National Association of Secretaries of State

March 20, 2017

BRIEFING: Key Facts and Findings on Cybersecurity and Foreign Targeting of the 2016 U.S. Elections

As Congress examines the impact of Russian involvement in the November 2016 election, it is important to provide the clearest and most accurate public record possible regarding election cybersecurity and foreign targeting of U.S. election infrastructure. The following findings are based on all unclassified documentation and evidence available to the National Association of Secretaries of State (NASS):

1 The November 2016 election was NOT HACKED.

The voting process was not hacked or subject to manipulation in any way. No credible evidence of hacking, including attempted hacking of voting machines or vote counting, was ever presented or discovered in any state, including during recount efforts that took place after the election.[1] A joint DHS-DNI report details the foreign cyberattacks that took place against U.S. government, political and private sector entities that were attributed to Russia.[2] Election officials remain concerned by unfounded conjecture that a lack of such tangible evidence indicates that hacking might have been overlooked or hidden from discovery, despite collaborative efforts with our intelligence services, cybersecurity firms, network defenders and state and local officials.

2 Russian intrusions into state and local election boards in 2016 were limited to TWO INCIDENTS that did not involve systems used in vote tallying.

The U.S. Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS), along with state officials, are aware of two confirmed intrusions into government-owned voter registration databases that took place in summer 2016.[3] The FBI has confirmed that foreign-based hackers attempted to mine data from voter registration systems in Arizona and Illinois, but no voter registration data was modified or deleted.[4] In Arizona, a hacker attempted to probe voter registration data via a county-level infiltration, but was blocked from doing so by the system's controls. In Illinois, hackers were able to access publicly-available voter files. These incidents prompted the FBI to warn state election offices to increase their election security measures for the November 2016 election.[5]

3 Additional state voter registration systems were targeted by cyber hackers, but NO ADDITIONAL SYSTEMS were accessed or breached.

U.S. intelligence agencies have confirmed that Russian-based "cyber scanning or probing activities" were discovered against state voter registration systems, but this targeting does not equate to gaining

[1] Sanger, David E. "Obama Strikes Back at Russia for Election Hacking," The New York Times, December 29, 2016. Additional unclassified documents provided by DHS to NASS also support this finding in writing, as does the ODNI Joint Intelligence report entitled, "Assessing Russian Activities and Intentions in Recent U.S. Elections, released on January 6, 2017, pg. 3.
[2] Joint Statement from the U.S. Department of Homeland Security and Office of the Director of National Intelligence on Election Security, October 7, 2016. See also Joint Analysis Report (JAR) on GRIZZLY STEPPE – Russian Malicious Cyber Activity, December 29, 2016.
[3] Hearing Transcript. Committee on the Judiciary, U.S. House of Representatives. *September 28, 2016.* 114th Cong. 2nd session.
[4] Federal Bureau of Investigation Flash Alert, "Targeting Activity Against State Board of Election Systems," August 18, 2016.
[5] Ibid.

(Continued from Page 1)

access or actual breaches.[6] Claims that twenty or more states experienced Russian-led hacks or intrusions into their election systems are false and inaccurate.[7] Furthermore, while it is theoretically possible to disrupt an election via networked systems, compromising voter registration systems would not affect election results. Election registration databases are not linked to vote counting.

4 Just OVER HALF of all states took advantage of voluntary cybersecurity assistance provided by the U.S. Department of Homeland Security.

The U.S. Department of Homeland Security confirmed to NASS that 33 states and 36 county jurisdictions had taken advantage of the agency's voluntary assistance and services by Election Day on November 8, 2016.[8] NASS and DHS also achieved a joint goal of ensuring that all 50 states were notified of the federal government resources that were available to them upon request. DHS services included cyber hygiene scans on Internet-facing systems, risk and vulnerability assessments and resources identifying recommendations to improve online voter registration systems, election night reporting systems and other Internet-connected systems. Those states that did not seek to utilize DHS assistance received similar or more comprehensive support from their own state networks.

5 Our highly-decentralized, low-connectivity elections process provides BUILT-IN SAFEGUARDS against large-scale cyberattacks; however, states are strengthening their systems for future elections.

Our national intelligence agencies concurred with secretaries of state in concluding that our diverse and locally–run election process presents serious obstacles to carrying out large-scale cyberattacks to disrupt elections, and that standalone, disconnected voting systems present a low risk.[9] States are now working together to reinforce their preparedness against future cyber threats, most notably by replacing aging voting equipment. To assist in these efforts, the NASS Election Cybersecurity Task Force will advance collaboration on the unique priorities and challenges that exist regarding election cybersecurity. NASS is also supportive of a thorough accounting and resolution of documented instances of unauthorized scanning against several states' election networks that has been attributed to IP addresses utilized by the U.S. Department of Homeland Security.[10]

ABOUT NASS: Founded in 1904, the National Association of Secretaries of State (NASS) is the nation's oldest, nonpartisan professional organization of public officials in the U.S. Forty NASS members serve as their state's designated chief election official, overseeing the conduct of elections according to law. Ensuring the integrity of the voting process is central to this role, which includes cyber preparedness and contingency planning, as well as administrative and technical support for local election officials. Learn more by visiting our election cybersecurity initiatives page at: www.nass.org.

---

[6] Testimony by James Comey, Director of the FBI. Committee on the Judiciary, U.S. House of Representatives. *Hearing, September 28, 2016.* 114th Cong. 2nd sess. Print. Pg. 63.
[7] Information provided to NASS by the U.S. Department of Homeland Security. September 30, 2016.
[8] Information provided to NASS by the U.S. Department of Homeland Security. December 5, 2016
[9] Statement by Secretary Johnson Concerning the Cybersecurity of the Nation's Election Systems, U.S. Department of Homeland Security. September 16, 2016.
[10] Letter from DHS Inspector General John Roth to Georgia Secretary of State Brian Kemp. January 17, 2017.

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