OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

FOR IMMEDIATE RELEASE
Wednesday, July 5, 2017

For Information Contact:
Public Affairs (202) 254-4100

Allegations of Unauthorized Scans of Georgia Voting Systems are Unsubstantiated

A forensic investigation by the Office of Inspector has determined Department of Homeland Security (DHS) employees did not conduct unauthorized scans of Georgia's elections computer systems. The investigation was requested by Congress based on concerns raised by Georgia Secretary of State Brian Kemp, who cited 10 suspected attempts by DHS personnel to penetrate the state's firewall in 2016.

In a letter to Rep. Trey Gowdy, Chairman of the House Committee on Oversight and Government Reform, and Rep. Jody Hice, Inspector General John Roth reported that DHS employee interactions with the Georgia systems were limited to routine searches for publically available information on the state's public website and that none of the web pages visited were related to elections or voters.

The investigation was conducted by employees in OIG's specially trained Digital Forensics and Analysis Unit.

###

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

June 26, 2017

The Honorable Trey Gowdy, Chairman
Committee on Oversight and Government Reform
U.S. House of Representatives
2157 Rayburn House Office Building
Washington, DC 20515

The Honorable Jody Hice
U.S. House of Representatives
324 Cannon House Office Building
Washington, DC 20515

Dear Chairman Gowdy and Congressman Hice:

On January 11, 2017, then-Chairman Chaffetz and Congressman Hice wrote to me requesting an investigation into whether the Department of Homeland Security (DHS) conducted unauthorized scans of the Georgia Secretary of State's and other states' computer networks. Your request enclosed a letter from Georgia Secretary of State Brian Kemp to then-President-Elect Trump. In this letter, Secretary Kemp identified ten suspected attempts coming from DHS IP addresses to infiltrate his network, including "a large attack" on November 15, 2016, and nine additional "less intrusive scans." According to Secretary Kemp, the dates of these attempts coincided with events in the Georgia election process, including on Election Day itself.

We have recently completed our investigation into these allegations and have determined that the activity Georgia noted on its computer networks was the result of normal and automatic computer message exchanges generated by the Microsoft applications involved. Our investigation was conducted by the Office of Inspector General Digital Forensics and Analysis Unit, a specially recruited and trained unit within our Office of Investigations, who use industry-recognized forensic tools and training to analyze digital systems for proactive investigative or reactive forensic purposes. We conducted our investigation independently of DHS and in accordance with the *Quality Standards for Investigations* (November 2011), issued by the Council of the Inspectors

General on Integrity and Efficiency. While DHS received the results of our investigation, they had no input into our investigative conclusions.

We obtained and reviewed computer data from DHS and from Secretary Kemp's office, reviewed the findings of Microsoft engineers who had previously looked into this issue, interviewed the individual whose activity triggered the November 15th incident, and conducted our own simulated recreation of what that individual told us he did on Georgia's website. Based on this work, we did not substantiate the allegations that DHS attempted to scan or infiltrate the Georgia computer networks. Rather, the evidence demonstrated normal and appropriate use of Georgia's public website.

Our examination of DHS computer logs identified a contractor at the Federal Law Enforcement Training Center (FLETC) as the individual who accessed the Georgia website on November 15, 2016. We interviewed that contractor, who told us that he used the site to verify firearms certification license information for FLETC security guards, and that he copied and pasted that information into a Microsoft Excel spreadsheet.

Georgia's and DHS's computer logs both independently corroborated what the FLETC contractor told us. First, both logs showed that the website that was accessed at the particular time on November 15th was a page where public users can search the current licensing status for individuals. Second, both logs showed that the DHS computer automatically sent an "HTTP OPTIONS request" at that time. According to Microsoft, "this is a fairly typical request of Microsoft Office Applications to check web server compatibility" and is generated, for example, when data is copied from a website and pasted into an Excel spreadsheet. We tested this by searching licensing information on other states' websites and pasting the information into a spreadsheet. Each time we did that, we were able to determine from reviewing network traffic that an HTTP OPTIONS request was automatically sent.

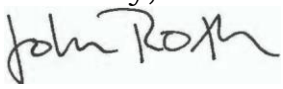
The available data for the other nine incidents reported by Secretary Kemp indicate the same normal and appropriate use of Georgia's website. In each case, an HTTP OPTIONS request was sent when a DHS computer accessed and searched a public records database on Georgia's website. None of the Georgia webpages accessed were related to elections or voters.

We also reviewed the architecture of the DHS web proxies through which the DHS users accessed the Georgia website. Web proxies are essentially intermediaries between a computer user and the website he or she is trying to access. DHS's web proxies are configured to ensure its users appropriately access the internet consistent with DHS's acceptable-use policies, and would not allow users to conduct port scanning or similar attacks on Georgia's systems. In other words, it simply would not have been possible for the DHS users to attack Georgia's systems from these DHS IP addresses.

A number of other states had previously suspected similar DHS attacks. We understand that DHS, in conjunction with the National Association of Secretaries of State, determined that the web traffic on those states' websites was entirely normal and non-malicious, and that those states did not question this finding. Because this was consistent with our findings related to Georgia, we did not actively investigate the DHS traffic on those other sites.

Please call me with any questions, or your staff may contact Erica Paulson, Assistant Inspector General for External Affairs, at (202) 254-4100.

Sincerely,



John Roth
Inspector General

cc: The Honorable Elijah E. Cummings, Ranking Member
Committee on Oversight and Government Reform
The Honorable John F. Kelly, Secretary of Homeland Security
The Honorable Brian P. Kemp, Secretary of State of Georgia