Department of Justice

STATEMENT OF

NIKKI FLORIS
DEPUTY ASSISTANT DIRECTOR
COUNTERINTELLIGENCE DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON THE JUDICIARY
U.S. HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED
"SECURING AMERICA'S ELECTIONS PART II:
OVERSIGHT OF GOVERNMENT AGENCIES"

PRESENTED

OCTOBER 22, 2019

STATEMENT OF
NIKKI FLORIS
DEPUTY ASSISTANT DIRECTOR
COUNTERINTELLIGENCE DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON THE JUDICIARY
U.S. HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED
"SECURING AMERICA'S ELECTIONS PART II: OVERSIGHT OF GOVERNMENT AGENCIES"

PRESENTED
OCTOBER 22, 2019

Chairman Nadler, Ranking Member Collins, and Members of the Committee, I am pleased to appear before you today to discuss the FBI's efforts to combat foreign influence operations.

As Director Wray described during his all House and Senate briefing on this issue, we face multi-faceted foreign threats to our election security. And while our focus today is on election security, these adversaries are seeking to influence our national policies and public opinion in important ways beyond electoral cycles.

Foreign influence operations—which include covert, coercive, or corrupt actions by foreign governments to influence U.S. political sentiment or public discourse, or interfere in our processes themselves— are not a new problem. But the interconnectedness of the modern world, combined with the anonymity of the Internet, have changed the nature of the threat and how the FBI and its partners must address it. The goal of these foreign influence operations directed against the United States is to mislead, sow discord, and, ultimately, undermine confidence in our democratic institutions and values.

Foreign influence operations have taken many forms and used many tactics over the years. Most widely reported these days are attempts by adversaries—hoping to reach a wide swath of Americans covertly from outside the United States—to use false personas and fabricated stories on social media platforms to discredit U.S. individuals and institutions.

The FBI is the lead federal agency responsible for investigating foreign influence operations. In the fall of 2017, Director Christopher Wray established the Foreign Influence Task Force ("FITF") to identify and counteract malign foreign influence operations targeting the United States.

The FITF is led by the Counterintelligence Division and is comprised of agents, analysts, and professional staff from the Counterintelligence, Cyber, Counterterrorism, and Criminal Investigative Divisions. It is specifically charged with identifying and combating foreign influence operations targeting democratic institutions and values inside the United States. In all instances, the FITF strives to protect democratic institutions and public confidence; develop a common operating picture; raise adversaries' costs; and, reduce their overall asymmetric advantage.

The task force brings the FBI's national security and traditional criminal investigative expertise under one umbrella to prevent foreign influence in our elections. This better enables us to frame the threat, to identify connections across programs, to aggressively investigate as appropriate, and – importantly – to be more agile.

Coordinating closely with our partners and leveraging relationships we have developed in the technology sector, we had a number of instances where we were able to quickly relay threat indicators that those companies used to take swift action, blocking budding abuse of their platforms.

Following the 2018 midterm elections, we reviewed the threat and the effectiveness of our coordination and outreach. As a result of this review, we further expanded the scope of the FITF. Previously, our efforts to combat malign foreign influence focused solely on the threat posed by Russia. Utilizing lessons learned over the last year and half, the FITF is widening its aperture to confront malign foreign operations of China, Iran, and other global adversaries. To address this expanding focus and wider set of adversaries and influence efforts, we have also added resources to maintain permanent "surge" capability on election and foreign influence threats.

We have also further refined our approach. All efforts are based on a three-pronged approach, which includes: investigations and operations; information and intelligence sharing; and, a strong partnership with the private sector.

<u>Investigations and operations:</u>

Our Foreign Influence Task Force partners with the 56 field offices across the country on open FBI investigations with a foreign influence nexus. Think of the Task Force as the hub, with spokes out to our 56 field offices, and our expansive front line agents, analysts, and professional staff. Investigations with a cyber nexus are worked collaboratively with our Cyber Division and the Cyber Task Forces throughout the nation to quickly respond to these threats to protect systems and work with the Intelligence Community to determine attribution.

Our investigative approach also seeks to affirmatively impose costs on our adversaries, particularly key influencers or enablers. Just last fall, we charged Elena Khusyaynova, a Russian national, with criminal violations stemming from her efforts to influence the 2016 and 2018 elections in her role as Chief Accountant for Project Lakhta—a Russian disinformation

organization (connected to the Internet Research Agency) that had budgeted over $10 million in the first half of 2018 alone for initiatives to undermine the U.S. political system and candidates.

Another Russian national, Maria Butina, was sentenced in federal court a few months ago for conspiring with a Russian intelligence service to influence unwitting American political organizations and advocacy groups.

Information and intelligence sharing:

Make no mistake, we are working closely with our partners at every level to establish a common understanding of the threat landscape, share intelligence, and detect, disrupt, and deter our adversaries. In 2018, that effort culminated in the creation of *Protected Voices.*

Through this program, we developed a series of videos, available through the FBI's public website, to help political campaigns better understand this threat. In the past months, we have expanded Protected Voices, providing webinars and in-person briefings to the presidential campaigns on cyber and malign foreign influence threats. In the coming months, the FBI will further expand the audience to include congressional campaigns and their many supporting entities.

The FBI, in partnership with ODNI and DHS, is working to update and expand this resource for the 2020 election season, to provide even more information on how to identify and report foreign intelligence efforts against campaigns and their staffs.

We also are collaborating extensively with our U.S. Government partners, particularly DHS, to provide information nationwide to state governments, local election officials, private election vendors, and others so they can harden their systems against cyberattacks. The majority of technical information the FBI has been able to provide these groups and the public since 2016 was a direct result of self-reporting and cooperation with the FBI from social media companies and election officials and vendors. By partnering with the FBI, these groups are helping the nation combat our adversaries' activities.

Relationship with the private sector:

Technology companies have a front-line responsibility to secure their own networks, products, and platforms. We have provided actionable intelligence to help them address abuse of their platforms by foreign actors. In turn, social media companies have passed to FBI several hundred previously unknown accounts being used by bad actors, which we, in turn, have shared with our partners in the wider Intelligence Community.

In the run up to the 2018 mid-term elections, social media companies deactivated more than 1,000 inauthentic social media accounts linked to malign foreign influence actors. The companies made these decisions informed by dialogue and information exchanges with the FBI and other government agencies.

Our relationship with social media companies works best when they also give us notice when they see foreign threat actors testing out new techniques and tactics online. That helps us refine, enhance, and sharpen our efforts to tackle this threat.

Conclusion

To our knowledge, no foreign government has attempted to tamper with U.S. vote counts. We do know that our adversaries are actively trying to influence public opinion and electoral processes in advance of the 2020 election.

We must continue to take this threat seriously, be ready to evolve as it inevitably will, and keep tackling it with fierce determination and focus.

We look forward to continuing this important work and appreciate the support of this committee. Thank you for the opportunity to appear before you today. I am happy to answer any questions you may have.