The Washington Times

Election Security is National Security

Congress should pass the Graham-Klobuchar Amendment

Bruce Fein

The U.S. Senate should enthusiastically pass the Graham-Klobuchar amendment to H.R. 2810, the National Defense Authorization Act for fiscal 2018.

The amendment would enormously strengthen defenses against cyber attacks that could compromise the integrity of elections in the United States and undermine legitimacy of government. Public confidence in the reliability of elections is a cornerstone of national security—the willingness of the people to fight and die for their country. Experts agree that the Vietnam War was lost because the South Vietnamese Army would not risk that last full measure of devotion on behalf of a corrupt, fraudulently elected government. To the extent citizens lose confidence in electoral results, to that extent military morale diminishes.

The near-misses during the 2016 election cycle underscore the urgency of the Graham-Klobuchar amendment. It would provide federal funding to states through Election Technology Improvement Grants. The funds would be used for voting system investments conditioned on adherence to best practices recommended by an expert Commission.

States would be eligible for a grant only if their election systems survive a Security Risk and Vulnerability Assessment from the Department of Homeland Security, including correcting detected vulnerabilities. Grants must be applied to satisfying the cyber-security and cyber-hygiene recommendations of a federal-state commission.

Commission members would include representatives of the National Institute of Standards and Technology, the Secretary of the Department of Homeland Security, the National Association of Secretaries of State, the National Association of State Election Directors, the National Association of Election Officials, the International Association of Government Officials, the National Association of State Chief Information Officers, the Multi-State information Sharing and Analysis Center, the Election Assistance Commission Technical Guidelines Development Committee, the Election Assistance Commission Standards Board, the Election Assistance Commission Board of Advisors, and such other members as the Commission determines would be necessary and proper.

The Commission would be transparent. Public hearings would be held to receive the views of citizens, researchers, manufacturers and academics. It would be tasked to study best practices for securing and storing voting systems and records and election auditing procedures that fortify the integrity of election results. Among other things, the commission would examine the probability of foreign interference in the 2016 elections, nation-state sponsored advanced persistent threat groups, cyber-mercenaries, cyber-criminals, and remote threats. The information unearthed by the examinations would be used to establish best practices for storing and safeguarding voter registration data and for

modernizing and securing each and every component of election infrastructure that was designated by the Secretary of Homeland Security on January 6, 2017, as a sub-sector of a critical infrastructure sector pursuant to section 2001 of the Homeland Security Act of 2002.

The commission would develop election administration profiles anchored to the NIST cyber security framework to lessen the threat to election integrity posed by personnel acting with or without malicious intent; identify the threats posed by aging voting equipment; and, point to federal funding sources that states can tap to patch the vulnerabilities.

At present, election systems in the United States are predominantly amalgamations of insecure, obsolete, and antiquated technology, poorly designed black-box proprietary code, and slapdash applications and graphical interfaces. They lack the security features of a 2006 cellular phone. Without the Graham-Klobuchar amendment, an adversary could poison a manufacturer update server or spear-phish an election management system, laterally navigate across a network to the central tabulator, and subtly alter election results using historical voting data within acceptable margins of error of a minimal auditing process to alter the results of a district or pivotal swing state without detection.

According to a county election agency IT manager, the cost of minimal securing of machines approximates $38 to $50 per voter, which is beyond the means of most electoral jurisdictions. That shows the fiscal justification for the Graham-Klobuchar amendment.

To reiterate: Its major objectives are to secure voter registration logs, upgrade election auditing processes, promote information sharing to stymie emerging threats, and strengthen transparency, intergovernmental communications, and oversight.

Electoral integrity is too important to be left to amateurs. The Graham-Klobuchar amendment is long overdue. Our electoral systems are living on borrowed time.

Bruce Fein served as associate deputy attorney general and general counsel of the Federal Communications Commission under President Reagan. He is now a partner in the firm Fein & DelValle, PLLC.