The Office of Secretary of State

Brian P. Kemp
SECRETARY OF STATE

TESTIMONY OF GEORGIA SECRETARY OF STATE BRIAN KEMP BEFORE THE HOUSE COMMITTEE ON GOVERNMENT OVERSIGHT,

INFORMATION TECHNOLOGY SUBCOMMITTEE

Will Hurd, Chairman (R-TX)

September 28, 2016

Good afternoon. I would like to thank the Committee and Chairman Hurd for inviting me to discuss election security, the safeguards on our elections, and my perspective as the top election official in Georgia, the eighth largest state in our union.

As Georgia's Secretary of State, I currently serve as co-chair of the National Association of Secretaries of State Elections Committee, and within the last three weeks, I have agreed to serve on the Department of Homeland Security's Election Infrastructure Cyber Security Working Group, organized by Secretary Jeh Johnson.

Recent events including the hack of the DNC database, as well as successful cyber-attacks against voter registration databases in Arizona and Illinois, have rightfully caused great alarm among the public as well as election officials; however, it is imperative that we as a nation respond the correct way to these attacks.

Administering elections is a great, but unique responsibility. The foundation of our Republic rests on the trust that Americans have in the way we elect representatives in our government. If that trust is eroded, our enemies know that will create fissures in the bedrock of American democracy. We cannot allow this to happen.

The D.C. response to these attacks has been to take steps towards federalizing aspects of elections, election systems, and standardizing security measures. There is a better way to face these attacks and future potential threats than what has currently been proposed by DHS with designating elections systems critical infrastructure.

POTENTIAL THREATS AND SECURITY SAFEGUARDS

In discussing election security, it is important to understand the difference between the components of the election system. This system is actually comprised of campaign systems, registration and reporting systems, as well as voting systems.

Campaign systems are databases not held by the states, such as the databases held by national parties. Attacks on these systems do not disrupt activities within the states' jurisdiction, although they can cause harm, as seen recently by the attack on the DNC.

Registration and reporting systems are held by the states, but they do not impact the true canvassed results of an election. These systems manage the voter registration rolls and report unofficial results on election night. Although these systems are more prone to attack than the voting system because many are web-based platforms, attacks on these systems cannot change votes that are cast. These systems are also tested regularly, have redundancies, fail-safes, and backups.

Finally, voting systems are the actual equipment used on Election Day. They are non-networked pieces of hardware that do not connect to the internet. They are tested by vendors, by states, and by the EAC. Even before they are deployed they are tested again by local technicians to ensure their security and accuracy.

In looking toward November, it is important for us to address the types of threats that may come against the nation's elections. I view the threats in three different categories.

First, there are threats that undermine the confidence in the outcome of the election. This has already started among conspiracy theorists, campaigns, and members of the media. Just last week Senator Dianne Feinstein of California accused Russia of "making a serious and concerted effort to influence the U.S. election." This narrative will likely continue through canvassing and beyond. Although election officials must be cognizant of these narratives and respond to them as needed, this threat cannot create actual harm to the system or the results of the election.

Second, there are threats that disrupt elections. These threats could be cyber-attacks on web-based systems, but they more commonly occur with threats of physical violence, verbal altercations, or misinformation distributed at polling locations. In my view this is far more likely to occur than a coordinated hacking of each individual voting unit in the United States. This type of threat is also not only more probable to occur, but would also have a far greater chilling effect on election participation.

The third type of threat is altering the outcome of the election. This requires an attack on the voting system itself. However, the voting system is layered with combinations of physical and technical security to address these concerns. The voting system is the most secure system in the election space. It is not networked. It is not on the internet. It is tested many times in many different ways. It has overlapping physical security features to defeat cyber-attacks and physical attacks. This threat requires far too much coordination, planning, and ability to physically manipulate thousands of machines at thousands of locations across the United States. Although it is possible, it is not probable and there is no evidence that it has ever occurred in a U.S. election.

Appropriate Federal Government Response

As I stated a moment ago, DHS Secretary Jeh Johnson responded to this threat of cyber-attack when he publicly began considering designating the election system "Critical Infrastructure." This suggestion caught many elections officials by surprise and rightfully so. The administration of elections is a state responsibility. Moreover, this suggestion came from an agency completely unfamiliar with the elections space and raised the level of public concern beyond what was necessary. This decision has been criticized by election officials and cyber-security experts alike.

DHS has yet to outline any practical benefits or make any compelling arguments on why this designation is necessary. I agree with EAC Commissioner Christy McCormick that this designation may be the first step towards creating a new federal security standard that could create legal liabilities for states. In addition, this action may open up state databases to the federal government as well as create new avenues where previously protected documents and information may become accessible to the general public, ultimately undermining the security of our elections.

I encourage the Federal government to respect the Constitutional lines our founders created, leaving the administration of elections to the states. This arrangement, as noted by the FBI as well as the White House, makes cyber-attacks and vote tampering far more difficult as election systems are decentralized among 9000 election jurisdictions. There are certainly ways for the federal government to provide assistance while working within this framework.

For instance, best practices, cyber security research, as well certain types of cyber tools provided by DHS can be useful in election preparation. Likewise, it is useful for states to receive security bulletins from federal agencies about known or potential attacks to safely guard their systems. These limited measures are useful and beneficial as they do not compel state officials, but allow them to make informed decisions about the best interest of their state.

The risks posed by foreign government hackers, cyber criminals and everyday hacktivists are not a new concept for election officials. In fact, states are always evaluating and adapting security measures to protect the integrity of our elections as part of emergency preparedness planning.

I think I speak for all state elections officials when I say we are committed to working with national security agencies and regular federal partners to solicit input on cyber threat response and risk mitigation in our elections. However, designating voting systems or any other election system as critical infrastructure would be a federal overreach, the cost of which would not equally improve the security of elections in the United States.

Looking Towards November and Beyond

Please keep in mind that timing is critical right now. Elections are not one-day events. Ballots have been printed, and many ballots have already been mailed to voters. Early in-person voting will begin in the next couple weeks, if not days in some states.

This is an important time for elections officials to finalize preparations for November. It is not the time for inexperienced federal agencies to guess at changes that should be made. Therefore I encourage you, as policy-makers, to listen to your Secretaries of State and elections officials.

Our elections are secure, and we are working around the clock to ensure they stay that way. We are open to federal assistance, but not in designating the elections system critical infrastructure. Uncertainty, fear mongering, and empty rhetoric during this critical time can damage Americans' trust in the election process and undermine the vote we will have in November.

Elections are the cornerstone of our republic, and defending them is an honor and a duty that I and my colleagues take very seriously. We will continue working with law enforcement agencies and stakeholders to prevent attacks on our system while preparing for November and ensuring every American has a voice in electing our nation's leaders as well as the next President of the United States.

Thank you for the opportunity to provide comment.

214 State Capitol • Atlanta, Georgia • 30334 • (404) 656-2881 • (404) 656-0513 Fax
www.sos.ga.gov

Secretary Kemp's Bio:

Georgia Secretary of State Brian Kemp has served as Secretary of State since 2010. The Secretary of State is responsible for the administration of secure, accessible, and fair elections; registration of corporations; regulation of securities, and oversight of professional license holders.

Secretary Kemp has implemented many e-government solutions while in office. He has also worked to communicate more efficiently with Georgia's businesses, promote voter registration, cut bureaucratic red tape, reduce costs on Georgia taxpayers, and deter corporate identity theft.

As Georgia's top elections official, Secretary Kemp works to ensure all eligible citizens have access to the polls. In March of 2014, Secretary Kemp announced Georgia's first Online Voter Registration System (OLVR). Georgians can easily access OLVR by either downloading the app "GA Votes" or visiting the website of the Secretary of State Elections Division.

Secretary Kemp has also been instrumental in moving Georgia to the forefront in the presidential nomination process. Working with his colleagues in Alabama, Arkansas, Oklahoma, Tennessee, Texas, and Virginia, Kemp lead the movement to hold a regional presidential preference primary on March 1, 2016. This date, now dubbed the "SEC Primary," is the largest regional primary since 1992 and is bringing the road to the White House through America's new heartland – the South.

Secretary Kemp was elected to the Georgia Senate in 2002 and served until 2006. During that time, he served as chair of the Public Safety and Homeland Security Committee and vice-chair of the Higher Education Committee. During his professional career, Secretary Kemp has founded and developed many small businesses. He remains an active small business owner today with companies involved in agribusiness, financial services, and real estate management and investment.

Secretary Kemp is a lifelong resident of Athens and a graduate of Clarke Central High School. He earned his Bachelor of Science degree in Agriculture from the University of Georgia. He is married to the former Marty Argo of Athens and they are proud parents of three daughters. The Kemps are actively involved in school activities, charities, and are members of Emmanuel Episcopal Church in Athens.