

Colorado Secretary of State's Office

Judd Choate, State Election Director

Trevor Timmons, Chief Information Officer

Bipartisan Election Advisory Commission

April 6, 2018



Russia's 2016 Meddling in U.S. Elections

Two Methods:

1. Successful Social Media Campaign
2. Attempted Election Manipulation



Successful Social Media Campaign



Billboard 1.4K Post

Barack Obama, 47, has been going strong in power since he was elected as the 44th president of the United States in 2008. He is a man of many talents, including being a skilled pianist, a skilled speaker, and a skilled leader.

Subscribe to our channel
[http://www.youtube.com/channel/UC12345678901234567890](#)

Following President Obama's speech on the economy, we have a video for you.



THE WORD OF TRUTH

1 Like 0 Comments 0 Shares

Instagram

www.instagram.com/BarackObama

OBAMA ASKS: WHAT DIFFERENCE DOES IT MAKE?



FOLLOW VETERANS - GO IF YOU KNOW THE DIFFERENCE!

[View More](#)

[📷](#) [📷](#) [📷](#) [📷](#)

www.instagram.com/BarackObama will make you understand what it feels like to love the person you love for the rest of your life. [#FollowVeteransGo](#)

Billboard 1.4K Post

Obama is a great leader. He has led us through the toughest times in our history. He has shown us that we can overcome our challenges and build a better future for ourselves and for our children.

Subscribe to our channel
[http://www.youtube.com/channel/UC12345678901234567890](#)

Following President Obama's speech on the economy, we have a video for you.



NOT MY PRESIDENT

November 13, 12 PM, Union Square, NYC

12 [Share to My President](#) [Share to My President](#) [Share to My President](#)

[View More](#)

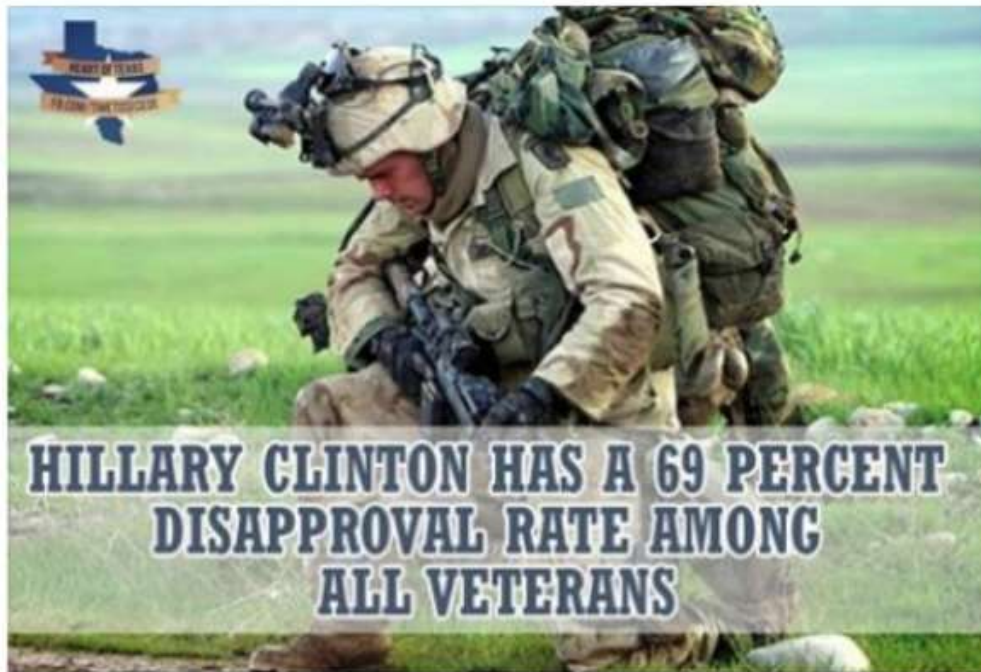


Heart of Texas

Sponsored ·

Like Page

Hillary Clinton has a 69 percent disapproval rate among all veterans. Indeed, there are many reasons for it. First of all, Benghazi: four people died on her watch and she did not send help. Secondly, Hillary refused to apologize to all veterans, when she has made several remarks about veterans "embellishing" the situation at the VA. Finally, Hillary is the only one politician (except Barack Obama) who is despised by the overwhelming majority of American veterans. If Hillary becomes the President of the US, the American army should be withdrawn from Hillary's control according to the amendments to the Constitution.



800 Reactions 84 Comments 308 Shares



Army of Jesus

Sponsored ·

Like Page

Today Americans are able to elect a president with godly moral principles. Hillary is a Satan, and her crimes and lies had proved just how evil she is. And even though Donald Trump isn't a saint by any means, he's at least an honest man and he cares deeply for this country. My vote goes for him!

**SATAN: IF I WIN CLINTON WINS!
JESUS: NOT IF I CAN HELP IT!**



PRESS 'LIKE' TO HELP JESUS WIN!

97 Reactions 15 Comments 29 Shares

Like

Comment

Share

CHEA

Indictments



Indictment Summary

1. **13 people and two businesses** were indicted for various violations of federal law that furthered a conspiracy to illegally influence the 2016 election.
2. The indictment states that the Russian conspiracy **dates back to at least 2014.**
3. The Russian plot **was substantial and is ongoing.**
4. US **citizens were not co-conspirators.** Instead, Americans were “unwitting members, volunteers and supporters of the Trump campaign.”
5. The Internet Research Agency **created millions of impostor social media accounts** largely to **support Donald Trump and oppose Hillary Clinton.**
6. Charges include **violations of campaign finance laws** forbidding foreign nationals from making expenditures in US elections.
7. Russians **traveled to U.S. cities (including Denver)** in which Russian agents “posed as US persons and and contacted US social and political activists.”
8. Russians **posted on social media** and adopted election-related hashtags including “#TrumpTrain” “#Trump2016” “MAGA” and “Hillary4Prison.”

Attempted Election Manipulation

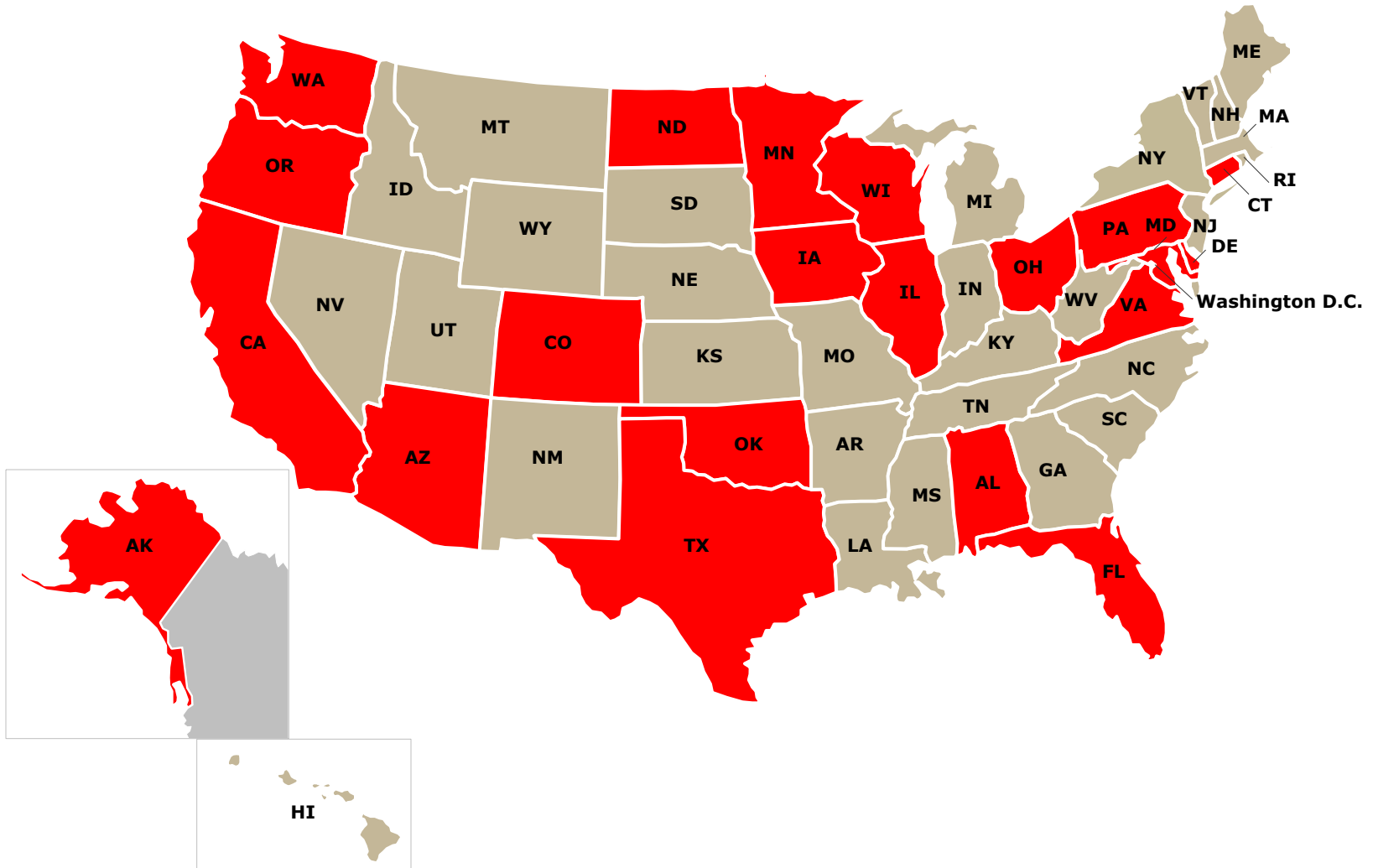


What is Known about Russian Election Attacks?

1. Attacks on 21 states
2. Two worrisome states
3. One intrusion – download of 77,000 voter files
4. No evidence of:
 - File alterations, deletions, or additions
 - Voting system targets
 - ENR manipulation



21 States Targeted by the Russians





Cisco 2018
Annual Cybersecurity Report

POLITICS > ELECTIONS

CONGRESS WHITE HOUSE JUSTICE DEPARTMENT NATIONAL SECURITY

EXCLUSIVE

POLITICS

FEB 28 2018, 12:11 PM ET

U.S. intel: Russia compromised seven states prior to 2016 election

by CYNTHIA MCFADDEN, WILLIAM M. ARKIN, KEVIN MONAHAN and KEN DILANIAN

SHARE

f Share

🐦 Tweet

✉ Email

🖨 Print

The U.S. intelligence community developed substantial evidence that state websites or voter registration systems in seven states were compromised by Russian-backed covert operatives prior to the 2016 election — but never told the states involved, according to multiple U.S. officials.

Top-secret intelligence requested by President Barack Obama in his last weeks in office identified seven states where analysts — synthesizing months of work — had reason to believe [Russian operatives](#) had compromised state websites or databases.

Three senior intelligence officials told NBC News that the intelligence community believed the states as of January 2017 were Alaska, Arizona, California, Florida,



Critical Infrastructure Designation



- Fact Sheets Archive
- Press Release Archive
- Speeches Archive

Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector



Release Date: January 6, 2017

For Immediate Release
 Office of the Press Secretary
 Contact: 202-282-8010

I have determined that election infrastructure in this country should be designated as a subsector of the existing Government Facilities critical infrastructure sector. Given the vital role elections play in this country, it is clear that certain systems and assets of election infrastructure meet the definition of critical infrastructure, in fact and in law.

I have reached this determination so that election infrastructure will, on a more formal and enduring basis, be a priority for cybersecurity assistance and protections that the Department of Homeland Security provides to a range of private and public sector entities. By "election infrastructure," we mean storage facilities, polling places, and centralized vote tabulations locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments.

Prior to reaching this determination, my staff and I consulted many state and local election officials; I am aware that many of them are opposed to this designation. It is important to stress what this designation does and does not mean. This designation does not mean a federal takeover, regulation, oversight or intrusion concerning elections in this country. This designation does nothing to change the role state and local governments have in administering and running elections.

The designation of election infrastructure as critical infrastructure subsector does mean that election infrastructure becomes a priority within the National Infrastructure Protection Plan. It also enables this Department to prioritize our cybersecurity assistance to state and local election officials, but only for those who request it. Further, the designation makes clear both domestically and internationally that election infrastructure enjoys all the benefits and protections of critical infrastructure that the U.S. government has to offer. Finally, a designation makes it easier for the federal government to have full and frank discussions with key stakeholders regarding sensitive vulnerability information.

Particularly in these times, this designation is simply the right and obvious thing to do.

Critical Infrastructure Designation

What is Critical Infrastructure?

How does it work?

What is the state/county/NASS/NASED/EAC role?

What is DHS's role?

Several conference calls led to the following steps:

- a. Create Government Coordinating Council (GCC)
- b. Adopt charter
- c. Create Sector Coordinating Council (SCC)
- d. Adopt a Sector Specific Plan
- e. Adopt a communication protocol




GCC Progress

1. Critical Infrastructure Plan is in progress – awaiting GCC approval
2. Sector Coordinating Council has been created
 - ExCom - Kathy Rogers, Kay Stimson, Ericka Haas, Brian Finney, and Ben Martin
3. Creating a Communication Plan – So every elections jurisdiction gets all the information it needs...but...
 - Not be inundated with info
 - Speak in a common language
 - Provide correct information for size and nature of jurisdiction
 - Information should go both ways
4. Evaluate MS-ISAC and get “Alberts” installed

(Sorta) New Services





Summary of Services: Cybersecurity Assessments

Needs	DHS Services	Summary
Identifying and Limiting Vulnerabilities	 Cyber Hygiene Scanning	Automated, weekly recurring scans of internet facing systems that provide the perspective of the vulnerabilities and configuration errors that a potential adversary could see
	 Risk and Vulnerability Assessment (RVA)	<ul style="list-style-type: none"> • Penetration testing • Social engineering • Wireless access discovery • Database scanning • Operating system scanning
	 Phishing Campaign Assessment	<ul style="list-style-type: none"> • Measures susceptibility to email attack • Delivers simulated phishing emails • Quantifies click rate metrics over a 10 week period
Cyber Risk and IT Security Program Assessment	Cyber Resilience Review (CRR)	One day, onsite engagement, conducted on an enterprise-wide basis to provide insight on areas of strength and weakness, guidance on increasing organizational cybersecurity posture, preparedness, and ongoing investment strategies.
	External Dependencies Management Assessment	To assess the activities and practices utilized by an organization to manage risk arising from external dependencies that constitute the information and communication technology service supply chain.
	Cyber Infrastructure Survey (CIS)	Assesses an organization's implementation and compliance with over 80 cybersecurity controls.



Summary of Services: Continuous Monitoring

Needs	MS-ISAC Services	Summary
Network Protection	 Network Monitoring (Albert) *	Albert service consists of an IDS sensor placed on an organization's network—typically inside the perimeter firewall monitoring an organization's Internet connection—that collects network data and sends it to the ISAC for analysis. Based on the ISAC's vast repository of indicators of compromise, analysts are able to identify malicious activity and alert the effected organization.
Vulnerability Monitoring & Notification	 Vulnerability Management Program (VMP) *	The ISAC uses member-provided IP addresses and domains to identify an organization's vulnerable/out-of-date systems. VMP notifies members on a monthly basis about any outdated software that could pose a threat to assets.
Breach Notification	Victim Notification (in partnership with Public and Private partners)	The ISAC receives notices from trusted partners, both public and private, where the partners share information regarding the potential compromise of an SLTT system. This information is analyzed and passed along to the affected SLTT organization.

What have we done here in Colorado?

1. Multi-jurisdictional Election Day Operations Center in 2016 & 17
 - Governor's Office of Information Technology & Office of Information Security
 - U.S. Department of Homeland Security
 - Department of Public Safety
 - MS-ISAC (now the EI-ISAC)
 - Federal Bureau of Investigation
 - Colorado National Guard
 - City & County of Denver
 - Jefferson County
 - Others

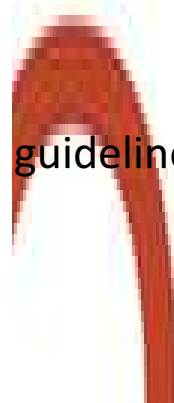


What Have We Done In Colorado?

1. Upgraded perimeter firewalls
2. Upgraded endpoint protection systems for CDOS & Counties
3. Added threat intelligence sharing feeds
4. CTIS (Colorado Threat Intelligence Sharing) network
 - Jefferson County, City of Aurora, City of Arvada, City & County of Denver, State of Colorado, U.S. Dept. of Homeland Security, C.I.A.C., CDOS, ...
5. Penetration testing
6. DHS services
 - Cyber Hygiene, Risk & Vulnerability Assessment, Phishing Campaign Assessment, Onsite Cyber Security Evaluation Assessment
7. MS-ISAC services
 - Albert network monitoring, Vulnerability Management Program, Exercises and Training, ISAC membership

What Have We Done In Colorado?

1. DDoS Protection
2. Risk-limiting Audits
3. Cyber Storm VI – elections scenarios
4. Obtaining security clearances
5. And (old news)
 - 2-factor authentication
 - Annual cybersecurity awareness training
 - Mock elections
 - On-site audits
 - Endpoint malware protection
 - Strong acceptable use policies
 - Incident Response policies and guidelines



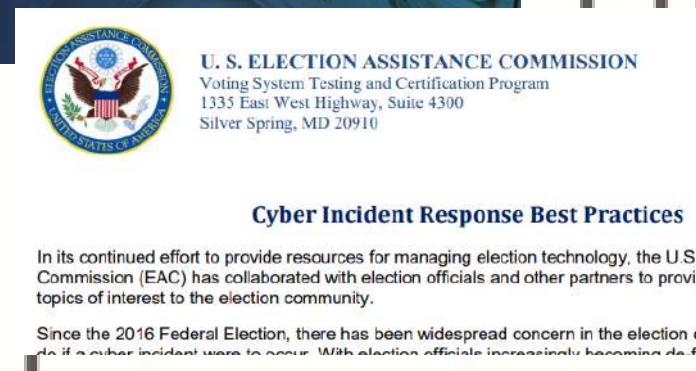
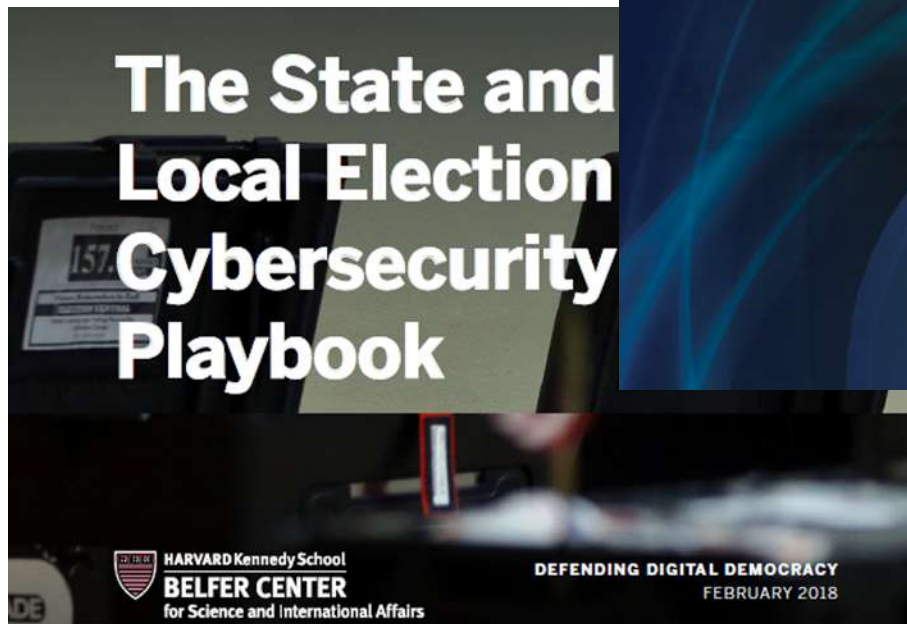
CIVIC HEAD

What Have We Done In Colorado?

Standards & Best Practices Development



Version 1.0
February 2018



What Is on the Horizon in Colorado?

1. Upgraded internal firewalls (moving toward “no-trust” networks)
2. Privileged Access Management
3. Endpoint detection
4. Improved DDoS protection
5. Database Access Monitoring tools
6. Tabletop Exercises
7. Improving Risk-limiting Audits
8. Improving quality and security of data exchanges
9. Improved USB controls

