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

INTRODUCTION

Contact Information

David Dove
Chief of Staff & Legal Counsel
Georgia Secretary of State's Office
214 State Capitol
Atlanta, Georgia 30334
404.656.2881
ddove@sos.ga.gov

GEORGIA
SECRETARY OF STATE
BRIAN P. KEMP

INTRODUCTION

CRITICAL INFRASTRUCTURE

SOS NETWORK SECURITY

DHS HACKING ATTEMPTS

NATIONAL REACTION

MOVING FORWARD

INTRODUCTION

Georgia's Election System

- Voter Registration Database (SOS)
- Voter Registration Activities (County Offices)
- Election Equipment
  - Purchased by the State in 2002
  - Maintained by Counties
  - Maintenance by vendor and counties
- Kennesaw Center for Elections Systems

GEORGIA
SECRETARY OF STATE
BRIAN P. KEMP

INTRODUCTION

CRITICAL INFRASTRUCTURE

SOS NETWORK SECURITY

DHS HACKING ATTEMPTS

NATIONAL REACTION

MOVING FORWARD

INTRODUCTION

Georgia's Election System

- Voter Registration Database → Web Based Platform
- Voting System → Closed, Air-Gapped, Certified
- DNC/RNC Systems → **Completely Unrelated**

GEORGIA
SECRETARY OF STATE
BRIAN P. KEMP

INTRODUCTION

CRITICAL INFRASTRUCTURE

SOS NETWORK SECURITY

DHS HACKING ATTEMPTS

NATIONAL REACTION

MOVING FORWARD

INTRODUCTION

Georgia's Election System

- Preparations for 2016 Cycle began in 2014
- Three Multi-Day Training Conferences in 2015
- Survey of Election Equipment
- Certification of Election Officials
- Online Poll Worker Training Module
- Review of Agency Security Protocols

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

Comments by Jeh Johnson to New York Times

U.S. Seeks to Protect Voting System From Cyberattacks

By JULIE HIRSCHFELD DAVIS AUG. 3, 2016

"That varied infrastructure and those different systems also pose a difficult challenge to potential hackers," Mr. Earnest added. "It's difficult to identify a common vulnerability."

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?

1. Critical Infrastructure is a Term of Art and carries with it implications beyond the ordinary meaning of the phrase.
2. Sixteen sectors have been designated "Critical Infrastructure" by the Federal Government.
   a) Chemicals
   b) Commercial Facilities
   c) Communications
   d) Critical Manufacturing
   e) Dams
   f) Defense Industrial Bases
   g) Emergency Services
   h) Energy Grid
   i) Financial Services
   j) Food & Agriculture
   k) Government Facilities
   l) Healthcare & Public Health
   m) Information Technology
   n) Nuclear Reactors & Waste
   o) Transportation Systems
   p) Water Sources
3. The last Sector to be added was Financial Services in 2009.
4. Sectors can only be designated "Critical Infrastructure" by the President or by the Secretary of Homeland Security. No Rulemaking is required.

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

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

Secretary Kemp Lead the Opposition to Designating Election Systems as CI

- Aug 15 – First Call with Jeh Johnson
- Aug 25 – Kemp Named to DHS Election Cyber Security Working Group
- Sept 8 – First Conference Call with Working Group
- Sept 21 – Second Conference Call with Working Group
- Sept 28 – Kemp Testifies before US House Oversight Committee in DC**
- Oct 6 – First meeting with DHS Field Staff ahead of Election Day
- Oct 11 – Second meeting with DHS Field Staff ahead of Election Day
- Oct 20 – Kemp meets with Georgia Tech Cyber Security Experts
- Oct 26 – Third meeting with DHS Field Staff ahead of Election Day
- Oct 28 – Call with DHS Officials and NASS members

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

- 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.

GEORGIA
SECRETARY OF STATE
BRIAN P. KEMP

INTRODUCTION

CRITICAL INFRASTRUCTURE

SOS NETWORK SECURITY

DHS HACKING ATTEMPTS

NATIONAL REACTION

MOVING FORWARD

SOS NETWORK SECURITY

Understanding Different Systems

Two Different Systems at Related to Elections in the Secretary of State Environment:

1. **The Voting System** – Where ballots are actually cast; non-networked; air-gapped; never connected to the internet; certified and maintained by non-partisan 3rd party at KSU Center for Elections; certified by the Election Assistance Commission; stored and used in each county with no crossover among units. There are no credible threats against this system.

2. **The Voter Registration System** – System that holds voter information; only used on Election Day when you check-in; maintained on servers with stringent IT protocols and security; cannot affect the outcome of an election; network security monitored by one of world's best system security providers.

GEORGIA
SECRETARY OF STATE
BRIAN P. KEMP

INTRODUCTION

CRITICAL INFRASTRUCTURE

SOS NETWORK SECURITY

DHS HACKING ATTEMPTS

NATIONAL REACTION

MOVING FORWARD

SOS NETWORK SECURITY

Understanding Different Systems

Secretary of State Security Measures

- Full-time IT Security Officer
- Protocols and procedures consistent with latest industry best practices, reviewed by public and private sector security consultants
- Network security provider ranked as one of the best in the world that also oversees network security for many Fortune 500 companies.
- Advanced encryption for all sensitive information stored within the environment
- Mandatory security training for all employees in the Secretary of State's office as well as county elections officials.
- Regular systems testing in accordance with industry best practices.

GEORGIA
SECRETARY OF STATE
BRIAN P. KEMP

INTRODUCTION

CRITICAL INFRASTRUCTURE

SOS NETWORK SECURITY

DHS HACKING ATTEMPTS

NATIONAL REACTION

MOVING FORWARD

DHS HACKING ATTEMPTS

Timeline

Nov 15 – Network Security Provider notified SOS Security Officer of medium-level reconnaissance scan against outer ports on main SOS site

Nov 15-Dec 8 – Internal investigation into the nature of the attempted intrusion into the system including attribution of the origin

Dec 8 – Secretary Kemp sends a letter to DHS Secretary Jeh Johnson informing him of unauthorized scanning activity against our system which was traced to DHS. Kemp demands answers.

Dec 9 – SOS IT staff begins working with DHS to trace origin of attack. DHS suggests attack originated with an employee's misconfigured workstation. DHS also assured SOS they could recreate the event.

Dec 12 – MOU is signed by both parties to ensure confidentiality of SOS Network Security Protocols. NASS sends survey to all states. DHS sends an interim update and suggests that the issue is closed.

GEORGIA
SECRETARY OF STATE
BRIAN P. KEMP

INTRODUCTION

CRITICAL INFRASTRUCTURE

SOS NETWORK SECURITY

DHS HACKING ATTEMPTS

NATIONAL REACTION

MOVING FORWARD

DHS HACKING ATTEMPTS

Timeline

Dec 13 – Further investigation reveals 9 other attempts to access SOS network throughout 2016. Secretary Kemp responds to DHS letter suggesting matter is closed and calls on President Trump's administration to investigate after he takes office.

Dec 14 – Results from NASS survey show that Kentucky and West Virginia were also scanned. Indiana, Nevada, and Maine also begin investigations to look into scanning activity.

Dec 16 – DHS holds a conference call with all state election officials to announce the attack against Georgia was caused by a contract employee at FLETC using an older version of Microsoft Word that created an open option call against the Georgia SOS firewall. However, DHS was unable to explain how this theory could have occurred. They also were not able to replicate the action.

GEORGIA
SECRETARY OF STATE
BRIAN P. KEMP

INTRODUCTION

CRITICAL INFRASTRUCTURE

SOS NETWORK SECURITY

DHS HACKING ATTEMPTS

NATIONAL REACTION

MOVING FORWARD

DHS HACKING ATTEMPTS

Timeline

Jan 11 – US Rep Jason Chaffetz and US Rep Jody Hice send a joint letter to Jon Roth, Inspector General for the Department of Homeland Security asking for an independent federal investigation into the attack against Georgia's system.

Jan 24 – Secretary Kemp received the first communication from DHS OIG office requesting documents related to their investigation.

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
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 *hours* 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."

GEORGIA
SECRETARY OF STATE
BRIAN P. KEMP

INTRODUCTION

CRITICAL INFRASTRUCTURE

SOS NETWORK SECURITY

DHS HACKING ATTEMPTS

NATIONAL REACTION

MOVING FORWARD

MOVING FORWARD

Takeaways

1. Secretary Kemp as well as many other bipartisan elections officials oppose the designation of elections systems as a Critical Infrastructure Sector. They have called on President Trump for the designation to be repealed.

2. DHS attempted, but did not gain access to Georgia's Secretary of State Network which contains the Georgia Voter Registration database.

3. The security measures the SOS office has in place worked. No penetration was successful against our system.

4. DHS has still not provided clear answers regarding the attack, and we are grateful for Congress' leadership through Rep. Jason Chaffetz and Rep. Jody Hice for calling on an independent investigation into DHS actions.

5. Voters can have confidence that the voting system was not affected through any of this activity.

GEORGIA
SECRETARY OF STATE
BRIAN P. KEMP

INTRODUCTION

CRITICAL INFRASTRUCTURE

SOS NETWORK SECURITY

DHS HACKING ATTEMPTS

NATIONAL REACTION

MOVING FORWARD

MOVING FORWARD

1. Open Investigation into DHS Attacks on Georgia's System

2. Trump consideration of rescinding Critical Infrastructure designation

3. Public outcry from elected leaders across the country.

GEORGIA
SECRETARY OF STATE
BRIAN P. KEMP

INTRODUCTION

CRITICAL INFRASTRUCTURE

SOS NETWORK SECURITY

DHS HACKING ATTEMPTS

NATIONAL REACTION

MOVING FORWARD

MOVING FORWARD

Questions?