Senate Intel Releases Election Security Findings in First Volume of Bipartisan Russia Report (/public/index.cfm/pressreleases?ID=64E1C6F5-71D2-4325-BA1D-AFB2182AF639)

Jul 25 2019

WASHINGTON – Today, Senate Select Committee on Intelligence Chairman Richard Burr (R-NC) and Vice Chairman Mark Warner (D-VA) released "*Russian Efforts Against Election Infrastructure (https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf)*," the first volume in the Committee's bipartisan investigation into Russia's attempts to interfere with the 2016 U.S. elections.

Today's installment builds upon the unclassified summary findings on election security released (https://www.intelligence.senate.gov/press/senate-intel-committee-releases-unclassified-1st-installment-russia-report-updated) by the Committee in May 2018. This was the first volume completed due to the fundamental importance and urgency of defending our democratic elections.

As part of its investigation, the Committee will also release final volumes examining the Intelligence Community Assessment (ICA) of Russian interference, the Obama Administration's response to Russian interference, the role of social media disinformation campaigns, and remaining counterintelligence questions. The Committee has submitted its volume on social media for declassification review and intends to release the remaining installments in fall 2019.

Over the last two and half years, the Committee's investigation has spanned more than 15 open hearings, more than 200 witness interviews, and nearly 400,000 documents.

Statement from Chairman Burr:

"In 2016, the U.S. was unprepared at all levels of government for a concerted attack from a determined foreign adversary on our election infrastructure. Since then, we have learned much more about the nature of Russia's cyber activities and better understand the real and urgent threat they pose. The Department of Homeland Security and state and local elections officials have dramatically changed how they approach election security, working together to bridge gaps in information sharing and shore up vulnerabilities. The progress they've made over the last three years is a testament to what we can accomplish when we give people the opportunity to be part of a solution.

"There is still much work that remains to be done, however. I am grateful to the many states that provided their points of view, which helped inform our recommendations. It is my hope that the Senate Intelligence Committee's bipartisan report will provide the American people with valuable insight into the election security threats still facing our nation and the ways we can address them."

Statement from Vice Chairman Warner:

"When the Russians attacked elections systems in 2016, neither the federal government nor the states were adequately prepared. Our bipartisan investigation identified multiple problems and information gaps that hindered our ability to effectively respond and defend against the Russian attack in 2016. Since then – and in large part as a result of the bipartisan work done on this issue in our Committee – the intelligence community, DHS, the FBI, and the states have taken steps to ensure that our elections are far more secure today than they were in 2016. But there's still much more we can and must do to protect our elections. I hope the bipartisan findings and recommendations outlined in this report will underscore to the White House and all of our colleagues, regardless of political party, that this threat remains urgent, and we have a responsibility to defend our democracy against it."

You can read, "*Volume I: Russian Efforts Against Election Infrastructure*" **here (https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf)**.

Key Findings and Recommendations:

- **The Russian government directed extensive activity against U.S. election infrastructure**. The Committee found the activity directed at the state and local level began in at least 2014 and carried into at least 2017. The Committee has seen no evidence that any votes were changed or that any voting machines were manipulated.
- **Russian efforts exploited the seams between federal authorities and capabilities, and protection for the states.** The Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI) are, by design,

limited in domestic cybersecurity authorities. State election officials, who have primacy in running elections, were not sufficiently warned or prepared to handle an attack from a hostile nation-state actor.

- **DHS and FBI warnings to the states in the late summer and fall of 2016 did not provide enough information or go to the appropriate people.** The Committee found that while the alerts were actionable, they provided no clear reason for states to take the threat more seriously than other warnings.
- **DHS has redoubled its efforts to build trust with the states and deploy resources to assist in securing elections.** Since 2016, DHS has made great strides in learning how election procedures vary across states and how to best assist those states. The Committee determined DHS's work to bolster states' cybersecurity has likely been effective but believes more needs to be done to coordinate efforts.
- **Russian activities demand renewed attention to vulnerabilities in U.S. voting infrastructure.** Cybersecurity for electoral infrastructure at the state and local level was sorely lacking in 2016. Despite increased focus over the last three years, some of these vulnerabilities, including aging voting equipment, remain. As states look to replace machines that are now out of date, they should purchase more secure voting machines. At a minimum, any machine purchased going forward should have a voter-verified paper trail.
- **Congress should evaluate the results of the $380 million in state election security grants allocated in 2018.** States should be able to use grant funds provided under the Help America Vote Act (HAVA) to improve cybersecurity in a variety of ways, including hiring additional IT staff, updating software, and contracting vendors to provide cybersecurity services. When those funds are spent, Congress should evaluate the results and consider an additional appropriation to address remaining insecure voting machines and systems.
- **DHS and other federal government entities remain respectful of the limits of federal involvement in state election systems.** America's decentralized election system can be a strength against cybersecurity threats. However, the federal government and states should each be aware of their own cybersecurity limitations and know both how and when to obtain assistance. States should remain firmly in the lead on running elections, and the federal government should ensure they receive the necessary resources and information.
- **The United States must create effective deterrence.** The United States should communicate to adversaries that it will view an attack on its election infrastructure as a hostile act and respond accordingly. The U.S. government should not limit its response to cyber activity; rather, it should create a menu of potential responses that will send a clear message and create significant costs for the perpetrator.

###

Press Releases (/public/index.cfm/pressreleases?type=PressReleases) Intelligence (/public/index.cfm/pressreleases?label=Intelligence) Russia (/public/index.cfm/pressreleases?label=Russia)

Permalink: https://www.warner.senate.gov/public/index.cfm/2019/7/senate-intel-releases-election-security-findings-in-first-volume-of-bipartisan-russia-report (https://www.warner.senate.gov/public/index.cfm/2019/7/senate-intel-releases-election-security-findings-in-first-volume-of-bipartisan-russia-report)