(U) Summary Table of Findings

CHAPTER 1: RUSSIAN CAMPAIGNS IN EUROPE
(U) Finding #1: The Kremlin exploits free or independent media spaces and open democracies to conduct active measures in Europe.
(U) Finding #2: Russia supports fringe political parties and non-governmental organizations in Europe to further the Kremlin's agenda while also disparaging or discrediting politicians and groups seen as hostile to Moscow.
(U) Finding #3: Russia conducts increasingly aggressive cyber operations against European governments; a tactic that will continue to present a profound threat.
(U) Finding #4: Russia targets disaffected European populations and exploits social, political, and racial divisions in an effort to sow discord, encourage unrest, and incite protests.
(U) Finding #5: Russia leverages business and economic ties in Europe to achieve the Kremlin's goals, message displeasure, or inflict punishment.
(U) Finding #6: European governments and media outlets are conducting a variety of activities to combat Russian influence campaigns.
CHAPTER 2: RUSSIA ATTACKS THE UNITED STATES
(U) Finding #7: Russia conducted cyberattacks on U.S. political institutions in 2015-2016.
(U) Finding #8: Russian-state actors and third-party intermediaries were responsible for the dissemination of documents and communications stolen from U.S. political organizations.
(U) Finding #9: The Russian government used RT to advance its malign influence campaign during the 2016 U.S. presidential election.
(U) Finding #10: Russian intelligence leveraged social media in an attempt to sow social discord and to undermine the U.S. electoral process.
CHAPTER 3: AMERICA REACTS
(U) Finding #11: The Federal Bureau of Investigation's notification to numerous Russian hacking victims was largely inadequate.
(U) Finding #12: Communication between the Department of Homeland Security and state election officials was impeded by state officials' mistrust of federal government overreach coupled with a unprecedented level of Russian cyber intrusions.

(U) Summary Table of Findings (cont.)

CHAPTER 3: AMERICA REACTS (CONT.)
(U) Finding #13: The joint Office of the Director of National Intelligence and Department of Homeland Security public statement attributing election interference to Russia was ineffective.
(U) Finding #14: The Executive Branch's post-election response was insufficient.
(U) Finding #15: The majority of the Intelligence Community Assessment judgments on Russia's election activities employed proper analytic tradecraft.
(U) Finding #16: The Intelligence Community Assessment judgments on Putin's strategic intentions did not employ proper analytic tradecraft.
(U) Finding #17: The Federal Bureau of Investigation opened an enterprise counterintelligence investigation into the Trump campaign after receiving information related to Trump campaign foreign policy advisor George Papadopoulos.
(U) Finding #18: As part of the enterprise counterintelligence investigation into the Trump campaign, the Federal Bureau of Investigation opened an individual counterintelligence investigation into Carter Page.
(U) Finding #19: The dossier compiled by Christopher Steele formed an essential part of an application to the Foreign Intelligence Surveillance Court to obtain electronic surveillance on Carter Page.
(U) Finding #20: Special Counsel Robert Mueller indicted Paul Manafort on several charges, none of which relate to allegations of collusion, coordination, or conspiracy between the Trump campaign and the Russian government.
(U) Finding #21: [classified]
(U) Finding #22: General Flynn pleaded guilty to making a false statement to the Federal Bureau of Investigation regarding his December 2016 conversations with Ambassador Kislyak, even though the Federal Bureau of Investigation agents did not detect any deception during Flynn's interview.
(U) Finding #23: Executive Branch officials did not notify the Trump campaign that members of the campaign were assessed to be potential counterintelligence concerns.
(U) Finding #24: The February 2018 indictment of the Internet Research Agency and Russian nationals exposes Russian actors and their intent to spread distrust towards the candidates and the political system in general.

(U) Summary Table of Findings (cont.)

CHAPTER 4: CAMPAIGN LINKS WITH RUSSIA
(U) Finding #25: When asked directly, none of the interviewed witnesses provided evidence of collusion, coordination, or conspiracy between the Trump campaign and the Russian government.
(U) Finding #26: The Committee found no evidence that President Trump's pre-campaign business dealings formed the basis for collusion during the campaign.
(U) Finding #27: The Republican national security establishment's opposition to candidate Trump created opportunities for two less-experienced individuals with pro-Russia views to serve as campaign advisors: George Papadopoulos and Carter Page.
(U) Finding #28: The change in the Republican Party platform regarding Ukraine resulted in a stronger position against Russia, not a weaker one, and there is no evidence that Paul Manafort was involved.
(U) Finding #29: There is no evidence that Trump associates were involved in the theft or publication of Clinton campaign-related emails, although Trump associates had numerous ill-advised contacts with WikiLeaks.
(U) Finding #30: Carter Page did not travel to Moscow in July 2016 on behalf of the Trump campaign, but the Committee is concerned about his seemingly incomplete accounts of his activity in Moscow.
(U) Finding #31: George Papadopoulos' attempts to leverage his Russian contacts to facilitate meetings between the Trump campaign and Russians was unsuccessful.
(U) Finding #32: Donald Trump Jr., Jared Kushner, and Paul Manafort attended a June 9, 2016, meeting at Trump Tower where they expected to receive—but did not ultimately obtain—derogatory information on candidate Clinton from Russian sources.
(U) Finding #33: Donald Trump Jr. briefly met with a Russian government official at the 2016 National Rifle Association annual meeting, but the Committee found no evidence that the two discussed the U.S. presidential election.
(U) Finding #34: The Committee found no evidence that meetings between Trump associates—including Jeff Sessions—and official representatives of the Russian government—including Ambassador Kislyak—reflected collusion, coordination, or conspiracy with the Russian government.

(U) Summary Table of Findings (cont.)

CHAPTER 4: CAMPAIGN LINKS WITH RUSSIA (CONT.)
(U) Finding #35: Possible Russian efforts to set up a "back channel" with Trump associates after the election suggest the absence of collusion during the campaign, since the communication associated with collusion would have rendered such a "back channel" unnecessary.
(U) Finding #36: Prior to conducting opposition research targeting candidate Trump's business dealings, Fusion GPS conducted research benefitting Russian interests.
(U) Finding #37: The law firm Perkins Coie hired Fusion GPS on behalf of the Clinton campaign and the Democratic National Committee to research candidate Trump's Russia ties.
(U) Finding #38: Christopher Steele claims to have obtained his dossier information second- and third-hand from purported high-placed Russian sources, such as government officials with links to the Kremlin and intelligence services.
(U) Finding #39: Christopher Steele's information from Russian sources was provided directly to Fusion GPS and Perkins Coie and indirectly to the Clinton campaign.
CHAPTER 5: INTELLIGENCE COMMUNITY ASSESSMENT LEAKS
(U) Finding #40: Leaks of classified information regarding Russian intentions to sow discord in the U.S. presidential election began prior to the election day—November 8, 2016.
(U) Finding #41: Leaks of classified information alleging Russian intentions to help elect candidate Trump increased dramatically after the election day—November 8, 2016.
(U) Finding #42: The leaks prior to the classified Intelligence Community Assessment's publication, particularly leaks occurring after the U.S. presidential election, correlate to specific language found in the Intelligence Community Assessment.
(U) Finding #43: Continued leaks of classified information have damaged national security and potentially endangered lives.
(U) Finding #44: Former Director of National Intelligence James Clapper, now a CNN national security analyst, provided inconsistent testimony to the Committee about his contacts with the media, including CNN.

(U) Summary Table of Recommendations

CHAPTER 1: RUSSIAN CAMPAIGNS IN EUROPE
(U) Recommendation #1: European governments, non-governmental organizations, businesses, think tanks, and academia should strengthen legal and regulatory environments, promote media pluralism, build professional media associations, and improve the financial sustainability of legitimate news outlets.
(U) Recommendation #2: European governments, non-governmental organizations, businesses, think tanks, and academia should implement and encourage multi-pronged, country-wide efforts by both public and private entities to combat Russian propaganda, technical, and cyber operations.
(U) Recommendation #3: European governments, non-governmental organizations, businesses, think tanks, and academia should implement more stringent cyber security practices, such as multifactor authentication and encryption of sensitive data, as well as educating workforces on basic cyber security topics and best practices.
(U) Recommendation #4: European governments should look to long-term solutions to lessen economic dependence on Russia.
CHAPTER 2 & 3: RUSSIA ATTACKS THE UNITED STATES AND AMERICA REACTS
(U) Recommendation #5: Congress should identify options available to the private sector and federal government that would address the social media vulnerabilities exploited by the Russian government.
(U) Recommendation #6: Congress should consider updating the Foreign Intelligence Surveillance Act to cover malicious international cyber actors.
(U) Recommendation #7: The Federal Bureau of Investigation should improve cyberattack victim notification.
(U) Recommendation #8: Threats identified by the Intelligence Community to state and local elections infrastructure should be immediately briefed to appropriate state and local officials. When threats are identified, the federal government should conduct an expedited declassification review to ensure that the threat information can reach all necessary state and local officials in a timely manner.
(U) Recommendation #9: The Secretary of Homeland Security should provide certain designated state and local election officials appropriate security clearances to enable those officials to respond to election-related threats.

(U) Summary Table of Recommendations (cont.)

CHAPTER 2 & 3: RUSSIA ATTACKS THE UNITED STATES AND AMERICA REACTS (CONT.)
(U) Recommendation #10: Significant threats to U.S. elections identified by the Intelligence Community, including cyberattacks directed at political organizations, should be immediately reported to the Congressional intelligence committees.
(U) Recommendation #11: Congress should encourage the adoption of National Institute of Standards and Technology cyber security standards, such as those adopted by the Elections Assistance Commission, by providing federal resources to state and local governments to facilitate such adoption. Funds should be tied to the adoption and certification of elections systems to appropriate standards.
(U) Recommendation #12: Congress should consider additional funding for the National Institute of Standards and Technology to enable better outreach to state and local governments.
(U) Recommendation #13: Congress should consider a one-time grant to state and local election agencies to conduct a risk assessment of those agencies' computer systems.
(U) Recommendation #14: Congress should consider strengthening the Help America Vote Act of 2002 to ensure that both statewide voter registration and tabulation systems are better protected from foreign cyber threats.
(U) Recommendation #15: The Department of Homeland Security should provide the owner or operator of any electronic election infrastructure affected by any significant foreign cyber intrusion with a briefing and include steps that may be taken to mitigate such intrusions.
(U) Recommendation #16: State and local governments should be encouraged to establish redundancies that are not dependent on current elections infrastructure, such as a mechanism that retains individual vote records, ensuring the integrity of the vote in the event of a compromise of voting infrastructure due to a foreign cyberattack. An example of such a redundancy is a contemporaneously created paper record reflecting the voter's selections.
(U) Recommendation #17: While it is important to implement lessons learned from the Executive Branch's response, Congress should not hamper the Executive Branch's ability to use discretion in responding to a particular foreign threat.
(U) Recommendation #18: Congress should consider repealing the Logan Act.

CHAPTER 2 & 3: RUSSIA ATTACKS THE UNITED STATES AND AMERICA REACTS (CONT.)
(U) Recommendation #19: All U.S. presidential campaigns should receive unclassified counterintelligence briefings at an appropriate time prior to a nomination convention.
(U) Recommendation #20: When consistent with national security, the Intelligence Community should immediately inform U.S. presidential candidates when it discovers a legitimate counterintelligence threat to the campaign, and promptly notify Congress.
(U) Recommendation #21: Both houses of Congress should consider requiring all staff to receive an annual counterintelligence awareness briefing.
CHAPTER 4: CAMPAIGN LINKS TO RUSSIA
(U) Recommendation #22: Political campaigns and law enforcement should ensure that their counterintelligence defenses appropriately account for the role of cut-outs and intermediaries.
(U) Recommendation #23: Congress should consider amending current campaign finance laws to further increase transparency regarding services provided by foreign persons or entities.
CHAPTER 5: INTELLIGENCE COMMUNITY ASSESSMENT LEAKS
(U) Recommendation #24: Each component of the Intelligence Community should update its guidance regarding media contacts to ensure the guidance applies to every employee, including senior officials.
(U) Recommendation #25: Congress should consider legislation to increase the penalties for unauthorized disclosures of classified information.
(U) Recommendation #26: The Executive Branch should consider instituting mandatory polygraphs for all non-confirmed political appointees that have top secret clearances.