JASON CHAFFETZ, UTAH
CHAIRMAN

ONE HUNDRED FOURTEENTH 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: Ensuring the Integrity of the Ballot Box"
Subcommittee on Information Technology

September 28, 2016

Thank you, Mr. Chairman.

Last week, after receiving classified briefings on threats to the upcoming elections, Senator Dianne Feinstein and Representative Adam Schiff accused Russia of, and I quote, "making a serious and concerted effort to influence U.S. elections."

Recently, Director of National Intelligence James Clapper also cited a long history of Russia's efforts to influence elections abroad.

The Director said that Russia's apparent efforts to compromise U.S. elections, quote, "shouldn't come as a big shock to people."

But attempts to influence the outcome of our elections are not just limited to foreign governments.

According to law enforcement and the FBI, cyberattacks in August against voter registration databases in Illinois and Arizona were most likely criminally-motivated, possibly targeting voters' personally identifiable information.

To know that my own state suffered this attack is extremely troubling, not only because of the threat of identity theft, but because of what hackers could do once they have access to these databases.

For example, perhaps they could they change a voter's listed party affiliation in a way that affects primary elections? Or could they perhaps modify voter addresses to invalidate registrations?

We must address these questions and do absolutely everything we can to defend against future attacks.

In today's hearing, we will be addressing this crucial question: How secure is our electoral infrastructure from any cyberattack, regardless of the source?

According to security experts, a massive attack against the infrastructure as a whole is not the biggest cyber vulnerability in our election process.

Rather, it is the individual voting machines that pose some of the greatest risks.

According to a 2015 report from the Brennan Center for Justice, many voting machines were designed and engineered in the 1990s or early 2000s.

These machines were designed before the Internet faced the sort of advanced cyber risks that are now all-too-common in our current threat environment. For example, in 2015 Virginia's Board of Elections decertified a voting system used in 24% of precincts after finding that an external party could access the machine's wireless features to, quote, "record voting data or inject malicious data."

But beyond cyberattacks, these machines are also vulnerable to operational failures like crashes and glitches.

As one security expert at Rice University put it, quote, "These machines, they barely work in a *friendly* environment."

As we examine this upcoming election and beyond, we must consider what sorts of investments we must make to our voting infrastructure.

Today's hearing will provide us with an opportunity to learn just how vulnerable our elections might be to hackers, and what our local, state, and federal governments can do to protect our electoral processes.

But I must also add that I also hope that we have more hearings on the topic of the right to vote, and the access to the ballot box.

Far too many states across this country have enacted troubling voter suppression laws since the Supreme Court decision in *Shelby County v. Holder*, and I have been deeply disappointed at the lack of interest across the aisle in addressing this issue.

We must repair the damage done to the Voting Rights Act through legislation, and that must be a top priority.

To preserve the integrity of our ballot box, we must also protect citizens' access to it.

Mr. Chairman, thank you again for holding this important hearing.

Contact: Jennifer Werner, Communications Director, (202) 226-1004.