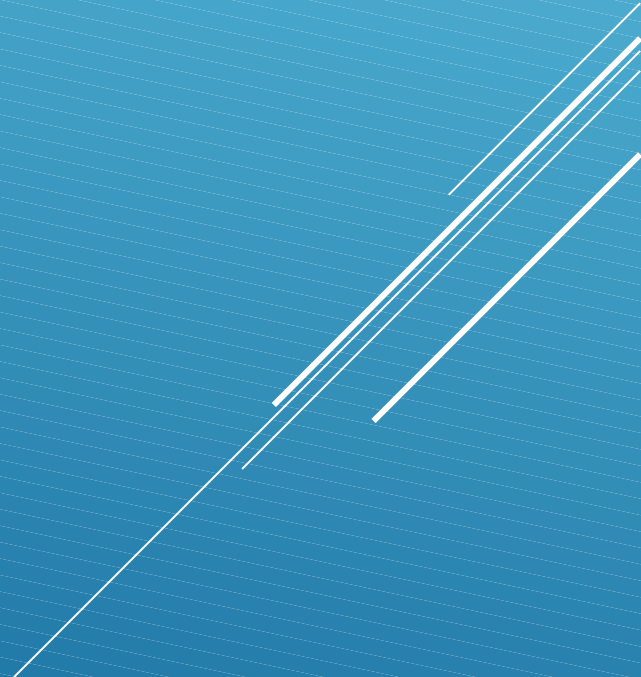


“South Carolina Freedom Fighters”

Is a 50 State “Tore Says”
Grassroots Affiliate



Tore Maras – A former Intelligence Contractor turned whistleblower/podcaster, has helped organize and educate “the PEOPLE” in All 50 states, to use the power of the “pen” and our State and U.S. Constitution to demand change!

Decorative white lines consisting of three parallel diagonal strokes in the bottom right corner of the slide.

Civil lawsuit

Filed on August 29, 2022 in
United States District Court in
Columbia,
South Carolina

UNITED STATES DISTRICT COURT
SOUTH CAROLINA

[REDACTED]

Civil Action No. 3:22-cv-2872-SAL-PJG

COMPLAINT

Plaintiff,

V.

GOVERNOR HENRY MCMASTER,
HOWARD KNAPP, WANDA HEMPHILL,
CHRIS WHITMIRE, JOHN WELLS, JOANNE
DAY, LINDA MCCALL, CLIFFORD EDLER
SCOTT MOSELY, MARCI ANDINO
Defendants.

TABLE OF CONTENTS

1. PARTIES TO THE PROCEEDINGS
2. JURISDICTIONS AND VENUE
3. DISCLOSURE
4. PRELIMINARY STATEMENT
5. CONSTITUTIONAL QUESTIONS
6. INTRODUCTION
7. EXCESSIVE FEDERAL INVOLVEMENT IN SOUTH CAROLINA ELECTIONS
8. UNACCREDITED VOTING SYSTEMS TEST LABORATORIES
9. MISUSE OF STATE AND FEDERAL FUNDS
10. FOREIGN INTERFERENCE IN SOUTH CAROLINA ELECTIONS
11. ELECTION MACHINE VULNERABILITY AND CONNECTION TO THE INTERNET
12. PRIVACY VIOLATIONS
13. PRAYER FOR RELIEF

I. PARTIES TO THE PROCEEDINGS

Plaintiff(s), pro se, hereby file and serve this Complaint against Defendants, Governor Henry McMaster, Howard Knapp, Wanda Hemphill, Chris Whitmire, John Wells, JoAnne Day, Clifford J. Edler, Linda McCall, Scott Moseley, Marci Andino. In support of the claims set forth herein, Plaintiff(s) allege, and cover facts as follows: **Defendant(s) knowingly and willfully:**

- a. **neglected to uphold the Constitution**
- b. **had foreknowledge of the events unfolding**
- c. **partnered with agencies that federalized our state elections**
- d. **chose to perpetrate unconstitutional measures by violating election laws, privacy laws, sovereignty of state laws, as well as misuse of state funds**
- e. **all of the above constitutes breach of contract through the violations of their Oaths of Office (SC CONST. art. VI § 5, 5 U.S.C. §3331)**

1. As a result of the above-mentioned actions of the Defendants, the quality, security, accuracy, and effectiveness of the Plaintiff(s)' expression of their will, intent, and consent of their vote(s) were impaired and Plaintiff(s) are entitled to remedy under the U.S. Constitution Guarantee Clause. (U.S. CONST. art IV, § 4)
2. Plaintiff(s) have a vested interest in protecting the quality, accuracy, and effectiveness of their individual votes. Plaintiff(s) demand their votes are cast in a sovereign state without the external interference of Federal Agencies.
3. Plaintiff(s) seek an Order that the Defendant(s) must adhere to the constitutionally protected process of collecting and counting votes that ensures integrity and transparency. This Order is to require hand-marked paper ballots that can be cast with anonymity, following all South Carolina state election laws. Plaintiff(s) demand that the partnership with Federal Agencies cease and desist, "For Federal Government cannot commandeer a state into enacting a certain law". *New York v. United States, 505 U.S. 144 (1992)*

Constitutional Provisions

U.S. CONST. art. I, § 1.

U.S. CONST. art IV (4), § 4.

US CONST. amend X (10)

US CONST. amend XIII (13), § 1.

US CONST. amend XIV (14)

SC. Const. art. VI (6), § 5.

S.C. Const. art. VI (6), § 3.

S.C. Const. art. II, § 1.

Acts

HIPAA - (Health Insurance
Portability and Accountability)

HAVA of 2002 § 231(b) – (Help
America Vote Act)

Privacy act of 1975

Judiciary Act of 1789

Civil Rights Act of 1964

21 United States Codes

U.S.C. app. 2 §1-15.

U.S.C. §551

5 USC_§ 3331

18 U.S.C. §§ 593, 595

18 U.S.C. § 245

28 U.S.C. §§ 1331, 1343

28 U.S.C. §§ 2201, 2202

28 U.S.C. § 1343

28 U.S.C. §1391

42 **U.S.C.** § Code § 1983

42 **U.S.C** § 1985

42 **U.S.C** § 1986

42 U.S.C. § 1983

52 U.S.C § 10101

52 U.S.C. § 10307

52 U.S.C. §551

52 U.S.C. § 20511 (42:15483)

52 U.S.C. §20901

52 U.S.C. §20962

52 U.S.C Code § 20971

377 U.S.C 533 (1964)

South Carolina Codes

SC Code 7-13-1620 (2019)

SC Code 7-3-20

SC CODE 16-9-10

SC Code § 16-13-230

XII. PRAYER FOR RELIEF

117. Plaintiff(s) ask the court, due to the Defendant(s) gross negligence in protecting the vote of South Carolina Citizens, as well as their failure to uphold their oaths made to the South Carolina and United States Constitutions (SC Code 8-3-10), that the following remedies be made:

118. Plaintiff(s) ask the court for immediate temporary and permanent injunctions of the election machines.

119. That South Carolina shall not take active part in the CISA/DHS/CIS partnerships in election processes, as they are in violation of (18 U.S.C. §§ 593, 595).


120. That South Carolina will only use paper ballots, will only allow same-day voting, and will no longer use election machines.

121. That the SC SEC and its leadership, as well as County Election Boards under SEC direction, be disbanded, and their roles be returned to the “elected” position of Secretary of State.

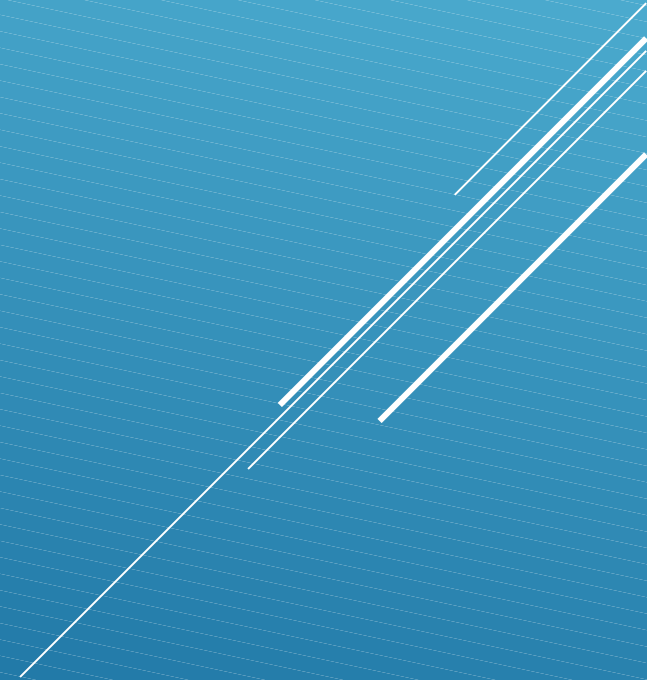
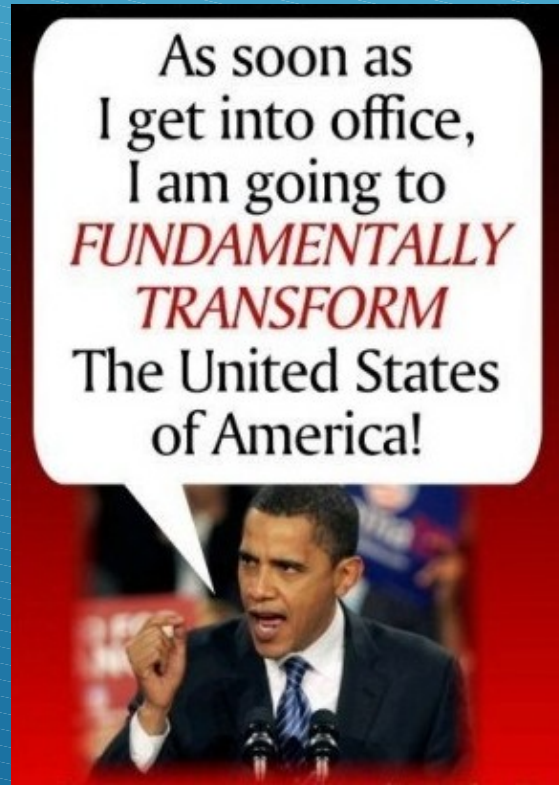
122. That the Secretary of State of SC, remain an elected position, as it holds more transparency and accountability than any other position.

123. That the South Carolina General Election of 2020 be decertified, including all South Carolina midterm elections preceding the General Election of 2020, due to federal overreach, foreign involvement, hackability of election machines, and gross oversight on the part of the Defendant(s).

WHY have
South Carolina
Elections been
FEDERALIZED?



Obama's Campaign Promise



Valerie Jarrett, Senior Advisor to Obama said, “No election to worry about after this is over...” referring to Hillary Clinton if she had won the election in 2016.



Valerie Jarrett - “After We Win This Election, It’s Our Turn. Payback Time.”

“After we win this election, it’s our turn. Payback time. Everyone not with us is against us and they better be ready because we don’t forget. The ones who helped us will be rewarded, the ones who opposed us will get what they deserve. There is going to be hell to pay.

Congress won’t be a problem for us this time. No election to worry about after this is over and we have two judges ready to go.”

Valerie Jarrett, born in Iran, Senior Advisor to Obama. Quoted by a White House Insider. See link for full story. She calls all the shots in the White House except for the drones, Obama loves his drones.

DHS Secretary

Jeh Johnson

Designates Elections

CRITICAL

INFRASTRUCTURE

January 6, 2017



- Topics ▾
- News ▾
- In Focus ▾
- How Do I? ▾
- Get Involved ▾
- About DHS ▾

[Home](#) » [About Us](#) » [Site Links](#) » [Archived](#) » [News Archive](#) »

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

- News
 - All DHS News
 - Apps
 - Blog
 - Comunicados de Prensa
 - Data
 - Events
 - Fact Sheets
 - Featured News
 - Homeland Security LIVE
 - Media Contacts
 - Media Library
 - National Terrorism Advisory System

Archived Content

In an effort to keep DHS.gov current, the archive contains outdated information that may not reflect current policy or programs.

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

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.

At present, there are sixteen critical infrastructure sectors, including twenty subsectors that are eligible to receive prioritized cybersecurity assistance from the Department of Homeland Security. The existing critical infrastructure sectors are:

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Material, and Waste
- Transportation Systems
- Water and Wastewater Systems

Entities within these sectors all benefit from this designation and work with us closely on cybersecurity. For example, we have developed joint cybersecurity exercises with numerous companies within the communications, information technology, financial services and energy sectors to improve our incident response capabilities. We have also streamlined access to unclassified and classified information to critical infrastructure owners and operators in partnership with information sharing and analysis organizations. Moreover, many critical infrastructure sectors include assets and systems owned and operated by state and local governments, such as dams, healthcare and public health, and water and wastewater systems.

Now more than ever, it is important that we offer our assistance to state and local election officials in the cybersecurity of their systems. Election infrastructure is vital to our national interests, and cyber attacks on this country are becoming more sophisticated, and bad cyber actors – ranging from nation states, cyber criminals and hackers – are becoming more sophisticated and dangerous.

Further, our increasingly digital and connected world has reshaped our lives. It has streamlined everyday tasks and changed the way we communicate. But, just as the continually evolving digital age has improved our quality of life, it has also introduced an array of cyber threats and implications.

Cybersecurity continues to be a top priority for DHS, as it is for state and local election officials across the country. This designation enables the states, should they request it, to leverage the full scope of cybersecurity services we can make available to them.



Updated September 18, 2019

The Designation of Election Systems as Critical Infrastructure

Prior to the 2016 federal election, a series of cyberattacks occurred on information systems of state and local election jurisdictions. Subsequently, in January 2017 the Department of Homeland Security (DHS) designated the election infrastructure used in federal elections as a component of U.S. critical infrastructure. The designation sparked some initial concerns by state and local election officials about federal encroachment of their prerogatives, but progress has been made in overcoming those concerns and providing assistance to election jurisdictions.

What Led to the Designation?

In August 2016, the Federal Bureau of Investigation (FBI) announced that some state election jurisdictions had been the victims of cyberattacks aimed at exfiltrating data from information systems in those jurisdictions. The attacks appeared to be of Russian-government origin. That same month, DHS contacted state election officials to offer cybersecurity assistance for their election infrastructure. Most states accepted the offer. Although the cyberattacks did not appear to affect the integrity of the election infrastructure, some observers began calling for it to be designated as critical infrastructure (CI). On January 6, 2017, the Secretary of Homeland Security announced that designation.

What Is Critical Infrastructure?

Under federal law, CI refers to systems and assets for which “incapacity or destruction ... would have a debilitating impact on security, national economic security, national public health or safety, or any combination” of them (42 U.S.C. §5195c(e)). Most CI entities are not government-owned or -operated. Presidential Policy Directive 21(PPD 21) identified 16 CI sectors, with some including subsectors. Sectors vary in scope and in degree of regulation. For example, the financial services sector is highly regulated, whereas the information technology sector is not. Election infrastructure has been designated as a subsector of government facilities. That sector includes two previously established subsectors: education facilities, and national monuments and icons.

The Homeland Security Act of 2002 (P.L. 107-296) gave DHS responsibility for several functions aimed at promoting the security and resilience of CI with respect to both physical and cyber-based hazards, either human or natural in origin. Among those functions are providing assessments, guidance, and coordination of federal efforts.

Each CI sector has been assigned one or two federal sector-specific agencies (SSAs), which are responsible for coordinating public/private collaborative efforts to protect the sector, including incident management and technical assistance. DHS has regulatory authority over two sectors: chemical and transportation systems. It serves as SSA for

several, including the elections infrastructure subsector (EIS).

The components of the EIS as described by DHS include physical locations (storage facilities, polling places, and locations where votes are tabulated) and technology infrastructure (voter registration databases, voting systems, and other technology used to manage elections and to report and validate results). It does not include infrastructure related to political campaigns. However, DHS does provide cyber vulnerability assessments and risk mitigation guidance to political campaigns upon request as resources permit.

Does the Designation Permit Federal Regulation of Election Infrastructure?

DHS does not have regulatory authority over EIS. Five other agencies have significant roles with respect to federal elections, but none has claimed regulatory authority over the EIS:

- The Election Assistance Commission (EAC), created by the Help America Vote Act (HAVA, P.L. 107-252), provides a broad range of assistance to states, including development of voluntary technical standards for voting systems, voluntary guidance on implementing HAVA requirements, and research on issues in election administration. It also has statutory authority for administering formula payments to states to assist them in meeting HAVA requirements and improving election administration, including \$380 million appropriated in FY2018 in response to security concerns.
- The National Institute of Standards and Technology (NIST) assists the EAC on technical matters, including development of the voting system standards, certification of voting systems, and research.
- The Department of Justice (DOJ) has some enforcement responsibilities with respect to requirements in HAVA and other relevant statutes.
- The Department of Defense (DOD) assists military and overseas voters.
- The Federal Election Commission (FEC) is responsible for enforcement of campaign finance law but is not involved in election administration by state and local jurisdictions.

HAVA expressly prohibits the EAC from issuing regulations of relevance to the CI designation, and it leaves the methods of implementation of the act’s requirements to the states. However, it does permit DOJ to bring civil actions if necessary to implement HAVA’s requirements.

What Does the Designation Mean?

While both DHS and the EAC provided assistance to states in addressing the security concerns that arose in the run-up to the November 2016 election, the CI designation had several notable consequences:

- It raised the priority for DHS to provide security assistance to election jurisdictions that request it and for other executive branch actions, such as economic sanctions that the Department of the Treasury can impose against foreign actors who attack elements of U.S. CI, including tampering with elections.
- It brings the subsector under a 2015 United Nations nonbinding consensus report (A/70/174) stating that nations should not conduct or support cyber-activity that intentionally damages or impairs the operation of CI in providing services to the public. It also states that nations should take steps to protect their own CI from cyberattacks and to assist other nations in protecting their CI and responding to cyberattacks on it. The report was the work of a group of governmental experts from 20 nations, including Russia and the United States.
- It provided DHS the authority to establish formal coordination mechanisms for CI sectors and subsectors and to use existing entities to support the security of the subsector. Those mechanisms are used to enhance information sharing within the subsector and to facilitate collaboration within and across subsectors and sectors. For example, both the FBI and the Office of the Director of National Intelligence (ODNI) have participated in briefing election officials on threats to the EIS.

Among the coordination mechanisms for the subsector are the following:

- *Government Coordinating Council.* The GCC consists of representatives of DHS and the EAC, as well as secretaries of state, lieutenant governors, and elections officials who altogether represent 24 state and local governments. It also includes non-voting members from other relevant federal agencies. The GCC facilitates coordination across government entities both within EIS and in other sectors. Activities include communications, planning, issue resolution, and implementation of the security missions of the entities.
- *Sector Coordinating Council.* The SCC consists of representatives of nongovernment entities, most of which are providers of voting systems and other election-related products and services. SCCs are self-organized and self-governed. They are intended to represent private-sector interests and to facilitate collaboration activities, including information sharing, among the private-sector entities in the CI sector and with government entities.
- *Sector-Specific Plan.* Public- and private-sector partners have created SSPs for each of the 16 CI sectors. The plans are components of an overall National Infrastructure Protection Plan and provide a means for the sectors to establish goals and priorities for

addressing risks. They are generally updated on a four-year cycle. DHS is currently drafting an SSP for the EIS.

The CI designation for election infrastructure is also intended to facilitate use of existing resources, such as

- *Cybersecurity and Infrastructure Security Agency (CISA).* CISA, an agency within DHS, serves as the SSA for the EIS.
- *Critical Infrastructure Partnership Advisory Council.* CIPAC provides election officials access to a broad range of relevant expertise and participation in sensitive planning conversations.
- *Multi-State Information Sharing and Analysis Center.* The MS-ISAC is one of the centers created to facilitate the sharing of security information for different CI sectors. It works with CISA, all states, and many local governments to assist them in cybersecurity. The MS-ISAC supports the EIS-ISAC, created in 2018 to facilitate information-sharing activities for and among more than 500 members consisting of state and local election offices, as well as the National Association of Secretaries of State (NASS) and the National Association of State Election Directors (NASSED).

Pursuant to the EIS designation, DHS and the EAC assisted both jurisdictions and vendors in preparations on election security for the 2018 federal election. For more information, see <https://www.dhs.gov/topic/election-security>, <https://www.eac.gov/election-officials/elections-critical-infrastructure/>, <https://www.cisecurity.org/ei-isac/>.

Why Was the Designation Initially Controversial?

Misgivings about DHS involvement were raised when it first offered assistance to election jurisdictions in August 2016. Some observers feared that DHS would begin to exert control over the administration of elections or to engage in unrequested security activities.

Controversy over the federal role in election administration is not new. Concerns about federal regulation of the election process were prominent during the legislative debate over HAVA and led to the inclusion of the regulatory restrictions in the law. Furthermore, bills in prior Congresses that would have provided DHS broad regulatory authority over cybersecurity have all failed.

The CI designation does not contravene the HAVA restrictions on EAC regulations or create DHS regulatory authority for the EIS. DHS provides assistance to election jurisdictions only on a voluntary basis. In the 115th Congress, a few bills would have established mandatory standards or federal rule-making authority, but none received committee or floor action. Bills with relevant provisions have also been introduced in the 116th Congress.

Brian E. Humphreys, bhumphreys@crs.loc.gov, 7-0975

IF10677

CISA & Election Infrastructure

As the nation's **risk advisor**, the Cybersecurity and Infrastructure Security Agency's (CISA) mission is to ensure the security and resiliency of our critical infrastructure.

The 2017 designation of election infrastructure as **critical infrastructure** provides a basis for the Department of Homeland Security (DHS) and other federal agencies to:

- Recognize the importance of these systems;
- Prioritize services and support to enhancing security for election infrastructure;
- Provide the elections community with the opportunity to work with each other, the Federal Government, and through the Coordinating Councils; and
- Hold anyone who attacks these systems responsible for violating international norms.



Election Security Mission

To ensure the election community and American public have the necessary information and tools to adequately assess risks to the election process and protect, detect, and recover from those risks



Jen Easterly,
CISA Director

CISA & Election Infrastructure



Federal Partners



Partnership Model

- All **50 states** and over **3,000 local jurisdictions** and **private sector organizations** are members of the EI-ISAC
- 219 stakeholders** currently hold **security clearances** through the election infrastructure clearance program
- Between October 2020 and September 2021, CISA provided over **500 Vulnerability Scanning services** and **Cyber Assessments**
- Albert Sensors are deployed in all **50 states**
- Hosted **four national tabletop exercises** for EI stakeholders and more than **50 exercises for state and local election officials** and other stakeholders
- Between October 2020 and September 2021, CISA delivered tailored security products for **1,860 election administrators**



Sector Risk Management Agency for Election Infrastructure



Sector-Based Information Sharing and Analysis Centers



EI-ISAC



Election Infrastructure Information Sharing and Analysis Center

- Voluntary collaborative effort between CISA, the Center for Internet Security (CIS), and the Election Infrastructure Subsector Government Coordinating Council (EIS GCC)
- No cost to election officials
- Suite of elections-focused cyber defense tools, threat intelligence products, and incident response and forensics, training products, and more

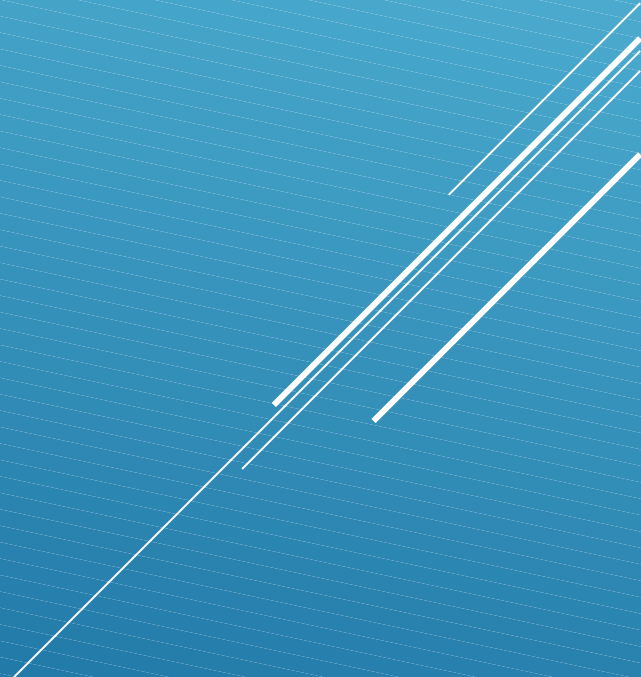
EI-ISAC Services

- Albert Sensors
- Malicious Domain Blocking and Reporting
- Threat Alerts
- & more

Visit <https://learn.cisecurity.org/ei-isac-registration> for more information



GEORGIA'S
2016
ELECTIONS



GEORGIA
SECRETARY OF STATE

BRIAN P. KEMP



INTRODUCTION

CRITICAL INFRASTRUCTURE

SOS NETWORK SECURITY

DHS HACKING ATTEMPTS

NATIONAL REACTION

MOVING FORWARD

LEGISLATIVE UPDATE

CRITICAL INFRASTRUCTURE & DHS HACKING ATTEMPTS

GEORGIA
SECRETARY OF STATE

BRIAN P. KEMP



INTRODUCTION

[CRITICAL INFRASTRUCTURE](#)

SOS NETWORK SECURITY

DHS HACKING ATTEMPTS

NATIONAL REACTION

MOVING FORWARD

CRITICAL INFRASTRUCTURE

Comments by Jeh Johnson to New York Times

U.S. Seeks to Protect Voting System From Cyberattacks

By JULIE HIRSCHFELD DAVIS

AUG. 3, 2016

“We should carefully consider whether our election system, our election process is critical infrastructure, like the financial sector, like the power grid,” Mr. Johnson told reporters in Washington. “There’s a vital national interest in our electoral process.”

GEORGIA
SECRETARY OF STATE



BRIAN P. KEMP

INTRODUCTION

CRITICAL INFRASTRUCTURE

SOS NETWORK SECURITY

DHS HACKING ATTEMPTS

NATIONAL REACTION

MOVING FORWARD

CRITICAL INFRASTRUCTURE

What is Critical Infrastructure?

5. Enabling Statute: 6 U.S.C.S. § 131 *et seq.* “The Homeland Security Act of 2002”
6. Powers:
 - a) Prevents disclosure of information related to “Critical Infrastructure.”
 - b) Allows the Department to audit and compel reports from entities within a Critical Infrastructure Sector on the maintenance, development, and status of Critical Infrastructure Systems.
 - c) Allows the Department to review and publish best practices for systems.
 - d) Allows for grants to be issued to entities within CI Sectors for implementation of best practices.
 - e) Allows the Department to conduct additional system testing in coordination with an entity (or without permission for some entities) including penetration tests, cyber hygiene scans, etc.

GEORGIA
SECRETARY OF STATE



BRIAN P. KEMP

INTRODUCTION

CRITICAL INFRASTRUCTURE

SOS NETWORK SECURITY

DHS HACKING ATTEMPTS

NATIONAL REACTION

MOVING FORWARD

CRITICAL INFRASTRUCTURE

Opposition to Critical Infrastructure

Why Seek to Name Elections Systems Critical Infrastructure?

- Unconfirmed threats against the election.
- Hacks of DNC emails, Podesta emails, and wiki leaks
- *No Threats to Actual Election System.*

GEORGIA
SECRETARY OF STATE

BRIAN P. KEMP



INTRODUCTION

CRITICAL INFRASTRUCTURE

SOS NETWORK SECURITY

DHS HACKING ATTEMPTS

NATIONAL REACTION

MOVING FORWARD

CRITICAL INFRASTRUCTURE

Opposition to Critical Infrastructure

Why Oppose this Designation?

- Broad federal power, the extent of which has been intentionally left vague by Congress.
- Duplicative of the roll the Election Assistance Commission plays in regulating and securing the Election System Environment.
- Lack of Transparency for Voters
- DHS employees are not election experts. There are many technologies unique to elections that they have not developed standard protocols on how to test.
- Lack of uniformity of voting systems across 50 states and over 5000 election jurisdictions. Standardization of processes creates vulnerabilities.

GEORGIA
SECRETARY OF STATE



BRIAN P. KEMP

INTRODUCTION

CRITICAL INFRASTRUCTURE

SOS NETWORK SECURITY

DHS HACKING ATTEMPTS

NATIONAL REACTION

MOVING FORWARD

CRITICAL INFRASTRUCTURE

Opposition to Critical Infrastructure

Who Opposes this Designation?

- US Senator Mitch McConnell (R)
- US Senator Harry Reid (D)
- Speaker Paul Ryan (R)
- Leader Nancy Pelosi (D)
- White House Spokesperson Josh Earnest (D)
- EAC Commission Chair Tom Hicks (D)
- EAC Commissioner Matt Masterson (R)
- EAC Commissioner Christy McCormick (R)
- Sec. of State Denise Merrill (D-CT)
- Sec. of State Jim Condos (D-VT)
- Sec. of State Jon Husted (R-OH)
- Sec. of State Connie Lawson (R-IN)
- Sec. of State Tom Schedler (R-LA)
- Sec. of State Matt Dunlap (D-ME)
- Professor Merle King
- Georgia Secretary of State Brian Kemp



INTRODUCTION

CRITICAL INFRASTRUCTURE

SOS NETWORK SECURITY

DHS HACKING ATTEMPTS

NATIONAL REACTION

MOVING FORWARD

CRITICAL INFRASTRUCTURE

Opposition to Critical Infrastructure

- Because of widespread bipartisan opposition to designating Election Systems “Critical Infrastructure,” DHS Secretary Jeh Johnson decided to reconsider moving forward with the designation.
- Instead, DHS offered states who wished to participate the option of receiving free penetration tests and cyber hygiene scans for their systems prior to election day.
- Georgia refused participation in these tests due to already having protocols in place where our systems are testing in the same way by private sector security providers.
- It was reported that 48 states accepted DHS assistance in scanning. However, this number has not been confirmed and with informal surveys of several states, the number seems to be closer to 30.



INTRODUCTION

CRITICAL INFRASTRUCTURE

SOS NETWORK SECURITY

DHS HACKING ATTEMPTS

NATIONAL REACTION

MOVING FORWARD

DHS HACKING ATTEMPTS

All 2016 Attacks

Day	Date	Time	Relevance to Timing of Scanning Activity
Tuesday	Feb. 2, 2016	13:03 CST	This scan was conducted the day after Georgia's voter registration deadline for the Presidential Preference Primary.
Sunday	Feb. 28, 2016	13:19 CST	This scan was conducted on a Sunday afternoon, two days before Georgia's Presidential Preference Primary dubbed the SEC Primary.
Monday	May 23, 2016	08:42 CDT	This scan was conducted the day before Georgia's General Primary.
Monday	Sep. 12, 2016	11:52 CDT	This scan was conducted just before a conference call between DHS & GEMA to discuss designating elections systems as critical infrastructure, and only three days after a call between elections officials and Secretary Johnson on designating elections systems critical infrastructure.

GEORGIA
SECRETARY OF STATE

BRIAN P. KEMP



INTRODUCTION

CRITICAL INFRASTRUCTURE

SOS NETWORK SECURITY

[DHS HACKING ATTEMPTS](#)

NATIONAL REACTION

MOVING FORWARD

DHS HACKING ATTEMPTS

All 2016 Attacks

Day	Date	Time	Relevance to Timing of Scanning Activity
Wednesday	Sep. 28, 2016	07:54 CDT	This scan was conducted just <i>hours</i> before Secretary Kemp's testimony opposing the designation of elections systems as critical infrastructure.
Monday	Oct. 3, 2016	10:41 CDT	This scan was conducted on the Monday after Kemp's Congressional testimony opposing the designation of elections systems as critical infrastructure.
Thursday	Oct. 6, 2016	10:14 CDT	This scan was conducted the week after Congressional testimony and same day as a meeting with DHS field staff ahead of Election Day.
Monday	Nov. 7, 2016	12:15 CST	This scan was conducted the day before Election Day.
Tuesday	Nov. 8, 2016	07:35 CST	This scan was conducted on Election Day.
Tuesday	Nov. 15, 2016	07:43 CST	This scan was conducted exactly one week after the General Election, prior to election results being certified.

GEORGIA
SECRETARY OF STATE



BRIAN P. KEMP

INTRODUCTION

CRITICAL INFRASTRUCTURE

SOS NETWORK SECURITY

DHS HACKING ATTEMPTS

NATIONAL REACTION

MOVING FORWARD

NATIONAL REACTION

Potential DHS Attacks

- States began scanning systems to see if IP addresses associated with DHS have accessed or attempted to access their system.
- So far West Virginia, Kentucky, and Maine have reported unauthorized scanning activity against their systems.
- The Election Assistance Commission has investigated intrusion into their network from a DHS IP address.
- Election leaders from around the country have called for an investigation into DHS.

GEORGIA
SECRETARY OF STATE



BRIAN P. KEMP

INTRODUCTION

CRITICAL INFRASTRUCTURE

SOS NETWORK SECURITY

DHS HACKING ATTEMPTS

NATIONAL REACTION

MOVING FORWARD

NATIONAL REACTION

Critical Infrastructure

- January 6 – Despite bipartisan opposition to the designation, and with only two weeks remaining in his administration, Jeh Johnson designated Elections Systems a Critical Infrastructure Sector. He gave the following reasons for his decision:
 - DNC Hack
 - Hack of Podesta emails
 - This will help stop Russia from targeting elections
 - Allows documents to be exempt from open records laws.
 - Allows states to receive better service from DHS
- Secretaries of State, Election Officials, EAC Commissioners, and academics have called on President Trump to rescind the designation.
- Secretary Kemp has stated that the timeline of these events and the designation of election systems as Critical Infrastructure “smacks of partisan politics.”

“Free Thought Project” Article

By JACK BURNS

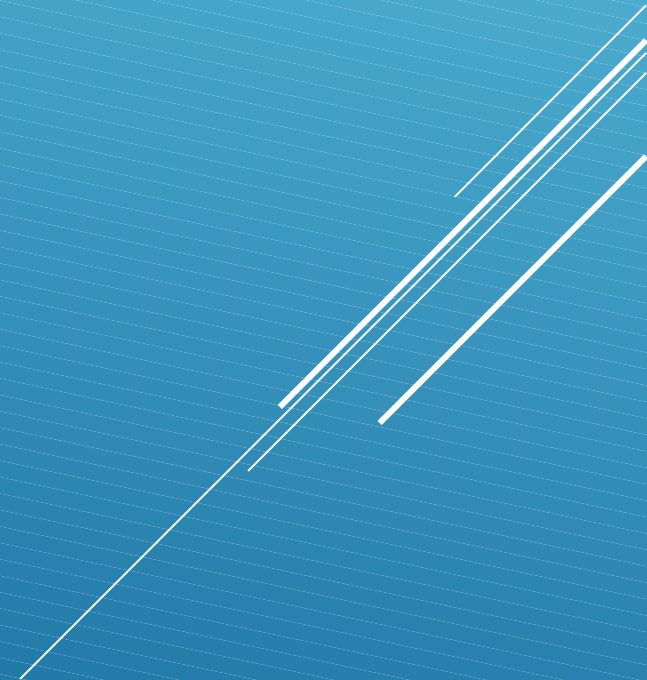
DEC 15, 2016

All 10 Election Hacks Inside the US in Georgia Have Been Tracked to DHS -- NOT RUSSIA

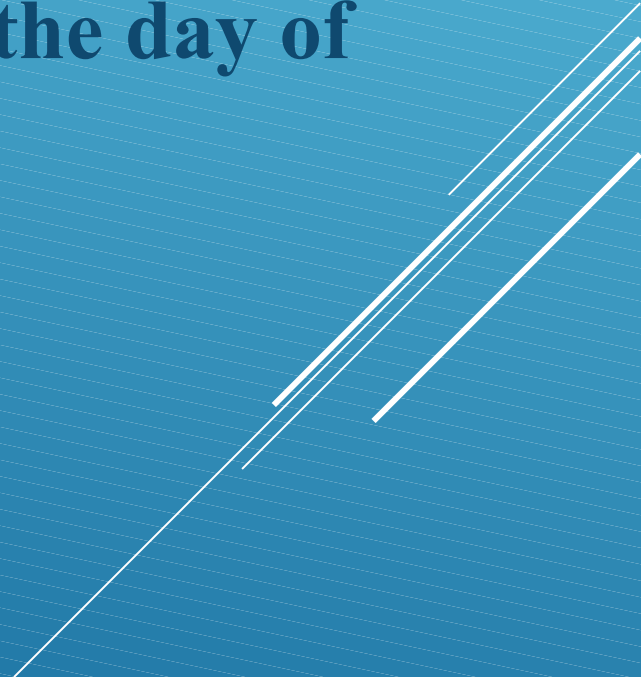
- Corporate Media is dead silent on the fact that DHS was just caught hacking the Georgia state election servers, not once, not twice, but ten times!

Late breaking developments have emerged in the case of Georgia vs. The Department of Homeland Security. As Claire Bernish of “The Free Thought Project” reported on December 9th, Georgia’s secretary of State Brian Kemp penned a letter to DHS Secretary Jeh Johnson, asking the director if he was aware that DHS had attempted to hack into the server hosting the state’s voter registration database, and if so, why was DHS doing so. Today it was revealed that not only did DHS attempt to penetrate GA’s firewall once, **but it had in fact attempted to do so a total of 10 times.**

With the official narrative coming from the Obama administration, indeed, the president himself, that the Russians stand guilty of hacking the presidential election of 2016, many are left scratching their heads in disbelief that the only government found to be hacking a state election systems, thus far, is DHS.



Atlanta's WSB-TV spoke with Kemp who said, "We need to know! We're being told something that they think haven't figured out yet, nobody's really shown us how this happened." The attacks came in February (2nd, 28th), May (23rd), and November (7th, 8th), totaling 10 in all, with the two latest attacks **coming on the day before and the day of the presidential election.**

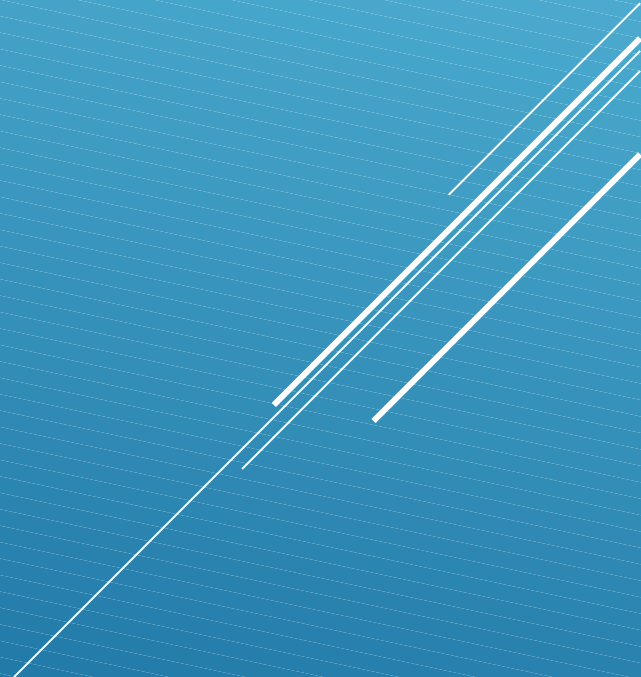


South Carolina Elections DESIGNATED CRITICAL INFRASTRUCTURE!



The background of the slide is a close-up, slightly blurred image of the American flag. The blue field with a white star is prominent in the upper right, while the red and white stripes are visible in the lower left and center. The overall color palette is dominated by blue, red, and white.

2018 Year in Review



Overview

We can achieve more collectively than we can individually.

This guiding principle of the Elections Infrastructure Information Sharing & Analysis Center™ (EI-ISAC®) was evident throughout its inaugural year.

During 2018, the EI-ISAC evolved from an idea to a formalized collective of dedicated election officials, their staff members, associations, technology vendors, federal partners, and cybersecurity experts working tirelessly to help secure the U.S. elections infrastructure. From sharing information about the threat landscape to creating educational opportunities and implementing technical cybersecurity controls, the EI-ISAC's members, staff, and partners made substantial strides toward ensuring the security and integrity of our elections.

The EI-ISAC is a voluntary and collaborative effort based on a strong partnership between CIS* (Center for Internet Security®), the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), and the Election Infrastructure Subsector Government Coordinating Council (EIS-GCC).



This initiative dates back to January 2017, when DHS designated election infrastructure as a critical infrastructure subsector. Following this designation, the EIS-GCC was established consisting of representatives from DHS, the U.S. Election Assistance Commission (EAC), the National Association of Secretaries of State (NASS), and the National Association of State Election Directors (NASED).

The newly formed EIS-GCC determined that an Information Sharing and Analysis Center (ISAC) focused on election infrastructure would provide immense value to the elections community and recommended its creation. The next step was implementing a pilot program to test the viability of the idea and to develop a framework that would prove the value of the new ISAC and establish a clear path forward. The EIS-GCC turned to CIS and MS-ISAC® (the Multi-State Information Sharing & Analysis Center®) to support these efforts, as the MS-ISAC had been designated as DHS's key cybersecurity resource for cyber threat prevention, protection, response, and recovery for all U.S. State, Local, Tribal, and Territorial (SLTT) governments. After the completion of the pilot, which ran from October 2017 until February 2018, the EIS-GCC held a vote on February 15 to formally launch the Elections Infrastructure ISAC on March 7, 2018.

The EI-ISAC has continued to evolve since its creation, and offers its members a variety of services that include the following:

- Access to a 24/7/365 Security Operations Center (SOC)
- Cyber incident response and remediation
- Threat and vulnerability monitoring
- Election-specific threat intelligence
- Training sessions and webinars
- A National Cyber Situational Awareness Room (NCSAR)
- Security best practice recommendations and tools

The EI-ISAC has positioned itself at the forefront of our nation's effort to secure our election systems, and will continue to operate in partnership with members and stakeholders nationwide to ensure the integrity of elections in the United States.

The Pilot

The EIS-GCC and MS-ISAC first began their formal collaboration in October 2017 with a pilot that included representatives from seven states (Colorado, Indiana, New Jersey, Texas, Utah, Virginia, Washington) and two local election organizations (Travis County, Texas; Weber County, Utah). The DHS Election Task Force (ETF), EAC, and NASED worked alongside the MS-ISAC to develop a program that could serve as an ISAC for the Election Infrastructure Subsector. The MS-ISAC quickly formed an elections team to leverage their existing suite of products and services, as well as their relationships with state and local government IT staff, to address the vision of the pilot participants.

Throughout the subsequent five months, pilot participants offered insight and expertise through weekly calls and open lines of communication that would lead to the creation of an Elections-Focused Cyber Defense Suite. The development of elections-focused products and services presented challenges for the MS-ISAC's newly formed elections team, who were accustomed to working with Chief Information Security Officers (CISOs), Information Technology (IT) staff, and other Information Security constituents. Providing valuable resources for the elections community meant pivoting from the more strictly technical content of the MS-ISAC and offering executive level context and guidance specifically for election officials.

The pilot helped focus these efforts, which resulted in the creation of four new product lines that leveraged a new set of subject matter experts and created a robust formal notification process for its new stakeholders.

Beyond adapting their approach, the EI-ISAC was presented with logistical challenges as well. The pilot program called for the deployment of "Albert," the MS-ISAC's Intrusion Detection System (IDS), on every pilot state's elections network to protect the voter registration database if it was not covered by an existing Albert sensor. This required securing the funding and approval, deciphering whether each state was covered, working with the states to execute agreements, identifying and educating stakeholders from various departments and vendors, ordering and configuring the hardware, and, finally, supporting the pilot members during installation. This effort had election officials and information security leaders successfully working hand-in-hand to help the EI-ISAC staff navigate the logistics of this challenge.

Even with the enormous dedication of the pilot participants, Albert deployments proved to be a challenge, with only five of the seven states successfully incorporating Albert sensors by the end of the pilot phase. The remaining two states were not far behind – one state went online the day after the pilot closed, and the final pilot sensor was installed and running by early March.

On February 15 the EIS-GCC reviewed the pilot's current efforts and future plans, and voted in favor of the formal creation of the EI-ISAC, operated by CIS alongside the MS-ISAC. The following weeks were filled with collaboration across CIS to create the permanent infrastructure necessary to formalize the EI-ISAC's efforts. This infrastructure included legal agreements, a webpage and a way for members to join, staff training, and further collaboration with the partners and leadership that had supported them thus far. The Elections Infrastructure Information Sharing & Analysis Center was formally launched on March 7, 2018.

MS-ISAC Integration

The EI-ISAC was conceived as a means of leveraging the many capabilities and the infrastructure of the MS-ISAC. The integration of the two continued after the EI-ISAC's formal launch in March. Both the MS-ISAC and EI-ISAC benefit by operating under the auspices of CIS. This allows them to work together to educate and protect SLTT governments from the myriad cyber threats that are aimed at both the traditional government IT systems and those specific to elections.



Both ISACs continue to utilize centralized, and in many cases shared, resources to enable a greater level of visibility and information sharing across the elections and the SLTT government sector to benefit the constituencies of both organizations. Furthermore, everything from webcasts to workgroups to in-person meetings integrate the needs of both ISACs, offering efficiency and consistency for the Membership. The support structure behind the ISACs includes:

- Security Operations Center (SOC) to provide 24/7/365 incident triage and immediate response.
- Computer Emergency Response Team (CERT) to provide incident response and forensic services.
- Cyber Intelligence Team to provide forward-leaning analysis, written products, and presentations.
- Engineering Team to provide sensor deployment and technical assistance.
- Stakeholder Engagement Team to provide member support and engagement.

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

Promoting Engagement



Membership

When the EI-ISAC was formally launched, the supporting partners—including the NASS, NASED, Election Center, EAC, and International Association of Government Officials (iGO)—graciously assisted the EI-ISAC in spreading the word of the new structure. An informational kickoff webcast was held on March 16, and by the end of the month the EI-ISAC had 364 member organizations. This growth continued throughout 2018, and by the end of the year, the EI-ISAC boasted 1,447 members in total, making it the fastest-growing ISAC of any critical infrastructure subsector. Members include all 50 states, three territories, 1,384 local governments spread across 44 states, seven associations, and 14 supporting members from the private sector. This included seven states (Florida, Maryland, Nevada, New York, Ohio, Rhode Island, and South Carolina) with 100 percent participation by the state's local elections offices.

While integration with the existing MS-ISAC foundation was paramount for the EI-ISAC's success, the added pressure of an upcoming midterm election sparked staff across CIS and both ISACs to continuously analyze the efficiency of their processes. This spirit was evident even on the day the ISAC was launched.

Traditionally, while membership in the ISACs has always been no-cost, members were required to complete a Membership Agreement in order to join. While this document was not extensive, it did create an extra step

in the process. To streamline the membership process due to the large number of elections offices that were joining, ISAC staff worked with teams across CIS to make one seemingly small change: replacing the Membership Agreement (which required handwritten signatures of both parties) with a checkbox on the online registration form for potential members to agree to a set of terms and conditions. This led to unprecedented membership growth in both the EI-ISAC and MS-ISAC; in fact, MS-ISAC membership grew by over 150 percent in 2018.

Events

While simplifying the process to join was instrumental, the EI-ISAC also needed to reach out to potential members and inform them that these resources existed. EI-ISAC staff attended more than 40 events across 29 states and three territories in 2018 to spread awareness about the new organization and the services available to state and local elections offices. In addition to the efforts of EI-ISAC staff, partner organizations and members banded together to inform potential members about this new organization and to encourage them to join.

While spreading awareness and growing the membership of the EI-ISAC were key initiatives, these events also focused heavily on preparing election officials for the primary and general elections and on providing cybersecurity education. For instance, in New York, Colorado, and Illinois, EI-ISAC staff participated with election officials in tabletop exercises created to give



participants the opportunity to practice handling cybersecurity scenarios that could occur during an election. In Washington and Kansas, EI-ISAC staff participated in cyber-focused trainings to broaden election officials' knowledge base.

In addition to traveling across the nation to support member and partner initiatives, the EI-ISAC also hosted its own webcasts throughout 2018. This included informational sessions for new and prospective members and a joint Monthly Member Call with the MS-ISAC to provide updates, best practices, and a look at the current threat landscape. In October, the EI-ISAC hosted its first Quarterly Membership Call, attended by more than 250 members, which highlighted observed activity and cybersecurity posture in advance of the upcoming November 6 Election Day.

In April 2018, the EI-ISAC joined forces with the MS-ISAC for its Annual Meeting in New Orleans. EI-ISAC members used the meeting as an opportunity to network, learn from one another and the ISAC staff, and discuss cybersecurity with subject matter experts from across the country. During the course of this three-day event, the EI-ISAC held special elections-focused sessions where more than 30 members were able to share perspectives on challenges, best practices, and considerations for elections security.

The newly formed EI-ISAC used this special elections-focused session to learn what the top concerns were for its members and partners in order to better prioritize the services being developed. The Membership stressed that creating uniform messaging to the public was, as always, a major topic of concern. Other critical concerns were the need to define what election infrastructure includes, determining the role the EI-ISAC would play in security, and suggestions on ways that states could

of the first times the EI-ISAC acted as an instrument for true peer-to-peer information sharing, with discussions covering one state's plan to create a "cyber navigator" program, plans for integration with fusion centers, sharing insight regarding federal resources available to elections offices, and the sharing of useful guides and templates between members.

Partnerships

The EI-ISAC could not have achieved the success that it has without the expertise and camaraderie of many organizations in government and industry. From the expertise of NASS and NASED at the state level, to iGO and the Election Center's valuable insight into local government election organizations, the EI-ISAC has been fortunate to have the strong support of the elections community. The invaluable support and guidance of DHS made it possible for EI-ISAC services to be available at no-cost to all members, while simultaneously supporting the purchase and deployment of IDS sensors for elections offices around the country. The EIS-GCC and the pilot participants provided much-needed direction and support to the young EI-ISAC, and the EIS Sector Coordinating Council (EIS-SCC) offered important insight into the crucial partnerships between vendors and elections offices, allowing the EI-ISAC to understand what it would take to truly support its Membership.

In addition, working with the FBI's Cyberhood Watch provided the EI-ISAC with an opportunity for bi-directional sharing of valuable threat information, while other partners like Democracy Works furnished information to assist with outreach to local elections offices. Creating and fostering these partnerships accelerated the acceptance of the EI-ISAC as a trusted resource for its Membership, an essential quality for its mission to improve the overall cybersecurity posture of U.S. elections offices.

Addressing the Threat



Albert Network Security Monitoring & Analysis

The Elections-Focused Cyber Defense Suite created by the EI-ISAC offers members a variety of resources and services to help secure their organizations and information, ranging from a federally funded Intrusion Detection System (IDS) with 24/7/365 support, almost 100 intelligence products, and a National Cyber Situational Awareness Room for coordination and collaboration on election days.

Albert

A focus of the EI-ISAC's efforts throughout 2018 was a federally funded initiative to deploy its IDS, known as Albert, on elections networks throughout the United States. Under the MS-ISAC, sensors had already been funded for each state and territorial network and were developed to be specific to the SLTT government environment. The EI-ISAC expanded this initiative to cover the voter registration databases of any state or territory where the voter registration database was not already covered by an existing sensor, as well as to place sensors in 42 of the most populous local election jurisdictions in which voter registration data were hosted on local hardware.

The Albert expansion benefited the entire EI-ISAC community by providing a deeper understanding of, and actionable intelligence on, the threats directly affecting the elections community. This knowledge informed EI-ISAC members so that they could create tailored response plans to shifts in the cyber threat landscape, while simultaneously allowing both DHS and the EI-ISAC to focus future services to the needs of the Membership. After identifying two pilot states as being covered by existing sensors and successfully implementing sensors on the remaining five pilot states, the EI-ISAC identified an additional 18 states covered by existing sensors.

"The Albert sensor was a great benefit to our small agency. We use many of your services and we recommend them to our counties, and we are in deep gratitude for your mission and the professionalism in which you carry it out. You are truly making a difference to the security of elections in our state and across the nation." – EI-ISAC Member

The EI-ISAC launch in early March gave the team eight months to deploy as many of the remaining 72 federally funded Albert sensors as possible prior to the general election.

Since ordering and receiving a sensor typically takes three to five weeks, the EI-ISAC team expedited the process by ordering sensors in blocks of 15 to 20 based on the sizing information obtained during the ISAC pilot and supplemental incoming data from the states. Additionally, the EI-ISAC developed a survey that allowed the sensors to ship immediately to each organization once complete. This streamlined the process, building in faster procedures along with concurrent actions, which negated the need to wait for the completion of a Pre-Installation Questionnaire before shipping the hardware.

A combination of logistical expediting, a Membership that was incredibly supportive of the efforts, and extensive outreach and technical support efforts by EI-ISAC staff and partners paid off with DHS Secretary Kirstjen Nielsen sharing that on Election Day, approximately 90 percent of all voters in the United States would cast a ballot in a jurisdiction or state monitored by Albert.

Once Election Day 2018 arrived, 45 states, one territory, and 84 local jurisdictions (18 of which were federally funded) had Albert sensors protecting their voter registration data. This was a monumental feat considering that many of the eligible organizations had never heard of Albert or the EI-ISAC nine months earlier.


The teamwork shown by the combined ISAC staff, elections offices, and information security staff that support them—and the fact they created the Albert network that has now been deployed across the country—demonstrates that our partners feel the same way, and the numbers speak for themselves. As of the end of 2018, the elections-specific Albert devices had reported 155 billion records and a total of 10 petabytes of data, leading to 3,389 actionable notifications to members.

Having a couple of Albert sensors here and there does not provide a big picture or additional situational awareness. However, when these sensors are deployed nationwide, experts at the ISAC are able to track trends and intrusions and then share that information with election organizations at both the state and local level to better prepare them for the challenges that lie ahead. According to CIS President and CEO John Gilligan, "When you start to get dozens, hundreds of sensors, like we have now, you get real value."

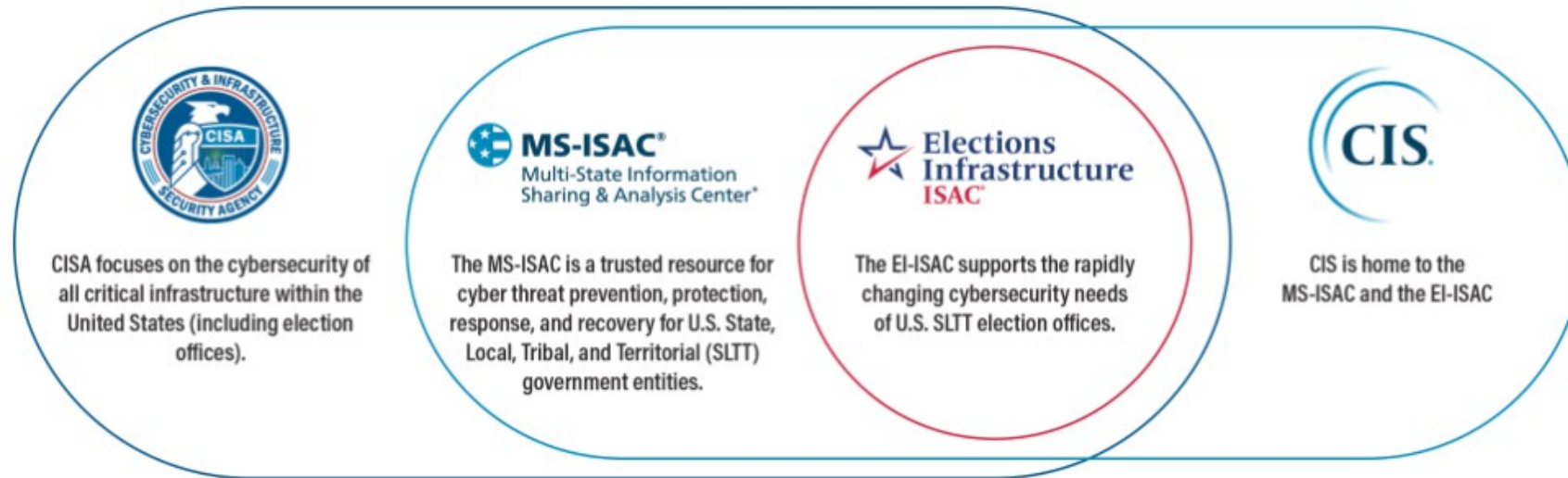
Albert Deployments
as of December 31, 2018



CIS Partnership with
South Carolina
Board of Elections, State and
County



CIS is home to the MS-ISAC and the EI-ISAC



The scale and impact of cyber-attacks continue to escalate. While many public sector organizations are challenged to keep pace, there is help available.

The Center for Internet Security® (CIS®) is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®) and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®). They provide a variety of services that augment and enhance members' cybersecurity teams.



[JOIN MS-ISAC →](#)



[JOIN EI-ISAC →](#)

We value your questions and feedback

At CIS, we are committed to serving the greater IT security community.

[CONTACT US TODAY →](#)



Center for Internet Security

January 19 · 🌐



SLTT governments are encouraged to participate in the Nationwide Cybersecurity Review (NCSR)! It evaluates [#cybersecurity](#) maturity, provides actionable feedback and metrics, and has many other benefits. Learn more about NCSR here. [#SLTT https://bit.ly/31FyScB](#)



CISEcurity.ORG

Nationwide Cybersecurity Review (NCSR)

The Nationwide Cybersecurity Review is a no-cost, anonymous, annual self-assessment design...



7



Center for Internet Security

November 12, 2021 · 🌐



We've reached 12,000 MS-ISAC members!

MS-ISAC has reached **12,000** Members!



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

Established in 2004, the MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial (SLTT) government entities.

12,000

MS-ISAC Membership by the Numbers

50 States + 6 Territories

- American Samoa
- District of Columbia
- Guam
- Marianas Islands
- Puerto Rico
- Virgin Islands



Top 5 States by Membership

- Texas: 1,048
- California: 983
- Michigan: 634
- New York: 540
- Pennsylvania: 509

Top 5 Entity Types



- Local Government: 3,056
- K-12 Education: 2,997
- City: 1,414
- County/Parish/Borough: 1,282
- Public Higher Education: 683



7

1 Share



Like



Comment



Share

Rhode Island - Westerly Public Schools
South Carolina - Aiken County

South Carolina - Allendale County
South Carolina - Allendale County Voter Registration
South Carolina - Anderson County Board of Elections and Voter Registration
South Carolina - Bamberg County Board of Voter Registration and Elections
South Carolina - Beaufort County

South Carolina - Beaufort County School District
South Carolina - Berkeley County Elections and Voter Registration
South Carolina - Calhoun County Board of Voter Registration and Elections
South Carolina - Charleston County Elections and Voter Registration
South Carolina - Charleston Water System
South Carolina - Cherokee County
South Carolina - Cherokee County School District
South Carolina - Chesterfield County
South Carolina - Chesterfield County Voter Registration and Elections
South Carolina - City of Anderson
South Carolina - City of Bennettsville
South Carolina - City of Charleston
South Carolina - City of Columbia
South Carolina - City of Goose Creek
South Carolina - City of Greer
South Carolina - City of Isle of Palms
South Carolina - City of Mullins
South Carolina - City of North Myrtle Beach
South Carolina - City of Spartanburg

South Carolina - Abbeville County Voter Registration and Elections
South Carolina - Aiken County Board Of Voter Registration and Elections
South Carolina - Allendale County Schools
South Carolina - Anderson County
South Carolina - Anderson School District 3
South Carolina - Bamberg County
South Carolina - Bamberg School District 1
South Carolina - Barnwell County Elections
South Carolina - Beaufort County Board of Voter Registration and Elections
South Carolina - Berkeley County
South Carolina - Berkeley County School District
South Carolina - Charleston County
South Carolina - Charleston County Consolidated 911 Center
South Carolina - Charleston County Park and Recreation Commission
South Carolina - Charter Institute at Erskine
South Carolina - Cherokee County Elections and Voter Registration
South Carolina - Chester County Elections and Voter Registration
South Carolina - Chesterfield County School District
South Carolina - City of Aiken
South Carolina - City of Beaufort
South Carolina - City of Cayce
South Carolina - City of Clinton
South Carolina - City of Florence
South Carolina - City of Greenville
South Carolina - City of Hartsville
South Carolina - City of Lancaster
South Carolina - City of Myrtle Beach
South Carolina - City of Rock Hill
South Carolina - City of Sumter

South Carolina - Clarendon County
South Carolina - Clemson University
South Carolina - Colleton County
South Carolina - Darlington County Board of Voter Registration and Elections
South Carolina - Dorchester County Board of Voter Registration and Elections

South Carolina - Fairfield County
South Carolina - Fairfield County Voter Registration and Elections
South Carolina - Florence County Sheriff's Office
South Carolina - Florence School District Three
South Carolina - Georgetown County
South Carolina - Greenville Arena District
South Carolina - Greenville County Voter Registration and Elections Board
South Carolina - Greenwood Commissioners of Public Works
South Carolina - Greenwood County Voter Registration and Elections
South Carolina - Greer Commission of Public Works

South Carolina - Hampton County School District One
South Carolina - Horry County
South Carolina - Horry County Voter Registration and Elections
South Carolina - Jasper County School District
South Carolina - Kershaw County

South Carolina - Kershaw County School District
South Carolina - Lancaster County Voter Registration and Elections

South Carolina - Laurens County Public Library
South Carolina - Lexington County

South Carolina - Clarendon County Voter Registration and Elections
South Carolina - Coastal Carolina University
South Carolina - Colleton County Voter Registration and Elections
South Carolina - Dillon County Voter Registration
South Carolina - Dorchester County
South Carolina - Easley Combined Utilities
South Carolina - Edgefield County Board of Voter Registration and Elections
South Carolina - Fairfield County Public Schools
South Carolina - Florence County
South Carolina - Florence County Voter Registration
South Carolina - Fort Mill Police Department
South Carolina - Georgetown County Voter Registration and Elections
South Carolina - Greenville County
South Carolina - Greenville Water
South Carolina - Greenville-Spartanburg Airport District
South Carolina - Greenwood County
South Carolina - Greenwood School District 50
South Carolina - Hampton County Board of Voter Registration and Elections
South Carolina - High Point Academy
South Carolina - Horry County Schools
South Carolina - Horry-Georgetown Technical College
South Carolina - Jasper County Voter Registration and Elections Board
South Carolina - Kershaw County Board of Elections and Voter Registration
South Carolina - Lancaster County
South Carolina - Laurens County Board of Voter Registration and Elections
South Carolina - Lee County Voter Registration and Elections
South Carolina - Lexington County Voter Registration and Elections

- South Carolina - Lexington School District Four
- South Carolina - Marion County
- South Carolina - Marlboro County Voter Registration and Elections
- South Carolina - McCormick County Voter Registration and Elections
- South Carolina - Myrtle Beach International Airport
- South Carolina - Newberry County School District
- South Carolina - Oconee County Voter Registration and Elections
- South Carolina - Orangeburg Consolidated School District Five
- South Carolina - Orangeburg County Voter Registration and Election Commission
- South Carolina - Pickens County Board of Voter Registration and Elections
- South Carolina - Richland County
- South Carolina - Richland County School District One
- South Carolina - Saluda County Voter Registration
- South Carolina - School District 5 of Lexington and Richland Counties
- South Carolina - South Carolina Public Service Authority (Santee Cooper)
- South Carolina - South Carolina State University
- South Carolina - Spartanburg County Department of Voter Registration and Elections
- South Carolina - Summerville Police Department
- South Carolina - Sumter County Voter Registration and Elections Board
- South Carolina - Town of Blythewood
- South Carolina - Town of Mount Pleasant
- South Carolina - Trident Technical College
- South Carolina - Union County Schools
- South Carolina - Williamsburg County
- South Carolina - Winthrop University
- South Carolina - York County Board of Voter Registrations and Elections
- South Carolina - Lexington School District Two
- South Carolina - Marion County Voter Registration and Elections
- South Carolina - McCormick County School District
- South Carolina - Medical University of South Carolina
- South Carolina - Newberry County
- South Carolina - Newberry County Voter Registration and Elections
- South Carolina - Odyssey Online Learning
- South Carolina - Orangeburg County
- South Carolina - Pelion Police Department
- South Carolina - Pickens County
- South Carolina - Piedmont Municipal Power Agency
- South Carolina - Poplar Springs Fire Department
- South Carolina - Richland County Elections and Voter Registration
- South Carolina - Saluda County
- South Carolina - Santee Lynches Council of Governments
- South Carolina - School District of Oconee County
- South Carolina - South Carolina School Board Association
- South Carolina - South Carolina State Ports Authority
- South Carolina - Spartanburg County
- South Carolina - Spartanburg County School District 3
- South Carolina - Spartanburg District Five Schools
- South Carolina - Sumter County
- South Carolina - The Citadel
- South Carolina - Town of Hilton Head Island
- South Carolina - Town of Port Royal
- South Carolina - Union County Board of Voter Registration and Elections
- South Carolina - University of South Carolina
- South Carolina - Williamsburg County Voter Registration and Elections
- South Carolina - York County
- South Carolina - York Preparatory Academy

**MEMORANDUM OF AGREEMENT
BETWEEN THE CENTER FOR INTERNET SECURITY/ELECTION
INFRASTRUCTURE INFORMATION SHARING AND ANALYSIS CENTER
AND**

**FOR
CYBERSECURITY SERVICES
(Federally Funded Election Services)**

This MEMORANDUM OF AGREEMENT ("Agreement") by and between the Center for Internet Security, Inc. ("CIS"), operating in its capacity as the Elections Infrastructure Information Sharing and Analysis Center ("EI-ISAC"), located at 31 Tech Valley Drive, East Greenbush, NY 12061-4134, and ~~State of New York~~ ("Entity") with its principal place of business at: ~~State of New York~~ for Cybersecurity Services, as defined herein below (CIS and Entity each a "Party" and collectively referred to as the "Parties").

WITNESSETH:

WHEREAS, CIS operates a twenty-four hours a day, seven days per week (24/7) Security Operations Center ("SOC"); and

WHEREAS, CIS has entered into an agreement with the US Department of Homeland Security ("DHS") to provide Cybersecurity Services, including Cybersecurity Services for state election entities; and

WHEREAS, the Entity is a state election entity designated to receive Cybersecurity Services;

NOW, THEREFORE, in consideration of the mutual covenants contained herein, the Parties do hereby agree as follows:

I. Purpose

The purpose of this agreement is to set forth the mutual understanding between Entity and CIS with respect to the provision of Cybersecurity Services to Entity.

II. Definitions

A. Security Operation Center (SOC) - 24 X 7 X 365 watch and warning center that provides network monitoring, dissemination of cyber threat warnings and vulnerability identification and mitigation recommendations.

B. Cybersecurity Services or CSS - Combined Netflow and intrusion detection system monitoring and analysis of related data, and delivery and management of associated devices, hardware and software necessary for delivery of CSS. Also referred to as Albert monitoring services.

III. Consideration

Pursuant to the agreement with DHS, CIS is providing Cybersecurity Services and associated security devices at no charge to Entity.

IV. Responsibilities

Appendix A, which is attached hereto and incorporated herein, contains the specific responsibilities for Entity and CIS regarding the CSS. Entity understands and agrees that, as a condition to commencement of CSS under the terms of this Agreement, it must:

A. agree to comply with the terms and conditions applicable to Entity as set forth in Appendix A; and

B. execute the Entity Certification form attached as part of Appendix A.

V. Title

CIS will at all times retain title to hardware and/or software provided to Entity during the Term of this Agreement. Upon termination or expiration of this Agreement, Entity will return all hardware and/or software provided under this Agreement within thirty (30) days of such expiration or termination.

VI. Term of this Agreement

This Agreement will commence on the date it is signed by both Parties, and shall continue in full force and effect until terminated (the "Term"). Either Party may terminate this Agreement by providing written notice to the other Party ninety (90) days prior to termination.

Additionally, if during the Term of this Agreement, Entity makes changes to its hardware or network configuration in such a manner that CIS is no longer able to provide the CSS to Entity, CIS shall have the ability to terminate this Agreement upon written notice to Entity.

The ability and obligation of CIS to provide these Cybersecurity Services and devices to the Entity is, at all times, contingent on the availability and allocation of federal funds for this purpose.

VII. Amendments to this Agreement

This Agreement may only be amended as agreed to in writing by both Parties.

VIII. No Third Party Rights

Nothing in this Agreement shall create or give to third parties any claim or right of action of any nature against Entity or CIS.

IX. Disclaimer

Both Parties disclaim all express and implied warranties with regard to the CSS provided for herein, and neither Party assumes any responsibility or liability for the accuracy of the information that is the subject of this Agreement, or for any act or omission or other performance related to the CSS provided under this Agreement.

X. Confidentiality Obligation

CIS acknowledges that information regarding the infrastructure and security of Entity information systems, assessments and plans that relate specifically and uniquely to the vulnerability of Entity information systems, the results of tests of the security of Entity information systems insofar as those results may reveal specific vulnerabilities or otherwise marked as confidential by Entity ("Confidential Information") may be provided by Entity to CIS in connection with the services provided under this Agreement. The Entity acknowledges that it may receive from CIS trade secrets and confidential and proprietary information ("Confidential Information"). Both Parties agree to hold each other's Confidential Information in confidence to the same extent and the same manner as each Party protects its own confidential information, but in no event will less than reasonable care be provided and a Party's information will not be released in any identifiable form without the express written permission of such Party or as required pursuant to lawfully authorized subpoena or similar compulsive directive or is required to be disclosed by law, provided that the Entity shall be required to make reasonable efforts, consistent with applicable law, to limit the scope and nature of such required disclosure. CIS shall, however, be permitted to disclose relevant aspects of such Confidential Information to its officers, employees, agents and CIS's cybersecurity partners, including federal partners, provided that such partners have agreed to protect the Confidential Information to the same extent as required under this Agreement. The Parties agree to use all reasonable steps to ensure that Confidential Information received under this Agreement is not disclosed in violation of this Section. These confidentiality obligations shall survive any future non-availability of federal funds to continue the program that supports this Agreement or the termination of this Agreement.

Appendix A

CSS Responsibilities

- I. **Entity Responsibilities** - Entity acknowledges and agrees that CIS's ability to perform the Cybersecurity Services provided by CIS for the benefit of Entity is subject to Entity fulfilling certain responsibilities listed below. Entity acknowledges and agrees that neither CIS nor any third party provider shall have any responsibility whatsoever to perform the Cybersecurity Services in the event Entity fails to meet its responsibilities described below.
 - A. For purposes of this Agreement, Entity acknowledges and agrees that only those security devices supported by CIS fall within the scope of this Agreement. Entity will ensure the correct functioning of devices except where Entity elects to have CIS manage the devices.
 - B. Entity shall provide logistic support in the form of rack space, electricity, Internet connectivity, and any other infrastructure necessary to support communications at Entity's expense.
 - C. Entity shall provide the following to CIS prior to the commencement of service and at any time during the term of the Agreement if the information changes:
 1. Current network diagrams to facilitate analysis of security events on the portion(s) of Entity's network being monitored. Network diagrams will need to be revised whenever there is a substantial network change;
 2. In-band access via a secure Internet channel to manage the device(s).
 3. Outbound access via a secure Internet channel for log transmission.
 4. Reasonable assistance to CIS as necessary, to enable CIS to deliver and perform the CSS for the benefit of Entity;
 5. Maintenance of all required hardware, virtual machines, or software necessary for the sensor located at Entity's site, and enabling access to such hardware, virtual machines, or software as necessary for CIS to provide the CSS;
 6. Public and Private IP address ranges including a list of servers being monitored including the type, operating system and configuration information; and list of IP ranges and addresses that are not in use by the Entity (DarkNet space);
 7. Completed Pre-Installation Questionnaires (PIQ). The PIQ will need to be revised whenever there is a change that would

- affect CIS's ability to provide the Cybersecurity Services;
8. Accurate and up-to-date information, including the name, email, landline, mobile, and pager numbers for all designated, authorized Point of Contact(s) who will be provided access to the portals, and;
 9. The name, email address, and landline, mobile, and pager numbers for all shipping, installation and security points of contact.

D. With respect to the shipping and delivery of any required hardware, Entity agrees to the following:

1. For any hardware shipped directly to Entity, upon receipt of the hardware, Entity shall contact CIS to confirm the serial number of the hardware. Upon confirmation of the serial number, CIS will ship an identification tag to Entity. Entity agrees to place the identification tag on the hardware as per the accompanying instructions, and upon placement of the identification tag, to confirm in writing to CIS that the tag has been placed on the hardware.
2. In certain instances, CIS may ship hardware and software to Entity prior to the final execution of this Agreement. Notwithstanding the foregoing, Entity acknowledges that commencement of CSS is contingent on the execution of this Agreement by the parties.

E. During the term of this Agreement Entity shall provide the following:

1. Written notification to CIS SOC (SOC@MSISAC.ORG) at least thirty (30) days in advance of changes in hardware or network configuration affecting CIS's ability to provide Cybersecurity Services, or a change to the physical location of the hardware; any notice relating to change in physical location shall include the new physical address of the hardware;
2. Written notification to CIS SOC (SOC@MSISAC.ORG) at least twelve (12) hours in advance of any scheduled downtime or other network and system administration scheduled tasks that would affect CIS's ability to provide the service;
3. A completed Escalation Procedure Form including the name, e-mail address and 24/7 contact information for all designated Points of Contact (POC). A revised Form must be submitted when there is a change in status for any POC;
4. Sole responsibility for maintaining current maintenance and technical support contracts with Entity's software and hardware vendors for any device affected by CSS that has not

- 5. been supplied by CIS;
- 6. Active involvement with CIS SOC to resolve any tickets requiring Entity input or action;
- 7. Reasonable assistance in remotely installing and troubleshooting devices including hardware and communications,
- 8. Upon reasonable notice from CIS and during normal business hours, access for CIS to inspect the hardware.
- 9. Response to biennial written confirmation notice from MS-ISAC as to the physical location of all hardware provided by CIS.

F. **Certification.** Entity shall complete the attached Entity Certification documenting compliance with the following:

- 1. That the Entity provides notice to its employees, contractors and other authorized internal network users (collectively, "Computer Users") that contain in sum and substance the following provisions:
 - (a) Computer Users have no reasonable expectation of privacy regarding communications or data transiting, stored on or traveling to or from Entity's information system; and
 - (b) Any communications or data transiting, stored on or traveling to or from the Entity's information system may be monitored, disclosed or used for any lawful government purpose; and
- 2. That all Entity Computer Users execute some form of documentation or electronic acceptance acknowledging his/her understanding and consent to the above notice. Examples of notice documentation include, but are not limited to:
 - a) log-on banners for computer access with an "I Agree" click through;
 - b) consent form signed by the Computer User acknowledging Entity's computer use policy; or
 - c) computer use agreement executed by the Computer User.

II. CIS Responsibilities

- A. CIS will be responsible for the correct functioning of managed devices.
- B. CIS shall be responsible for the purchase of certain hardware, and shall arrange for the shipping of such hardware to a location designated by Entity. Upon notice from Entity that the hardware has been delivered and upon confirmation of the serial number of the hardware, CIS shall be responsible for providing Entity with an identification tag to be placed on the hardware.
- C. CIS will provide the following as part of the service:
 - 1. Analysis of logs from monitored security devices for attacks and malicious traffic;
 - 2. Analysis of security events;
 - 3. Correlation of security data/logs/events with information from other sources;
 - 4. Notification of security events per the Escalation Procedures provided by Entity.
 - 5. Ensuring that all upgrades, patches, configuration changes and signature upgrades are applied to managed devices. CIS will provide the appropriate license and support agreements for the upgrade for devices provided by CIS. The Entity is responsible for maintaining the appropriate license and support agreements for devices own by the Entity.
- D. Access to Stored Flow Data. CIS shall provide access to normalized logs, security events and netflow data through batch queries.
- E. CIS Security Operation Center. CIS will provide 24/7 telephone (1-866-787-4722) availability for assistance with events detected by the CSS.
- F. Biennial Confirmation for Hardware Location. Every two years, CIS will send Entity a request for confirmation of the physical location of the hardware provided as part of the CSS, including description, serial number and address of physical location of hardware.

ENTITY CERTIFICATION

On behalf of _____ ("Entity"), I hereby certify the following:

1. Entity provides notice to its employees, contractors and other authorized internal network users ("collectively "Computer Users") that contain in sum and substance the following provisions:

-Computer Users have no reasonable expectation of privacy regarding communications or data transiting, stored on or traveling to or from Entity's information system; and

-Any communications or data transiting, stored on or traveling to or from the Entity's information system may be monitored, disclosed or used for any lawful government purpose.

2. All Entity Computer Users execute a form of documentation or electronic acceptance acknowledging his/her understanding and consent to the above notice.

3. I am authorized to execute this Certification on behalf of Entity.

Dated this 19 day of October, 2018.

DocuSigned by:

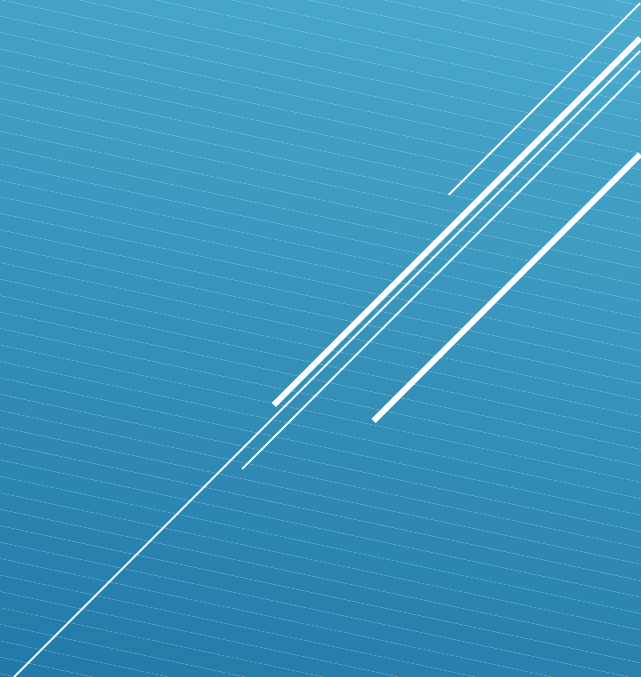


7E46A946770F438

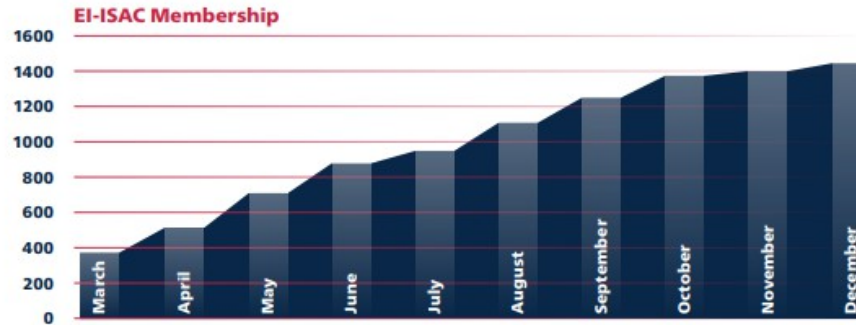
Name: _____

Title: County Judge

In 2018, CIS went to
ONLINE Registration,
Agreement to Terms and
Conditions for
Partnership

Decorative white lines consisting of three parallel diagonal strokes in the bottom right corner of the slide.

Promoting Engagement



Membership

When the EI-ISAC was formally launched, the supporting partners—including the NASS, NASED, Election Center, EAC, and International Association of Government Officials (iGO)—graciously assisted the EI-ISAC in spreading the word of the new structure. An informational kickoff webcast was held on March 16, and by the end of the month the EI-ISAC had 364 member organizations. This growth continued throughout 2018, and by the end of the year, the EI-ISAC boasted 1,447 members in total, making it the fastest-growing ISAC of any critical infrastructure subsector. Members include all 50 states, three territories, 1,384 local governments spread across 44 states, seven associations, and 14 supporting members from the private sector. This included seven states (Florida, Maryland, Nevada, New York, Ohio, Rhode Island, and South Carolina) with 100 percent participation by the state’s local elections offices.

While integration with the existing MS-ISAC foundation was paramount for the EI-ISAC’s success, the added pressure of an upcoming midterm election sparked staff across CIS and both ISACs to continuously analyze the efficiency of their processes. This spirit was evident even on the day the ISAC was launched.

Traditionally, while membership in the ISACs has always been no-cost, members were required to complete a Membership Agreement in order to join. While this document was not extensive, it did create an extra step

in the process. To streamline the membership process due to the large number of elections offices that were joining, ISAC staff worked with teams across CIS to make one seemingly small change: replacing the Membership Agreement (which required handwritten signatures of both parties) with a checkbox on the online registration form for potential members to agree to a set of terms and conditions. This led to unprecedented membership growth in both the EI-ISAC and MS-ISAC; in fact, MS-ISAC membership grew by over 150 percent in 2018.

Events

While simplifying the process to join was instrumental, the EI-ISAC also needed to reach out to potential members and inform them that these resources existed. EI-ISAC staff attended more than 40 events across 29 states and three territories in 2018 to spread awareness about the new organization and the services available to state and local elections offices. In addition to the efforts of EI-ISAC staff, partner organizations and members banded together to inform potential members about this new organization and to encourage them to join.

While spreading awareness and growing the membership of the EI-ISAC were key initiatives, these events also focused heavily on preparing election officials for the primary and general elections and on providing cybersecurity education. For instance, in New York, Colorado, and Illinois, EI-ISAC staff participated with election officials in tabletop exercises created to give



FOIA CISA

Email Communications
regarding elections

Three parallel white lines of varying lengths are positioned in the bottom right corner of the slide, slanted upwards from left to right.

Catalano, John

From: Election Infrastructure SSA <EISSA@cisa.dhs.gov>
Sent: Thursday, July 16, 2020 4:58 PM
To: Election Infrastructure SSA
Subject: [External] Emergency Directive 20-03, Critical Vulnerability (CVE-2020-1350)

Dear Elections Infrastructure GCC and SCC Partners,

CISA is sharing the below emergency directive issued to federal agencies today with you to highlight the significance of this vulnerability and need to patch ASAP. Please let us know if you have any questions.

Today, the Director of the Cybersecurity and Infrastructure Security Agency (CISA) issued Emergency Directive 20-03 (<https://cyber.dhs.gov/ed/20-03>). This is a follow-up action from the Current Activity alert regarding the urgency to mitigate a critical vulnerability (CVE-2020-1350) released on Tuesday, July 14th on a vulnerability in the Windows Domain Name System (DNS) Server.

A remote code execution vulnerability exists in how Windows Server is configured to run the Domain Name System (DNS) Server role. If exploited, the vulnerability could allow an attacker to run arbitrary code in the context of the Local System Account. To exploit the vulnerability, an unauthenticated attacker could send malicious requests to a Windows DNS server.

CISA is unaware of active exploitation of this vulnerability but assesses that the underlying vulnerabilities can be quickly reverse engineered from a publicly available patch. Aside from removing affected endpoints from the network, there are two known technical mitigations to this vulnerability: a software update and a registry modification. For more information on the registry work around, check the guidance provided by Microsoft: <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1350>.

CISA has determined that this vulnerability poses significant risk to the Federal Civilian Executive Branch and requires an immediate and emergency action. This determination is based on the likelihood of the vulnerability being exploited, the widespread use of the affected software across the Federal enterprise, the high potential for a compromise of agency information systems, and the grave impact of a successful compromise.

Thank You,

EI SSA

EI SSA/ESI, National Risk Management Center

Cybersecurity and Infrastructure Security Agency

Email: EISSA@CISA.DHS.GOV



Catalano, John

From: Election Infrastructure SSA <EISSA@cisa.dhs.gov>
Sent: Friday, October 30, 2020 11:04 AM
To: Election Infrastructure SSA
Subject: [External] Microsoft Warns of Continued Exploitation of Netlogon Vulnerability

Election Partners,

Microsoft released a [blog post](#) on cyber actors exploiting CVE-2020-1472, an elevation of privilege vulnerability in Microsoft Netlogon. A remote attacker can exploit this vulnerability to breach unpatched Active Directory domain controllers and obtain domain administrator access. CISA has observed nation state activity exploiting this vulnerability.

CISA urges network administrators to patch all domain controllers immediately. Until every domain controller is updated, the entire infrastructure remains vulnerable, as threat actors can identify and exploit a vulnerable system in minutes. CISA released a [patch validation script](#) to detect unpatched Microsoft domain controllers. Network administrators should take follow-on actions described in [guidance released by Microsoft](#) to prepare for the second half of Microsoft's Netlogon migration process, which is scheduled to conclude in February 2021.

For more information, please visit: us-cert.cisa.gov/ncas/current-activity/2020/10/29/microsoft-warns-continued-exploitation-cve-2020-1472.

EI SSA

EI SSA/ESI, National Risk Management Center
Cybersecurity and Infrastructure Security Agency
Email: EISSA@CISA.DHS.GOV



Catalano, John

From: JOHNSON, LAUREN <lauren.johnson@cisa.dhs.gov> on behalf of Election Infrastructure SSA <EISSA@cisa.dhs.gov>
Sent: Wednesday, October 7, 2020 2:09 PM
To: Andino, Marci; Election Infrastructure SSA
Cc: DaRosa, Antonio
Subject: RE: [External] RE: Classified Briefing

Ok, great.

Lauren A. Johnson
Election Infrastructure Sector-Specific Agency
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
Office: (703) 705-6671
Cell: (202) 853-1679
NEW: lauren.johnson@cisa.dhs.gov

From: Andino, Marci <marci@elections.sc.gov>
Sent: Wednesday, October 7, 2020 2:05 PM
To: Election Infrastructure SSA <EISSA@cisa.dhs.gov>
Cc: DaRosa, Antonio <Antonio.Darosa@cisa.dhs.gov>; JOHNSON, LAUREN <lauren.johnson@cisa.dhs.gov>
Subject: RE: [External] RE: Classified Briefing

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Thanks, Lauren. I have been contacted by Denzor Richberg (DHS) and he is coordinating using the FBI's room.

From: JOHNSON, LAUREN <lauren.johnson@cisa.dhs.gov> On Behalf Of Election Infrastructure SSA
Sent: Wednesday, October 7, 2020 1:57 PM
To: Andino, Marci <marci@elections.sc.gov>
Cc: DaRosa, Antonio <Antonio.Darosa@cisa.dhs.gov>; JOHNSON, LAUREN <lauren.johnson@cisa.dhs.gov>
Subject: [External] RE: Classified Briefing

Thanks Marci. We will coordinate with the briefing facility in Charleston to confirm your attendance.

Thanks!

Lauren A. Johnson
Election Infrastructure Sector-Specific Agency
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
Office: (703) 705-6671
Cell: (202) 853-1679
NEW: lauren.johnson@cisa.dhs.gov

Catalano, John

From: Andino, Marci
Sent: Wednesday, October 7, 2020 11:44 AM
To: Election Infrastructure SSA
Subject: Classified Briefing

I plan to attend the classified briefing on October 16th. I attended the last meeting in Columbia, SC.

Marci

Marci Andino
Executive Director
SC State Election Commission
1122 Lady Street, Suite 500
Columbia, SC 29201

Office (803) 734-9001
Fax (803) 734-9366
scVOTES.gov

every vote matters.
every vote counts.



This message originates from the South Carolina State Election Commission. If you have received this message in error, we would appreciate it if you would immediately notify the South Carolina State Election Commission by sending a reply e-mail to the sender of this message. Thank you.

Catalano, John

From: Election Infrastructure SSA <EISSA@cisa.dhs.gov>
Sent: Wednesday, October 21, 2020 4:23 PM
To: Election Infrastructure SSA
Subject: [External] General Election 2020 Operations Room Invitation

Election Partners,

You are cordially invited to the General Election 2020 Operations Room. Due to COVID 19, we adjusting the set up and operation *in order to keep everyone safe and are trying to gauge interest and plan on shifts for CISA personnel if needed.* *If you wish to attend in person, please RSVP no later than Friday, October 23 by noon.* Once we hear back from all individuals interested in attending in-person, we will contact you to confirm your attendance and your shift preference (if any). If you are not able to attend in person, we can establish virtual check-ins at your convenience.

As in previous elections, we will be working from the Glebe Building at 1110 N. Glebe Rd., Arlington, VA. The Election Day Operations Room (Suite 1128) will be open from 6:00 a.m. on Tuesday, November 3, to the end of primary reporting (potentially early morning on Wednesday, November 4). Masks are required while in the building and social distancing guidelines will be maintained. Disinfectant spray and hand sanitizer will be provided.

We will have escorts in the main lobby on the first floor and on the 7th floor to help you with security screening/processing and assistance with accessing the 11th floor Operations Room. We recommend wearing comfortable attire (business casual). Additional administration information is attached. The closest Metro stop is Ballston/MU, and limited parking is available in the area.

Due to COVID 19, neighboring restaurants and markets are limited. Limited refreshments and snacks will be provided; however, it is recommended to bring your own preferences in enough quantity to last the duration of your stay.

If you have questions or need additional information, please email the EI-SSA Box (EISSA@hq.dhs.gov).

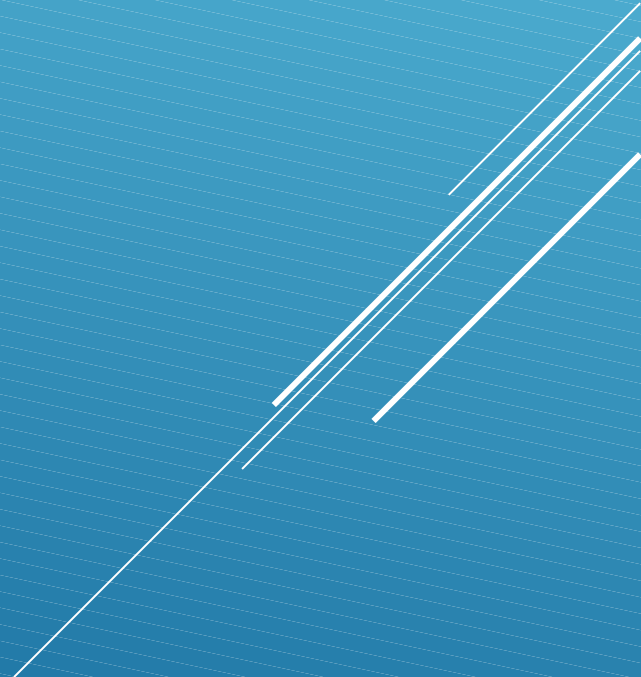
Thank you,

EI SSA
EI SSA/ESI, National Risk Management Center
Cybersecurity and Infrastructure Security Agency
Email: EISSA@CISA.DHS.GOV



- ▣ **According to Local News: WLTX Published: 9:57 AM EDT
May 13, 2021, Executive Director of SC Election Commission
resigns**
- ▣ COLUMBIA, S.C. — In a letter to the Chairman of the South Carolina Election Commission (SCEC), Marci Andino, Executive Director of the Commission, submitted her resignation to be effective at the end of 2021.
- ▣ Andino has been the director of the agency overseeing voter registration and elections in the state for the past 18 years, as it's fourth director.
- ▣ In her years at SCEC, she oversaw a new statewide voter registration system, implementation of state laws -- including Photo ID laws -- and established a "fair and transparent" filing system when legislation changed in 2013.

- Andino writes that the long term goal set by the first executive director was to implement a uniform statewide voting system. In 2019, she oversaw a second statewide voting system that enhanced security at the polls and added paper records of every vote cast.
- In her last two years as director, she saw a pandemic affect thousands as they went to the polls. "The results were extraordinary. Record numbers voted, polling places were safe, wait times were low, results were reported on time, and very few election protests were filed," she wrote.
- Due to the pandemic, Andino pushed the SC Legislature to allow all voters to vote absentee, apply for absentee ballots online and allow absentee ballots to be returned via drop box. She also asked lawmakers to allow election officials more time to count the returned absentee votes.

- Marci Andino Resigned at the end of 2021
 - She was given a PROMOTION as Senior Director of EI-ISAC that is funded by the Department of Homeland Security.
- 



“We believe that strong elections are cyber strong, and it is our mission and privilege as the EI-ISAC to support election officials and the election community with the resources at the heart of the Cyber STRONG Campaign.”

Marci Andino

Senior Director of EI-ISAC



STATESCOOP

Written by [Benjamin Freed](#)

JUL 8, 2022 | STATESCOOP

Four years into its existence, a cybersecurity and intelligence-sharing operation built for state and local election officials now numbers more than 3,400 members, has added several new products and has become a mainstay of a once-skeptical community of election administrators scattered across the country.

Amid that growth, though, and [rising staff turnover](#) at individual election offices, the Election Infrastructure Information Sharing and Analysis Center, or EI-ISAC, is “reintroducing” itself, the operation’s director, Marci Andino, told StateScoop this week.

“We’ve got a lot of people out there conducting elections who weren’t there in 2018,” Andino, a former statewide election director in South Carolina, said in a phone interview ahead of the National Association of Secretaries of State conference taking place in Baton Rouge, Louisiana.

Andino was [hired last year](#) to lead the EI-ISAC, which is funded by the U.S. Department of Homeland Security and operated by the Center for Internet Security, the Upstate New York nonprofit group that also runs the [Multi-State ISAC](#) providing state and local governments with cybersecurity information and services.

Election offices, Andino said, rely on new and seasonal workers, particularly in the run-up to a general election. With one coming in

Election offices, Andino said, rely on new and seasonal workers, particularly in the run-up to a general election. With one coming in four months, the EI-ISAC this month started promoting a campaign called [“Cyber STRONG,”](#) an acronym whose parts refer to employee education, communications, device and network security and public awareness.

The program stresses employee trainings, including [tabletop drills](#) that simulate election disasters and anti-phishing exercises that test people’s ability to not click on a malicious link or attachment.

“Users are the weakest link in any system,” Andino said. “Officials are extremely busy and they bring on lots of seasonal workers. This is reminding them of phishing, threats out there.”

Andino said she’s also trying to pitch more election offices to sign up for the Center for Internet Security’s technical products, like vulnerability assessments or the organization’s [malicious domain blocking](#) and endpoint detection services, which are offered free to EI-ISAC members.

There are also monthly publications focused on specific threats, with July covering [insider threats](#), the risk of which she said rises naturally as new people are brought in.

“[Officials] can’t conduct elections without bringing in lots of new employees or seasonal workers, so it increases that insider threat,” Andino said.

CALL TO ACTION:

- FILE EMERGENCY INJUNCTIONS IN EACH COUNTY CITING THE STATE CASE CIVIL ACTION # 3:22-cv-2872-SAL-PJGTO CEASE AND DESIST THE ELECTION MACHINES