
NATIONAL CYBERSECURITY CENTER
NCC


NCC
NATIONAL
CYBERSECURITY
CENTER

Agenda

Introduction
Background
NCC Overview
Cyber for State Leaders
Secure the Vote

History & Background

MISSION

We strive to be a leader and convener in cyber education, workforce development, and informing public policy.


Gov. Hickenlooper signs bill for cyber workforce development and research funding

May 30, 2018 Jared Verner

Gov. John Hickenlooper signs SB 18-086 "Cyber Coding Cryptology for State Records" into law May 30, 2018.

The National Cybersecurity Center (NCC) is a 501(c)(3) non-profit for cyber innovation and awareness. Established in 2016 from the vision of United States Senator from Colorado John Hickenlooper, in coordination with several people from the University of Colorado Colorado Springs (UCCS) and the community, the NCC serves both public and private organizations and individuals through training, education and research.

Programs

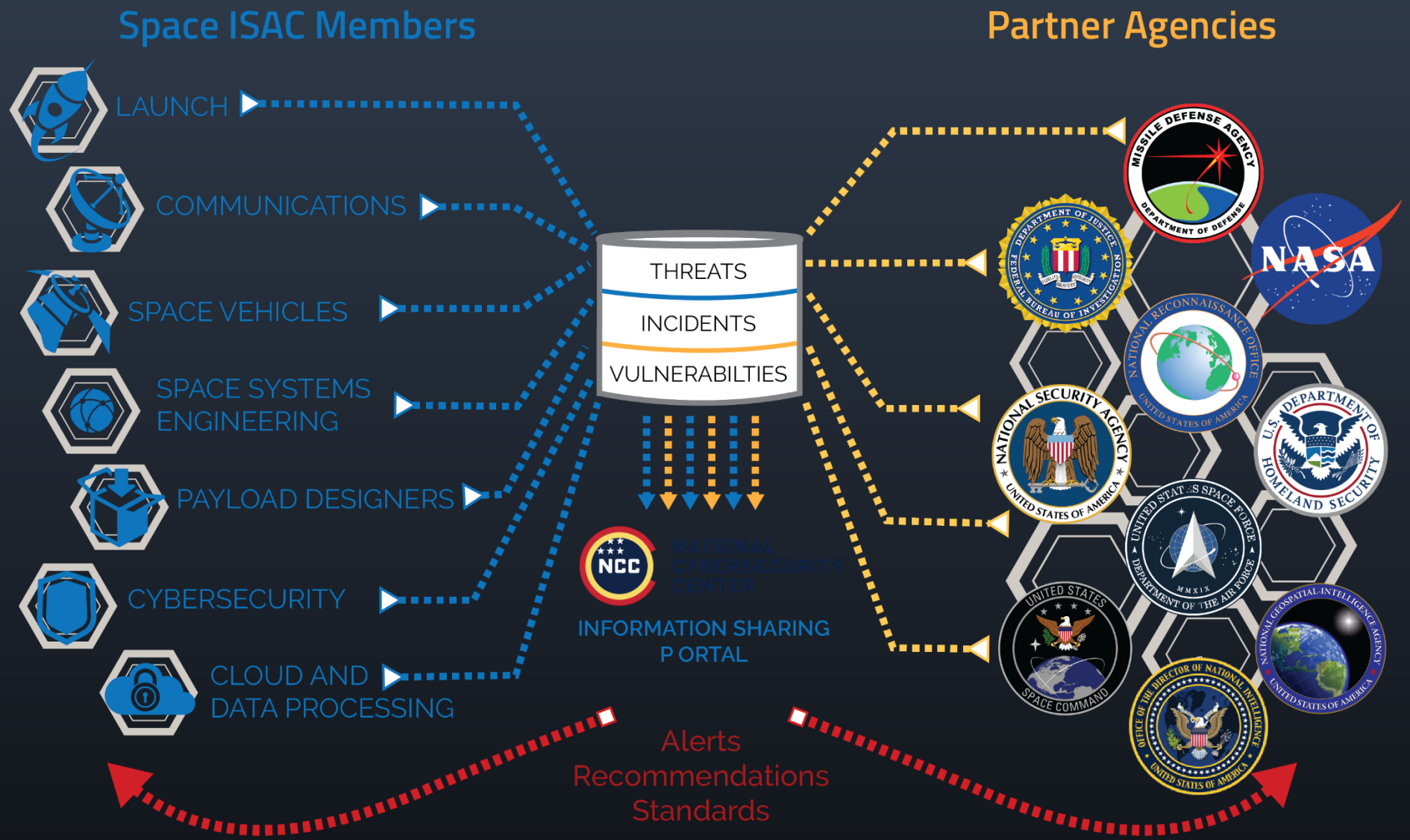
CYBERSECURITY FOR STATE LEADERS

SPACE ISAC

STUDENT ALLIANCE CYBER EDUCATION

Colorado Cyber Resource Center

Space ISAC Communities



Notes: Including International Partner Agencies (ESA, JAXA, DLR, etc.)

Founding Board Members

SPACE ISAC

national council of ISACs

NORTHROP GRUMMAN

PARSONS

Booz | Allen | Hamilton

SES

UCCS University of Colorado Colorado Springs

APL JOHNS HOPKINS APPLIED PHYSICS LABORATORY

MITRE

AEROSPACE

LOCKHEED MARTIN

Microsoft

Space Dynamics LABORATORY Utah State University

KRATOS READY FOR WHAT'S NEXT™

PURDUE UNIVERSITY

L3HARRIS™ FAST. FORWARD.

STUDENT ALLIANCE

CYBER EDUCATION

COLORADO K-12 CYBER INITIATIVE

- NCC trained over 1000+ students in 2020
- NCCSA is a Cyber Patriot Center of Excellence
- We now have an adult re-skilling program in pilot that has given out more than 100+ certificates (Security+, Network +)
- We directly teach in 3 school districts across Colorado providing hands on cybersecurity education

Colorado Cyber Resource Center

PISCES

Coordinating entity for Project PISCES

Pairs under-resourced jurisdictions in Colorado with advanced cybersecurity students in the state to provide no-cost network monitoring for the jurisdictions & hands-on training for students

Cyber Range

A virtual, statewide cyber range available to K-12 students & adults transitioning into cybersecurity or upskilling

Users receive a year-long license to access over 10 Learning Paths & over 600 modules on a variety of beginner, intermediate and advanced topics

Critical Impact Assessments

Assessments for local jurisdictions (beginning March 2022):

- Identifying most critical operational assets,
- Interdependency between operations
- Prioritization of security activities to prevent additional damage in the case of a cyber incident

Webinars and ongoing resource support

- Monthly special topic webinars covering basic topics such as incident response planning and management;

- Free, basic cybersecurity awareness training available each month for local governments, SMBs and non-profits (starting Feb 2022)

CYBERSECURITY
FOR STATE LEADERS

Cybersecurity for State Leaders

Background

Decision makers – particularly on the state level – must internalize cybersecurity as a core policy issue underlying the delivery effectiveness and efficiency of a diverse set of government services.

A key challenge to the normalization and prioritization of cybersecurity infrastructure is the significant lack of IT and technical background on the part of most state legislators in the U.S.

In order to accomplish a sustained level of cybersecurity awareness, we are launching a training for legislators and their staff to support better cyber hygiene at the state legislative levels, supported by Google. By empowering legislators and their staff to become more cyber safe, we are creating an additional layer of security for each state in the battle against ongoing cyber attacks.

CYBERSECURITY
FOR STATE LEADERS

Our mission is to raise the level of cybersecurity awareness among state-level decision makers so that they become an active part of defense for states by adopting cybersecurity best practices, and lead states into a strategic and secure future.

Unpacking Recent Threats

Ransomware

Ransomware Attack Hits Las Cruces, New Mexico Public Schools

The attack early in the morning of October 29 has taken all of the school district's systems offline.

In 2019, over 10,000 computers in Las Cruces School District were hit with ransomware. Almost 4 weeks passed where students and school teachers were unable to perform routine business functions while the school districts infrastructure was being rebuilt.

The hackers were able to do so by infecting the school network using phishing. A common tactic most of us more commonly call scam email. It cost over $1 Million dollars and the school district was hit again less then a year later.

Key Takeaways:

- *Prevention is always cheaper than response.*
- *80% of business and government today is automated, what are the implications from a ransomware attack on your business?*
- *How do school districts commonly train and educate on cybersecurity?*

CYBERSECURITY FOR STATE LEADERS

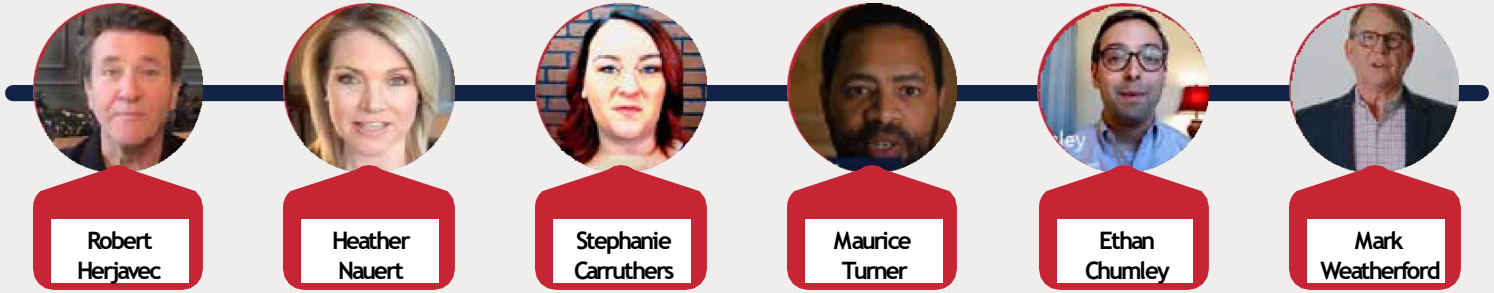
Over 1000 education districts were targeted in 2020.

62 Percent increase in attacks worldwide

75% of all businesses worldwide experienced a successful phishing attack

THE CURRICULUM

SOME OF OUR INSTRUCTORS



Robert Herjavec
Shark Tankstar & CEO of Herjavec Group

Heather Nauert
former State Dept spokesperson

Stephanie Carruthers
IBM Chief People Hacker

Maurice Turner
Alliance for Securing Democracy Fellow

Ethan Chumley
Sr Cybersecurity Strategist, Microsoft's Defending Democracy

Mark Weatherford
former DHS Deputy Cybersecurity Undersecretary

Deborah Blyth
former CO CISO

Leslie Kershaw
Founder of CyWren Solutions, LLC

Lucian Teo
Google's Online Global Safety Lead

Sunny Consolvo
Google's Sr User Privacy Experience Team Lead

Meredith Graffanti
FTI Crisis Communications Leader

Kevin Taylor
Comcast Cybersecurity Fellow

BASED ON THE DON'T GET D.U.P.E.D. METHOD

- Deploy Multi-Factor Authentication
- Update your software
- Passwords must be strong
- Encrypt your files
- Don't click on things you shouldn't

Google

IBM

HERJAVEC GROUP

Microsoft

CROWDSTRIKE

FTI CONSULTING

alliance for securing democracy

COMCAST

TRAINING DEPLOYMENTS

852 LIVE BRIEFINGS

383 ON-DEMAND BRIEFINGS

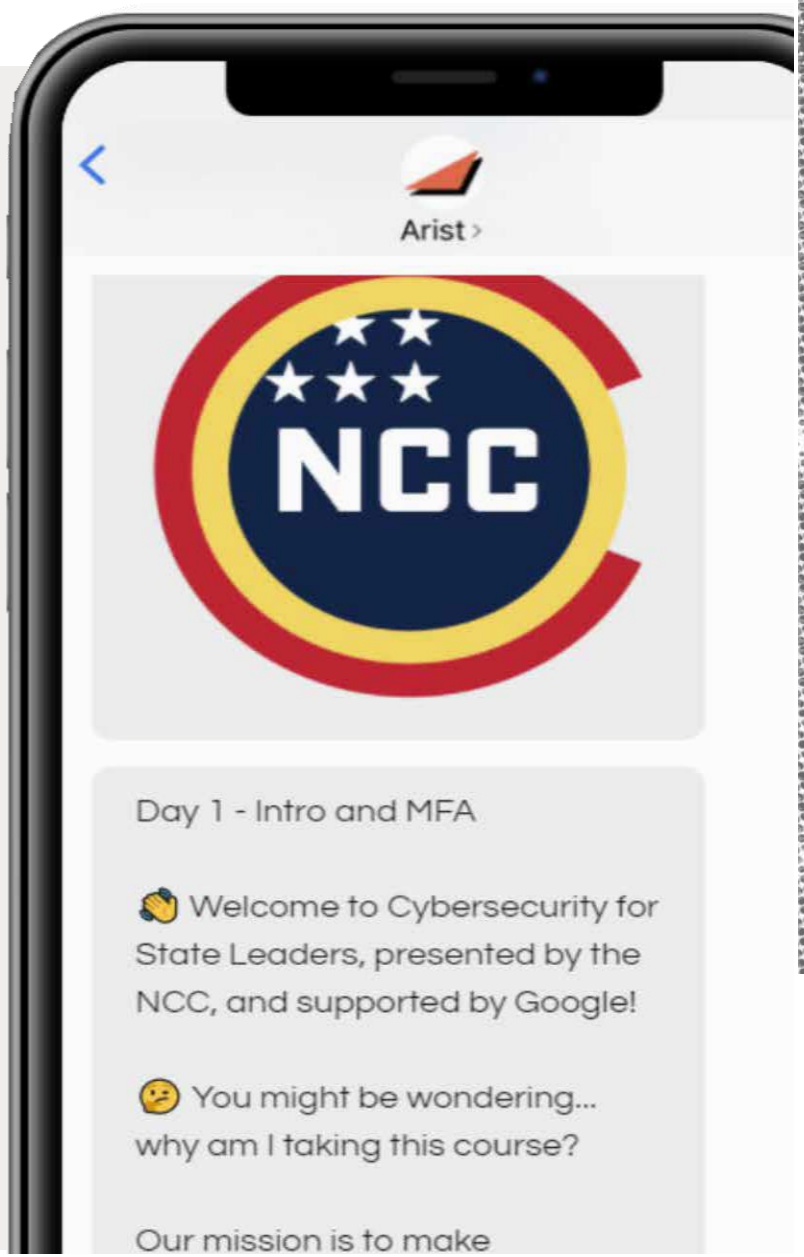
31 TEXT-TO-LEARN BRIEFINGS

In only four months (Aug – Dec)

76 INDIVIDUALIZED BRIEFINGS

Program Report

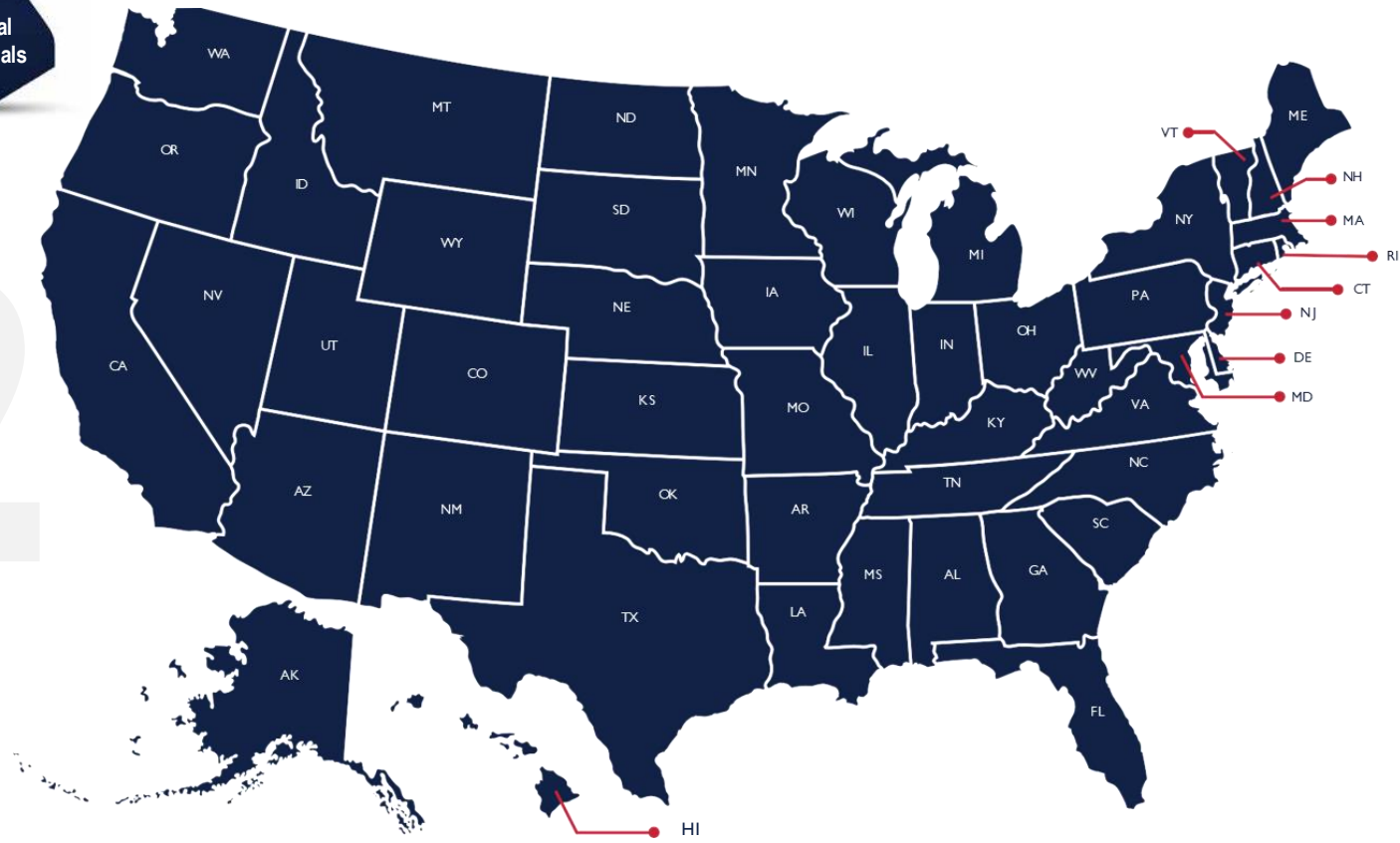
OVER 160,000 OUTREACHED



Cyber for State Leaders recap

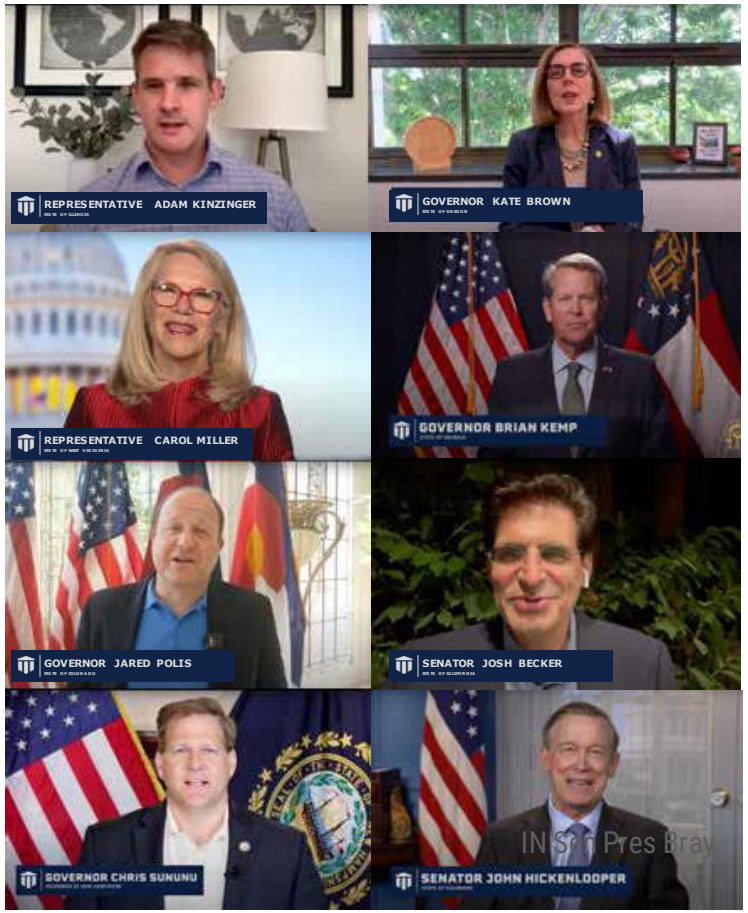
1,342

STATE AND LOCAL LEADERS BRIEFED



BY THE NUMBERS

48 HIGH-PROFILE CHAMPIONS



ISSUED CERTIFICATES

825

12,970 WEBSITE PAGEVIEWS

1,096 NEWSLETTER SUBSCRIBERS

PRESS IMPACT

POLITICO

STATESCOOP

FOX BUSINESS

GOVERNING
THE FUTURE OF STATES AND LOCALITIES

techradar.pro

SHNS
STATE HOUSE NEWS SERVICE

The Gazette

Charleston Gazette-Mail
an WVmedia company
A PULITZER PRIZE-WINNING NEWSPAPER

DENVER BUSINESS JOURNAL

Federal Champions

CO Sen John Hickenlooper
WV Sen Shelley Moore Capito
WV Sen Joe Manchin
WV Rep Carol Miller
IIL Rep Adam Kinzinger
SC Rep Nancy Mace

Governors

MS Gov Tate Reeves
MT Gov Greg Gianforte
OR Gov Kate Brown
GA Gov Brian Kemp
CO Gov Jared Polis
ID Gov Brad Little

AZ Gov Doug Ducey
MD Gov Larry Hogan
NH Gov Chris Sununu
ND Gov Doug Burgum
MA Gov Charlie Baker

OH Lt Gov Husted
MA Lt Gov Polito
AR Lt Gov Tim Griffin

State Leaders

MA CIO Curtis Wood
FL Cyber Director Ron Sanders
OK-ISAC Director Chance Grubb
TX Deputy CISSP Suzi Hilliard
OH SoS* Frank LaRose
CO CISO Debbi Blythe
CO SoS Jenna Griswold
OR SoS Shemia Fagan
IN Cyber Hub Director Chetrice Romero
SC Cyber Exec Director Tom Scott
SC State Cyber Liaison Sean Fay
MN Sen Mark Koran
IL Rep Keith Wheeler
MA President Karen Spilka
CA Senator Josh Becker
OH Rep Rick Carfagna
MT Rep Ken Holmlund
MT Sen Jen Pomnichowski
WV Delegate Moore Capito
MD Delegate Reid Novotny
MD Sen Katie Frye Hester

*SoS – Secretary of State

MAKING A BUZZ

151,431
TOTAL IMPRESSIONS

TWEET COUNT **406**

2,878 ENGAGEMENTS

41,121
TOTAL IMPRESSIONS

6,591
VIDEO VIEWS

20,774
REACH ON POSTS

13,799
VIEWS ON REELS

3,071
VIEWS

Stakeholders & Challenges

Stakeholders

Project Sponsor: Google

State Elected Officials

Corporate Speakers and guests

NCC Staff & Board of Directors

Challenges

Engaging with 50 States & US Territories to get significant attendance was difficult to do in one calendar year

Online trainings can be boring and tiresome

Coordination of speakers and materials over 100 presentations was difficult

Small staff

Opportunities

Increased turnout

Opportunity for self guided education

Narrower focus on specific regions or offices


SECURE THE VOTE
(Retired)
NCC

Secure the Vote Background

Secure the Vote emerged in response to state and local election officials' expressed concerns about the security of overseas voting options.

In 31 states (plus DC), overseas voters may use a variety of options to return ballots – primarily, email, fax, and web portals, with only five of those states allowing for voting over a web portal. The other 19 states do not allow for any online return of a ballot.

In order to address the security concerns of email and fax, an increasing number of jurisdictions have become interested in piloting mobile voting applications and platforms for overseas voters. Secure the Vote became involved in those pilots as an independent, third-party auditor. The first pilot was conducted in 2019 in the City and County of Denver.

Since the first pilot, Secure the Vote has worked to develop best practices in the digital voting space with the understanding that the nexus between technology and elections is likely to grow.

Our priority is to ensure that standards exist for the online and mobile voting applications, sufficient training of election officials and voter education is in place, and clear auditability standards are met.

Secure the Vote Overview

Secure the Vote seeks to increase voter confidence in the accuracy of vote-counting, and to generate greater awareness of possible solutions to critical gaps in the voting infrastructure. Secure the Vote supports jurisdictions' efforts to offer a secure, auditable mobile voting option for overseas voters through coordinating and evaluating pilots across the country, Additionally, Secure the Vote conducts cyber hygiene and security trainings for election officials, with a focus on underserved jurisdictions. ***We are committed to the belief that if we secure the vote, we secure the world.***

Vision	**Increased voter confidence in the accuracy and security of elections**
Mission	**Reduce and mitigate risks to voting securely through enhancing voting technologies, dismantling disinformation threats, and increasing cyber training and resources for elections administrators**

Core Programs

Mobile Voting Pilots	Coordinate and audit pilots testing mobile voting applications that serve overseas and disabled voters to address the insecurity of email and fax ballot returns options; create best practices and audit standards for digital voting (RLA for digital space)
Dismantling misinformation	Combat impacts of election misinformation and disinformation by unpacking the 'black box' of elections to help voters better understand how votes are processed and counted, and how they can protect themselves, and advancing technologies that enable elections transparency

Pilot Description

Gaps & Goals

	Voter registration	Vote casting	Vote Tabulation	Results Reporting	Post-Election Audit
Gaps	Security of voter registration systems & voter identification processes for electronic voting	Concerns about votes being counted as cast; lack of E2E verification for electronic voting	Malware infection; physical security practices	Security of websites for reporting	Limited deployment of state-required risk-limiting audits to prove results
Goals	Support enhancing elections ecosystem security & voter identification technology	Support ballot tracking options & security; standardize requirements for E2E	Explore technologies that improve security of tabulation machines & enforce audit trails for e-voting	Support enhancing elections ecosystem web security	Advocate for RLA processes in post-election audit; develop standards around e-voting audits

Impacts

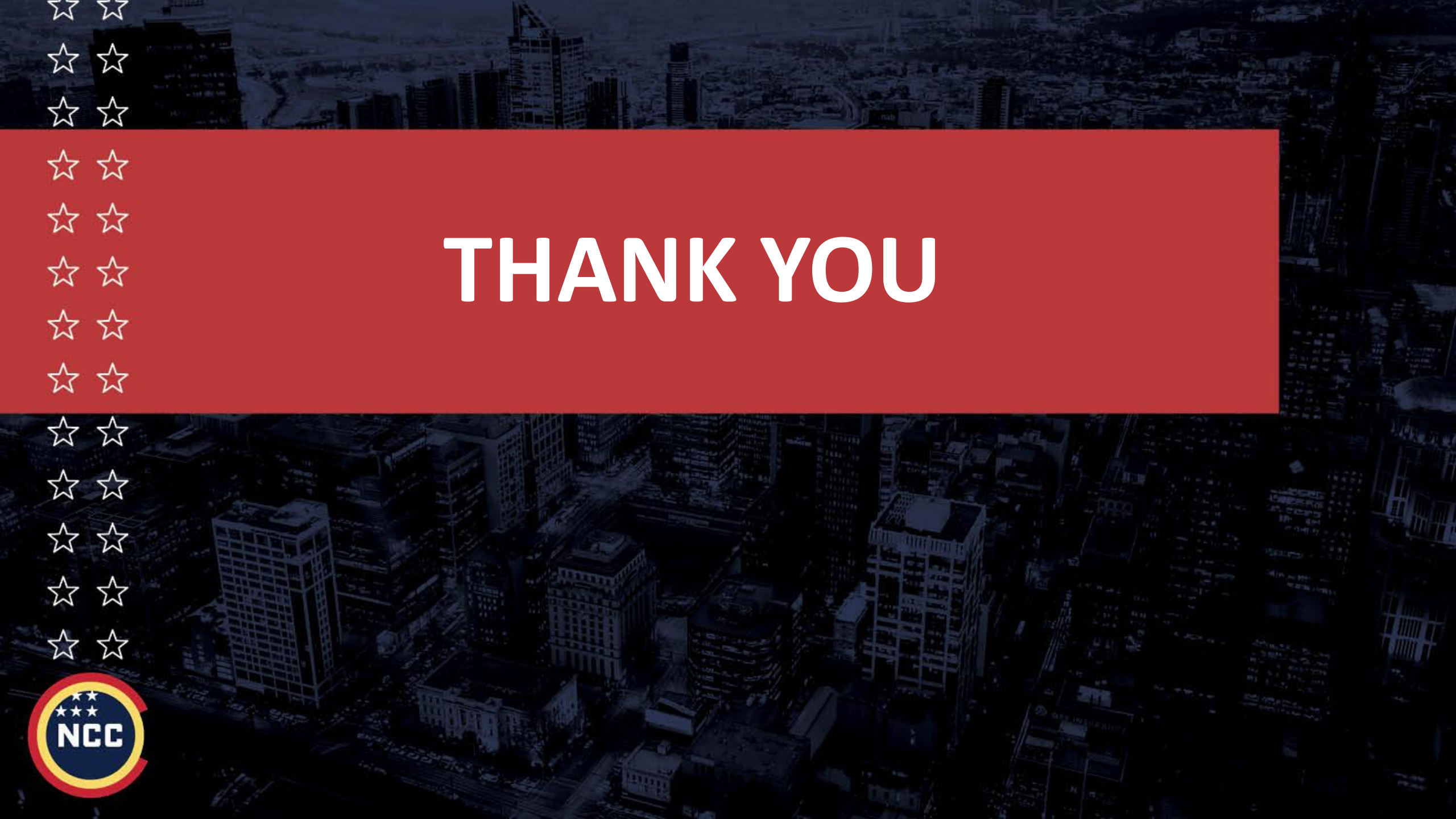
Successful Mobile Voting Pilots
City & County of Denver
Umatilla County, Oregon
Jackson County, Oregon
Utah County, Utah
King County, Washington
UT GOP Convention
West Virginia
Delaware
South Carolina

Mobile Voting Pilots	Conduct additional audits; key outcome is document that translates VVSG to electronic voting & MITRE partnership
Dismantling misinformation	More education for voters and elections administrators on the future of voting (webinars, etc.); international pilots on transparency app that enhances civic engagement thereby enhancing accountability

Challenges

Politics. Politics. Politics

Online/Mobile Voting is controversial	Hacked by MIT. Chased down by reporters. Highly difficult to be non-partisan and pragmatic.
Funding	We had a major foundation that was interested in the work. But no other sources of revenue to maintain the program for growth or investment.


THANK YOU
NCC