Durbin, Hastings work to strengthen Illinois' election systems from future acts of cyberwarfare

June 15 2017 2:56 PM

WASHINGTON – Amid reports that Russia's cyberattack on the U.S. electoral system leading up to the 2016 election was far more widespread than had been publicly revealed, U.S. Senator Dick Durbin (D-IL) and Illinois State Senator Michael E. Hastings (D-IL-19) are working with 110 local Illinois election authorities to assess the

current state of Illinois' election system's cybersecurity and to see how the federal and state governments might best assist their efforts to strengthen the cybersecurity of Illinois' election systems.

"Like you, we believe safe and fair elections are a sacred institution within our democracy. Needless to say, election boards across Illinois are part of our national election infrastructure and essential to the continued success of our democratic process. Therefore, we cannot allow for the unauthorized and malicious interference in elections in Illinois to continue," Sen. Durbin and State Sen. Hastings wrote in letters to 110 Illinois County Clerks and Election Board Executive Directors. **"It is our view that a secure election process, without the malicious interference of foreign or domestic entities, is of utmost importance and we are confident that you are dedicated to ensuring such intrusions are dealt with in a proper manner. Thank you for your valuable work, and we look forward to your timely response."**

Beginning in June 2016, the Illinois State Board of Elections (BOE) was the target of a malicious, month-long cyberattack. A May 4, 2017, hearing in the Illinois State Senate Subcommittee on Cybersecurity revealed the breach enabled the intruder to retrieve confidential voter information from nearly 80,000 voter profiles whose information originated from every one of the 110 election authorities in Illinois. Authorities have confirmed that Illinois was one of two states targeted, along with Arizona—and recent reports indicate that these attacks may have been broader and targeted at more states than previously understood. Most recently, Cook County was the first known U.S. governmental entity to be infected by the international WannaCry ransomware.

Full text of one of today's letters is available below:

June 15, 2017

Dear County Clerk,

We are deeply concerned about future cyberattacks on election systems in Illinois, and therefore write to request information about cybersecurity in your jurisdiction and what we can do to assist your efforts at the federal and state level.

As you know, beginning in June 2016, the Illinois State Board of Elections (BOE) was the target of a malicious, month-long cyberattack. A May 4, 2017, hearing in the Illinois State Senate Subcommittee on Cybersecurity revealed the breach enabled the intruder to retrieve confidential voter information from nearly 80,000 voter profiles whose information originated from every one of the 110 election authorities in Illinois. Authorities have confirmed that Illinois was one of two states targeted, along with Arizona—and recent reports indicate that these attacks may have been broader and

targeted at more states than previously understood. Most recently, Cook County was the first known U.S. governmental entity to be infected by the international WannaCry ransomware.

On January 6, 2017, the Office of the Director of National Intelligence released an unclassified report expressing the conclusion of the Central Intelligence Agency, the Federal Bureau of Investigation (FBI), and the National Security Agency about foreign interference in the 2016 election. The agencies made the deeply troubling determination that Russia deliberately interfered in our election to undermine U.S. democracy and support its preferred candidate. The evidence is overwhelming and a harbinger of future such interference in our elections and those of our Western democratic allies if we do not take action.

Earlier this year, the U.S. Department of Homeland Security designated our electoral systems as "critical infrastructure." Like you, we believe safe and fair elections are a sacred institution within our democracy. Needless to say, election boards across Illinois are part of our national election infrastructure and essential to the continued success of our democratic process. Therefore, we cannot allow for the unauthorized and malicious interference in elections in Illinois to continue.

While the Illinois BOE, alongside the FBI, conducted outreach to you and other local election authorities here in Illinois, we would like to seek your assistance in assessing the current state of our election system's cybersecurity. Please respond to the following questions:

1. Have you been hacked or suffered from a cyber-intrusion in recent history?
2. If so, have you worked with local or national law enforcement on the matter?
3. Did you perform an audit of your systems after the BOE was hacked?
4. Have you taken any steps that would make such cyberattacks less likely to be successful in the future? What steps have you taken, if any, to better secure the identities of Illinois voters?
5. Are you implementing any of the Top 5 Critical Cyber Security Controls outlined in the National Institute of Standard and Technology Cyber Security Framework of 2014? These include:
    1. Inventory of Authorized and Unauthorized Devices
    2. Inventory of Authorized and Unauthorized Software
    3. Secure Configurations for Hardware and Software
    4. Continuous Vulnerability Assessment and Remediation
    5. Controlled Use of Administrative Privileges
6. How could the federal and state governments best assist your efforts to strengthen the cybersecurity of your election systems?

We are both committed to helping state and local election authorities address these security and modernization issues and are supportive of a number of state and federal bills in this regard.

At the federal level, the State and Local Cyber Protection Act of 2017 would improve cybersecurity collaboration between the federal government and other stakeholders, including state and local governments. Additionally, the State Cyber Resiliency Act would create grants, administered by the Federal Emergency Management Agency, to assist state and local governments in preventing, preparing for, protecting against, and responding to cyber threats.

It is our view that a secure election process, without the malicious interference of foreign or domestic entities, is of utmost importance and we are confident that you are dedicated to ensuring such intrusions are dealt with in a proper manner. Thank you for your valuable work, and we look forward to your timely response.