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

March 06, 2018

Wyden Questions Voting Machine Manufacturer on Security Weakness Posed By Remote Access

ES&S Previously Failed to Answer Basic Questions About Its Cybersecurity Practices

Washington, D.C. –Sen. Ron Wyden, D-Ore., today asked the nation's largest voting machine manufacturer, ES&S, to explain whether it sells voting machines or other products with remote-access software, which could be exploited by hackers to compromise the machines.

The New York Times Magazine reported last month that ES&S sold voting machines and other election-management products with pre-installed remote-access software. Allowing remote access significantly weakens the security of voting machines, and could be exploited by hackers to sabotage machines or interfere with vote tallies.

"The American public has been repeatedly assured that voting machines are not connected to the internet, and thus, cannot be remotely compromised by hackers," Wyden wrote to the company.

"The default installation or subsequent use of remote-access software on sensitive election systems runs contrary to cybersecurity best practices and needlessly exposes our election infrastructure to cyberattacks," he continued.

Wyden originally questioned ES&S and other voting manufacturers about their cybersecurity practices last year. ES&S did not answer Wyden's questions about whether the company follows basic cybersecurity best practices.

Wyden is a senior member of the Senate Intelligence Committee and has pushed for years to improve cybersecurity practices in the public and private sector.

###