RUSSIAN TARGETING OF ELECTION INFRASTRUCTURE DURING THE 2016 ELECTION

SUMMARY OF DRAFT SSCI RECOMMENDATIONS

The Senate Select Committee on Intelligence has examined evidence of Russian attempts to target election infrastructure during the 2016 U.S. elections. The Committee has reviewed the steps state and local election officials take to ensure the integrity of our elections and agrees that U.S. election infrastructure is fundamentally resilient. The Department of Homeland Security, the Election Assistance Commission, state and local governments, and other groups have already taken beneficial steps toward addressing the vulnerabilities exposed during the 2016 election cycle, including some of the measures listed below, but more needs to be done. The Committee recommends the following steps to better defend against a hostile nation-state who may seek to undermine our democracy:

1. Reinforce States' Primacy in Running Elections

- States should remain firmly in the lead on running elections, and the Federal government should ensure they receive the necessary resources and information.

2. Build a Stronger Defense, Part I: Create Effective Deterrence

- The U.S. Government should clearly communicate to adversaries that an attack on our election infrastructure is a hostile act, and we will respond accordingly.
- The Federal government, in particular the State Department and Defense Department, should engage allies and partners to establish new international cyber norms.

3. Build a Stronger Defense, Part II: Improve Information Sharing on Threats

- The Intelligence Community should put a high priority on attributing cyber attacks both quickly and accurately. Similarly, policymakers should make plans to operate prior to attribution.
- DHS must create clear channels of communication between the Federal government and appropriate officials at the state and local levels. We recommend that state and local governments reciprocate that communication.
- Election experts, security officials, cybersecurity experts, and the media should develop a common set of precise and well-defined election security terms to improve communication.
- DHS should expedite security clearances for appropriate state and local officials.
- The Intelligence Community should work to declassify information quickly, whenever possible, to provide warning to appropriate state and local officials.

4. Build a Stronger Defense, Part III: Secure Election-Related Systems

- Cybersecurity should be a high priority for those managing election-related systems. Basic but crucial security steps like two-factor authentication for those logging into voter databases can improve the overall election security posture. States and localities should also take advantage of DHS offerings, to include DHS's network monitoring capabilities.

- The Committee recommends DHS take the following steps:
  - Working closely with election experts, develop a risk management framework that can be used in engagements with state and local election infrastructure owners to document and mitigate risks to all components of the electoral process.
  - Create voluntary guidelines on cybersecurity best practices and a public awareness campaign to promote election security awareness, working through the U.S. Election Assistance Commission (EAC), the National Association of Secretaries of State (NASS), and the National Association of State Election Directors (NASED).
  - Expand capacity to reduce wait times for DHS cybersecurity services.
  - Work with GSA to establish a list of credible private sector vendors who can provide services similar to those provided by DHS.

5. Build a Stronger Defense, Part IV: Take Steps to Secure the Vote Itself

- States should rapidly replace outdated and vulnerable voting systems. At a minimum, any machine purchased going forward should have a voter-verified paper trail and no WiFi capability. If use of paper ballots becomes more widespread, election officials should re-examine current practices for securing the chain of custody of all paper ballots and verify no opportunities exist for the introduction of fraudulent votes.
- States should consider implementing more widespread, statistically sound audits of election results.
- DHS should work with vendors to educate them about the vulnerabilities of both the machines and the supply chains.

6. Assistance for the States

- The Committee recommends Congress urgently pass legislation increasing assistance and establishing a voluntary grant program for the states.
  - States should use grant funds to improve cybersecurity by hiring additional Information Technology staff, updating software, and contracting vendors to provide cybersecurity services, among other steps.
  - Funds should also be available to defray the costs of instituting audits.