The Department of Homeland Security's Response to Senator Ron Wyden's December 12, 2017 Letter

1. **Designate a senior White House official to "own" the issue of election cybersecurity and require that official to brief Congress regularly on cybersecurity threats, mitigation efforts underway, and key barriers to implementation.**

   Following consultation with the Assistant to the President for Homeland Security and Counterterrorism in January 2017, the then-Secretary of Homeland Security designated the Department of Homeland Security (DHS) as the sector-specific agency for the newly designated election infrastructure subsector. Officials from the Department and our Federal partners, including law enforcement and intelligence community agencies, regularly testify before Congressional hearings, and brief members of Congress and their staffs on efforts to address cybersecurity risks to our Nation's elections.

2. **Direct the National Institute of Standards and Technology and the Department of Homeland Security (DHS) to create an objective framework to grade states on their election cybersecurity and publish annual "scorecards" giving each state a letter grade and describing the areas in which each need to improve.**

   DHS regularly collaborates with the National Institute of Standards and Technology (NIST) on a range of cybersecurity efforts, including the NIST Cybersecurity Framework. The Framework is voluntary guidance for critical infrastructure organizations to better manage and reduce cybersecurity risks. Consistent with section 8 of Executive Order 13636, DHS works to promote adoption of the Framework.

   Separate from the Framework, DHS also works with NIST and the U.S. Election Assistance Commission (EAC) on the development of Voluntary Voting System Guidelines. NIST and EAC administer the Technical Guidelines Development Committee. DHS participates in the cybersecurity working group, and has presented to the committee and its broad audience of election officials on multiple occasions.

   Additionally, DHS also works with the election infrastructure subsector to better understand cybersecurity risk across the Nation. DHS continues to enhance its understanding of the diversity of voting systems and versions of voting software operated by thousands of election jurisdictions under various administrative processes and security practices. Decisions regarding what systems and processes are used to administer an election are the responsibility of state and local election officials. DHS is focused on voluntary efforts to assist election officials with mitigating cybersecurity and physical security risk. Auditability is an important assurance mechanism for any critical process. Paper ballots are one way to provide a measure of auditability but not the only method. Some digital voting machines provide a paper audit trail. There may also be other innovations in the market or in development that provide sufficient mitigations.

3. **Direct DHS to designate political campaigns as part of our nation's critical infrastructure so that campaigns can receive cybersecurity assistance if they request it.**

   DHS is already authorized to provide political campaigns with cybersecurity assistance upon request. Section 227 of the Homeland Security Act of 2002, as amended, authorizes a national cybersecurity and communications integration center at DHS. Through this center, DHS is authorized to facilitate multi-directional and cross-sector information sharing related to cyber threat indicators, defense measures, cybersecurity risks, incidents, analysis, and warnings; and upon request, provide timely technical assistance, risk management support, and incident response capabilities for Federal and non-Federal entities.

   During the 2016 election cycle, DHS reached out to the major political units of the two major political parties to share information about assistance available upon request. Additionally, DHS reached out to the Presidential and Vice Presidential campaigns which were receiving Secret Service protection. While the proactive outreach was limited to these entities in 2016, assistance has been available to any political entity upon request.

   DHS will continue to offer cybersecurity assistance to political campaigns.

4. **Direct the Secret Service to expand Presidential candidate security to include cybersecurity. At the very least, the Secret Service should help candidates and their campaigns secure email, voice, and text communications.**

   The United States Secret Service is authorized to protect certain persons (18 U.S.C. § 3056). Of course, many Americans recognize the Secret Service as the entity charged with protecting the President and his family. In addition to other persons, they are also authorized to protect "major Presidential and Vice Presidential candidates and, within 120 days of the general Presidential election, the spouses of such candidates." Candidates that meet this threshold are "those individuals identified as such by the Secretary of Homeland Security after consultation with an advisory committee consisting of the Speaker of the House of Representatives, the minority leader of the House of Representatives, the majority and minority leader of the Senate, and one additional member selected by the other members of the committee.

   Available cybersecurity assistance for candidates and their campaigns is addressed above in response to number three.