

Dear Commissioners:

We hope to work with the Election Assistance Commission (EAC) to ensure all U.S. elections remain free from foreign interference. Our country relies on the EAC's expertise on voting technology and security. The EAC played a crucial role before the 2016 general election by working with state and local election officials, the Department of Homeland Security (DHS) and the Federal Bureau of Investigation to coordinate an appropriate response to cybersecurity threats to our democracy. The EAC's mission of assisting the state and local election officials that administer our elections has never been more important than it is today.

We have deep concerns about Russian interference in both U.S. elections and the federal government. The events surrounding Michael Flynn's resignation raise serious questions about interactions between the President's campaign and transition teams and Russian officials. Seventeen intelligence agencies—including the Federal Bureau of Investigation, the Central Intelligence Agency, and DHS—have reported that the Russian government interfered in the 2016 election in an attempt to affect the outcome. We know that hacking extended beyond the Democratic National Committee emails to include attempts to hack into our nation's voter registration systems.

As motivated and sophisticated cybercriminals will continue to target our election systems, we must ensure that our state and local election administrators have the resources they need to make critical cybersecurity upgrades. Aging machines are vulnerable to hacking since they lack the latest security features. In 2016, 43 states used electronic voting machines that were at least 10 years old. While there was no reported damage to actual voting machines or voter registration data last year, we hope you will agree when we say that the 2016 election was a wake-up call. We must do more to protect our U.S. elections from foreign interference.

As a first step, we are writing to request a full account of the EAC's efforts in the cybersecurity sphere in 2016. Based on your work with election officials, cybersecurity experts and federal law enforcement, we also would appreciate an impartial assessment of the challenges that state and local election officials face in protecting future U.S. elections from cybersecurity threats. Specifically, we ask that you answer the following questions:

- What actions did the EAC take before the November 2016 election to protect U.S. elections from threats to cybersecurity?
- To your knowledge, please describe the full extent of foreign interference and hacking that occurred in any national, state or local election system—including voter registration databases and voting infrastructure—during the November 2016 election.
- In your opinion, are current state and local election systems appropriately prepared to respond to and resolve cybersecurity threats to U.S. elections?

- In your opinion, are state and local election systems currently able to identify instances of foreign interference in U.S. elections through tools like post-election audits?
- What foreign cybersecurity threats are we most likely to encounter in future elections?
- What are the EAC's plans moving forward to prevent foreign interference in U.S. elections?
- Does the EAC have recommendations to Congress and the Administration on appropriate actions to defend our U.S. election system from foreign interference and respond to threats?

We are committed to strengthening the security of our democracy's infrastructure and look forward to receiving your responses and working with the EAC to achieve this goal.

Sincerely,