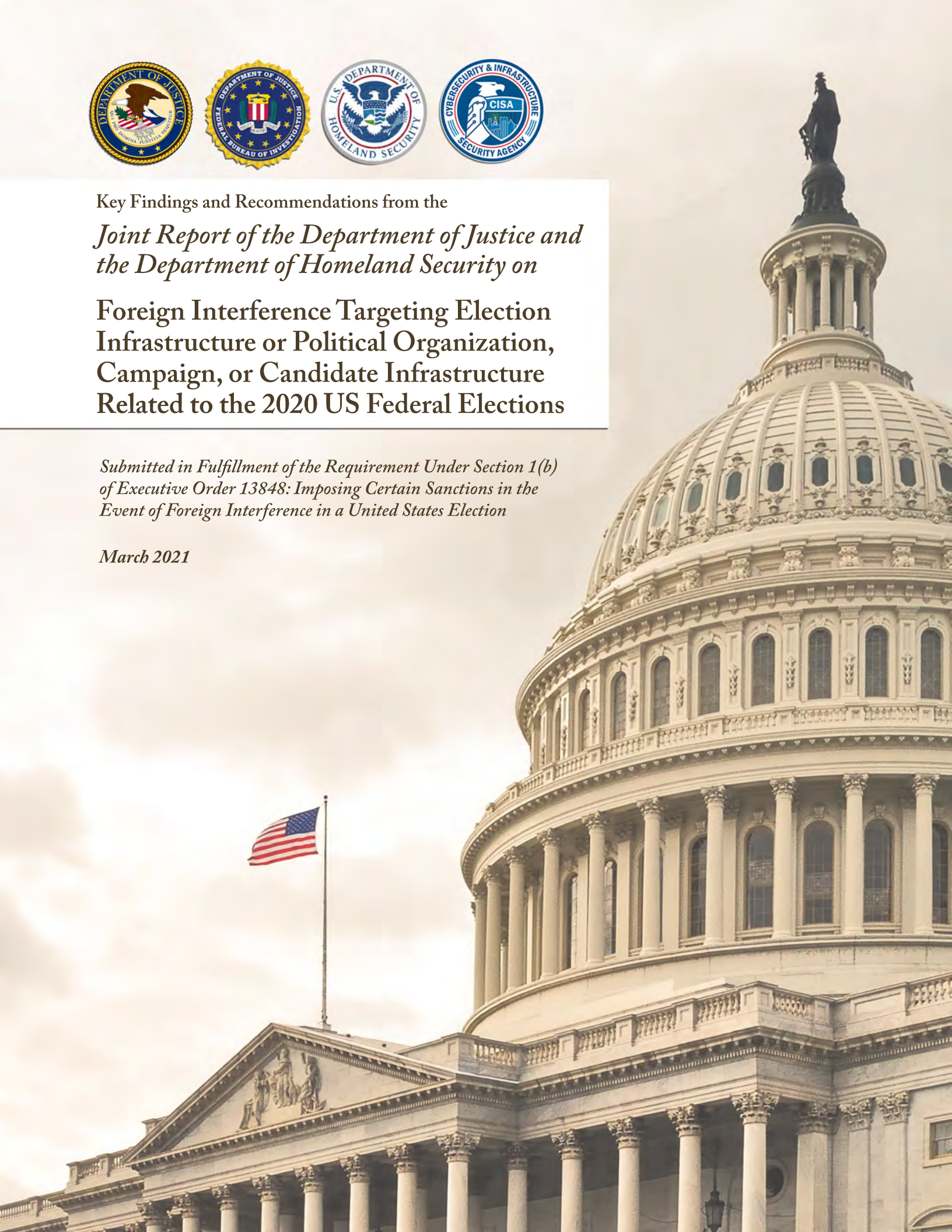

Key Findings and Recommendations from the

Joint Report of the Department of Justice and the Department of Homeland Security on

Foreign Interference Targeting Election Infrastructure or Political Organization, Campaign, or Candidate Infrastructure Related to the 2020 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

March 2021

Background

This product provides a declassified overview of findings and recommendations 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 2020 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 2020 US elections.

Scope Note

In February 2021, the Department of Justice, including the Federal Bureau of Investigation (FBI), and the Department of Homeland Security, including 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 2020 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, 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, nor did it address the impact of non-state foreign actors like cybercriminals.

Sources of Information

Foreign government activities were included regardless of whether the IC has assessed that they were undertaken with the purpose of interfering in a 2020 federal election. Foreign governments may target election or political and campaign infrastructure for a variety of reasons, including intelligence collection, and the purpose of any activity may not always be apparent. The impact to covered infrastructure was evaluated by considering, among other information, FBI forensic analyses; CISA cyber incident response activities, risk analysis, and stakeholder information; IC reporting; and open-source reporting.

Key Findings

*For the purposes of 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. Additional definitions are included at the end of the report.*

We—the Department of Justice, including the FBI, and Department of Homeland Security, including CISA—have no evidence that any foreign government-affiliated actor 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 of any ballots cast during 2020 federal elections.

- Broad Russian and Iranian campaigns targeting multiple critical infrastructure sectors did compromise the security of several networks that managed some election functions, but they did not materially affect the integrity of voter data, the ability to vote, the tabulation of votes, or the timely transmission of election results.
- Iranian claims that sought to undermine the public's confidence in US election infrastructure were false or inflated.

We identified several incidents when Russian, Chinese, and Iranian government-affiliated actors materially impacted the security of networks associated with or pertaining to US political organizations, candidates, and campaigns during 2020 federal elections.

- In most cases, the IC has assessed that it is unclear if those actors sought these accesses to inform broader foreign policy interests or election-specific operations.
- Several such actors gathered at least some information they could have released in influence operations, but ultimately we did not see any such materials deployed, modified, or destroyed.

The IC—including the FBI and the IC elements of DHS—has previously assessed 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 cyber security monitoring of voting systems across the country.

- We are aware of multiple public claims that one or more foreign governments—including Venezuela, Cuba, or China—owned, directed, or controlled election infrastructure used in the 2020 federal elections; implemented a scheme to manipulate election infrastructure; or tallied, changed, or otherwise manipulated vote counts. Following the election, the Department of Justice, including the FBI, and the Department of Homeland Security, including CISA, investigated the public claims and determined that they are not credible.
- We have no evidence—not through intelligence collection on the foreign actors themselves, not through physical security and cybersecurity monitoring of voting systems across the country, not through post-election audits, and not through any other means—that a foreign government or other actors compromised election infrastructure to manipulate election results.

Recommendations

Improvements in cyber and physical security, supply chain risk management, partnerships, and public messaging enhanced the resilience of the electoral process to the vulnerabilities actors sought to exploit during the 2020 federal elections. We recommend the US Government continue and expand its support of these efforts.

- **Physical Security and Cyber Hygiene.** Since 2018, election officials, 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, and multifactor authentication, pre-election testing of voting equipment, federal and state certification of such equipment, cybersecurity training for government personnel, and separation of election-specific systems from other computer networks all helped to protect the integrity of infrastructure. Implementing redundancy measures like paper pollbooks backups, auditable ballots, and post-election audits ensures election officials could limit the impact of a cyber incident with minimal disruption to voting, conduct credible recounts, and stay alert to potential manipulation or errors. We recommend that the US Government continue to help election officials, political organizations, and campaigns adopt best practices for infrastructure and election security.

- **Third-Party Vendor Security and Supply Chain Risk Management.** Recent supply chain compromises highlight the dependencies and vulnerabilities shared across vendor and client networks. State, local, and private sector election partners continue to lean on the federal government to share best practices for supply chain risk management. Since 2018, election officials and vendors have begun to incorporate software bill of goods and breach notification requirements into acquisition and contract management activities. We recommend that the US Government continue assisting election officials, political organizations, and campaigns with establishing and refining supply chain risk management procedures.

- **Engagement and Collaboration.** Since 2018, 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 nearly 3,000 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 2018, the US Government significantly increased public messaging and education to provide accurate and timely information about cyber threats pertaining to elections. This included public attribution to help educate the public about adversary goals, defensive steps to improve cybersecurity, warning of potential threat activities to mitigate their effects, and fact checks to control the proliferation of misinformation. However, the resonance of baseless claims concerning foreign interference after the election demonstrates the need to bolster public confidence in reliable sources of information, such as state and local election officials. We recommend the US Government continue to increase the quantity and quality of public messaging and education.

Definitions

For the purposes of this report, the following terms were defined as:

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.

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.