Office of Infrastructure Protection
National Protection and Programs Directorate
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

April 16, 2018

The Honorable Elijah E. Cummings
U.S. House of Representatives
Washington, DC 20515

Dear Representative Cummings:

Thank you for your October 20, 2017 letter.

In addition to testifying before the committee on November 8, 2017 regarding the Department of Homeland Security's (DHS) efforts to enhance the security of elections, we are also able to brief the Committee. In the meantime, I would like to address your concerns regarding DHS's communications with chief state election officials.

In 2016, the Department took unprecedented action to alert chief state election officials of relevant cybersecurity threats. DHS issued several public statements between August and Election Day to share information regarding the threat and urged election officials to seek cybersecurity assistance from either DHS or other experts. The Secretary held multiple phone calls with election officials to highlight the seriousness of the threat. As early as August 2016, we broadly shared specific tactics and indicators observed against some states—specifically information regarding targeting of voter registration systems—with state and local governments to increase awareness of the threat and asked recipients to check their systems for similar activity. DHS and the Office of the Director of National Intelligence declassified attribution and alerted the public to malicious activity directed towards our elections on October 7, 2016. Several days later, DHS's National Cybersecurity and Communications Integration Center and the Federal Bureau of Investigation published and shared with election officials a joint analysis report containing recommendations and over 650 technical indicators of compromise to assist election officials with detecting malicious activity on their networks. Some of these indicators had previously been classified and were pulled from analysis of previous incidents relevant to the threat. Between August and Election Day, DHS and other interagency partners shared several other products, including best practices specific to election infrastructure, intelligence assessments, risk assessments, and technical information to assist election officials with network protection. Further information relevant to officials was declassified in the January 2017 Intelligence Community Assessment, "Assessing Russian Activities and Intentions in Recent U.S. Elections."

It is important to recognize the methods by which DHS learns of a cyber incident: an affected entity voluntarily self-reports to DHS; DHS is informed of a cyber incident at an affected entity by a trusted third party, such as another government or private sector partner; or

DHS operated capabilities identify a cyber incident on an affected entity's system. During the 2016 election period, through trusted third parties and cybersecurity operators in the states, the Department and its partners learned of specific communications or attempted communications from malicious infrastructure to known state or local government networks in at least 21 states. Our assessment regarding the scale and scope triggered further outreach to share threat information with election officials and offer voluntary services to assess cybersecurity of election infrastructure and processes.

Individual incident reports, at the time did not include attribution to Russia. These individual incident reports, given that the majority of the observed communications were preparatory in nature and indicated no evidence of compromise, were sometimes further shared by those network operators with election officials and sometimes were not. Some Secretaries of State and other state chief election officials expressed frustration at not being aware of whether their states were included in the 21 states referenced in DHS's June 2017 testimony before Congress. To address these concerns, DHS reached out to the chief election official in all States to let them know if their state was or was not included in DHS's assessment.

For future elections, DHS is working with state and local election officials to improve the effectiveness of information sharing protocols, both from DHS and among state officials. As the sector-specific agency, DHS is providing overall coordination guidance on election infrastructure matters to subsector stakeholders. As part of this process, the Election Infrastructure Subsector (EIS) Government Coordinating Council (GCC) was established. The EIS GCC is a representative council of federal, state, and local partners with the mission of focusing on sector-specific strategies and planning. This includes development of information sharing protocols and establishment of key working groups, among other priorities. Additionally, DHS has begun discussions with a range of relevant private sector companies to establish of a Sector Coordinating Council (SCC). The SCC will be focused on security issues relevant to private sector companies that support the administration of our election processes.

Thank you again for your letter. The co-signers of your letter will receive separate, identical responses. Should you wish to discuss this further, please do not hesitate to contact me.

Sincerely,

Robert Kolasky
Deputy Assistant Secretary