CLICK HERE FOR INFRASTRUCTURE LAW RESOURCES
(https://www.wyden.senate.gov/imo/media/doc/Wyden_Infastructure%20Guide%202021.pdf)

October 03, 2017

Wyden Questions Voting Machine Manufacturers on Security Measures

Following Cyber Threats in 2016 Election, Wyden Asks Manufactures How They Are Protecting Americans' Votes from Hacking

Washington, D.C. –Sen. Ron Wyden, D-Ore., asked the top six U.S. voting machine manufacturers what steps they are taking to protect themselves from cyberattack, in a letter sent today.

Wyden's letter follows repeated warnings from intelligence agencies that Russia and other foreign actors may try to target U.S. election infrastructure in upcoming elections, and comes after the Department of Homeland Security reported that Russian hackers targeted 21 states last year.

"As our election systems have come under unprecedented scrutiny, public faith in the security of our electoral process at every level is more important than ever before," Wyden said. **"Ensuring that Americans can trust that election systems and infrastructure are secure is necessary to protecting confidence in our electoral process and democratic government."**

Read Wyden's letters to Dominion Voting, Election Systems & Software, Five Cedars Group, Hart InterCivic, MicroVote and Unisyn Voting Solutions. Wyden sent similar letters to two voting system test laboratories accredited by the U.S. Election Assistance Commission: Pro V&V and SLI Compliance.

Wyden asked the companies to answer the following questions by October 31:

1. Does your company employ a Chief Information Security Officer? If yes, to whom do they directly report? If not, why not?
2. How many employees work solely on corporate or product information security?
3. In the last five years, how many times has your company utilized an outside cybersecurity firm to audit the security of your products and conduct penetration tests of your corporate information technology infrastructure?
4. Has your company addressed all of the issues discovered by these cybersecurity experts and implemented all of their recommendations? If not, why not?
5. Do you have a process in place to receive and respond to unsolicited vulnerability reports from cybersecurity researchers and other third parties? How many times in the past five years has your company received such reports?
6. Are you aware of any data breaches or other cybersecurity incidents in which an attacker gained unauthorized access to your internal systems, corporate data or customer data? If your company has suffered one or more data

breaches or other cybersecurity incidents, have you reported these incidents to federal, state and local authorities? If not, why not?

7. Has your company implemented the best practices described in the National Institute of Standards and Technology (NIST) 2015 Voluntary Voting Systems Guidelines 1.1? If not, why not?
8. Has your firm implemented the best practices described in the NIST Cybersecurity Framework 1.0? If not, why not?

###