ELIJAH E. CUMMINGS, MARYLAND
CHAIRMAN

ONE HUNDRED SIXTEENTH CONGRESS

JIM JORDAN, OHIO
RANKING MINORITY MEMBER

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5051
MINORITY (202) 225–5074

http://oversight.house.gov

Opening Statement
Subcommittee Chairman Stephen F. Lynch
Hearing on "Securing U.S. Election Infrastructure and Protecting Political Discourse"
Subcommittee on National Security
May 22, 2019

Today we will examine the security of our nation's election infrastructure systems, as well as how the federal government is working with private sector partners to respond to malicious attempts to unduly influence public opinion, sow discord, and undermine confidence in our political institutions.

The purpose of today's hearing is not to relitigate the outcome of the 2016 presidential election. Rather, our goal is to safeguard the fundamental democratic principle underscored by President Abraham Lincoln: "Elections belong to the people." Indeed, no less than the integrity of our democracy is at stake.

In January 2017, the Intelligence Community released an assessment that our democracy had come under attack by a foreign adversary. With "high-confidence," our nation's 17 intelligence agencies unanimously found that "Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election." The Russian effort included clandestine intelligence operations coupled with blatant meddling by Russian Government agencies, state-funded media organizations, third party intermediaries, and paid social media users, or "trolls."

Special Counsel Robert Mueller's report, which followed his nearly two-year, independent investigation into Russian interference, confirmed and augmented the Intelligence Community's "high-confidence" judgment. According to the Special Counsel: "The Russian Government interfered in the 2016 presidential election in sweeping and systematic fashion."

Thanks to the Special Counsel, we know that Russia's interference campaign involved so-called "active measures" led by the St. Petersburg-based Internet Research Agency designed to sow discord in the U.S. through "information warfare." Its primary components included the creation of fictitious social media accounts, the purchase of online ads to promulgate divisive political material, the deployment of automated bot networks to amplify content, and the organization of political rallies in the U.S. At the same time, Russia's military agency, the GRU, perpetrated a hacking operation targeting U.S. individuals, political committees, state election boards, state secretaries of state, county governments, and private manufacturers of election-related software and voting machines. In response to these malign activities, the Special Counsel criminally indicted 13 Russian nationals, 12 military officers, and three Russian companies.

In its post-election review, Facebook alone estimated that accounts controlled by the Internet Research Agency may have reached 126 million people prior to their deactivation in August of 2017, including nearly 30 million Americans.

Russian interference in U.S. elections has continued beyond 2016 – with Iran, China, and other hostile state actors following suit. In September 2018, the Department of Justice charged a Russian national with conspiring to interfere in the 2018 midterm elections in connection with her work as a chief accountant for "Project Lakhta," a social media influence campaign funded by the same Russian oligarch already indicted by the Special Counsel for financing the Internet Research Agency. On the eve of the midterms, Facebook announced that it had suspended over 100 Facebook and Instagram accounts due to their potential affiliation with the Internet Research Agency.

In submitting a classified Intelligence Community report on foreign interference in December 2018, Director of National Intelligence Dan Coats stated: "Russia, and other foreign countries, including China and Iran, conducted influence activities and messaging campaigns targeted at the United States to promote their strategic interests."

As we approach the 2020 presidential election cycle, U.S. intelligence officials and security experts have warned that malign foreign influence operations will continue to evolve. According to FBI Director Christopher Wray, Russia likely viewed its influence activities in 2018 as a "dress rehearsal for the big show in 2020." In his 2019 Worldwide Threat Assessment, DNI Director Coats added: "We expect our adversaries and strategic competitors to refine their capabilities and add new tactics as they learn from each other's experiences, suggesting the threat landscape could look very different in 2020 and future elections."

The nonpartisan Brookings Institution predicts that foreign state actors will increasingly rely on artificial intelligence to conduct political warfare in the form of disinformation campaigns that are almost impossible to detect. To this end, our adversaries are refining the use of so-called "deepfakes," synthetically-doctored audio, photos, and videos that are highly-believable, inexpensive to produce, and have unlimited potential to go viral. Foreign influence campaigns are also trending towards subtler and harder to detect tactics, including by targeting specific audiences and amplifying divisive organic content over the creation of fake news and accounts, which are easier to identify.

In light of these threats, we must undertake a frank and bipartisan assessment of the vulnerabilities that remain in our election process.

While the Department of Homeland Security has established multiple task forces to combat foreign election interference, the DHS Inspector General reports that their effectiveness has been undermined by dramatic staffing cuts, leadership turnover, and a lack of coordination with state election officials. Meanwhile, the Election Assistance Commission, which is responsible for administering the $380 million in state grant funding that Congress appropriated for election security in 2018, is experiencing a shortage of technical expertise, including the recent departure of its top technology official in charge of testing and certifying voting systems.

Information sharing amongst intelligence agencies, state and local governments, and private sector technology companies has markedly increased since 2016. However, there is still significant room for improvement. The FBI's recent notification to state and local officials in Florida that Russian operatives had successfully hacked voter registration files in two counties in 2016, came nearly three years after the breach and over 6 months after the 2018 midterms. Social media companies and federal law enforcement agencies also must continue to improve their ability to communicate specific threat information and potential vulnerabilities in real-time.

Securing the integrity of our election process will require a collective and renewed commitment on the part of the public and private sectors to address these and other challenges. Only then can we be confident that future U.S. election outcomes truly reflect the will of the American people.

I now yield to the Ranking Member for his opening statement.

Contact: Aryele Bradford, Communications Director, (202) 226-5181.