Key Findings and Recommendations from the

Joint Report of the Attorney General and the Secretary of Homeland Security on

Foreign Interference Targeting Election Infrastructure or Political Organization, Campaign, or Candidate Infrastructure Related to the 2022 US Federal Elections

Submitted in Fulfillment of the Requirement Under Section 1(b) of Executive Order 13848: Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election

December 2023

Background

This product provides a declassified overview of findings from a classified joint report from the Attorney General and Secretary of Homeland Security addressing the impact of activities by foreign governments and their agents targeting election infrastructure or infrastructure pertaining to political organizations, candidates, or campaigns used in the 2022 US federal elections on the security or integrity of such infrastructure. Pursuant to Executive Order (EO) 13848, the joint report relied on the Intelligence Community Assessment (ICA) addressing foreign threats to the 2022 US elections.

Scope Note

In February 2023, the Department of Justice (DOJ), including the Federal Bureau of Investigation (FBI), and the Department of Homeland Security (DHS), including the Office of Intelligence and Analysis (I&A) and the Cybersecurity and Infrastructure Security Agency (CISA), prepared a classified joint report to fulfill the requirement under EO 13848 § (1)(b) that the Attorney General and the Secretary of Homeland Security deliver a joint report to the President, the Secretary of State, the Secretary of the Treasury, and the Secretary of Defense evaluating, with respect to the 2022 federal elections:

> (i) the extent to which any foreign interference that targeted election infrastructure materially affected the security or integrity of that infrastructure, the tabulation of votes, or the timely transmission of election results; and
>
> (ii) if any foreign interference involved activities targeting the infrastructure of, or pertaining to, a political organization, campaign, or candidate, and the extent to which such activities materially affected the security or integrity of that infrastructure, including by unauthorized access to, disclosure or threatened disclosure of, or alteration or falsification of, information or data.

The purpose of this report was solely to evaluate the impact of foreign government activity on the security or integrity of the covered infrastructure. It did not address the effect of foreign government activity on public perception or the behavior of any voters. Although not required by EO 13848, this report includes limited discussion of reported unattributed activity targeting election infrastructure observed over the election cycle.

Sources of Information

This report is based on the ICA disseminated to the Executive Branch as well as intelligence reporting and other information contained in other Intelligence Community (IC) assessments. This includes, among other information, FBI forensic analyses; CISA cyber incident response activities; risk analysis and stakeholder information; IC reporting; and open-source reporting.

This report evaluates activities that met three criteria. First, the activity was identified in the ICA or another IC assessment within the relevant time frame. Second, the activity was attributed by the IC to a foreign government, or any person acting as an agent of or on behalf of a foreign government. Third, the activity targeted election infrastructure or infrastructure of, or pertaining to, a political organization, campaign, or candidate ("campaign infrastructure") during the 2022 federal elections period.

Activities that met all three criteria were included regardless of whether the IC has assessed that they were undertaken with the purpose of interfering in a 2022 federal election. Foreign governments may target election or campaign infrastructure for a variety of reasons, including intelligence collection, and the purpose of any activity may not always be apparent.

Definitions

The term "**foreign interference**" means "any covert, fraudulent, deceptive, or unlawful actions or attempted actions of a foreign government, or of any person acting as an agent of or on behalf of a foreign government, undertaken with the purpose or effect of influencing, undermining confidence in, or altering the result or reported result of, the election, or undermining public confidence in election processes or institutions." EO 13848 § 8(f)

The term "**election infrastructure**" means "information and communications technology and systems used by or on behalf of the Federal Government or a State or local government in managing the election process, including voter registration databases, voting machines, voting tabulation equipment, and equipment for the secure transmission of election results." EO 13848 § 8(d)

The term "infrastructure of, or pertaining to, a political organization, campaign, or candidate" similarly refers to the information and communications technology and systems used by or on behalf of, or closely associated with, a political organization, campaign, or candidate and is hereafter referred to as "**campaign infrastructure**" in this report.

The term "**security**" refers to protecting information and information systems from unauthorized access, use, disclosure, and disruption.

The term "**integrity**" refers to protecting against unauthorized modification or destruction of information.

Key Findings

We – the Department of Justice, including the FBI, and Department of Homeland Security, including the Office of Intelligence and Analysis and CISA – have no evidence that any foreign government-affiliated actor materially affected the security or integrity of any election infrastructure in the 2022 federal elections. We did detect some cyber activity that did not compromise election infrastructure networks, including from pro-Russian hacktivists and suspected People's Republic of China (PRC) actors.

- Pro-Russian hacktivists claimed to have conducted a Distributed Denial of Service (DDoS) attack that resulted in temporarily restricted access to a public-facing US state election office website.
- Suspected PRC cyber actors scanned both election-related and non-election state government websites. Other suspected PRC cyber actors also collected publicly-available US voter information, probably to collect personal identifying information and other data on US voters.
- We have no evidence that any detected activity prevented voting, changed votes, or disrupted the ability to tally votes or to transmit election results in a timely manner; altered any technical aspect of the voting process; or otherwise compromised the integrity of voter registration information or any ballots cast during 2022 federal elections.

The IC—including the FBI and the IC elements of DHS—assessed in September 2022 that it would be difficult for a foreign actor to manipulate election processes at scale without detection by intelligence collection, post-election audits, or physical and cybersecurity monitoring of voting systems across the country.

We identified multiple incidents when Russian, Iranian, and Chinese government-affiliated actors connected to campaign infrastructure during the 2022 federal elections, including PRC cyber actors broadly scanning state political party domains.

- While some cyber activity resulted in accessing some components of campaign infrastructure, we do not have any indications of any information obtained through this activity released in influence operations or otherwise deployed, modified, or destroyed.
- The IC has assessed that it is unclear if actors sought these accesses to inform broader foreign policy interests or election-specific operations.

We do not have any indications of unattributed or cybercriminal activity which materially affected the integrity of voter data, the ability to vote, the tabulation of votes, or the timely transmission of election results. We have indications of multiple instances of unknown cyber actors and cybercriminals targeting, and sometimes compromising, US state and local government networks which may include non-voting election infrastructure.

Recommendations

Improvements in cybersecurity, partnerships, and public messaging enhanced the resilience of the electoral process to the vulnerabilities that actors sought to exploit during the 2022 federal elections. We recommend the US Government continue and expand its support to these efforts.

- **Cybersecurity and Resilience**. Since 2020, election officials, third-party vendors, political organizations, and campaigns implemented significant defensive measures to enhance the security of their infrastructure and limit the disruptive potential of an intrusion. Implementing defensive measures such as firewalls, up-to-date-patching, multifactor authentication, supply chain risk management practices, pre-election testing of voting equipment, federal and state certification of such equipment, cybersecurity training, and separation of election-specific systems from other computer networks all helped to protect the integrity of infrastructure. Implementing redundancy measures like paper pollbook backups, auditable ballots, and post-election audits ensures election officials could limit the impact of a cyber incident with minimal disruption to voting. These measures also allow election officials to conduct credible recounts and stay alert to potential manipulation of errors. We recommend the US Government continue to help election officials, third-party vendors, political organizations, and campaigns adopt best practices for infrastructure and election security.

- **Engagement and Collaboration.** Since 2020, federal, state, local, and private sector partners nationwide worked together in unprecedented ways to combat foreign interference efforts, to support state and local officials in safeguarding election infrastructure, and to assist political organizations, campaigns, and candidates in protecting their own infrastructure. The US Government sought to foster an environment in which state and local officials, political organizations, campaigns, and candidates could share information on malicious or suspicious cyber activities, ultimately receiving and sharing information efficiently with all 50 US states and more than 3,500 local jurisdictions. We recommend continued US Government focus on actively engaging with and fostering collaboration and coordination with federal, state, local, and private sector partners.

- **Public Messaging and Education.** Since 2020, the US Government significantly increased public messaging and education to provide accurate and timely information about cyber threats pertaining to elections. This included efforts to help educate the public about adversary goals, defensive steps to improve cybersecurity, warning of potential threat activities to mitigate their effects, and amplification of reliable sources of information, such as state and local elections officials. We recommend the US Government continue to increase the quantity and quality of public messaging and education, to include expanding translation of public messaging into other languages spoken by US voters.