

Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<http://oversight.house.gov>

January 11, 2017

The Honorable John Roth
Inspector General
U.S. Department of Homeland Security
245 Murray Lane SW
Washington, D.C. 20528

Dear Mr. Roth:

Last month, Georgia Secretary of State Brian Kemp wrote a letter to Secretary of Homeland Security Jeh Johnson, in which he identified an “unsuccessful attempt to penetrate the Georgia Secretary of State’s firewall” originating from a DHS-registered IP address.¹ A subsequent letter from Secretary Kemp to the President-Elect identified nine additional but “less intrusive scans” dating back to February 2, 2016.² Each incident occurred at or near the time of an event in the Georgia elections process, including on November 8, 2016, the day of the general election. Another similar incident occurred on the morning of September 28, 2016, shortly before Secretary Kemp testified on election cybersecurity before the Committee.³

These allegations raise serious concerns. While the exact nature of the scans is not made clear in the letters, scanning generally refers to a category of techniques used—by good and bad actors alike—to assess computers for security weaknesses. Network administrators scan their own computers to test their security while malicious actors scan others’ systems as an initial step in a cyber-attack.⁴ Although the types of scans vary, as do their levels of intrusiveness, a common type of scan called a “port scan” is often described as the “electronic equivalent of rattling doorknobs” to see if they are unlocked.⁵

¹ Letter from Brian P. Kemp, Sec’y of State, Georgia, to Jeh C. Johnson, Sec’y of Homeland Sec., U.S. Dep’t of Homeland Sec. (Dec. 8, 2016); AM. REGISTRY FOR INTERNET NOS., WHOIS-RWS Search of [REDACTED] [https://whois.arin.net/rest/net/NET-216-81-80-0-1/pft?s=\[REDACTED\]](https://whois.arin.net/rest/net/NET-216-81-80-0-1/pft?s=[REDACTED]) (registered May 7, 2008).

² Letter from Brian P. Kemp, Sec’y of State, Georgia, to Jeh C. Johnson, Sec’y of Homeland Sec., U.S. Dep’t of Homeland Sec. (Dec. 13, 2016).

³ *Id.*; *Cybersecurity: Ensuring the Integrity of the Ballot Box: Hearing before the Subcomm. on Information Technology of the H. Comm. on Oversight & Gov’t Reform*, 114th Cong. (2016).

⁴ *E.g.*, *United States v. Phillips*, 477 F.3d 215, 217 (5th Cir. 2007).

⁵ *E.g.*, *id.*; Briefing (telephonic) to Congress by Dr. Andy Ozment, Ass’t Sec’y for Cybersecurity & Commc’ns, Dep’t of Homeland Sec. (Dec. 9, 2016); *see also* INTERNET ENGINEERING TASK FORCE, INTERNET SECURITY GLOSSARY, <https://tools.ietf.org/html/rfc4949> (2d ed. 2007).

If these allegations are true, they implicate state sovereignty and various other constitutional issues, as well as federal and state criminal laws.⁶ The Department was not authorized to scan or conduct penetration testing or otherwise “rattle doorknobs” on the Georgia Secretary of State’s network in any way.⁷ The unanswered question then, is whether DHS scanned the Secretary of State’s network anyways.

On December 12, 2016, Secretary Johnson responded to the Secretary of State’s letter, in an attempt to answer that question. In his response, Secretary Johnson explained the incident identified in Secretary Kemp’s first letter was “normal . . . interaction” by a DHS contractor with the Georgia Secretary of State’s website.⁸ His response was unequivocal that “there was no scanning” or security assessment of the Secretary of State’s network by DHS’s cybersecurity experts.⁹ The Department traced the activity back to a contractor at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia, who was engaged in verifying professional licenses of prospective armed guards for the Center.¹⁰ The Georgia Secretary of State Professional Licensing Boards Division operates a publicly accessible website for the purpose of verifying professional licenses.¹¹ According to DHS, the FLETC contractor accessed the Georgia Secretary of State’s website for the purpose of verifying individuals’ professional licenses but used a less common but still legitimate method of doing so called HTTP OPTIONS.¹² The use of HTTP OPTIONS, DHS told us, triggered false positives for suspicious activity on the Georgia Secretary of State’s servers.¹³

However, in Secretary Johnson’s one-page response and his staff’s telephonic briefings, DHS did not provide adequate information to verify or validate any of those statements. Indeed, the Secretary acknowledged in the letter that those were “initial findings” and that his letter was an “interim response . . . subject to change.”¹⁴ We also question the Department’s ability to remain neutral in investigating its own potential misconduct and think an independent investigation of these incidents is warranted.

⁶ *E.g.*, 18 U.S.C. § 1030 (the Computer Fraud and Abuse Act of 1986); GA. CODE ANN. § 16-9-93 (Georgia Computer Systems Protection Act). *But see* Moulton v. VC3 (N.D. Ga. 2000) (holding that a port scan did not rise to the level of “impairment to the integrity or availability of the network” required under 18 USC 1030(e)(8)).

⁷ Letter from Brian P. Kemp to Jeh C. Johnson (Dec. 8, 2016), *supra* note 1.

⁸ Letter from Jeh C. Johnson, Sec’y of Homeland Sec., U.S. Dep’t of Homeland Sec. to Brian P. Kemp, Sec’y of State, Georgia (Dec. 12, 2016).

⁹ Letter from Jeh C. Johnson to Brian P. Kemp (Dec. 12, 2016), *supra* note 5 (emphasis in original).

¹⁰ *Id.* The Federal Law Enforcement Training Center (FLETC) is organizationally located within the Department of Homeland Security. Its mission is to train those who protect the homeland by providing career-long training to federal, state, and local law enforcement officials. *See, e.g.*, FED. LAW ENF’T TRAINING CTR., LEARN ABOUT FLETC, <https://www.fletc.gov/learn-about-fletc> (last accessed Jan. 4, 2017).

¹¹ GEORGIA SECRETARY OF STATE, PROFESSIONAL LICENSING, <http://verify.sos.ga.gov/verification/> (last accessed Jan. 4, 2017).

¹² Briefing by Dr. Andy Ozment, Ass’t Sec’y for Cybersecurity & Commc’ns, Dep’t of Homeland Sec. to Congress (Dec. 12, 2016); Briefing by Dep’t of Homeland Sec. to Congress (Dec. 16, 2016); Email from Dep’t of Homeland Sec. to Congress (Dec. 16, 2016, 4:46 PM ET)

¹³ Briefing by Dr. Andy Ozment to Congress, *supra* note 12; Email from Dep’t of Homeland Sec. to Congress, *supra* note 12.

¹⁴ Letter from Jeh C. Johnson to Brian P. Kemp (Dec. 12, 2016), *supra* note 5.

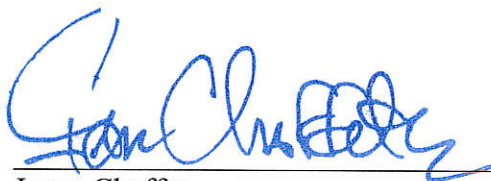
Therefore, we request you investigate Secretary Kemp's allegations that the Department of Homeland Security (DHS) conducted unauthorized scans of his office's computer network. We request that your investigation include a re-creation, subject to Secretary Kemp's permission, of the FLETC contractor's searches to determine whether Secretary Johnson's statements adequately explain the ten incidents Secretary Kemp identified in his letter of December 13, 2016, to the President-Elect. Additionally, we request that to the best of your ability you determine the answers to the following questions, initially posed by Secretary Kemp in his letter of December 8, 2016:

1. Did the Department conduct an unauthorized scan of the Georgia Secretary of State's computer network(s)?
2. If so, who authorized the scan(s)?
3. Has the Department conducted an unauthorized scan(s) of any other state's systems?
4. If so, which states did DHS scan without authorization?

In furtherance of our request, we have enclosed copies of the four letters cited in this letter: the initial letter Secretary Kemp sent to Secretary Johnson on December 8, 2016; Secretary Johnson's response on December 12, 2016; and two subsequent letters from Secretary Kemp on December 13, 2016—one to the President-Elect and the second to Secretary Johnson. In addition, we have enclosed a copy of a relevant email from DHS to our staff.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and may at "any time" investigate "any matter" as set forth in House Rule X.

Please have your staff contact Liam McKenna of Chairman Chaffetz' staff at (202) 225-5074 with any questions about this request. Thank you for your attention to this matter.



Jason Chaffetz
Chairman

Sincerely,



Jody B. Hice
Member of Congress

Enclosures (5)

cc: The Honorable Elijah E. Cummings, Ranking Minority Member
The Honorable Jeh C. Johnson, Secretary of Homeland Security
The Honorable Brian P. Kemp, Secretary of State of Georgia



The Office of Secretary of State

Brian P. Kemp
SECRETARY OF STATE

December 8, 2016

The Honorable Jeh Johnson
Secretary of Homeland Security
Department of Homeland Security
Washington, D.C. 20528

Secretary Johnson,

On November 15, 2016, an IP address associated with the Department of Homeland Security made an unsuccessful attempt to penetrate the Georgia Secretary of State's firewall. I am writing you to ask whether DHS was aware of this attempt and, if so, why DHS was attempting to breach our firewall.

The private-sector security provider that monitors the agency's firewall detected a large unblocked scan event on November 15 at 8:43 AM. The event was an IP address (██████████) attempting to scan certain aspects of the Georgia Secretary of State's infrastructure. The attempt to breach our system was unsuccessful.

At no time has my office agreed to or permitted DHS to conduct penetration testing or security scans of our network. Moreover, your Department has not contacted my office since this unsuccessful incident to alert us of any security event that would require testing or scanning of our network. This is especially odd and concerning since I serve on the Election Cyber Security Working Group that your office created.

As you may know, the Georgia Secretary of State's office maintains the statewide voter registration database containing the personal information of over 6.5 million Georgians. In addition, we hold the information for over 800,000 corporate entities and over 500,000 licensed or registered professionals.

As Georgia's Secretary of State, I take cyber security very seriously. That is why I have contracted with a global leader in monitored security services to provide immediate responses to these types of threats. This firm analyzes more than 180 billion events a day globally across a 5,000+ customer base which includes many Fortune 500 companies. Clearly, this type of resource and service is necessary to protect Georgians' data against the type of event that occurred on November 15.

Georgia was one of the only few states that did not seek DHS assistance with cyber hygiene scans or penetration testing before this year's election. We declined this assistance due to having already implemented the security measures suggested by DHS. Under 18 U.S.C. § 1030, attempting to gain access or exceeding authorized access to protected computer systems is illegal. Given all these facts, a number of very important questions have been raised that deserve your attention:

1. Did your Department in fact conduct this unauthorized scan?
2. If so, who on your staff authorized this scan?
3. Did your Department conduct this type of scan against any other states' systems without authorization?
4. If so, which states were scanned by DHS without authorization?

I am very concerned by these facts provided by our security services provider, as they raise very serious questions. I would appreciate your prompt and thorough response.

Sincerely,



Brian P. Kemp

CC:

The Honorable Johnny Isakson
United States Senate

The Honorable Rob Woodall
United States House of Representatives

The Honorable David Perdue
United States Senate

The Honorable Austin Scott
United States House of Representatives

The Honorable Buddy Carter
United States House of Representatives

The Honorable Doug Collins
United States House of Representatives

The Honorable Sanford Bishop
United States House of Representatives

The Honorable Jody Hice
United States House of Representatives

The Honorable Lynn Westmoreland
United States House of Representatives

The Honorable Barry Loudermilk
United States House of Representatives

The Honorable Hank Johnson
United States House of Representatives

The Honorable Rick Allen
United States House of Representatives

The Honorable John Lewis
United States House of Representatives

The Honorable David Scott
United States House of Representatives

The Honorable Tom Price
United States House of Representatives

The Honorable Tom Graves
United States House of Representative



**Homeland
Security**

December 12, 2016

The Honorable Brian P. Kemp
Secretary of State
State of Georgia
214 State Capitol
Atlanta, GA 30334

Dear Secretary Kemp:

Thank you for your December 8, 2016 letter. Due to the publicity that your letter has generated, I wanted to respond promptly to you with initial findings.

Working with your staff, we have been able to locate, in prompt fashion, the workstation from which the activity that you highlight in your letter occurred. We have reviewed the technical logs and interviewed the user of this computer. The user is a contractor of our Federal Law Enforcement Training Center (FLETC) located in Georgia; he is not a member with our cybersecurity team. We interviewed the contractor and he told us that he accessed your website as part of his normal job duties at FLETC to determine whether incoming FLETC contractors and new employees had a certain type of professional license – a service that, as I understand it, your website provides to the general public. The technical information we have corroborates the contractor's statement, and indicates normal Microsoft Internet Explorer interaction by the contractor's computer with your website.

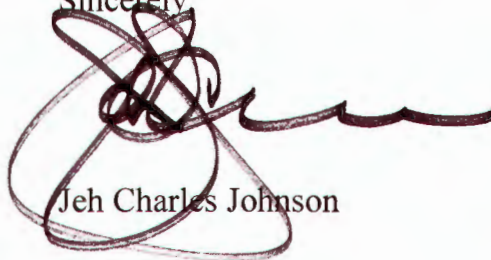
Most important: there was no scanning of your systems by our cybersecurity experts. As stated before, the contractor using your website is not one of our cybersecurity experts, nor were these inquiries made for the purpose of assessing or determining the security of your website. As we have explained to you and other state election officials, when DHS conducts a cybersecurity scan of a network or system, we do so only with the cooperation and consent of the system owner.

The Honorable Brian P. Kemp

Page 2

This is an interim response to your inquiry, subject to change. Given the publicity around your inquiry, I wanted to provide this response as soon as possible. We look forward to continue working with you and your team on this matter.

Sincerely,

A handwritten signature in dark ink, appearing to read 'Jeh Charles Johnson'. The signature is highly stylized and somewhat illegible due to its cursive nature and overlapping loops.

Jeh Charles Johnson

cc:

The Honorable Johnny Isakson
United States Senate

The Honorable Rob Woodall
United States House of Representatives

The Honorable David Perdue
United States Senate

The Honorable Austin Scott
United States House of Representatives

The Honorable Buddy Carter
United States House of Representatives

The Honorable Doug Collins
United States House of Representatives

The Honorable Sanford Bishop
United States House of Representatives

The Honorable Jody Hice
United States House of Representatives

The Honorable Lynn Westmoreland
United States House of Representatives

The Honorable Barry Loudermilk
United States House of Representatives

The Honorable Hank Johnson
United States House of Representatives

The Honorable Rick Allen
United States House of Representatives

The Honorable John Lewis
United States House of Representatives

The Honorable David Scott
United States House of Representatives

The Honorable Tom Price
United States House of Representatives

The Honorable Tom Graves
United States House of Representative



The Office of Secretary of State

Brian P. Kemp
SECRETARY OF STATE

December 13, 2016

The Honorable Jeh Johnson
Secretary of Homeland Security
Department of Homeland Security
Washington, D.C. 20528

Secretary Johnson,

I am in receipt of your letter dated December 12, 2016. I understand that you have general information supporting the claim that this was an issue with a Microsoft product; however, the scenario that DHS proposed has still not been verified by Microsoft. There are still many questions regarding the origin and intent of this attack that remain unanswered.

In order to ensure this issue receives the attention it deserves, I will be elevating my concerns to the incoming administration.

Sincerely,

Brian P. Kemp



The Office of Secretary of State

Brian P. Kemp
SECRETARY OF STATE

December 13, 2016

President-Elect Donald J. Trump
725 Fifth Avenue
New York, NY 10022

Dear President-Elect Trump,

I respectfully write today to request that you task your new Secretary of Homeland Security with investigating the failed cyber-attacks against the Georgia Secretary of State's network firewall.

In my letter dated December 8, 2016 to current DHS Secretary Jeh Johnson, I detailed a large attack on our system from November 15, 2016 that traced back to an IP address associated with the Department of Homeland Security.

In addition to this event, my staff has uncovered further instances in 2016 when IP addresses connected to DHS attempted to infiltrate our network. These events were less intrusive scans that did not raise as many red flags. However, the timing is very concerning as these scans correspond to key election dates and times when I was speaking out against DHS' plans to designate elections systems as "critical infrastructure."

The dates in question include the day I testified against DHS' position before the House Oversight Committee; the day of a conference call discussing the designation of Critical Infrastructure with Georgia officials; and several other key election dates, including Election Day. An outline of these attacks are attached to this letter.

Since contacting DHS with these concerns, we have collaborated with the agency and provided extensive, additional information. Last night I received a letter from Secretary Johnson which lacked any specific information as to the attacks' intent or origin despite the fact that many questions remain unanswered.

The people of Georgia are very concerned about what exactly happened here, and they are demanding transparent and honest answers. It appears that will not happen with the current administration. Given that we are a few weeks away from the transition, I write to ask for your help in providing those answers when you assume the Presidency later next month.

Sincerely,

A handwritten signature in blue ink that reads "B.P.K." with a stylized flourish at the end.

Brian P. Kemp

CC:

General John Kelly
Secretary of Homeland Security Designate

The Honorable Johnny Isakson
United States Senate

The Honorable David Perdue
United States Senate

The Honorable Buddy Carter
United States House of Representatives

The Honorable Sanford Bishop
United States House of Representatives

The Honorable Lynn Westmoreland
United States House of Representatives

The Honorable Hank Johnson
United States House of Representatives

The Honorable John Lewis
United States House of Representatives

The Honorable Tom Price
United States House of Representatives

The Honorable Rob Woodall
United States House of Representatives

The Honorable Austin Scott
United States House of Representatives

The Honorable Doug Collins
United States House of Representatives

The Honorable Jody Hice
United States House of Representatives

The Honorable Barry Loudermilk
United States House of Representatives

The Honorable Rick Allen
United States House of Representatives

The Honorable David Scott
United States House of Representatives

The Honorable Tom Graves
United States House of Representative

SCANNING ACTIVITIES FROM 2016

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.
Wednesday	Sep. 28, 2016	07:54 CDT	This scan was conducted just <i>hours</i> before my 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 my 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 my Congressional testimony opposing the designation of elections systems as critical infrastructure.
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.

McKenna, Liam

From: [REDACTED]
Sent: Friday, December 16, 2016 4:46 PM
Cc: [REDACTED]
Subject: Georgia Call Follow-Up

The information below responds to several questions raised during today's call.

First, regarding ports, all of the web traffic sent to the GA SOS websites was sent via ports 80 and 443, which are used for normal web traffic. Second, during the call we discussed the "HTTP OPTIONS" command. Specifically, a DHS contractor visited the GA SOS website as part of his normal duties to obtain the armed security guard license numbers for his armed security guards. When viewing the website on November 15, he used the "copy and paste special" function to copy the license number from the website to a spreadsheet he maintains. Software vendor engineers confirm that doing the "copy and paste special" function sends an "HTTP OPTIONS" command to the website. The "HTTP OPTIONS" command asks the website what functions it can perform. Essentially, "HTTP OPTIONS" is asking the website "will you allow me to do this?" before it does what the user has asked. Based on documents provided to DHS by the GA SOS, their managed service provider automatically generated a "medium priority" ticket as a result of detecting the "HTTP OPTIONS" command and categorized it as "possible scanning activity." While the "HTTP OPTIONS" command is one of many techniques that could be used to scan for a vulnerability, that was not the way it was used in this case. A review of DHS-generated web traffic shows that DHS sends over 4,800 "HTTP OPTIONS" command during a typical business day. Counterparts at other federal agencies also observe their departments generating "HTTP OPTIONS" commands.

I hope this information is helpful to answering the questions raised during today's call. Have a good weekend,

[REDACTED]
Legislative Affairs
Department of Homeland Security

[REDACTED]



National Security Archive,
Suite 701, Gelman Library, The George Washington University,
2130 H Street, NW, Washington, D.C., 20037,
Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu