCORE database must complete this training within 30 days of hire. Election judges are the only exception to the SANS training requirement, but they must complete a unique security awareness program called "Election Judge – Staying Cyber Safe" through the Secretary of State online learning platform. Users who do not complete training by their given deadline lose system access.

SECURITY AWARENESS TRAINING

Training modules include:

- Browsing
- Data Security
- Email, Phishing & Messaging
- Passwords
- Social Engineering
- Physical Security
- Personally Identifiable Information (PII)

2. Securing oversees and military ballot return with encryption

Technology has better enabled election officials to serve voters covered by the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA). But again, technological advances have exposed vulnerabilities that threatened to degrade election integrity.

Postal mail is notoriously unreliable in some parts of the world, especially areas where our troops are operating. Electronic delivery—begun in Colorado in 2006 for overseas military voters and extended to all overseas voters in 2011—provided a more reliable and timely way to get ballots out to UOCAVA electors. But those electors still had to rely on the postal service to return voted ballots, find increasingly-less-available fax machines, or risk the anonymity of their ballot by emailing them back to their county election official.

So Colorado adopted state-of-the-art encryption technology to secure voted ballots on return to county election administrators. The **secure ballot return (SBR) system**—implemented for the 2016 General Election—solves the security problem while preserving voter convenience. Secure ballot return allows UOCAVA voters to return their ballots via a web portal, directly to their county of residence. SBR provides increased security with an encrypted channel (TLS 1.2) for the ballot transfer, secure logging, and

centralized county administrator two-factor authentication access. This encryption standard uses industry best-practice technology to keep unauthorized users from accessing the content of the message as it travels across the internet. The system also provides a delivery receipt notice to voters, so they can be sure their vote will be recorded.

Once implemented for UOCAVA, the SBR system provided additional opportunities for enhanced election security. For example beginning the Monday before Election Day, if a voter delivers a mail ballot to the wrong county, the county can use secure ballot return to securely send a copy of the back of the ballot envelope with the voter's signature to the correct county—allowing the county to receive the ballot into SCORE in advance of receiving the physical ballot. This also serves as notification that a ballot has been received by another county.

In the 2016 General Election, more than half of Colorado's UOCAVA voters returned their ballot electronically. Of those, 87 percent used the SBR system.

3. Colorado Threat Information Sharing and Joint Fusion Centers coordinate and expand cybersecurity resources to protect Colorado elections

State election officials must take a leadership role in coordinating the variety of resources available to proactively secure election systems and defensively fight off cyber-attacks. State election officials occupy a critical space in the nation's election system, in between federal authorities who often have greater resources and technical expertise, and county officials who carry out most administrative functions. The U.S. Department of Homeland Security's critical infrastructure designation in January 2017 was a wake-up call to state election officials. It is clear that state election officials must do more to pro-actively coordinate resources and increase knowledge sharing. Colorado is leading by example with the **Colorado Threat Information Sharing (CTIS)** project.

In 2016, the Colorado Secretary of State expanded efforts and placed an even higher priority on information sharing and situational awareness with respect to its cyber security posture and emerging threats. The Secretary of State partnered with the Colorado Governor's Office, Colorado Governor's Office of Information Technology, U.S. Department of Homeland Security, Colorado Department of Public Safety, Multi-State Information Sharing & Analysis Center (MS-ISAC), FBI, Colorado National Guard, City & County of Denver, Jefferson County, and others to rally around protection, monitoring, detection and response in the face of known and unknown threats. The Department stood up joint fusion centers on Election Day 2016 to share information quickly and securely across jurisdiction boundaries.

This allowed the Secretary of State to harness cybersecurity expertise and resources from across the state for monitoring and analysis during peak election periods. This community complements the federal and state partnerships coming together under the critical infrastructure framework with a similarly-structured community organized within the State of Colorado.

The information sharing paid dividends on Election Day 2016 during two significant events. First, the commercial building housing the Secretary of State's command center was temporarily evacuated on Election Day due to a fire alarm. Because of the multi-site capability in place for monitoring and response to elections incidents, all parties were quickly able to attribute the evacuation to a non-critical event and continue to apply our focus to Election Day monitoring during the fire alarm evacuation.

Second, in the early afternoon, the state voter registration system became unresponsive for approximately 23 minutes. The resources monitoring the system were able to rapidly rule out cyber-attacks as a potential source of the service interruption, which allowed resources to focus on triage and

restoring service to the system. The system was returned to service in under 30 minutes. Without the focused and intense work of the county and state resources, incident analysis likely would have consumed more time and possibly could have resulted in more serious impact on Election Day.

Colorado Threat Information Sharing (CTIS)

The partnership, begun in 2016, grew in 2017. As a result, instead of the Secretary of State having three department staff available on Election Day for cybersecurity analysis and response, we had eight Colorado National Guard personnel on-site in two four-person shifts, two private sector cybersecurity experts, three county cyber experts, and state and federal cybersecurity staff monitoring election activities, essentially quadrupling the number of individuals monitoring and assessing network traffic and potential cyberthreats.

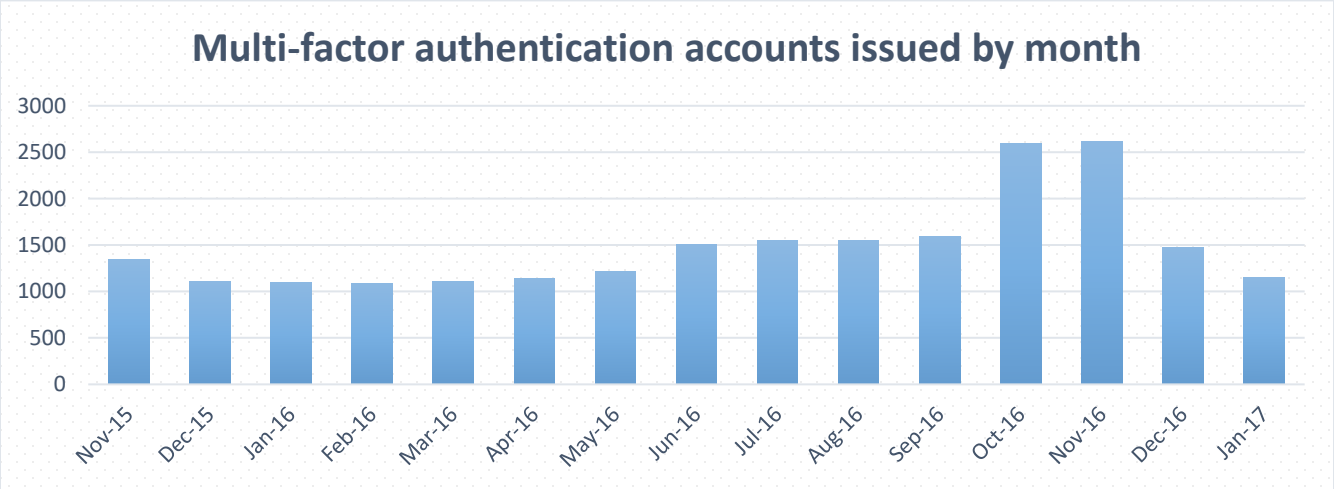
The CTIS community has also provided benefits outside of service to key election activities. Within the past six months, it has also been used to share information on phishing campaigns, ransomware incidents, and to share information on general cybersecurity issues.

Conclusion

State chief election officials play a critical and unique role in creating and implementing standards and best practices while also coordinating resources among partners and advocates to ensure election integrity. In this area, Colorado is leading on both fronts: implementing emerging technologies to enhance voter convenience and election administration efficiency, while implementing standards and coordinating resources that secure election systems and protect election integrity.

Impacts/Results

Multi-factor authentication



Secure Ballot Return (SBR)

Oversees and military vote metrics from the 2016 General Election

Registered UOCAVA voters and ballots sent *	
Military	11,913
Overseas	26,712
Total	**38,625**

** Includes active and inactive*

UOCAVA ballots voted by method	
Mail	9,918
Electronic*	12,663
Fax	509
Total	**23,090**

** Includes both email and Secure Ballot Return*

Breakdown of ballots returned electronically	
Email	1,585
Secure Ballot Return	11,078
Total	**12,663**

Colorado Threat Information Sharing and Joint Fusion Centers

CTIS Alerts shared Nov '16 to Jan '18		
Time Period	Number of Alerts	Number of Topics
2016	5	4
First half 2017	23	12
Second half 2017	20	10
2018 year-to-date	1	1

Breakdown of alerts available in supporting documentation section below

Supporting Materials

Securing the statewide voter registration system

Multi-factor authentication

Step 1.

Users see this traditional username and password as the first step to log into SCORE, the Colorado statewide voter registration database.

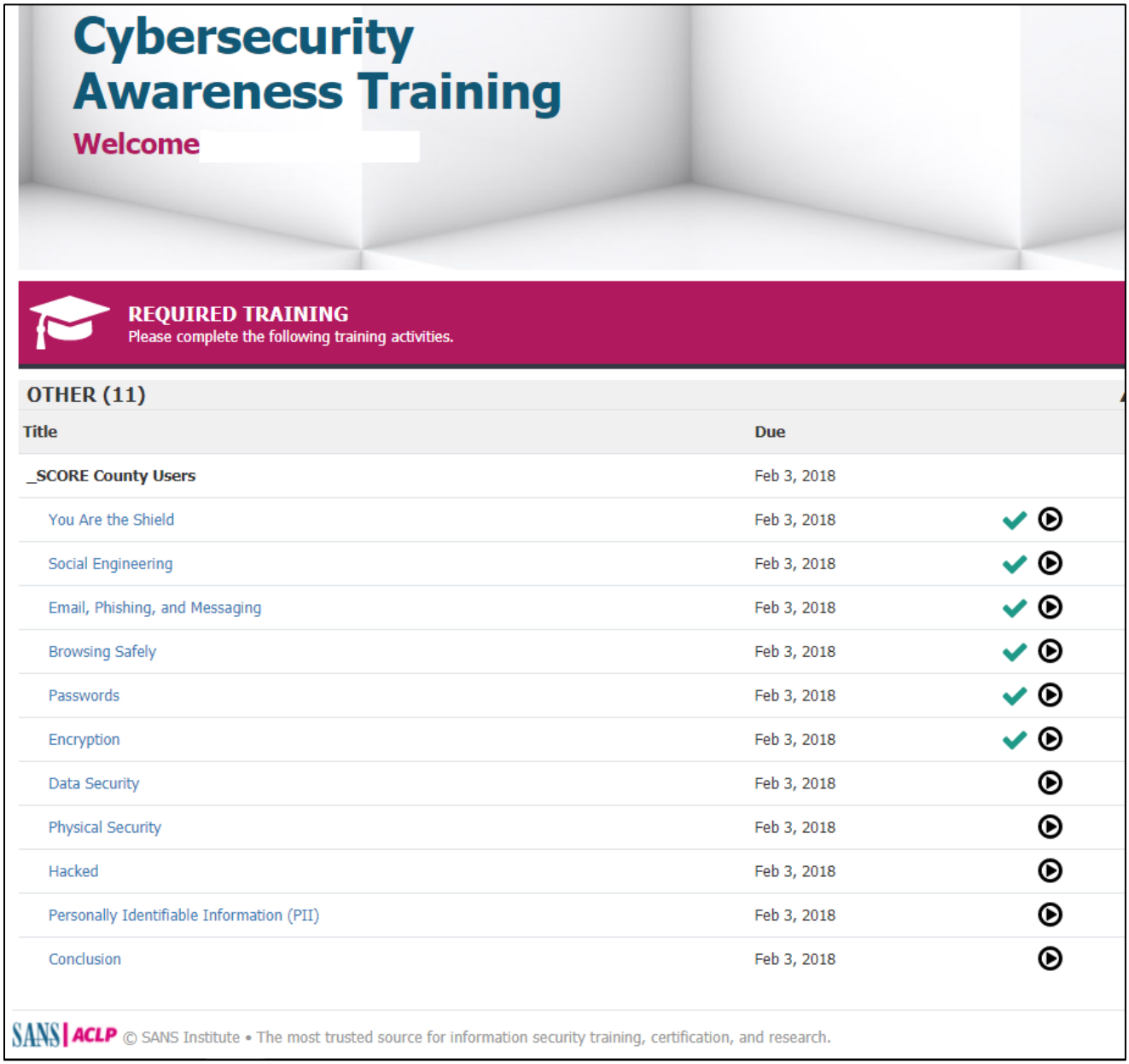
Step 2.

On the next screen, the system prompts the user with a challenge, citing the specific card number assigned to the user. This is the second factor in the multi-factor authentication.

	A	B	C	D	E	F	G	H	I	J
1	J	P	7	X	9	3	F	9	0	E
2	P	R	V	V	2	K	2	8	X	W
3	9	2	P	M	F	R	6	1	F	P
4	8	Y	0	X	D	0	N	2	X	N
5	J	N	Y	X	J	6	9	6	4	P

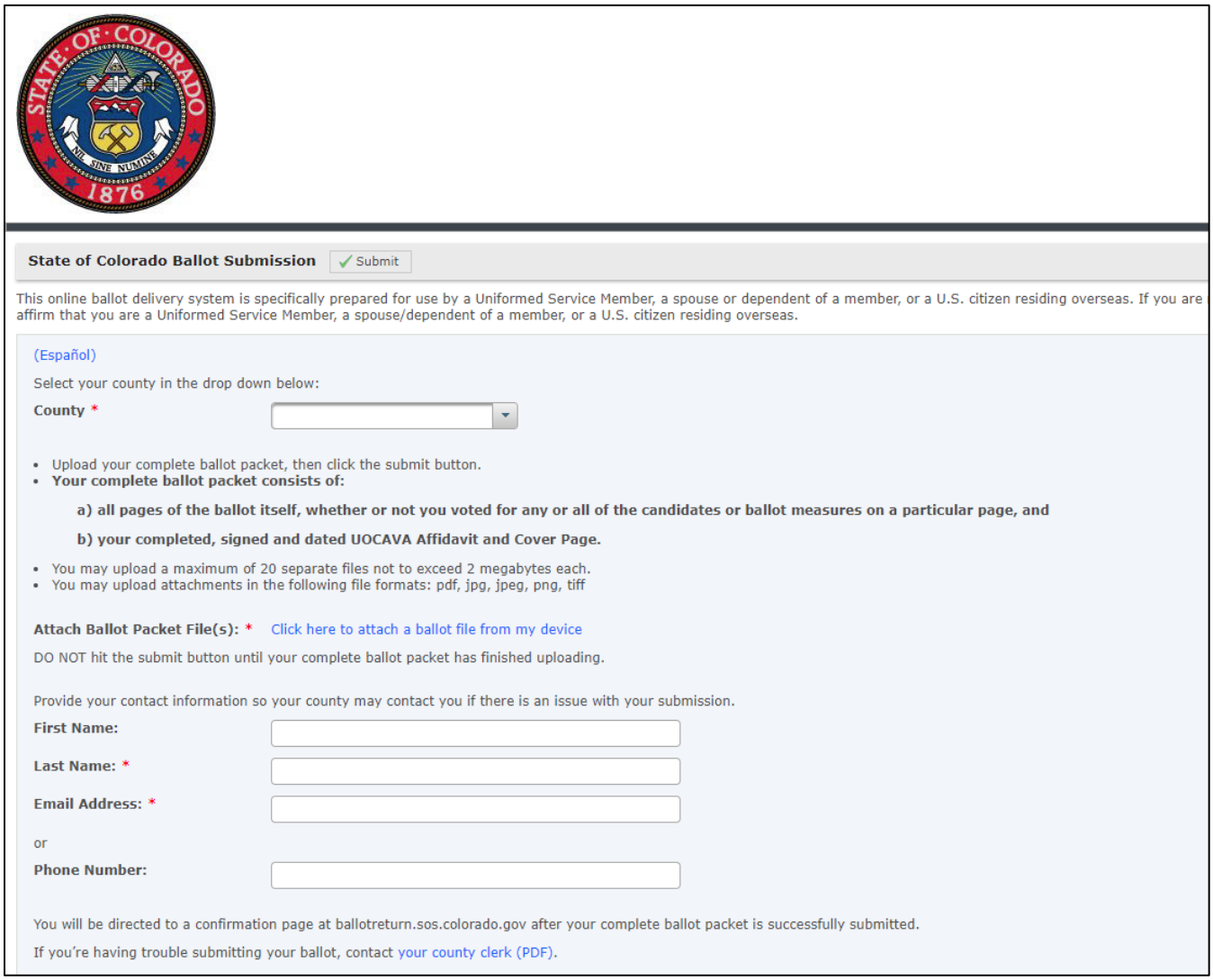
Users have either an electronic card—shown above here—or a physical card, unique to each user. When prompted by the challenge screen above, the user references the card to enter the appropriate response.

Security awareness training



Screenshots from the SANS *Securing the Human* training required for all users who access the Colorado statewide voter registration system.

Securing oversees and military ballot return with encryption



State of Colorado Ballot Submission ✓ Submit

This online ballot delivery system is specifically prepared for use by a Uniformed Service Member, a spouse or dependent of a member, or a U.S. citizen residing overseas. If you are affirm that you are a Uniformed Service Member, a spouse/dependent of a member, or a U.S. citizen residing overseas.

(Español)

Select your county in the drop down below:

County *

- Upload your complete ballot packet, then click the submit button.
- **Your complete ballot packet consists of:**

  a) all pages of the ballot itself, whether or not you voted for any or all of the candidates or ballot measures on a particular page, and

  b) your completed, signed and dated UOCAVA Affidavit and Cover Page.

- You may upload a maximum of 20 separate files not to exceed 2 megabytes each.
- You may upload attachments in the following file formats: pdf, jpg, jpeg, png, tiff

Attach Ballot Packet File(s): * Click here to attach a ballot file from my device

DO NOT hit the submit button until your complete ballot packet has finished uploading.

Provide your contact information so your county may contact you if there is an issue with your submission.

First Name:

Last Name: *

Email Address: *

or

Phone Number:

You will be directed to a confirmation page at ballotreturn.sos.colorado.gov after your complete ballot packet is successfully submitted.

If you're having trouble submitting your ballot, contact your county clerk (PDF).

Screenshot from the Colorado Secure Ballot Return application for overseas and military voters.

Coordinating cybersecurity resources and information-sharing

Colorado Threat Information Sharing (CTIS)

Date	Description
1/5/2018	Notice on Meltdown/Spectre vulnerabilities
12/19/2017	Report of password brute force attempts
12/12/2017	Report of persistent phishing attack
12/7/2017	Notice of phishing emails
12/5/2017	Notice of credential stealing phishing emails
11/16/2017	Information on DHS cyber review engagement
11/14/2017	Information on DHS cyber review engagement
11/14/2017	Information on DHS cyber review engagement
11/14/2017	Information on DHS cyber review engagement
10/18/2017	Notice of phishing emails
10/16/2017	Notice of phishing emails
10/11/2017	Notice of phishing emails
9/15/2017	Notice of phishing emails targeting organization
9/15/2017	Notice of phishing emails targeting organization
9/15/2017	Notice of phishing emails targeting organization
7/13/2017	Notice of organization targeted by hacking
7/13/2017	Notice of organization targeted by hacking
7/12/2017	Notice of organization targeted by hacking
7/12/2017	Notice of organization targeted by hacking
7/3/2017	Notice of Office 365 phishing attempts
7/3/2017	Notice of Office 365 phishing attempts
6/28/2017	Alert on ransomware
6/28/2017	Alert on ransomware
6/27/2017	Alert on ransomware
6/21/2017	Alert on malware
6/20/2017	Alert on malware
6/1/2017	Notice of phishing emails
6/1/2017	Notice of phishing emails
6/1/2017	Notice of phishing emails
6/1/2017	Notice of phishing emails
5/15/2017	Notice on Wannacry
5/15/2017	Notice on Wannacry
5/15/2017	Verizon outage notice
5/14/2017	Alert with Wannacry signatures
5/12/2017	Alert with Wannacry signatures
5/12/2017	Alert with Wannacry signatures

4/28/2017	Notice of organization targeted by whaling/spearphishing
4/6/2017	Lessons from organization targeted by phishing
4/5/2017	Lessons from organization targeted by phishing
3/28/2017	Alert on ransomware
3/20/2017	Alert on multiple organizations targeted by ransomware
3/13/2017	Alert on multiple organizations targeted by ransomware
3/10/2017	Alert on unauthorized access attempt
1/12/2017	Notice of phishing emails targeting organization
12/12/2016	Notice of ransomware incident from organization
11/23/2016	Notice of website defacement
11/18/2016	Lessons from organization on specific firewall issues
11/2/2016	Additional information on potential phishing attack
11/1/2016	Alert on potential phishing attack