116TH CONGRESS
1st Session

SENATE

REPORT
116-XX

(U) REPORT

OF THE

SELECT COMMITTEE ON INTELLIGENCE

UNITED STATES SENATE

ON

RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION

VOLUME 5: COUNTERINTELLIGENCE THREATS AND VULNERABILITIES

Caplin & Drysdale

V. (U) RECOMMENDATIONS

(U) The Committee's inquiry highlighted several ways in which hostile actors were able to capitalize on gaps in laws or norms and exert influence. Those areas included unclear laws regarding foreign advocacy, flawed assumptions about what intelligence activity looks like, and a campaign's status as a private entity intertwined with the structures of democracy. Further, the freedom of expression at the root of our democratic society became an opportunity for Russian influence to hide in plain sight.

(U) The Committee's recommendations, outlined below, present a variety of paths through which Congress, the executive branch, and private entities and individuals can and should begin to respond to these threats, both jointly and independently. These recommendations, however, do not mark the end of the Committee's work in this space, which requires ongoing vigilance by the United States government and further consideration of legislative and policy responses. To that end, the Committee will continue to evaluate and consider the results of this investigation as part of its ongoing oversight and legislative responsibilities and its efforts to understand and address malign foreign interference targeting U.S. democratic processes.

1. (U) Review, Update, and Enforce the Foreign Agents Registration Act and Related Statutes

(U) The Committee recommends that Congress update the Foreign Agents Registration Act (FARA), and that the Department of Justice (DOJ) clarify the statute's requirements by issuing public guidance on enforcement and more stringently enforcing the existing statute. FARA was enacted over 80 years ago, in large part to target Nazi propaganda. FARA seeks to aid the U.S. Government and the American people in understanding and evaluating the activities, statements, and motives of individuals and entities functioning as agents of foreign principals in the United States. Since that time, Congress has made some modifications to the statute to increase transparency with respect to lawyers and lobbyists who also engage in political activity on behalf of foreign powers inside the United States. However, loopholes still exist, and foreign actors exploited those loopholes in 2016. The Committee's investigation revealed a number of lawyers, public relations experts, businesses, political consultants, and campaign operatives working in the United States in coordination with, or at the request of, foreign principals. Many of these individuals and businesses did not register under FARA.

- (U) DOJ should increase enforcement of FARA. For years, DOJ failed to pursue criminal penalties for even the most flagrant violations of the statute. While recent enforcement efforts have resulted in several successful criminal prosecutions, the Committee found numerous incidents where FARA registrations were excessively delayed, retroactive, incomplete, inaccurate, or otherwise insufficient to accomplish the objectives of the law.

Committee Sensitive

- (U) DOJ should publish comprehensive public guidance on FARA. In part as a result of limited enforcement, the public has insufficient information about the statute's scope and application. DOJ's interpretation of the statute is largely untested and undefined. While DOJ has made efforts to publish more information about its interpretation of the statute, including through the publication of advisory opinions, these are overly redacted and incomplete. Comprehensive public guidance has been beneficial for other similarly-situated statutes, and those publications, such as DOJ's *Resource Guide to the U.S. Foreign Corrupt Practices Act,* may serve as a helpful model in issuing useful and practical guidance on FARA.

- (U) Congress should update FARA to more clearly define the activities covered by the statute. This may include narrowing or redefining the breadth of some provisions, such as those that may apply to purely foreign consulting, while strengthening other provisions, such as activities targeting the U.S. Government or the American people.

- (U) Congress should remove the Lobbying Disclosure Act (LDA) exemption to FARA registration. Currently, FARA registrants for foreign principals who are not themselves foreign governments or political parties may register under the LDA regime rather than the more comprehensive registration regime under FARA. The Committee found that individuals not formally affiliated with a foreign government may nonetheless sufficiently represent that government's interest, even if that government is not the principal beneficiary, to merit the application of FARA's heightened requirements.

(U) Congress should also examine whether other foreign agent laws and the Espionage Act need to be updated to more effectively address the reality of modern intelligence operations targeting the United States.

- (U) For example, 18 U.S.C. § 951 makes it a crime to operate as an agent of a foreign government, to include an agent with respect to non-political activity, without first notifying the Attorney General. While DOJ has generally reserved prosecutions under this statute for behavior that resembles espionage, the statute's overlap with FARA and its general scope may need refined and updated. 18 U.S.C. § 219 provides criminal penalties for a public official of the United States to be or act as an agent of a foreign principal required to register under FARA. Together, these and other interrelated law make up a patchwork of overlapping and ill-defined prohibitions that are overdue for a more thorough review.

(U) Although DOJ makes FARA registration filings publicly available on its website, there is no obligation on registrants to disclose this information when they are engaged in covered political activities. As a result, the registration materials do little to further the statute's goal of transparency for the American public. This lack of transparency is especially acute in the

Capitol Hill Publishing

media space, where messaging by a single FARA registrant has the potential to reach millions of Americans.

- (U) Congress should amend FARA to mandate, or the Federal Communications Commission (FCC) and other relevant authorities should impose a requirement, that FARA-registered news agencies operating in the United States provide clear, prominent, and regular notifications to audiences regarding the outlet's FARA-registered status. Transparency should be affirmatively provided to audiences on a regular basis so that the American public is able to make informed decisions about information consumption.

- (U) In addition, all U.S. media outlets should clearly label or otherwise identify content that appears in connection with FARA-registered work, even if it comes in the form of an opinion column. It is the ultimate responsibility of the editorial staff at U.S. media outlets to understand the origins of the information that their journalists and outside contributors are promoting, and to inform their audiences when that information is in some way sponsored or influenced by a foreign agent.

- (U) More broadly, all U.S. media outlets should clearly label opinion content as such, in particular when opinion content, in tone or in format, could be mistaken for journalistic reporting.

2. (U) Recognize Russia's Use of Non-Traditional Intelligence Actors for Influence

(U) The Russian government treats oligarchs, organized crime, and associated businesses as tools of the state, rather than independent, private entities. The Kremlin uses these entities to pursue Kremlin priorities, including money laundering, sanctions evasion, and influence operations. This is a fundamentally different model than in the United States.

- (U) While U.S. companies can and should conduct business as they see fit within the bounds of the law, they should proceed with maximum caution when doing business in Russia. Business exchanges can be a vehicle for compromise of electronic devices, collection of compromising information for influence efforts, theft of proprietary business information, and recruitment by intelligence services. Such efforts can be overt or covert, and can target national security information and hamper the competitiveness of U.S. companies. American business leaders need to understand that they, too, are a target and take precautions.

- (U) Politically-active U.S. organizations, including non-profits and advocacy groups, should likewise recognize that they can also be, and likely are, targeted by foreign intelligence services. Although the known targeting in 2016 was directed toward conservative organizations, organizations of all political and ideological stripes should be prepared for it. Hostile foreign governments may seek to influence U.S. policy in foreign

Committee Sensitive

affairs, energy and environmental policy, military conflict, and others matters involving international relations, through indirect channels like these. Leadership in such organizations should consider conducting due diligence, as appropriate, when dealing with counterparts from adversarial countries, and adopting sound cyber security practices to protect their networks and sensitive information.

- [redacted] Just as business leaders need to recognize their counterparts may be extensions of the Russian state, the U.S. Government should similarly treat non-governmental entities close to the Kremlin as legitimate targets for intelligence collection and surveillance. The U.S. Government needs the tools and authorities in place to determine whether a non-governmental entity is operating on behalf of the Russian state and mitigate the counterintelligence threat, particularly if that entity seeks to operate in the United States or allied countries. These tools and authorities should augment the entire spectrum of U.S. Government activities, including to the ability to deny visas, the ability to conduct surveillance akin to that used against suspected intelligence officers, and the ability to target financial operations, such as the ability to deny transactions or seize assets.

3. (U) Protect Campaigns from Foreign Influence Efforts

(U) As part of its counterintelligence mission, FBI should offer defensive briefings to all presidential campaigns, including during the primaries, for both candidates and staff. FBI should provide detailed briefings as specific issues arise. When nominees are official, FBI should undertake a renewed effort to educate campaigns—from leadership to schedulers—about the avenues of influence adversaries use. These briefings should include specific, if hypothetical, examples and clear defensive steps campaigns can take. FBI has traditionally delivered these briefings as brief conversations; given the aggressive efforts Russia undertook in 2016 and the likelihood of similar future efforts by Russia and others, these conversations should cover cybersecurity best practices and how to recognize approaches that are outside ordinary relationship building.

(U) Future presidential campaigns should perform thorough vetting of staff, particularly those staff who have responsibilities that entail interacting with foreign governments. Diligence, experience, and caution are all the more critical when interacting with representatives of adversaries' governments.

(U) Campaigns should recognize that campaign staff are attractive targets for foreign intelligence services, and that staff who have not previously been sensitized to counterintelligence threats are especially vulnerable to targeting and exploitation. Presidential campaigns should require staff who interact with foreign governments to receive counterintelligence training from the FBI. Further, that staff should report to designated campaign leadership any foreign contacts, including any offers of foreign assistance, so that the

Committee Sensitive

campaign can recognize patterns in foreign outreach. Campaigns should institute a centralized reporting structure to ensure that suspicious contacts with foreign governments or their proxies are documented and can be shared with law enforcement when appropriate, in a timely and accurate manner. This information would assist U.S. counterintelligence efforts to more quickly identify patterns and a clearer picture of nation-level threats. FBI and law enforcement should treat the information passed by campaigns as extremely sensitive, and protect the information from inadvertent disclosure, such as by limiting the number of personnel with access. In addition, a full understanding of the problem will encourage law enforcement agencies to pass defensive information back to campaigns.

(U) To facilitate these activities, campaigns should designate specific individuals to be responsible for counterintelligence and for cybersecurity issues. These individuals should be clearly identified within the campaign as a point of contact for security-related questions or concerns, but will also serve as an accountable entry point for the FBI's interaction and information sharing with the campaign.

(U) Campaigns should notify FBI of all foreign offers of assistance, and all staff should be made aware of this expectation. In order to not encourage, or amplify, foreign influence efforts, campaigns should reject the use of foreign origin material, especially if it has potentially been obtained though the violation of U.S. law.

(U) The Russian Government has sought to understand, and potentially exploit, vulnerabilities in the U.S. campaign finance system in furtherance of Russia's election influence activities. Russia's interest in this tactic is longstanding. The Committee is not aware of specific successful efforts in this regard related to the 2016 U.S. election, however the Committee's insight is limited, and in other countries Russia has gone to great lengths to launder money intended for election influence. The DOJ, the Intelligence Community, regulators and legislators should work together to identify and address any loopholes that could be abused, by Russia or any other foreign actor, in malign influence operations targeting U.S. elections.

4. Protect Government Employees from Foreign Influence Efforts

(U) Congressional leadership should work with the IC and federal law enforcement to assess the counterintelligence and foreign influence risk associated with foreign government-funded travel by congressional staff, in particular the Mutual Educational and Cultural Exchange Act. Congress does not allow registered lobbyists to pay for the travel or the meals of congressional staff due to concerns about undue influence. This same logic should apply to foreign governments. Congressional leadership should explore increasing the budget for staff travel, so that it is funded and managed by Congress and not by foreign governments.

Committee Sensitive

(U) In addition to enhanced cybersecurity training for all U.S. Government personnel, all federal government employees who travel internationally, regardless of agency or department, should be required to receive counterintelligence training.

5. (U) **Bolster Resources for IC Elements to Uncover Influence Campaigns and Focus the NIPF on Foreign Government Influence**

[redacted] These terms are vague and vast, and do not acknowledge the growing threat of disruption by foreign actors conducting malign influence activities targeting the United States.

- (U) The Committee recommends, therefore, that all future iterations of the NIPF, which is an exercise and tool used to distribute finite IC resources across a wide variety of threats, specify and prioritize foreign malign influence activities.

[redacted]

(U) FBI should empower its analysts to check assumptions underpinning FBI operations, to apply the rigor of intelligence analysis to assessments and confidential human sources, and to create a culture where questioning previously held assumptions is acceptable and encouraged.

6. (U) **Improve Victim Notification and Information Sharing**

Caplin & Drysdale

(U) While the Committee understands FBI's reluctance to force solutions on hacked victims, FBI should develop a clear policy to address how to escalate victim notifications within a hacked entity, particularly for those involved in an election, when it appears that entity has not successfully remediated a cyber breach.

(U) In addition, the FBI's Cyber Division should have an escalation policy for how to engage a victim entity when the victim is not responsive to the FBI's investigative needs. The policy should include how to communicate with the victim entity about escalation, and, in narrow situations where the security of the election is at risk, the potential use of compulsory process. Channels of communication, both within the FBI and with political organizations, should be established early in a campaign cycle.

(U) The FBI should seek to downgrade and share classified information for defense against cyber intrusions whenever possible. If downgrading the information is not feasible, the FBI should work to find a cleared individual at the victim entity and brief that individual at the highest possible level about the incident, prior to or contemporaneous with engaging with the entity's IT staff.

(U) The FBI should develop clear best practices for dealing with cybersecurity vendors in incident response. Congress should consider legislation that mandates third-party cybersecurity vendors to report indicators of nation-state compromise to the U.S. Government, be it through FBI or other entities, which may include sharing malware, network traffic, forensic images, and other appropriate data to enable the U.S. Government to protect against nation-state cyber adversaries. Any sharing mandate should also include suitable protections for personally identifiable information or other sensitive or privileged material.

7. (U) Strengthen Congressional Authority to Challenge Executive Privilege

(U) Congress should consider amending the Senate's subpoena enforcement statute to remove or otherwise limit the carve out in 28 U.S.C. § 1365(a) that precludes enforcement against government officials asserting a "governmental privilege or objection." This exception, the Committee's investigation showed, allows for the potential abuse of executive privilege claims. Such an amendment should include a process to expedite judicial review of disputes between Congress and the executive branch over subpoena compliance, and clarify that a government official's mere assertion of a government privilege does not strip a federal court of jurisdiction.

Caplin & Drysdale