TREY GOWDY, SOUTH CAROLINA
CHAIRMAN

ONE HUNDRED FIFTEENTH CONGRESS

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143
MAJORITY (202) 225–5074
MINORITY (202) 225–5051
http://oversight.house.gov

Opening Statement
Ranking Member Robin Kelly

Hearing on "Cybersecurity Of Voting Machines"
Subcommittee on Information Technology and Subcommittee on Intergovernmental Affairs
Joint Hearing

November 29, 2017

Thank you, Chairmen Hurd and Palmer for holding this important hearing today.

There is no doubt that Russia, at the direction of President Vladmir Putin, attempted to manipulate our elections and has worked to manipulate those of our Western allies. It was a broad and coordinated campaign to undermine faith in democratic elections. Earlier this year, the IT subcommittee explored the Kremlin's efforts to use social media to influence voters.

Today, we are taking a look at another part of their effort to undermine our democracy by hacking our voting machines and election infrastructure.

More than one year ago, we held a hearing entitled: "Cybersecurity: Ensuring the Integrity of the Ballot Box." During that hearing, we took a look at state and federal preparations for any cyberattack on our voting machines.

Today, we have a clearer picture of what transpired but we're still discovering new facts. In September of this year, the Department of Homeland Security (DHS) notified 21 states that hackers affiliated with the Russian Government breached or attempted to breach their election infrastructure. In my home state of Illinois, the hackers illegally downloaded the personal information of 90,000 voters and attempted to change and delete data. Fortunately, they were unsuccessful.

While we continue learning about the full scope of Russia's election interference, one thing is clear: there will be another attempt to manipulate our elections. Whether it be Russia, another nation-state, or a non-state actor or even a terrorist organization, the threats to our election infrastructure are growing. So what are we doing about it?

Earlier this year, researchers at the DEFCON conference successfully hacked five different Direct-Recording Electronic voting machines, or DRE's, in a day. The first vulnerabilities were discovered in just 90 minutes. Even voting machines not connected to the internet still contained physical vulnerabilities like USB ports that can be used to upload

malware. Alarmingly, many DRE's lacked the ability to allow experts to determine that they had been hacked. Despite these flaws, DRE's are still commonly used. In 2016, 42 states used DRE's that were more than a decade old – with some running outdate software that is no longer supported by the manufacturer.

Updating our voting machines to auditable, paper-based machines, such as optical scanners, is a step we need to take right now. Our election infrastructure is broad and contains numerous vulnerabilities. If we are going to withstand a coordinated attack, we need a coordinated defense.

In January of this year, DHS designated election infrastructure as "critical infrastructure." In this announcement, then-DHS Secretary Jeh Johnson was clear that this designation was not to be a federal takeover of state and local election infrastructure. Rather, it was a designation intended to ensure the current state and local officials had the resources necessary to secure their elections. Since then, former DHS Secretary and now White House Chief of Staff, General John Kelly has supported this designation.

This designation can help ensure that the cornerstone of our democracy—our elections—remain fair and secure.

But if this designation is to be successful, we will all have to work together. DHS and our state election officials must do a better job of working together to detect and solve problems.

Thank you again Mr. Chairman for holding this crucial hearing. Thank you to our witnesses for being here. I look forward to hearing from you all about how we can continue protecting our democracy.

Contact: Jennifer Werner, Communications Director, (202) 226-5181.