CONGRESSIONAL TASK FORCE ON ELECTION SECURITY

PRELIMINARY FINDINGS AND RECOMMENDATIONS

One year ago, 139 million Americans cast their vote in the wake of a massive Russian cyber-enabled influence operation designed to "undermine public faith in the U.S. democratic process, denigrate Secretary [Hillary] Clinton, and harm her electability and potential presidency." Using a vast network of social media trolls, fake "bot" accounts, and state-owned news outlets, the Kremlin spread disinformation to the American electorate through more than 1,000 YouTube videos, 130,000 tweets, and 80,000 Facebook posts viewed by as many as 150 million people on Facebook platforms alone. They hacked into U.S. political organizations, selectively exposing sensitive personal information about DNC staffers using third-party intermediaries like WikiLeaks. Finally, according to U.S. intelligence reports, Russia targeted voter registration databases in at least 21 states and sought to infiltrate the networks of voting equipment vendors, political parties, and at least one local election board.

Although this election cycle was unlike any before, the U.S. Intelligence Community warns that it may be the "New Normal." Recent reports show that the vast majority of U.S. states are still relying on outdated, insecure voting equipment and other election technologies that lack even basic cybersecurity standards. Meanwhile, Republicans in Congress have shown little interest in fighting Russian interference, and have instead chosen to act on measures that would eliminate rather than bolster funding for the Election Assistance Commission (EAC), the Federal agency responsible for helping states secure these vulnerable systems.

With just over a year until the 2018 midterm elections, it is important that we reflect on lessons learned in the last year and focus the spotlight on election security to push for reforms that protect the integrity of the ballot box.

The Congressional Task Force on Election Security has spent the past five months working together to understand the threats to election infrastructure and how to address them. The Task Force found:

- ***Election security is national security, and our election infrastructure is critical infrastructure.*** Federal law defines critical infrastructure as systems and assets for which "incapacity or destruction … would have a debilitating impact on security, national economic security, national public health or safety," or any combination thereof. Such infrastructure is given priority access to threat intelligence, incident response, technical assistance, and other products and services to help owners and operators harden their defenses. It is hard to imagine a system failure that would inflict more damage than a foreign adversary infiltrating our voting systems to hijack our democratic process. Nonetheless, Trump's Homeland Security Department (DHS) has wavered on its commitment to honor the Obama Administration's decision to designate election systems as a critical infrastructure subsector. Whether the next Secretary of Homeland Security will take a firm stand and maintain the designation remains to be seen.

- ***Our election infrastructure is vulnerable.*** Many elections across our country are being run on equipment that is either obsolete or near the end of its useful life. In over 40 states, elections are carried out using voting machines and voter registration databases created more than a decade ago. These technologies are more likely to suffer from known vulnerabilities that cannot be patched easily, if at all. As we saw at this year's DEFCON Voting Village, even hackers with limited prior knowledge, tools, and resources are able to breach voting machines in a matter of minutes.

- ***These vulnerable systems are being targeted by one of the world's most sophisticated cyber actors.*** According to the U.S. Intelligence Community, Russian interference in the 2016 election "demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations," and warned that "Moscow will apply lessons learned from…the US presidential election to future influence efforts worldwide, including against US allies and their election processes." We cannot reasonably assume that state voting systems are secure enough to withstand a state-sponsored cyber-attack, and we have no reason to believe these attacks will subside.

- ***Fortunately, many of the security solutions and best practices are already known.*** We can mitigate many vulnerabilities with existing, time-tested cybersecurity fixes found in the NIST Cybersecurity Framework and the CIS "Top 20" Critical Security Controls. By adopting even the Top 5 security controls, organizations can thwart 85% of common cyberattacks. Security experts also tend to agree on the types of voting systems most susceptible to compromise, and are urging election officials to phase out paperless Direct Recording Electronic (DRE) machines, replace these machines with voter-marked paper ballots, and carry out risk-limiting audits to verify election results.

- ***Federal agencies like DHS and EAC are important partners in this effort, but they need resources and consistent support from Congress.*** We have a rare window of opportunity to promote the widespread adoption of common-sense security measures that protect the integrity of the ballot box. This is not the time to diminish Federal efforts or shut down important lines of dialogue between DHS and election administrators.

  DHS is able to provide participating state and local governments with cyber threat intelligence, vulnerability assessments, penetration testing, scanning of databases and operating systems, and other cybersecurity services at no cost. Despite some initial confusion about the critical infrastructure designation, DHS has worked to build relationships with election officials, clarify the voluntary nature of DHS services, resolve disparities in information sharing and victim notification, and assist the subsector in formally establishing a Coordinating Council, which had its first meeting this fall. Where DHS has rendered assistance, officials report that cyber hygiene scans and other services are valuable. However, there is currently a 9-month wait list for Risk and Vulnerability Assessments, and questions remain about how to ensure threat information reaches election officials, many of whom lack security clearances.

  The EAC has been a valuable partner to state and county election officials. The agency has played a crucial role in election security by serving as a clearinghouse of information for state and local election officials, facilitating communications between these officials and DHS, providing easy-to-use cybersecurity guidance, and testing and certifying voting machines. Numerous state and local officials have expressed support and appreciation for the agency's work. Unfortunately, in recent years Republicans have made several attempts to terminate the agency. Instead, Congress should support the EAC and provide it with the resources it needs to help states secure their election systems. In addition, the President should nominate and the Senate should confirm a fourth commissioner to the EAC so that the agency can operate with its full slate of commissioners.

In light of its preliminary findings, the Task Force makes the following recommendations:

- ***Maintain the designation of election infrastructure as a critical infrastructure subsector.*** This designation ensures that state and local election officials receive prioritized access to DHS' cybersecurity services. Defining election systems as critical infrastructure means these systems will, on a more formal and enduring basis, be a priority for DHS cybersecurity assistance. These services are an important force multiplier, especially at the state and local level, where resources are scarce.

- ***Help states fund and maintain secure election systems.*** We cannot ask our state and local election officials to take on a state actor like Russia alone. Although states and counties are largely responsible for elections, Congress has a role to play in helping states fund the purchase of newer, more secure election systems, and requiring such systems adhere to baseline cybersecurity standards. Election officials need money to replace aging voting systems, many of which do not provide an auditable paper trail. It is important to note, however, that cyber threats evolve at a rapid pace, and a one-time lump sum investment is not enough. States also need resources for maintenance and periodic upgrades, and cybersecurity training for poll workers and other election officials.

- ***States should conduct post-election risk-limiting audits.*** A risk-limiting audit involves hand counting a certain number of ballots to determine whether the reported election outcome was correct. Risk-limiting audits used advanced statistical methods to enable states to determine that the original vote count was accurate with a high degree of confidence. These audits are useful in detecting any incorrect election outcomes, whether they are caused by a cyberattack or something more mundane like a programming error. Moreover, conducting these audits as a matter of course increases public confidence in the election system.

- ***Empower Federal agencies to be effective partners in pushing out nationwide security reforms.*** With midterm elections in a year, election officials cannot afford to wait 9 months for valuable cybersecurity services like Risk and Vulnerability Assessments. At the same time, we cannot ask DHS to deliver election assistance at the expense of its other critical infrastructure customers. We should give DHS the resources it needs to provide election officials with timely assessments and other cybersecurity services, without detracting from its overall critical infrastructure mission. Similarly, Congress should fund EAC at a level commensurate with its expanded role in election cybersecurity and confirm a fourth commissioner so the agency is able to continue to serve as a resource on election administration.

- ***Establish clear and effective channels for sharing threat and intelligence information with election officials.*** Effective information sharing is critical to address the decentralized threat that our nation faces in terms of securing our elections. Prior to the 2016 elections, we have seen how information sharing failures can cause catastrophic events. The 9/11 terrorist attacks exposed serious gaps in information sharing within the Federal government and state and local law enforcement partners. It is imperative that election officials have access to the most timely and high-level security information. Chief election officials in each state should have expedited access to security clearances. DHS needs a formalized process to provide real-time appropriate threat information to state and local election officials to improve information flow and help prevent intrusions in our election infrastructure.

- ***Prioritize cybersecurity training at the state and local level.*** The events of 2016 demonstrate that human error is a significant vulnerability as it leaves systems open to spear-phishing and other forms of cyberattack. States and localities face the daunting task of training hundreds, if not thousands, of election officials, IT staff, and poll workers on cybersecurity and risk mitigation. It costs money for states to produce training materials, and takes staff time to implement statewide training programs. The federal government should provide training support either through the EAC or by providing funding to states to assist with their training programs.