The Department of Homeland Security's Response to
Senator Ron Wyden's February 28, 2018 Letter

1. **How did DHS and DOJ assess the likelihood that our election infrastructure was hacked without examining the voting machines for evidence of hacking?**

   Under Executive Order 13848, Imposing Certain Sanctions in the Event of Foreign Influence in a U.S. Election, the Department of Homeland Security (DHS) and the Department of Justice (DOJ) evaluated the impact of any foreign interference on election infrastructure or the infrastructure of political organizations, including campaigns and candidates in the 2018-midterm elections. This evaluation was informed by an assessment prepared by the Office of the Director of National Intelligence (ODNI). DHS and DOJ have concluded there is no evidence to date that any identified activities of a foreign government or foreign agent had a material impact on the integrity or security of election infrastructure or political/campaign infrastructure used in the 2018 midterm elections for the United States Congress. Furthermore, there is no evidence to date that any identified activities of a foreign government or foreign agent had a material impact on the tabulation of votes or the timely transmission of election results. The ODNI Assessment was based on all relevant sources of intelligence, as appropriate and consistent with applicable law and policy.

   While the information in the ODNI assessment remains classified, DHS and DOJ evaluated any identified foreign interference targeting election infrastructure based on information provided by the ODNI assessment and other relevant information as appropriate and consistent with applicable law, including technical information provided by elections infrastructure partners, other government agencies, potential victims, assessments regarding elections infrastructure led by DHS's Cybersecurity and Infrastructure Security Agency, and investigations led by the Federal Bureau of Investigation (FBI). This information could include data from net flow and intrusion detection sensors provided to election officials by DHS, commonly known as ALBERT sensors; information shared from state and local election officials and political campaigns; all-source intelligence; reported anomalies in state and local risk limiting post-election audits; and sensitive or classified FBI investigative information.

2. **How many voting machines used in the November 2018 election were running software with publicly known, exploitable security vulnerabilities?**

   Given the diverse nature of election jurisdictions across both state and local governments, a wide range of election systems remain in use. States and localities own and control access to their data on the precise number of voting machines within their individual jurisdictions. As the data and system owners, they are best positioned to provide information on the deployment of voting systems within their jurisdiction. This includes the standards to which those systems are certified, whether they are certified in one of the Election Assistance Commission's recognized Voting System Testing Laboratories or a state-level equivalent, and whether with the systems deployed have remaining exploitable security vulnerabilities.

To assist in these efforts, DHS provides numerous services to election officials and industry partners to identify and mitigate exploitable security vulnerabilities, such as remotely analyzing the vulnerabilities and configuration errors on a network, providing penetration testing, disassembling and analyzing voting machines to discover vulnerabilities, and facilitating coordinated vulnerability disclosures. DHS proactively shares actionable information on known security vulnerabilities with state, local, and private sector partners directly and through the Election Infrastructure Information Sharing and Analysis Center.

3. **What level of confidence does DHS have that no "foreign government or foreign agent had a material impact on the integrity or security of election infrastructure or political/campaign infrastructure used in the 2018 midterm election?" How does DHS define "material" in this context?**

   DHS and DOJ evaluated the extent to which any identified activities had an effect that was material—in other words, significant, important, or consequential—to the security or integrity of the covered infrastructure. For example, DHS and DOJ may consider whether any phishing or login attempts were successful; whether any website defacements or distributed-denial-of-service attacks resulted in any significant disruptions; whether any voter registration databases, voting machines, tabulation systems, unofficial reporting systems, information from election service vendors, or transmission systems were compromised; or whether any information was exfiltrated, altered, or disclosed.

4. **In response to my questions following the Intelligence Committee's June 21, 2017 hearing, DHS acknowledged that it had high confidence that it would detect cyber manipulation "intended to change the outcome of a national election," but that the Department had "not made an assessment of state-wide or local elections." DOJ and DHS recently issued a joint statement concluding that there is "no evidence to date that any identified activities of a foreign government or foreign agent had a material impact on the integrity or security of election infrastructure or political/campaign infrastructure used in the 2018 midterm election." Does this conclusion apply to statewide and local elections too? If yes, what changes have been made since 2016 to enable DHS to arrive at conclusions regarding state and local elections?**

   The DHS and DOJ statement was limited to "the 2018 midterm elections for the United States Congress." During the 2018 midterm election, DHS, in coordination with the federal interagency, state, local, and private sector partners nationwide—worked in unprecedented ways to combat foreign interference efforts, to support state and local officials in safeguarding election infrastructure, and to assist political organizations, campaigns and candidates in protecting their own infrastructure. DHS fostered an environment in which state and local officials, political organizations, campaigns, and candidates could share information on malicious or suspicious cyber activities. This concerted effort ultimately provided DHS the ability to receive and share information efficiently with all 50 U.S. States and more than 1,400 local jurisdictions. DHS continues to foster coordination with federal, state, local, and private sector partners to preserve the integrity and security of federal, state, and local elections and political/campaign infrastructure going forward.