Testimony on Election Security by the Hon. Tom Schedler, Louisiana Secretary of State

Thank you. I'm here today to talk about the security of the elections process from my perspective as Louisiana Secretary of State and past president of the National Association of Secretaries of State, which represents a majority of the nation's chief state election officials.

First, let me thank the Committee and Chairman Smith for the invitation to participate. It's important for you to hear directly from the authorities who oversee elections in this country. Our job is to make voting easy and cheating hard.

In light of recent events, including reports that parties tied to Russia may be behind recent efforts to mine data from voter registration systems in at least two states, the message is clear: We are now on high alert against foreign cyber threats that may be trying to impact our elections. States and localities must remain vigilant and take every necessary precaution to secure our election and voting systems against credible threats.

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. States are already deploying numerous resources for this cycle, including extensive testing for cyber threats described in a recent FBI alert. Additional steps may be taken based upon credible or specific threats that are identified in the run-up to Election Day. Secretaries of State are also taking part in a Department of Homeland Security Election Infrastructure Cybersecurity Working Group, created for sharing resources, best practices and technical advice.

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. As we speak, local officials in Louisiana are moving approximately thirty precincts in the wake of the historic flooding that inundated the Baton Rouge area in August.

Just as we must have contingency plans for floods and all kinds of natural phenomena, we must also be ready to deal with man-made threats. As we collaborate on appropriate steps to be taken, there are several key points that I want to share with you.

Our System Has Built-In Safeguards Against Systemic Fraud

For starters, we must ensure that actions to protect our elections do not create UNDUE alarm that can threaten voters' confidence in election outcomes, or end up perceived as a federal power grab over the voting process.

Our system has built-in safeguards against systemic fraud. Elections are administered by states and localities, with a minimal amount of federal involvement. Voting systems are spread out in a highly-decentralized structure covering more than 9,000 election jurisdictions and hundreds of thousands of polling locations. Voting machines are standalone and not designed to connect to the Internet. There are multiple layers of physical and technical security surrounding our systems.

While no state wants to see its voter registration system breached, the targeting of such systems does not easily result in fraud or disenfranchisement. This is because non-voting components of the election process have their own fail-safes and contingency solutions that make it extremely difficult to leverage them for changing election outcomes. In fact, no voter information was found to be added or deleted in recent state voter registration system breaches.

In Louisiana, information collected through our online voter registration system does not flow directly into our statewide registration database. Instead, voter information is sent from the website to each parish (county) registrar of voters' office for verification and final processing. Poll books, printed records, back-ups, and back-ups of back-ups also provide multiple layers of security around this part of the process.

Plus, anyone who discovers an issue with their voter registration status when they show up at a polling place still has options for casting a ballot.

Identifying and Understanding Legitimate Cyber Threats

Now to the voting machines. I'm happy to report that there is no evidence that ballot manipulation has ever occurred in the U.S. as the result of a cyberattack. As I've already stated, voting systems are standalone and do not connect to the Internet. The nationwide trend has been toward the adoption of voting systems that create both paper and electronic records, a combination that makes detection easy.

Before every election, Louisiana publicly performs a "test and seal" process in which we demonstrate that each machine is working properly before it is locked with a tamper-proof seal that is not removed until election morning. This testing process is repeated at the end of each election to again demonstrate that each machine is functioning as it was designed. State laws typically require voting equipment to be physically secured when not in use.

In all states, tabulations aren't final until the completion of an official canvass to review vote counting and certify the results. Election night reporting (ENR) systems may utilize electronic transmissions of tabulated voting results for reporting purposes, but they are always unofficial numbers subject to review. In Louisiana, just like our registration database, the public website is not where results are accumulated or tallied. The unofficial results are sent to Baton Rouge from across the state on closed lines using computers that are used only for election night transmissions. They are never connected to the internet. Those results are then processed and saved before they are shared on the public site. In other words, the public site has a secure backup that includes several layers of security.

Post-election audits, which are required in roughly sixty percent of all states, can help to further safeguard against deliberate manipulation of the election, as well as unintentional software, hardware or programming problems. If necessary, the majority of states can make paper ballots and/or audits available for recount or review.

Timing is Critical to this Conversation

Finally, please keep in mind that timing is critical right now. Elections are no longer one-day events. Ballots are printed, absentee ballots are in the mail and in-person early voting is nearly ready to begin. absentee ballots are in the mail and in-person voting begins in days in some states. To say this is an inopportune time for elections officials to be discussing this topic instead of real time preparations would be an understatement. During a call with DHS Secretary Jeh Johnson in mid-August, my colleagues and I were assured that the Department of Homeland Security has no intention of declaring our election system to be part of the nation's "critical infrastructure" before the November presidential election.

Many Secretaries of State, including myself, have been very vocal in their belief that no matter when it might occur, such a designation would greatly undercut traditional state and local control of elections and serve as a major distraction in moving forward together in securing our elections.

As of today, there isn't enough clear information on what this designation would mean, or why it is necessary, given that states can get what they need through existing federal networks. For example, the U.S. Election Assistance Commission and NIST (National Institute of Standards and Technology) can provide ongoing assistance to states by identifying the kind of testing that would reveal signs of tampering that a sophisticated nation-state adversary might conduct.

There is a role for Congress as well. Most states purchased their voting machines using federal dollars supplied by the Help America Vote Act (HAVA) back in 2005, but there is little interest from the Hill when it comes to helping officials replace these aging systems. In 2010, NASS produced a funding report noting that $396 million in HAVA funding remains to be appropriated. I suggest you revisit HAVA and see how an investment in voting technology could benefit our nation for the long-term.

In the meantime, we have received a sobering wake-up call on the serious nature of international cyber threats. States will continue to take a proactive approach to securing our election systems. At the end of the day, we all want Americans to know that votes – and votes alone – will determine the next President of the United States.

Thank you for the opportunity to provide comment.