STEPHEN F. LYNCH
8TH DISTRICT, MASSACHUSETTS

COMMITTEE ON FINANCIAL SERVICES
SUBCOMMITTEE ON CAPITAL MARKETS AND GOVERNMENT SPONSORED ENTERPRISES
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
RANKING MEMBER, SUBCOMMITTEE ON NATIONAL SECURITY
SUBCOMMITTEE ON GOVERNMENT OPERATIONS

ASSISTANT DEMOCRATIC WHIP

Congress of the United States
House of Representatives
Washington, DC 20515-2108

2268 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
202-225-8273
202-225-3984 FAX

1 HARBOR STREET
SUITE 304
BOSTON, MA 02210
617-428-2000
617-428-2011 FAX

PLYMOUTH COUNTY REGISTRY BUILDING
155 WEST ELM STREET
SUITE 200
BROCKTON, MA 02301
508-586-5555
508-580-4692 FAX

1245 HANCOCK STREET
SUITE 16
QUINCY, MA 02169
617-657-6305
617-773-0995 FAX

LYNCH.HOUSE.GOV

December 14, 2016

The Honorable Jason Chaffetz
Chairman
Committee on Oversight and Government Reform
2157 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Chaffetz:

As Ranking Member of the Subcommittee on National Security, I respectfully request that the Committee on Oversight and Government Reform commence a bipartisan investigation to examine reports that the Russian Federation ("Russia") engaged in cyberespionage targeting U.S. entities and individuals in order to interfere with the 2016 U.S. federal elections. This investigation would serve to identify continuing vulnerabilities in the cybersecurity systems deployed by public and private entities in order to safeguard the integrity of our most critical computer networks and the American people against the impact of a catastrophic data breach.

As underscored by Director of National Intelligence James Clapper in his recent *Worldwide Threat Assessment of the US Intelligence Community*, cyberattacks launched against U.S. Government and civilian systems and infrastructure remain a high-priority global security threat. In assessing the leading threat actors in this area, Director Clapper cited Russia as "*assuming a more assertive cyber posture based on its willingness to target critical infrastructure systems and conduct espionage operations even when detected and under increased public scrutiny.*"[1] Moreover, Director Clapper noted that Russian cyber operations will likely target U.S. interests in order to achieve multiple strategic objectives.[2] These include intelligence-gathering activities in support of Russian military and political goals, Russian foreign policy decisions in the Ukraine, Syrian, and other crises; and continued developments in the field of cybertechnology to prepare the country for "*future contingencies*."[3]

---

[1] *Worldwide Threat Assessment of the US Intelligence Community*, James R. Clapper, Director of National Intelligence (February 9, 2016) (online at https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf).
[2] *Id.*
[3] *Id.*

The grave security threat posed by Russian Government cyberoperations has been most recently evidenced by U.S. Intelligence Community reports indicating that Russia sought to interfere with the 2016 U.S. federal elections. On October 7, 2016, the Office of the Director of National Intelligence and the Department of Homeland Security issued an unprecedented joint statement expressing confidence on behalf of the U.S. Intelligence Community that the "*Russian Government directed the recent compromises of e-mails from US persons and institutions*" in order to "*interfere with the US election process*."[4] In the aftermath of this announcement, Adm. Michael Rogers, Director of the National Security Agency and Commander of the U.S. Cyber Command, stated that *"[t]his was a conscious effort by a nation-state to attempt to achieve a specific effect."*[5] As recently characterized by the New York Times, *"[w]hile there's no way to be certain of the ultimate impact of the hack, this much is clear: A low-cost, high-impact weapon that Russia had test-fired in elections from Ukraine to Europe was trained on the United States, with devastating effectiveness...For Russia, with an enfeebled economy and a nuclear arsenal it cannot use short of all-out war, cyberpower proved the perfect weapon: cheap, hard to see coming, hard to trace."*[6]

These reports clearly merit a robust and bipartisan examination by the Committee on Oversight and Government Reform. In the interest of national security, our Committee has already initiated a series of bipartisan investigations during the 114th Congress to examine cyberattacks in the public and private sectors including the devastating breach of information technology systems at the Office of Personnel Management in 2015 that compromised the personal identifiable information of over 22 million security clearance holders, clearance applicants, current and former federal employees, and other individuals. We have also investigated cybersecurity threats faced by private entities including massive data breaches at Target, Anthem Blue Cross and Blue Shield, JPMorgan Chase, and Home Depot. A bipartisan investigation to examine reports of Russian interference with U.S. federal elections would only further our ability to identify and address weaknesses in our public and private cyberdefenses in order to safeguard critical U.S. Government and private institutions against the sort of cyberattacks that the White House, the U.S. State Department, the Pentagon, and various commercial banks, retail chains, and other private companies have experienced in recent years.

In furtherance of this request, I would also note that reports of Russian interference with the 2016 U.S. elections have been a source of significant bipartisan concern. Just this week, Senators John McCain (R-AZ), Lindsey Graham (R-SC), Chuck Schumer (D-NY), and Jack Reed (D-RI) released a joint statement indicating that Russian cyberattacks have targeted our democratic institutions and that *"[r]ecent reports of Russian interference in our election should alarm every American."*[7] The joint statement also provides that "*Democrats and Republicans must work together, and across the jurisdictional lines of the*

---

[4] Office of the Director of National Intelligence and Department of Homeland Security, *Joint DHS and ODNI Election Security Statement* (October 7, 2016) (online at https://www.dni.gov/index.php/newsroom/press-releases/215-press-releases-2016/1423-joint-dhs-odni-election-security-statement).

[5] *NSA Chief Speaks Candidly of Russia and U.S. Election*, CBS News (November 17, 2016) (online at http://www.cbsnews.com/news/nsa-chief-adm-michael-rogers-speaks-candidly-of-russias-use-of-wikileaks-in-u-s-election/).

[6] *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, The New York Times, (December 13, 2016) (online at http://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=a-lede-package-region&region=top-news&WT.nav=top-news&_r=0).

[7] U.S. Senate Committee on Armed Services, *McCain, Graham, Schumer, Reed Joint Statement on Reports that Russia Interfered with the 2016 Election* (December 11, 2016) (online at http://www.armed-services.senate.gov/press-releases/mccain-graham-schumer-reed-joint-statement-on-reports-that-russia-interfered-with-the-2016-election).

Congress, to examine these recent incidents thoroughly and devise comprehensive solutions to deter and defend against further cyberattacks." [8]

For these reasons, I again respectfully request that you initiate a bipartisan investigation to examine reports of Russian interference with the 2016 U.S. elections. Thank you in advance for your consideration.

Sincerely,

STEPHEN F. LYNCH
Ranking Member
Subcommittee on National Security
(MA-08)

[8] *Id.*