Campaign and Election Security Policy: Overview and Recent Developments for Congress

January 2, 2020

Congressional Research Service
https://crsreports.congress.gov
R46146

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

Campaign and Election Security Policy: Overview and Recent Developments for Congress

SUMMARY

In the United States, state, territorial, and local governments are responsible for most aspects of selecting and securing election systems and equipment. Foreign interference during the 2016 election cycle—and widely reported to be an ongoing threat—has renewed congressional attention to campaign and election security and raised new questions about the nature and extent of the federal government's role in this policy area.

This report provides congressional readers with a resource for understanding campaign and election security policy. This includes discussion of the federal government's roles; state or territorial responsibilities for election administration and election security; an overview of potentially relevant federal statutes and agencies; and highlights of recent congressional policy debates. The report summarizes related legislation that has advanced beyond introduction during the 116th Congress. It also poses questions for consideration as the House and Senate examine whether or how to pursue legislation, oversight, or appropriations.

R46146

January 2, 2020

R. Sam Garrett, Coordinator
Specialist in American National Government

Sarah J. Eckman
Analyst in American National Government

Karen L. Shanton
Analyst in American National Government

In the 116th Congress, the FY2020 National Defense Authorization Act (NDAA; S. 1790; P.L. 116-92), enacted in December 2019, contains several provisions related to campaign and election security. Most provisions involve providing Congress or federal or state agencies with information about election interference. It also requires the Director of National Intelligence, in coordination with several other agencies, to develop a strategy for countering Russian cyberattacks against U.S. elections. In addition, the Consolidated Appropriations Act, 2020 (P.L. 116-93; H.R. 1158), also enacted in December 2019, includes $425 million for payments to states, territories, and the District of Columbia to make general improvements to the administration of federal elections, including upgrades to election technology and security.

As of this writing, 116th Congress legislation that has advanced beyond introduction in at least one chamber includes H.R. 1; H.R. 753; H.R. 1158; H.R. 2500; H.R. 2722; H.R. 3351; H.R. 3494; H.R. 3501; H.R. 4617; H.R. 4782; H.R. 4990; S. 482; S. 1060; S. 1321; S. 1328; S. 1589; S. 1790; S. 1846; S. 2065; and S. 2524. Other bills also could have implications for campaign and election security even though they do not specifically reference the topic (e.g., those addressing cybersecurity generally or voter access). Several congressional committees also have held legislative or oversight hearings on the topic.

Federal statutes—such as the Help America Vote Act (HAVA); Federal Election Campaign Act (FECA); and the Voting Rights Act (VRA)—all contain provisions designed to make campaign finance, elections, or voting more secure. Several federal agencies are directly or indirectly involved in campaign and election security. These include, but are not limited to, the Department of Defense (DOD); Department of Homeland Security (DHS); Department of Justice (DOJ); Election Assistance Commission (EAC); and Federal Election Commission (FEC).

Securing federal elections is a complex policy challenge that crosses disciplinary lines. Some of the factors shaping that complexity include divisions of authority between the federal and state (or territorial or local) governments; coordination among federal agencies, and communication with state agencies; funding; changing elections technology; and the different needs of different sectors, such as campaigns, administrators, and vendors.

This report does not attempt to resolve ongoing policy debates about what campaign and election security should entail. The report cites other CRS products that contain additional discussion of some of the topics discussed herein. The report does not address constitutional or legal issues.

Contents

Tables

Appendixes

Contacts

Introduction

Election security is one of the most prominent policy challenges facing Congress. A November 2019 warning from the heads of several federal agencies illustrates the interdisciplinary and ongoing nature of the threat to American elections. According to the joint statement, in the 2020 election cycle, "Russia, China, Iran, and other foreign malicious actors all will seek to interfere in the voting process or influence voter perceptions. Adversaries may try to accomplish their goals through a variety of means, including social media campaigns, directing disinformation operations or conducting disruptive or destructive cyber-attacks on state and local infrastructure."[1]

These are just the latest challenges in securing American elections. Traditionally, election administration emphasizes policy goals such as ensuring that all eligible voters, and only eligible voters, may register and cast ballots; that those ballots are counted properly; and that the voting public views that process as legitimate and transparent. Preserving election continuity is a chief concern. Election officials therefore have long prepared contingency plans that address various risks, such as equipment malfunctions, power outages, and natural disasters.

These traditional concerns remain, but have taken on new complexity amid foreign interference in U.S. elections. In addition to managing traditional security concerns about infrastructure and administrative processes (e.g., counting ballots), mitigating external threats to the accuracy of information voters receive, particularly from foreign sources, is a potential challenge for political campaigns, election administrators, and the public.

Addressing any one of these topics might involve multiple areas of public policy or law. Doing so also can involve complex practical challenges about which levels of government, or agencies, are best equipped or most appropriate to respond. How those entities can or should interact with political campaigns, the private sector, and voters, are also ongoing questions. Technical complexity in some areas, such as cybersecurity, and the federal structure of shared national, state or territorial, and local responsibility for administering federal elections make election security even more challenging.

Election security in general appears to be a shared policy goal, but debate exists in Congress about which policy issues and options to pursue. Debate over the scope of the federal government's role in election security shapes much of that debate. State, territorial, and local governments are responsible for most aspects of election administration, including security.

This report provides congressional readers with an overview that includes

- how campaign and election security has developed as a policy field;
- recent legislative activity, especially bills that have advanced beyond introduction;
- federal statutes and agencies that appear to be most relevant for campaign and election security;
- state, territorial,[2] or local roles in administering elections, and federal support for those functions; and

[1] U.S. Department of Justice et al., "Joint Statement from DOJ, DOD, DHS, DNI, FBI, NSA, and CISA on Ensuring Security of 2020 Elections," press release, November 5, 2019, at https://www.nsa.gov/news-features/press-room/Article/2009338/joint-statement-from-doj-dod-dhs-dni-fbi-nsa-and-cisa-on-ensuring-security-of-2/.

[2] In general, campaign and election security policy matters are similar in states and territories, although specific statutes

- highlights of recent policy debates, and potential future questions for congressional consideration.

Defining Election Security

There is no single definition of "election security," nor is there necessarily agreement on which topics should or should not be included in the policy debate. Broadly speaking, election security involves efforts to ensure fair, accurate, and safe elections. This can include a variety of activities that happen before, during, and after voters cast their ballots.

- A narrow definition of election security might address only efforts to protect traditional election infrastructure, such as voter registration databases, voting machines, polling places, and election result tabulations.
- More expansive definitions might also address issues affecting candidates and campaigns. This includes, for example, regulating political advertising or fundraising; providing physical or cybersecurity assistance for campaigns; or combating disinformation or misinformation in the political debate.

The policy debates discussed herein can affect different kinds of entities uniquely.

- Perhaps most notably, security concerns affecting campaigns can differ from those for safeguarding elections and voting. Campaigns in the United States are about persuading voters in an effort to win elections. They are private, not governmental, operations and are subject to relatively little regulation beyond campaign finance policy.
- Elections are more highly regulated, although specific practices can vary, as their administration is primarily a state- or local-level responsibility.
- Provisions in state or local law, and, to a lesser degree, federal law, regulate how voters cast ballots and who may do so. Some security discussions include issues related to voter access, while others view access as a separate elections policy matter. This report briefly notes that access can be a component of campaign and election security policy debates, but the report does not otherwise address access issues.[3]

This report does not attempt definitively to resolve ongoing policy debates about what campaign and election security entails or should entail, nor does it fully address all aspects of the policy issues discussed. Instead, it provides congressional readers with background information to consider that debate and decide whether or how to pursue legislation (including appropriations) or

distinguish between states and territories in some cases. A discussion of how federal election law applies to territories versus states is beyond the scope of this report. Unless otherwise noted, campaign and election security concerns discussed in the text of this report are relevant for territories.

[3] Because voter access is primarily a state-level responsibility, this report does not address the topic in detail, although it does address some Voting Rights Act provisions. For 116th Congress discussion of access issues, see, for example, U.S. Congress, House Committee on House Administration, Subcommittee on Elections, *Report on Voting Rights and Election Administration in the United States of America*, prepared by Chairperson Marcia L. Fudge, 116th Cong., 1st sess., at https://cha.house.gov/report-voting-rights-and-election-administration-united-states-america, which includes discussion of misinformation issues that are potentially relevant for election security; and U.S. Congress, House Committee on House Administration, *Subcommittee on Elections Voting Rights Act Findings: Minority Views*, 116th Cong., 1st sess., at https://republicans-cha.house.gov/voting-rights-act-minority-views. Both documents are undated and were released in 2019. See also, for example, House debate on H.R. 4, "Voting Rights Advancement Act of 2019," House debate, *Congressional Record*, daily edition, December 6, 2019, pp. H9308-H9334. Most issues related to H.R. 4 do not specifically address campaign and election security and are thus beyond the scope of this report.

oversight. Because all the topics noted above—and others discussed throughout the report—have been components of the recent congressional debate over how to safeguard American campaigns, elections, and voting, this report uses the general term *campaign and election security*.

Scope of the Report

This report discusses federal agencies, statutes, and policies designed to prevent or respond to deliberate domestic or foreign security threats to campaigns, elections, or voting. Concepts discussed in the report also have implications for some unintentional threats, such as natural disasters or other emergencies that could affect campaigns, elections, or voting. Legislation cited in the report contains specific references to campaign and election security. This includes bill text that uses variations of terms such as *campaign*, *election*, or *vote* near variations of the terms *interference* or *security*. Some readers might view areas addressed herein as more or less directly related to campaign or election security, and alternative methodologies could yield other bills or policy topics for consideration.

The report does not include detailed attention to more traditional aspects of campaign finance, election administration, or voting, particularly voter mobilization. For example, the report discusses Help America Vote Act provisions that authorize funding states may use to help secure elections, but not provisions that authorize funding for the Election Assistance Commission generally.[4] Similarly, the report briefly discusses Voting Rights Act provisions that prohibit voter intimidation, but it does not discuss other federal statutes enacted to make registration and voting easier.[5] In addition, the report briefly notes lobbying statutes that might be relevant for regulating certain corporate or foreign activity related to U.S. election interference, but it does not substantially address lobbying as a policy area.

The report emphasizes domestic implications of campaign and election security. This includes attention to protections for U.S. campaigns and elections from the effects of foreign disinformation and misinformation efforts. The **Appendix** at the end of this report includes sanctions or immigration legislation that specifically references interference in U.S. elections, and which has advanced beyond introduction during the 116th Congress. However, foreign policy implications of such interference, or a discussion of offensive operations and tactics that the United States might or might not use against foreign adversaries, are otherwise beyond the scope of this report.[6]

Because of the still-developing and complex policy challenges surrounding campaign and election security, other areas of law, policy, or practice might also be relevant but are not addressed here. The report references other CRS products that contain additional discussion of

[4] Similarly, the report does not address funds for aspects of election security other than securing election systems, such as Intelligence Community efforts to identify sources of election disinformation.

[5] Other CRS products contain additional discussion. See, for example, CRS Report R45302, *Federal Role in U.S. Campaigns and Elections: An Overview*, by R. Sam Garrett; CRS Report RS20764, *The Uniformed and Overseas Citizens Absentee Voting Act: Overview and Issues*, by R. Sam Garrett (originally authored by Kevin J. Coleman); and CRS Report R45030, *Federal Role in Voter Registration: The National Voter Registration Act of 1993 and Subsequent Developments*, by Sarah J. Eckman.

[6] For additional discussion of foreign policy implications and key concepts, see CRS Report R45142, *Information Warfare: Issues for Congress*, by Catherine A. Theohary; and CRS In Focus IF10771, *Defense Primer: Information Operations*, by Catherine A. Theohary; CRS In Focus IF10694, *Countering America's Adversaries Through Sanctions Act*, by Dianne E. Rennack, Kenneth Katzman, and Cory Welt; CRS In Focus IF10779, *U.S. Sanctions on Russia: An Overview*, by Dianne E. Rennack and Cory Welt; CRS Report R45415, *U.S. Sanctions on Russia*, coordinated by Cory Welt; and CRS In Focus IF10694, *Countering America's Adversaries Through Sanctions Act*, by Dianne E. Rennack, Kenneth Katzman, and Cory Welt.

several such topics. The report does not provide legal or constitutional analysis. It also does not attempt to catalog all alleged or established instances of campaign and election interference or security concerns, or to independently evaluate allegations.

Recent Legislative Activity

Highlights of recent legislative activity include the following. Additional discussion appears throughout the report.

- The 115th Congress (2017-2019) appropriated $380 million for FY2018 for improvements to the administration of federal elections, including upgrades to election technology and security.
- The 116th Congress (2019-2021) appropriated $425 million for FY2020 in the consolidated appropriations bill (H.R. 1158; P.L. 116-93) enacted in December 2019. The "Funding for States After the 2016 Election Cycle" section of this report contains additional detail.
- The 116th Congress enacted S. 1790 (P.L. 116-92), the FY2020 National Defense Authorization Act (NDAA), in December 2019. The legislation contains several provisions related to campaign and election security.

Table 1 below lists bills that have passed at least one chamber. The **Appendix** in this report briefly summarizes 116th Congress legislation containing campaign and election security provisions that has advanced beyond introduction.

Table 1. 116th Congress Legislation, Which Has Passed At Least One Chamber, Related to Campaign and Election Security

See the "Scope of the Report" section and the **Appendix** of this report for additional detail.

Bill Number	Short Title	Latest Major Action
H.R. 1	For the People Act of 2019	Passed House (234-193), 03/08/2019
H.R. 753	Global Electoral Exchange Act of 2019	Passed House (voice vote), 05/20/2019
H.R. 1158	Consolidated Appropriations Act, 2020	Became P.L. 116-93, 12/20/2019
H.R. 2500	National Defense Authorization Act for Fiscal Year 2020	Passed House (220-197), 07/12/2019
H.R. 2722	Securing America's Federal Elections (SAFE) Act	Passed House (225-184), 06/27/2019
H.R. 3351	Financial Services and General Government Appropriations Act, 2020	Passed House (224-196), 06/26/2019; see also H.R. 1158
H.R. 3494	Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020	Passed House (397-31), 07/17/2019
H.R. 4617	Stopping Harmful Interference in Elections for a Lasting Democracy Act (SHIELD Act)	Passed House (227-181), 10/23/2019

Bill Number	Short Title	Latest Major Action
S. 1321	Defending the Integrity of Voting Systems Act	Passed Senate (unanimous consent), 07/17/2019
S. 1328	Defending Elections against Trolls from Enemy Regimes (DETER) Act	Passed Senate (unanimous consent), 06/03/2019
S. 1790	National Defense Authorization Act for Fiscal Year 2020	Became P.L. 116-92, 12/20/2019
S. 1846	State and Local Government Cybersecurity Act of 2019	Passed Senate (unanimous consent), 11/21/2019

Source: CRS analysis of bill texts.

Notes: Bills in the table specifically reference campaign and election and security. Other legislation not included in the table could be relevant for campaign or election security once implemented or in practice. See the "Scope of the Report" section of this report and the **Appendix** for additional detail. The table excludes resolutions (e.g., proposed constitutional amendments) and routine appropriations bills that propose funding for agencies such as the Election Assistance Commission or Federal Election Commission, unless the appropriations bill also contains additional provisions specifically addressing campaign and election security.

- In addition, during the 116th Congress, committees in both chambers have held hearings on these and related campaign and election security topics.[7] The Committee on House Administration and Senate Committee on Rules and Administration exercise primary jurisdiction over federal elections. Several other committees oversee related areas, such as intelligence or voting rights issues. Another CRS product contains additional discussion of committee roles in federal campaigns and elections generally.[8]

Development of Federal Role in Campaign and Election Security

Foreign interference is only the highest-profile and latest campaign and election security policy challenge.[9] Physical security, to protect voters, ballots, and vote counts, has been an ongoing

[7] See, for example, U.S. Congress, Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, Volume 1: Russian Efforts Against Election Infrastructure with Additional Views, 116th Cong., 1st sess., July 25, 2019, at https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf; U.S. Congress, Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, Volume 2: Russia's Use of Social Media with Additional Views, 116th Cong., 1st sess., October 8, 2019, at https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf; U.S. Congress, Senate Committee on Rules and Administration, *Oversight of the U.S. Election Assistance Commission*, 116th Cong., 1st sess., May 15, 2019, S. Hrg. 116-74 (Washington: GPO, 2019); U.S. Congress, House Committee on Homeland Security, *Defending Our Democracy: Building Partnerships to Protect America's Elections*, 116th Cong., 1st sess., February 13, 2019, Serial No. 116-1 (Washington: GPO, 2019); and U.S. Congress, House Committee on Oversight and Reform, Subcommittee on National Security, *Securing U.S. Election Infrastructure and Protecting Political Discourse*, 116th Cong., 1st sess., February 13, 2019, Serial no. 116-28 (Washington: GPO, 2019). See also, for example, discussion and witness testimony presented during an October 22, 2019, House Judiciary Committee oversight hearing, "Securing America's Elections Part II: Oversight of Government Agencies." As of this writing, the hearing record does not appear to have been published. Video and written materials are available on the committee website, https://judiciary.house.gov/legislation/hearings/securing-america-s-elections-part-ii-oversight-government-agencies.

[8] See CRS Report R45302, *Federal Role in U.S. Campaigns and Elections: An Overview*, by R. Sam Garrett.

[9] According to the Office of the Director of National Intelligence (ODNI), foreign interference with U.S. elections falls into "five distinct categories." Collectively, these include "cyber" or "covert" operations. "Cyber operations" target

concern. Specifically, in modern history, the federal government's first role in securing elections was primarily about access and voting rights.[10] In 1965, Congress enacted the Voting Rights Act (VRA), which protects voters against race- or color-based discrimination in registration, redistricting, and voting.[11] More explicitly related to security, the VRA prohibits intimidation, threats, or coercion in voting.[12] Congress primarily tasked the U.S. Department of Justice (DOJ) with enforcing the statute and related criminal provisions. Federal law enforcement agencies, especially the Federal Bureau of Investigation (FBI), also support states and localities—which retain primary responsibility for election administration in the United States—in investigating election crimes and providing physical security at the polls.

The federal role in election administration expanded after the disputed 2000 presidential election. In response, Congress authorized federal funding for the states, the District of Columbia, and territories[13] to make improvements to the administration of federal elections. It also created the Election Assistance Commission (EAC) to administer those funds. Congress charged the agency with overseeing a voluntary voting system testing and certification program, and providing states and localities with voluntary election administration guidance, research, and best practices. These developments notwithstanding, securing campaigns and elections historically was not a major policy topic at the federal level, as most security matters were reserved for state- or local-level policy.

The policy environment changed dramatically during the 2016 election cycle, when media reports and subsequent congressional[14] and federal-agency[15] investigations documented Russian

election infrastructure, campaigns, parties, or public officials. "Covert" operations include efforts to "assist or harm" groups such as campaigns, to influence public opinion or sow social or political division, or covertly influence policymakers or the public. See Office of the Director of National Intelligence, National Counterintelligence and Security Center, *Foreign Threats to U.S. Elections: Election Security Information Needs*, at https://www.dni.gov/files/ODNI/documents/DNI_NCSC_Elections_Brochure_Final.pdf. The publication is not dated or paginated. The quoted material appears on the first full page of text. For additional discussion on influence operations generally, see CRS Report RL31787, *Information Operations, Cyberwarfare, and Cybersecurity: Capabilities and Related Policy Issues*, by Catherine A. Theohary.

[10] For an overview of the issues discussed in this paragraph, see CRS Report R45302, *Federal Role in U.S. Campaigns and Elections: An Overview*, by R. Sam Garrett.

[11] 52 U.S.C. §§10101-10702. For additional discussion, see, for example, CRS Testimony TE10033, *History and Enforcement of the Voting Rights Act of 1965*, by L. Paige Whitaker.

[12] 52 U.S.C. §30107.

[13] The Help America Vote Act (HAVA), which contains many of the provisions noted in this section, does not include coverage for the Commonwealth of the Northern Mariana Islands (CNMI). When Congress enacted the statute in 2002, there were no federal elections in the territory.

[14] See, for example, U.S. Congress, Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, Volume 1: Russian Efforts Against Election Infrastructure with Additional Views, 116th Cong., 1st sess., July 25, 2019, at https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf; U.S. Congress, Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, Volume 2: Russia's Use of Social Media with Additional Views, 116th Cong., 1st sess., October 8, 2019, at https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

[15] For example, Department of Homeland Security and Federal Bureau of Investigation, *GRIZZLY STEPPE—Russian Malicious Cyber Activity*, joint analysis report, JAR-16-20296A, December 29, 2016, at https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf; National Cybersecurity and Communications Integration Center, Department of Homeland Security, "Enhanced Analysis of GRIZZLY STEPPE Activity," analysis report, AR-17-20045, February 10, 2017, at https://www.us-cert.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf; Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections*, Intelligence Community assessment, ICA 2017-01D, January 6, 2017, at https://www.dni.gov/files/documents/ICA_2017_01.pdf.

government interference with that year's U.S. presidential election. According to Special Counsel Robert Mueller's report, these interference efforts targeted private technology firms that provide election-related software and hardware; state and local government entities; and a major political party and nominee.[16]

The investigations did not find that this activity was a determinative factor in the election outcome. However, the possibility of such activity, and of additional efforts to affect political attitudes or participation, remains. In July 2018 remarks at the Hudson Institute, then-Director of National Intelligence (DNI) Dan Coats, a former Senator, said that the Intelligence Community (IC) reported "aggressive attempts to manipulate social media and to spread propaganda focused on hot-button issues that are intended to exacerbate socio-political divisions" in elections.

To the extent that those efforts affect campaigns—including campaign security, or the information voters receive from campaigns—campaign finance policy and law could be relevant. The Federal Election Campaign Act (FECA) originated in the 1970s amid concerns about limiting domestic political corruption. The act also contains a wide-ranging prohibition on foreign-national involvement in federal, state, or local U.S. elections.[17] These provisions, and disclosure and disclaimer requirements for all "persons" who raise or spend funds to influence federal elections, are key elements of regulating both domestic and foreign efforts to affect political fundraising, spending, and advertising. Political committees (campaigns, parties, and political action committees [PACs]) are responsible for their own security measures, although, as noted elsewhere in this report, federal agencies (or private-sector entities) provide assistance in some cases.

Today, election security is one of the most rapidly evolving policy issues facing Congress and the federal government. Both chambers have passed legislation on the topic during the 116th Congress. Multiple House and Senate committees have held investigative and oversight hearings. Congress and the Obama and Trump Administrations have tasked federal agencies with new responsibilities for supporting states and thwarting future possible interference. The Intelligence Community has warned that countering foreign interference in U.S. elections "will require a whole-of-society approach, including support from the private sector and the active engagement of an informed public."[18]

Selected Federal Statutes

The U.S. Constitution and federal statutes regulate the division of governmental responsibility for elections. No existing statute is devoted specifically to election security, although, as discussed below, some statutes address aspects of the topic.[19] Most broadly, the Constitution's Elections

[16] Robert S. Mueller, III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, U.S. Department of Justice, Special Counsel report submitted pursuant to 28 C.F.R. §600.8(c), vol. 1, Washington, DC, March 2019, pp. 49-51.

[17] 52 U.S.C. §30121. For additional discussion of historical and recent campaign finance policy developments, see CRS Report R41542, *The State of Campaign Finance Policy: Recent Developments and Issues for Congress*, by R. Sam Garrett. See also CRS Report R45320, *Campaign Finance Law: An Analysis of Key Issues, Recent Developments, and Constitutional Considerations for Legislation*, by L. Paige Whitaker.

[18] Office of the Director of National Intelligence, National Counterintelligence and Security Center, *Foreign Threats to U.S. Elections: Election Security Information Needs*, at https://www.dni.gov/files/ODNI/documents/DNI_NCSC_Elections_Brochure_Final.pdf. The publication is not dated or paginated. The quoted material appears on the first full page of text.

[19] For example, certain provisions of HAVA address election security. For more on those provisions, see the "Federal

Clause assigns states with setting the "Times, Places and Manner" for House and Senate elections, and also permits Congress to "at any time … make or alter such Regulations."[20] As discussed in the "State and Local Role in Election Security" section of this report, the federal government thus plays a largely supporting role in election administration generally, and in election security specifically.

Two election-specific statutes can be particularly important for campaign and election security. Relevant legislation typically proposes amending one or both. First, the Help America Vote Act (HAVA, 2002) is the only federal statute devoted to assisting states with election administration. Congress relied on HAVA to establish the Election Assistance Commission, provide for a voluntary federal voting system testing and certification program, and authorize federal funding states could use to help secure their elections. Second, FECA's disclaimer and disclosure provisions, and the prohibition on foreign national fundraising or spending in U.S. elections, can be particularly relevant for concerns about foreign interference in U.S. elections. Several other statutes could be relevant in specific cases. **Table 2** below provides a brief summary.

Table 2. Selected Statutes Potentially Relevant for Campaign and Election Security

Statute	*U.S. Code* Citation	Brief Relevance for Campaign and Election Security
Criminal code	Various provisions in 18 U.S.C.	Prohibits various practices in elections/voting, such as use of intimidation or threats, election fraud, etc.; some provisions also prohibit computer fraud, which is referenced in some campaign and election security legislation
Federal Election Campaign Act (FECA)	52 U.S.C. §§30101-30146	Campaign finance statute; regulates disclaimer and disclosure requirements; prohibits foreign-national fundraising or spending; provides Federal Election Commission with civil enforcement authority; provides criminal penalties for knowing and willful violations
Foreign Agents Registration Act (FARA)	22 U.S.C. §§611-621	Relevant for some campaign and election security proposals/policy debates, such as disclosure of certain activity by foreign entities, or domestic entities with certain foreign ownership interests; primarily developed to address foreign propaganda; establishes disclosure requirements

Election Security Guidance" section of this report.

[20] U.S. Constitution, Art. I, §4.

Statute	*U.S. Code* Citation	Brief Relevance for Campaign and Election Security
Help America Vote Act (HAVA)	52 U.S.C. §§20901-21145	Primarily devoted to supporting state- and local-level election administration; authorizes funding for election administration-related purposes; establishes Election Assistance Commission; sets certain federal election administration requirements; and provides for a voluntary federal voting system testing and certification program
Homeland Security Act (HSA)	Various provisions in 6 U.S.C.	Established Department of Homeland Security; some election security bills, particularly regarding cybersecurity or government information-sharing, cite the HSA (note: see also 42 U.S.C. §5195c on critical infrastructure)
Lobbying Disclosure Act (LDA)	2 U.S.C. §§1601-1604	Primarily devoted to lobbying regulation generally; lobbyist reporting requirements (e.g., bundling disclosure) contained in act could be relevant for some campaign finance legislation
National Voter Registration Act (NVRA)	52 U.S.C. §§20501-20511	Primarily devoted to registration access; prohibits intimidation or coercion in registration, or knowingly providing false registration or tabulation information; establishes Chief State Election Official designation, which often is referenced in campaign and election security legislation
Telecommunications law	Various provisions in 47 U.S.C.	Primarily devoted to telecommunications provisions generally; political advertising disclaimer and disclosure requirements (e.g., 47 U.S.C. §§315, 317) can be relevant in some cases, and sometimes are referenced in campaign and election security legislation
Voting Rights Act (VRA)	52 U.S.C. §§10101-10702	Primarily devoted to voting access; prohibits intimidation, threats, or coercion in voting; authorizes deploying election observers and monitors to prevent discrimination based on race, color, or, in some cases, minority-language status

Source: CRS analysis of cited statutes, and adapted from CRS Report R45302, *Federal Role in U.S. Campaigns and Elections: An Overview*, by R. Sam Garrett.

Notes: See the report cited above for additional discussion of some of these statutes and of other campaigns and elections statutes. The table excludes general intelligence or law enforcement authorities that could be relevant in specific enforcement scenarios. It also excludes appropriations law. In some cases, agencies rely on

non-elections statutes or other authorities to support campaign and election security. This includes, for example, the January 2017 "critical infrastructure" designation from then-Homeland Security Secretary Jeh Johnson. See U.S. Department of Homeland Security, "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," press release, January 6, 2017, at https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical; and CRS In Focus IF10677, *The Designation of Election Systems as Critical Infrastructure*, by Brian E. Humphreys. The designation is still in effect, although Congress has not codified it. Some legislation proposes to do so, as noted in the **Appendix**.

Selected Federal Agencies

No single federal agency has responsibility for providing election or campaign security. Only two federal agencies—the Election Assistance Commission (EAC) and the Federal Election Commission (FEC)—are devoted entirely to campaigns and elections.

- The EAC administers congressionally appropriated federal funding, oversees a voluntary voting system testing and certification program, and provides voluntary election administration guidance, research, and best practices.
- The FEC is responsible for administration and civil enforcement of FECA.
- Other departments and agencies, primarily with responsibilities for other areas of public policy, support campaign and election security in specific cases.
- Some agency roles developed from a January 2017 "critical infrastructure" designation.[21] Additional detail appears below.

Additional information about agency roles appears below, and in the "Coordination By and Among Selected Federal Agencies" section of this report.

Election Assistance Commission (EAC)

The EAC is the only federal agency focused specifically on assisting states with election administration. Congress has charged the EAC with administering funding states may use to help secure their elections.

- The EAC also provides states and localities with election administration assistance, adopting voluntary voting system guidelines (VVSG, discussed below), providing for systems to be tested to the VVSG, and certifying systems as meeting the guidelines. It also conducts research about state election administration and voting, and shares information about best practices.
- Although not mandated by Congress, the EAC also participates in activities related to the designation of election systems as critical infrastructure, such as serving on the Election Infrastructure Subsector Government Coordinating Council (EIS-GCC) and on the EIS-GCC executive committee.[22]

[21] For additional discussion, see CRS In Focus IF10677, *The Designation of Election Systems as Critical Infrastructure*, by Brian E. Humphreys. For additional background on critical infrastructure designations generally, see CRS Report RL30153, *Critical Infrastructures: Background, Policy, and Implementation*, by John D. Moteff; and CRS Report R45809, *Critical Infrastructure: Emerging Trends and Policy Considerations for Congress*, by Brian E. Humphreys. Elections is a "subsector" within the Government Facilities sector.

[22] See Election Infrastructure Subsector, Governing Coordinating Council, *Charter*, October 18, 2017, at https://www.dhs.gov/sites/default/files/publications/govt-facilities-election-infrastructure-subsector-gcc-charter-2017-508.pdf.

Federal Election Commission (FEC)

The FEC enforces civil compliance with FECA provisions and commission regulations regarding campaign finance. This includes activities related to fundraising, spending, advertising disclaimers, and financial disclosure reports. These provisions are relevant for some aspects of security affecting political candidates or campaigns, parties, political action committees (PACs), or other entities (e.g., independent spenders that are not political committees) that raise or spend funds to affect federal campaigns.[23] The FEC does not regulate election administration or voting matters.[24]

Department of Homeland Security (DHS)

DHS provides states and localities with assistance mitigating risks to their election systems, especially concerning cybersecurity.

- DHS is the sector-specific agency (SSA) responsible for securing the election infrastructure subsector. Additional information appears later in this report.
- DHS's Cybersecurity and Infrastructure Security Agency (CISA) is responsible for most of the department's election security activities, including the Election Security Initiative (ESI).[25]
- DHS protects major presidential candidates through the U.S. Secret Service (USSS).[26] The Secret Service is also the lead security agency for "national special security events" (NSSEs), such as presidential nominating conventions.[27]

Department of Justice (DOJ)

The Department of Justice enforces several federal statutes, discussed above, that could be relevant for campaign and election security. Within DOJ, the FBI is the lead federal law enforcement agency supporting state and local election administration, and is the lead federal agency in investigating and prosecuting foreign influence campaigns.

[23] *Political committees* include candidate campaigns, parties, and PACs. See 52 U.S.C. §30101(4).

[24] Congress transferred the FEC's previous responsibilities in election administration and voting to the Election Assistance Commission in HAVA. For additional discussion, see CRS Report R45770, *The U.S. Election Assistance Commission: Overview and Selected Issues for Congress*, by Karen L. Shanton; and CRS Report R44318, *The Federal Election Commission: Overview and Selected Issues for Congress*, by R. Sam Garrett. It is possible that prohibited foreign spending to affect election administration or voting could fall under the FEC's jurisdiction. FEC commissioners have debated the agency's jurisdiction on matters not directly related to campaigns, a topic that is beyond the scope of this report.

[25] Before Congress established CISA in June 2018, the DHS National Protection and Programs Directorate (NPPD) served these functions. For background on CISA and other DHS cybersecurity roles, see CRS In Focus IF10683, *DHS's Cybersecurity Mission—An Overview*, by Chris Jaikaran.

[26] For additional discussion, see, for example, CRS Report RL34603, *The U.S. Secret Service: History and Missions*, by Shawn Reese; and CRS In Focus IF10130, *U.S. Secret Service Protection*, by Shawn Reese.

[27] CRS Report R43522, *National Special Security Events: Fact Sheet*, by Shawn Reese.

Intelligence Community (IC)

Several agencies contribute to or produce intelligence about election security threats.[28] For example, a declassified version of a January 2017 Intelligence Community Assessment (ICA) documenting Russian attempts to influence 2016-cycle U.S. elections contained information and analysis from the CIA, FBI, and NSA.[29] The "Coordination By and Among Selected Federal Agencies" section below provides additional discussion of the IC campaign and election security roles.

Selected Other Federal Agencies

- The State Department's Global Engagement Center (GEC) is charged with coordinating federal efforts to counter foreign propaganda and disinformation efforts aimed at undermining U.S. national security interests. The GEC partners with other U.S. government agencies, including those within the State Department, at the Defense Department, and elsewhere. [30]
- The Departments of Justice, State, and the Treasury all can be involved in administering sanctions for election interference. As noted previously, sanctions policy generally is beyond the scope of this report.[31]
- Via the FY2020 NDAA bill (S. 1790; P.L. 116-92), Congress assigned various agencies, especially DHS and the DNI, additional campaign and election security responsibilities. Most provisions involve providing Congress or federal or state agencies with information about election interference. The **Appendix** of this report provides additional detail.

Table 3 provides a brief overview of selected agency roles in campaign and election security.

[28] As CRS has explained elsewhere, the Intelligence Community (IC) includes "17 component organizations" within the federal government. These include, for example, the Central Intelligence Agency, National Security Agency, and intelligence divisions within other departments and agencies. For additional detail, see CRS In Focus IF10525, *Defense Primer: National and Defense Intelligence*, by Michael E. DeVine and Heidi M. Peters; CRS In Focus IF10527, *U.S. Intelligence Community Elements: Establishment Provisions*, by Michael E. DeVine and Heidi M. Peters; and CRS In Focus IF10470, *The Director of National Intelligence (DNI)*, by Michael E. DeVine.

[29] Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*, ICA 2017-01D, January 6, 2017, at https://www.dni.gov/files/documents/ICA_2017_01.pdf. For additional CRS discussion of these activities as a component of Russian foreign policy, a topic that is beyond the scope of this report, see, for example, CRS Report R44775, *Russia: Background and U.S. Policy*, by Cory Welt.

[30] For background on the GEC, see CRS Insight IN10744, *Global Engagement Center: Background and Issues*, by Matthew C. Weed. See also U.S. Department of State, "Global Engagement Center," at https://www.state.gov/r/gec/.

[31] For additional discussion, see, for example, CRS In Focus IF10694, *Countering America's Adversaries Through Sanctions Act*, by Dianne E. Rennack, Kenneth Katzman, and Cory Welt; CRS In Focus IF10779, *U.S. Sanctions on Russia: An Overview*, by Dianne E. Rennack and Cory Welt; CRS Report R45415, *U.S. Sanctions on Russia*, coordinated by Cory Welt; and CRS In Focus IF10694, *Countering America's Adversaries Through Sanctions Act*, by Dianne E. Rennack, Kenneth Katzman, and Cory Welt.

Table 3. Selected Agency Roles in Campaign and Election Security

Agency	Brief Description of Security Role
Department of Commerce	National Institute of Standards and Technology (NIST) advises EAC on technical and scientific matters, including voting system testing laboratory accreditation recommendations and assistance with developing the VVSG
Department of Defense	U.S. Cyber Command and other services provide cybersecurity and intelligence in some cases; U.S. Cyber Command and National Security agency Election Security Group task force tracks certain foreign threats; Federal Voting Assistance Program director included in EAC Board of Advisors; some National Guard units assist states with cybersecurity
Department of Homeland Security	Assists states on cybersecurity matters; Sector-Specific Agency (SSA) for Elections Infrastructure Subsector (EIS); Secret Service protects major presidential candidates
Department of Justice	Enforces criminal law and civil aspects of some elections statutes; DOJ included in EAC Board of Advisors; Federal Bureau of Investigation (FBI) investigates election crimes and participates in Intelligence Community; FBI Foreign Influence Task Force (FITF) investigates foreign influence operations; works with State Department and Treasury Department to administer sanctions for elections interference
Department of State	Global Engagement Center (GEC) coordinates federal efforts to counter foreign propaganda and disinformation, including in elections; State Department works with DOJ and Treasury Department to administer sanctions for elections interference
Department of the Treasury	Works with DOJ and State Department to administer sanctions for elections interference; can also participate in investigations of prohibited foreign interference in U.S. elections, such as through the department's Financial Crimes Enforcement Network (FinCEN)
Election Assistance Commission	Administers most HAVA funds, oversees a voluntary voting system testing and certification program, and provides voluntary election administration guidance, research, and best practices
Federal Election Commission	Administers and enforces civil campaign finance law; including disclaimer, disclosure, and foreign-national provisions that can be relevant for campaign and election security
Intelligence Community	Includes multiple agencies; assesses foreign efforts to influence U.S. campaigns and elections; Election Threat Executive is the principal elections adviser to Director of National Intelligence (DNI)

Source: Adapted from CRS Report R45302, *Federal Role in U.S. Campaigns and Elections: An Overview*, by R. Sam Garrett.

Coordination By and Among Selected Federal Agencies

Because no single federal agency is solely responsible for campaign and election security—and because state and local governments have most practical responsibility for election security—

coordination among agencies and governments is an ongoing congressional concern.[32] Adding to the complexity of the election security challenge, government agencies, in some cases, both support and regulate private actors—such as political campaigns—and sometimes rely on those private entities to provide threat information.

Highlights of federal coordination issues appear below. Because some of these relationships appear to be in development, some information about agency coordination, or the lack thereof, remains unclear in the public record. Similarly, some information about coordination among intelligence-gathering agencies is publicly unavailable, beyond the scope of this report, or both.[33] As such, other formal or information coordination among or by agencies likely occurs but is not reflected here.

Department of Homeland Security Coordination Roles

DHS takes a lead role in coordinating the federal support for campaign and election security. Most of the DHS coordination role stems from a January 2017 "critical infrastructure" designation that treats election infrastructure as an essential service requiring federal support and protection. The designation established the Elections Infrastructure Subsector (EIS) within the Government Facilities Sector, which includes various government buildings and equipment.[34]

- As a result of the critical infrastructure designation, DHS prioritizes support for the subsector, including to those state and local election jurisdictions that choose to accept such assistance. This includes sharing information about threats; and conducting cyber hygiene and risk and vulnerability assessments.[35]
- The critical infrastructure designation applies to physical and technical resources related to elections, such as communications technology, voting equipment, and

[32] See, for example, discussion and witness testimony presented during an October 22, 2019, House Judiciary Committee oversight hearing, "Security America's Elections Part II: Oversight of Government Agencies." As of this writing, the hearing record does not appear to have been published. Video and written materials are available on the committee website, https://judiciary.house.gov/legislation/hearings/securing-america-s-elections-part-ii-oversight-government-agencies. See also U.S. Congress, Senate Committee on Rules and Administration, *Oversight of the U.S. Election Assistance Commission*, 116th Cong., 1st sess., May 15, 2019, S. Hrg. 116-74 (Washington: GPO, 2019); U.S. Congress, House Committee on Homeland Security, *Defending Our Democracy: Building Partnerships to Protect America's Elections*, 116th Cong., 1st sess., February 13, 2019, Serial No. 116-1 (Washington: GPO, 2019); and U.S. Congress, House Committee on Oversight and Reform, Subcommittee on National Security, *Securing U.S. Election Infrastructure and Protecting Political Discourse*, 116th Cong., 1st sess., February 13, 2019, Serial no. 116-28 (Washington: GPO, 2019).

[33] For additional information on federal cybersecurity coordination (although not limited to elections issues), see CRS Report R41927, *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement*, by Kristin Finklea.

[34] U.S. Department of Homeland Security, "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," press release, January 6, 2017, at https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical. For additional discussion, see CRS In Focus IF10677, *The Designation of Election Systems as Critical Infrastructure*, by Brian E. Humphreys. For additional background on critical infrastructure designations generally, see CRS Report RL30153, *Critical Infrastructures: Background, Policy, and Implementation*, by John D. Moteff; and CRS Report R45809, *Critical Infrastructure: Emerging Trends and Policy Considerations for Congress*, by Brian E. Humphreys. Elections is a "subsector" within the Government Facilities sector.

[35] For an overview of DHS CISA services to state and local election jurisdictions, see, for example, U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, *Election Infrastructure Security Resource Guide*, May 2019. This document and several related publications are available for download on the agency's "Election Security Resource Library," at https://www.dhs.gov/publication/election-security-resource-library.

polling places. It does not apply to political campaigns. The designation does not give DHS regulatory authority over federal elections.[36]

DHS serves as the Sector-Specific Agency (SSA) for the EIS. As SSA, the agency plays various coordinating roles among public and private entities, as highlighted below.

- As SSA, DHS coordinates information sharing among various governmental and nongovernmental entities (e.g., vendors) responsible for election administration. In this role, DHS also coordinates activities for the EIS Government Coordinating Council (GCC).
- The EIS-GCC includes representatives from DHS, EAC, and state and local governments.
- DHS also works with a Sector Coordinating Council (SCC), which consists of industry representatives (e.g., voting-machine manufacturers).
- DHS also funds the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), a voluntary membership organization of state and local election jurisdictions run by the private Center for Internet Security. The EI-ISAC coordinates security information sharing among these entities.

Election Assistance Commission Coordination Roles

- As the only federal agency devoted specifically to election administration, the EAC helps facilitate communication between state or local election administrators and other federal agencies, and vice versa.
- EAC commissioners serve on the EIS Government Coordinating Council (EIS-GCC), coordinated by DHS, and on the EIS-GCC executive committee.

Intelligence Community Coordination Roles

As noted previously, the IC includes more than a dozen agencies from throughout the federal government. Highlights of the IC role in coordination surrounding campaign and election security appear below.

- In July 2019, then-DNI Coats created an IC Election Threats Executive (ETE) position to serve as the DNI's principal elections adviser and to coordinate IC election security work. Coats also directed IC agencies to assign a senior executive to serve as the point-of-contact for that agency's election security work and to serve on a new IC Election Executive and Leadership Board.[37]
- U.S. Cyber Command and the NSA monitors foreign threats to U.S. elections. This reportedly includes a recently established Election Security Group.[38] In

[36] For additional information, see CRS In Focus IF10677, *The Designation of Election Systems as Critical Infrastructure*, by Brian E. Humphreys. See also CRS In Focus IF10683, *DHS's Cybersecurity Mission—An Overview*, by Chris Jaikaran.

[37] It appears that the board could include representatives from non-IC agencies. For example, the press release announcing the ETE and board notes that "[m]embers of this board are senior-executive leads from across the IC and all relevant U.S. government organizations." See Office of the Director of National Intelligence, "Director of National Intelligence Daniel R. Coats Establishes Intelligence Community Election Threats Executive," press release, July 19, 2019, at https://www.dni.gov/index.php/newsroom/press-releases/item/2023-director-of-national-intelligence-daniel-r-coats-establishes-intelligence-community-election-threats-executive.

[38] See, for example, Dustin Volz, "NSA Forms Cybersecurity Directorate Under More Assertive U.S. Effort," *Wall*

addition, the FY2020 NDAA bill requires the DNI to appoint a national counterintelligence officer within the National Counterintelligence and Security Center to coordinate election security counterintelligence, particularly regarding foreign interference and equipment issues.[39]

Coordination Roles and Selected Other Federal Agencies

- In addition to coordination on IC threat assessments noted above, multiple federal agencies have collaborated on campaign and election security educational resources for political committees, election administrators, or voters.[40] Agencies also have issued joint warnings.[41]
- The State Department's Global Engagement Center (GEC) is charged with coordinating federal efforts to counter foreign propaganda and disinformation.
- The State Department also works with the Treasury Department and Justice Department to administer sanctions for election interference.

The FY2020 NDAA and Coordination Roles

- The FY2020 NDAA bill (S. 1790; P.L. 116-92), enacted in December 2019, requires the DNI to "develop a whole-of-government strategy for countering the threat of Russian cyberattacks and attempted cyberattacks against election systems and processes in the United States."[42]
- Congress specified that the strategy should include protecting federal, state, and local election systems, voter registration databases, voting tabulation equipment, and systems for transmitting election results.
- Congress also required the DNI to develop the strategy "in coordination" with the Secretaries of Defense, Homeland Security, State, and the Treasury, and with the Directors of the CIA and FBI.[43]

Federal Agency Roles and Campaign Security

Perhaps because the 2017 critical infrastructure designation does not apply to political campaigns or other political committees, it appears that no federal agency has specific responsibility for

Street Journal, July 23, 2019, accessed via CRS subscription; Olivia Gazis, "The NSA Prepares to Defend 2020 Elections, Drawing Lessons From 2018," CBS News Online, September 7, 2019, at https://www.cbsnews.com/news/the-nsa-prepares-to-defend-2020-elections-drawing-lessons-from-2018-midterms/; and Martin Matishak, "NSA, Cyber Command Reveal New Election Security Task Force Leaders," *Politico Pro*, November 7, 2019, accessed via CRS subscription. For additional discussion, see, for example, Ellen Nakashima, "U.S. Explores Information Warfare to Check Russia," *The Washington Post*, December 26, 2019, p. A1.

[39] See §6508, S. 1790; P.L. 116-92 (116th Congress).

[40] See, for example, a fact sheet jointly issued by eight federal agencies: *Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government*, n.d., at https://www.dhs.gov/publication/cyber-incident-reporting-unified-message-reporting-federal-government.

[41] See, for example, U.S. Department of Justice, et al., "Joint Statement from DOJ, DOD, DHS, DNI, FBI, NSA, and CISA on Ensuring Security of 2020 Elections," press release, November 5, 2019, at https://www.nsa.gov/news-features/press-room/Article/2009338/joint-statement-from-doj-dod-dhs-dni-fbi-nsa-and-cisa-on-ensuring-security-of-2/.

[42] See §6504, S. 1790; P.L. 116-92 (116th Congress).

[43] See §6504, S. 1790; P.L. 116-92 (116th Congress).

coordinating security preparations for these entities.[44] However, federal law enforcement agencies, particularly the FBI, can and do receive reports of, and investigate, suspected criminal activity. In preparation for the 2020 elections, the FBI also established a "Protected Voices" program that provides political campaigns,[45] private companies, and individuals with information about how to guard against and respond to cyberattacks and foreign influence campaigns. In addition, DHS (CISA), the FBI, and ODNI have jointly briefed some 2020 federal political campaigns on security threats and best practices.[46]

Federal Election Security Guidance

Federal election law takes a mostly voluntary approach to election security. Congress has set some security requirements for federal elections, such as directing election officials to provide a certain level of technological security for their HAVA-mandated computerized voter registration lists.[47] Most election security standards are set at the state or local levels.[48]

Some examples of the voluntary election security guidance the federal government provides are the research, best practices, and technical assistance described in the "Selected Federal Agencies" section of this report. HAVA also charges the EAC—with assistance from the agency's advisory bodies and NIST—with developing voluntary voting system guidelines (VVSG), accrediting laboratories to test voting systems to the VVSG, and certifying systems as meeting the VVSG.[49] The proposed update to the VVSG that was in development as of this writing (VVSG 2.0) includes some security-related principles and guidelines, such as ensuring that voting systems are auditable, limiting and logging access to voting systems, and preventing or detecting unauthorized physical access to voting system hardware.[50]

Participation in the federal voting system testing and certification program is voluntary under federal law.[51] The testing and certification program covers the "voting system" as defined by

[44] CISA offers assistance to campaigns on a voluntary basis. U.S. Congress, House Committee on the Judiciary, *Testimony of Matthew Masterson, Senior Cybersecurity Advisor, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security, for a Hearing on Securing America's Elections Part II: Oversight of Government Agencies*, hearing, 116th Cong., 1st sess., October 22, 2019, p. 6.

[45] The program also appears to provide services to political parties, and perhaps to other political committees (e.g., political action committees).

[46] See testimony from CISA Senior Cybersecurity Advisor (and former EAC Commissioner) Matthew Masterson, at an October 22, 2019, House Judiciary Committee oversight hearing, "Security America's Elections Part II: Oversight of Government Agencies." As of this writing, the hearing record does not appear to have been published. Video and written materials are available on the committee website, https://judiciary.house.gov/legislation/hearings/securing-america-s-elections-part-ii-oversight-government-agencies.

[47] 52 U.S.C. §21083; 52 U.S.C. §21081.

[48] For more on the role states and localities play in setting election security standards, see the "State and Local Role in Election Security" section of this report.

[49] 52 U.S.C. §§20961-20971. Technical Guidelines Development Committee, *Project Charter: VVSG Version 2.0*, June 26, 2016.

[50] National Institute of Standards and Technology, *Voluntary Voting System Guidelines VVSG 2.0: Draft Recommendations for Requirements for Voluntary Voting System Guidelines 2.0*, October 29, 2019, at https://collaborate.nist.gov/voting/pub/Voting/VVSG20DraftRequirements/vvsg-2.0-2019-10-29-DRAFT-requirements.pdf.

[51] Some states have chosen to make part or all of it mandatory under their own state laws. According to the Investigations and Oversight Subcommittee and Research and Technology Subcommittee of the House Committee on Science, Space, and Technology, 12 states required full federal certification of their voting systems as of 2019, and 8 states did not require any federal testing or certification. U.S. Congress, House Committee on Science, Space, and

HAVA, which does not include some components of the election system, such as voter registration databases and election night reporting systems.[52] Changes to one part of a voting system, such as updating software to patch security vulnerabilities, might require recertification of the system under the policies in effect as of this writing,[53] and updates to the VVSG require approval by a three-vote majority of the EAC's commissioners.[54]

Federal Funding for Securing Election Systems

Congress has responded to the threats that emerged during the 2016 election cycle, discussed above, in part with funding. Since the 2016 elections, it has provided funding for helping secure election systems both to states, territories, and the District of Columbia (DC), and to federal agencies.

Funding for States After the 2016 Election Cycle

The Consolidated Appropriations Act, 2020 (H.R. 1158; P.L. 116-93), and the Consolidated Appropriations Act, 2018 (P.L. 115-141), included $425 million and $380 million, respectively, for payments under provisions of HAVA that authorize funding for general improvements to the administration of federal elections. The explanatory statements accompanying the bills listed the following election security-specific purposes as potential uses of the funds:

- replacing voting equipment that only records a voter's intent electronically with equipment that utilizes a voter-verified paper record;
- implementing a post-election audit system that provides a high level of confidence in the accuracy of the final vote tally;
- upgrading election-related computer systems to address cyber vulnerabilities identified through DHS or similar scans or assessments of existing election systems;
- facilitating cybersecurity training for the state chief election official's office and local election officials;
- implementing established cybersecurity best practices for election systems; and

Technology, Subcommittee on Investigations and Oversight and Subcommittee on Research and Technology, *Election Security: Voting Technology Vulnerabilities*, hearing charter, 116th Cong., 1st sess., June 25, 2019, p. 2.

[52] 52 U.S.C. §21081; House Committee on Science, Space, and Technology, Subcommittee on Investigations and Oversight and Subcommittee on Research and Technology, *Election Security: Voting Technology Vulnerabilities*, p. 5.

[53] U.S. Election Assistance Commission, *Testing & Certification Program Manual, Version 2.0*, May 31, 2015, at https://www.eac.gov/assets/1/6/Cert_Manual_7_8_15_FINAL.pdf. Some observers have suggested that VVSG certification policies complicate decisions about patching vulnerabilities in voting system software. See, for example, U.S. Congress, House Committee on Science, Space, and Technology, Subcommittee on Investigations and Oversight and Subcommittee on Research and Technology, *Written Testimony of Josh Benaloh, Senior Cryptographer, Microsoft Research, Microsoft Corporation*, hearing on Election Security: Voting Technology Vulnerabilities, 116th Cong., 1st sess., June 25, 2019, p. 7. The EAC issued a notice of clarification about de minimis changes to voting system software on November 15, 2019. U.S. Election Assistance Commission, *NOC 19-01: Software De Minimis Changes*, Silver Spring, MD, November 15, 2019, at https://www.eac.gov/assets/1/6/NOC19.01_SoftwareDeMinimisChanges_11-15-2019.pdf.

[54] The VVSG was adopted by the EAC in 2005 and updated in 2015. As of this writing, another update is in development. The EAC lacked the quorum required to adopt an update from December 2010 to January 2015 and from March 2018 to February 2019. For more on the VVSG and quorums at the EAC, see CRS Report R45770, *The U.S. Election Assistance Commission: Overview and Selected Issues for Congress*, by Karen L. Shanton.

- funding other activities that will improve the security of elections for federal office.[55]

The 50 states, DC, American Samoa, Guam, Puerto Rico, and the U.S. Virgin Islands were eligible for both FY2018 and FY2020 payments. The Commonwealth of the Northern Mariana Islands (CNMI) was eligible for FY2020 funding.[56] Each recipient was guaranteed a minimum payment amount each year it was eligible—$3 million for each of the 50 states and DC and $600,000 per eligible territory—with the remainder of the appropriated funding distributed according to a formula based on voting-age population. Recipients are required to provide a 5% match for the FY2018 funds within two years of receiving a federal payment and a 20% match for the FY2020 funding.[57]

The EAC, which was charged with administering the payments, reported that all of the FY2018 funds were requested by July 16, 2018, and disbursed to the states by September 20, 2018.[58] Each state has five years to spend the funds, according to the EAC, and must report on its spending each fiscal year.[59] The EAC posts links to the states' reports—and spending plans—on its website and issues its own overview reports of state spending.[60]

Funding for Federal Agencies After the 2016 Election Cycle

As noted in the "Selected Federal Agencies" section of this report, multiple federal agencies are involved in helping secure election systems. Congress has designated some of the funding it has appropriated to such agencies specifically for election system security.[61] For example, following the designation of election systems as critical infrastructure in January 2017, the report language for DHS appropriations measures has specified funding for the department's election security

[55] Rep. Rodney Frelinghuysen, "Explanatory Statement Submitted by Mr. Frelinghuysen, Chairman of the House Committee on Appropriations, Regarding the House Amendment to Senate Amendment on H.R. 1625," explanatory statement, *Congressional Record*, daily edition, vol. 164, part 50 (March 22, 2018), p. H2519.

[56] CNMI did not hold federal elections when HAVA was enacted and, unlike the other territories listed here, was not covered by the act's funding provisions. The FY2020 appropriations bill includes a provision that extends its funding to CNMI.

[57] Agencies are permitted to waive matching fund requirements for certain U.S. territories. For information on previous disbursements to states, territories, and the District of Columbia, see U.S. Election Assistance Commission, *HAVA Funds State Chart View*, at https://www.eac.gov/payments-and-grants/hava-funds-state-chart-view/; and U.S. Election Assistance Commission, *Payments & Grants*, at https://www.eac.gov/payments-and-grants/managing-requirements-payments/.

[58] U.S. Election Assistance Commission, *Election Security Grant Funding Requests Received as of 7/16/2018*, at https://www.eac.gov/assets/1/6/ES_Requests_Received.pdf; The U.S. Election Assistance Commission, *Grant Expenditure Report: Fiscal Year 2018*, April 4, 2019, p. 10, at https://www.eac.gov/assets/1/6/FY2018HAVAGrantsExpenditureReport.pdf.

[59] Mark W. Abbott, 2018 HAVA Election Security Grants, U.S. Election Assistance Commission, July 2018, https://static1.squarespace.com/static/5a665c98017db2b60bc22084/t/5b5f7eda03ce644ee283b688/1532985050697/HAVA+Funding_Mark+Abbott_July+2018.pdf; U.S. Election Assistance Commission, *HAVA Funds State Chart View*, at https://www.eac.gov/payments-and-grants/hava-funds-state-chart-view/; and U.S. Election Assistance Commission. For more on states' spending of the FY2018 HAVA funds, see CRS In Focus IF11356, *Election Security: States' Spending of FY2018 HAVA Payments*, by Karen L. Shanton.

[60] See, for example, U.S. Election Assistance Commission, *Grant Expenditure Report, Fiscal Year 2018*, Silver Spring, MD, April 4, 2019, at https://www.eac.gov/assets/1/6/FY2018HAVAGrantsExpenditureReport.pdf.

[61] Congress has also designated funding for other purposes that might be relevant to election security, such as funding for the State Department's GEC, to address propaganda and disinformation. As noted above, funding for aspects of election security other than securing election systems is outside the scope of the report.

initiative.[62] The explanatory statement for the FY2018 spending bill also directed the FBI to use some of its funding to help counter threats to democratic institutions and processes.[63]

Agencies may also spend some of the funding they receive for more general purposes on activities related to election system security. The U.S. Department of Defense's (DOD's) Defense Advanced Research Projects Agency (DARPA) has provided funding under its System Security Integrated Through Hardware and Firmware (SSITH) program to advance development of a secure, open-source voting system, for example, and the EAC applies some of its operational funding to the federal voting system testing and certification program described in the "Federal Election Security Guidance" section of this report.[64]

State and Local Role in Election Security

Some threats to U.S. elections—including both intentional interference efforts and the unintended threats posed by errors and natural disasters—involve the state and local systems used to administer elections.[65] Other election security threats involve efforts to spread disinformation about elections or the integrity of the electoral process.[66]

States and localities may play a role in countering both types of threat.[67] First, states and localities take the lead on defending their election systems. As noted previously, states and localities have primary responsibility for administering elections in the United States. The federal government has provided some funding and technical support to help them secure the systems they use to run elections, but states and localities have primary responsibility for ensuring that their systems are physically and technologically secure.[68]

---

[62] U.S. Department of Homeland Security, "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," press release, January 6, 2017, at https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical; Rep. Rodney Frelinghuysen, "Explanatory Statement Submitted by Mr. Frelinghuysen, Chairman of the House Committee on Appropriations, Regarding the House Amendment to Senate Amendment on H.R. 1625," p. H2557; U.S. Congress, House Committee on Appropriations, *Making Further Continuing Appropriations for the Department of Homeland Security for Fiscal Year 2019, and For Other Purposes*, conference report to accompany H.J.Res. 31, 116th Cong., 1st sess., February 13, 2019, Report 116-9 (Washington: GPO, 2019), p. 492. For more on the designation of election systems as critical infrastructure, see CRS In Focus IF10677, *The Designation of Election Systems as Critical Infrastructure*, by Brian E. Humphreys.

[63] Rep. Rodney Frelinghuysen, "Explanatory Statement Submitted by Mr. Frelinghuysen, Chairman of the House Committee on Appropriations, Regarding the House Amendment to Senate Amendment on H.R. 1625," p. H2091.

[64] Defense Advanced Research Projects Agency, "Hacker Community to Take on DARPA Hardware Defenses at DEF CON 2019,"" press release, August 1, 2019, at https://www.darpa.mil/news-events/2019-08-01; U.S. Election Assistance Commission, *Fiscal Year 2020 Congressional Budget Justification*, March 18, 2019, p. 11, at https://www.eac.gov/assets/1/6/EACFY2020BudgetJustification.pdf.

[65] U.S. Congress, Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 1: Russian Efforts Against Election Infrastructure*, 116th Cong., 1st sess., 2019. As used in this section, "state" is intended also to include U.S. territories.

[66] U.S. Congress, Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia's Use of Social Media*, 116th Cong., 1st sess., 2019.

[67] For more information about the role states and localities play in election administration in general, see CRS Report R45549, *The State and Local Role in Election Administration: Duties and Structures*, by Karen L. Shanton.

[68] For more information about federal election security funding, see the "Federal Funding for Securing Election Systems" section of this report. For more on the technical assistance the federal government provides for securing state and local election systems, see the "Selected Federal Agencies" and "Federal Election Security Guidance" sections of the report.

That includes primary responsibility for funding election system security measures. Securing election systems may involve capital expenditures, such as replacing voting machines, that exceed funding provided by Congress. It may also involve ongoing costs—from identifying and addressing emerging security threats to renewing software licenses, paying election security staff, and conducting post-election audits—that extend beyond the period for which federal funding is available. Such expenses are covered, if they are covered, by states and localities.

State and local responsibility for election system security also includes primary responsibility for making and implementing most decisions about how to secure election systems. Federal law sets some general standards for the administration of elections, such as the voter registration list digitization requirement noted in the "Federal Election Security Guidance" section of this report.[69]

States and localities decide—within the broad parameters set by such general standards—which election equipment and procedures to use and how to mitigate risks to them. They choose, for example,

- whether to use electronic devices to capture or count votes; whether, when, and how to conduct post-election audits;
- whether and how to set security standards for election equipment vendors; whether to have in-house security staff in local jurisdictions or rely on state or vendor IT support;
- which cybersecurity tools and procedures to use;
- whether and how to train election officials and poll workers on election security;
- how to secure election materials between elections and ensure a secure physical chain of custody on Election Day; and
- what cyber and physical security standards to set for election equipment.

Second, states and localities can help combat disinformation or misinformation about elections or the integrity of the electoral process. They can, for example,

- use official websites and social media accounts to share accurate information about elections or counter false information; and
- help educate the public about the steps they take to safeguard the electoral process.

States also can work through their professional associations—using initiatives such as a public education campaign launched by the National Association of Secretaries of State (NASS) in November 2019—to help direct voters to trustworthy sources of election information.[70]

These efforts might occur as part of or in parallel with responses to disinformation or misinformation by the federal government or private entities like social media companies.[71] States

[69] For more information about federal standards for election administration, see CRS Report R45302, *Federal Role in U.S. Campaigns and Elections: An Overview*, by R. Sam Garrett; CRS Report RS20898, *The Help America Vote Act and Election Administration: Overview and Selected Issues for the 2016 Election*, by Arthur L. Burris and Eric A. Fischer; and CRS Report RS20764, *The Uniformed and Overseas Citizens Absentee Voting Act: Overview and Issues*, by R. Sam Garrett (originally authored by Kevin J. Coleman).

[70] National Association of Secretaries of State, *NASS Launches #TrustedInfo2020: A Public Election Education Initiative*, at https://www.nass.org/node/1749.

[71] See, for example, Cybersecurity and Infrastructure Security Agency, *#Protect2020*, at https://www.dhs.gov/cisa/protect2020; and Federal Bureau of Investigation, *Protected Voices*, at https://www.fbi.gov/investigate/

might partner with social media companies to remove posts containing election disinformation, for example, or adopt disclosure requirements that supplement or override the companies' policies on digital political advertising.[72]

Selected Recent Policy Issues for Congress

Table 4 below briefly summarizes selected policy issues and options that have shaped recent policy debates in Congress. In addition, the **Appendix** at the end of this report briefly summarizes legislation primarily devoted to campaign and election security that has advanced beyond introduction during the 116th Congress. The table reflects recent policy debates, but is not intended to be exhaustive. Some observers might consider other issues not reflected here to be relevant for campaign and election security.

counterintelligence/foreign-influence/protected-voices.

[72] See, for example, "California Launches New Effort to Fight Election Disinformation," *Capital Public Radio*, September 23, 2018; Kevin Collier, "As Feds Struggle, States Create Their Own Anti-Election Propaganda Programs," *CNN*, July 11, 2019; and Jim Brunner and Christine Clarridge, "Why Google Won't Run Political Ads in Washington State for Now," *The Seattle Times*, June 7, 2018.

Table 4. Selected Recent Policy Issues Related to Campaign and Election Security

Policy Issue	Status Quo	Selected Areas of Policy Debate	Selected Policy Options
Coordination among federal agencies *See also* Notification of election interference *row*.	No single federal agency responsible for campaign and election security; see report text for additional discussion	Whether or how much additional coordination is needed between agencies to improve information sharing about security threats; whether an expanded federal role is appropriate for federal elections or could usurp state authority to administer elections; whether additional federal role or regulation could be unnecessary, expensive, or both	Maintain status quo; provide additional (or less) funding to federal agencies; create new campaign and election security agency, office, or position to enhance coordination among federal agencies; expand (or reduce) campaign and election security enforcement authorities in federal law or for specific agencies; provide additional (or less) funding to states in addition to or in lieu of additional federal agency funding; provide additional federal agency support to states; focus on enforcement of existing statutes
Election equipment and procedures	States and localities primarily responsible for selecting, acquiring, and securing election equipment and procedures within broad parameters set by federal law; EAC oversees voluntary voting system testing and certification program, including VVSG that contain certain security-related recommendations; some HAVA funding provided to states may be used to help secure election equipment and procedures; DHS, EAC, and NIST provide other assistance with securing state and local election equipment and procedures, such as best practices and technical assistance, and FBI and IC provide investigative and intelligence support	What the security threats to election equipment and procedures are, and whether or how the federal government is best positioned to help address them; whether it is appropriate for the federal government to be more involved in funding election equipment and procedures and/or making decisions about them; whether states and localities need additional assistance to address security threats to election equipment and procedures, and, if so, which types of assistance would be most effective; whether existing federal assistance, such as the voluntary federal voting system testing and certification program, is sufficiently responsive to changes in the election security landscape; whether election services vendors should be subject to federal regulation	Maintain status quo; provide federal agencies or states and localities with additional funding to help secure election equipment and procedures; reduce the funding federal agencies receive to help secure election equipment and procedures; expand or codify nonfinancial federal assistance, such as research, best practices, technical assistance, and investigative or intelligence support; require use of specific election equipment or procedures; require use of election equipment or procedures that meet certain security standards; amend procedures for certifying and recertifying voting systems and/or updating the VVSG; require disclosure of or prohibit foreign ownership or control of election services vendors; require election services vendors to meet certain federal security standards

Policy Issue	Status Quo	Selected Areas of Policy Debate	Selected Policy Options
Election system security funding	States and localities primarily responsible for covering costs of implementing and maintaining election system security measures; some HAVA funding provided to states may be used to help secure election systems; some appropriations to federal agencies designated for use in helping secure election systems; some more general agency appropriations may also be applied to election security-related purposes	Whether additional funding should be provided to help secure elections, and, if so, how much; which entities or agencies should receive funding; what purposes funding should or may be used for; whether funding should be provided on an ongoing basis; whether funding recipients should be required to meet additional conditions in order to receive funding	Maintain status quo; provide states, localities, federal agencies, and/or independent researchers with additional funding to help secure election systems; reduce the funding federal agencies receive to help secure election systems; designate funding for general improvements to election security and/or specific security-related purposes, for meeting federal election security requirements and/or carrying out voluntary security activities, and/or for identifying new security solutions and/or implementing or maintaining established best practices; provide for limited duration and/or ongoing funding; set conditions on funding, such as spending deadlines, state match or maintenance of effort requirements, or plan, performance, or reporting requirements
Election security standards and guidance	States and localities primarily responsible for setting election security standards within broad parameters set by HAVA; EAC oversees voluntary voting system testing and certification program, including VVSG that contain certain security-related recommendations; DHS, EAC, and NIST provide other voluntary guidance on election security, such as research, best practices, and technical assistance	Whether the federal government should set additional federal standards or guidance for election security, and, if so, who should develop them; whether additional standards or guidance should be mandatory or voluntary; whether the voluntary federal testing and certification program should cover more of the election system; whether the federal testing and certification program is sufficiently responsive to changes in the election security landscape	Maintain status quo; mandate specified federal standards for election security; charge EAC, NIST, DHS, or other agency or commission with developing federal standards for election security; expand the HAVA definition of “voting system" to include parts of election system that are not currently covered by the federal testing and certification program; amend procedures for certifying and recertifying voting systems and/or updating the VVSG; expand or codify voluntary federal election security guidance, such as research, best practices, and technical assistance

Policy Issue	Status Quo	Selected Areas of Policy Debate	Selected Policy Options
Electronic poll books (e-poll books)	Used in at least one jurisdiction by 36 states and in 26.2% of jurisdictions nationwide during the 2018 election, representing a 48.0% increase in usage since 2016, according to the 2018 EAVS report; no federal guidelines; state cybersecurity or certification standards vary	How to maintain the integrity of real-time voter information; how to provide for continuity of election if e-poll book used to check in voters is offline or accessing invalid data	Maintain status quo; include e-poll books as part of HAVA voting systems; establish security standards or guidelines for e-poll books; require or encourage use of paper poll books or other backup systems
Foreign money *See also* Influence operations *row*.	Campaign finance law (FECA) prohibits fundraising or spending by foreign nationals (except permanent resident aliens) in federal, state, and local U.S. elections.	Potential for prohibited foreign funds to surreptitiously affect U.S. elections, particularly through entities that do not publicly disclose donors (e.g., politically active tax-exempt organizations, such as 501(c)(4) groups); whether existing FECA prohibition is sufficient; whether additional enforcement of existing prohibitions needed; whether foreign money is most appropriately addressed through lobbying or antipropaganda policy, rather than through campaign finance policy	Maintain status quo; pursue additional civil or criminal enforcement; increase donor disclosure; increase disclaimers through campaign finance or lobbying law; impose sanctions or immigration restrictions; increase reporting or government coordination to detect such funds
Influence operations (e.g., disinformation, misinformation) *See also* Foreign money *row*.	No current overarching federal statute; statutes such as FECA, FARA, and the Homeland Security Act contain provisions that can be relevant in specific circumstances. FBI Foreign Influence Task Force (FITF) lead agency for investigating foreign influence campaigns; DHS and EAC offer assistance to election administrators	Extent of emphasis on domestic versus foreign sources; whether government agencies or nongovernmental entities are best-equipped to combat influence operations; extent to which regulation should apply only to election-related information versus more general issue advocacy	Maintain status quo; require additional federal agency monitoring or enforcement; encourage or rely on voters or nongovernmental entities (e.g., advocacy groups, universities, etc.) to pursue civic literacy efforts; impose sanctions or immigration restrictions; increase reporting or government coordination to detect such operations

Policy Issue	Status Quo	Selected Areas of Policy Debate	Selected Policy Options
Notification of election interference *See also* Coordination among federal agencies *row*.	In general, there does not appear to be standard practice among various federal, state, and local agencies and political groups (e.g., campaigns) about sharing election-threat information; FY2020 NDAA (S. 1790; P.L. 116-92) enacted in December 2019 specifies some additional agency reporting requirements to Congress; DHS and FBI can provide consultations and investigations to election jurisdictions or political committees (e.g., campaigns).	Whether election-specific notification processes are necessary, and if so, whether they should be mandatory or recommended; how broadly such requirements should apply (e.g., governments versus political committees); how widely such information should be publicized and when; timeliness, consistency, and level of detail provided from federal agencies to states and local election jurisdictions; state and local and/or political committee capacity to utilize federal threat information	Maintain status quo; require federal agencies to notify each other of suspected election interference; require federal agencies to notify state/local election officials, political committees, or voters about election interference; provide additional or expedited security clearances for election officials; require political committees (e.g., campaigns) to notify FBI or other federal agency of suspected or offered foreign interference or "things of value"
Online political advertising	FEC regulations apply disclaimer and disclosure requirements to paid advertising relating to federal candidates (*independent expenditures*, *public communications*, and *electioneering communications*); issue advocacy generally is not regulated under campaign finance law.	Whether funding sources already are sufficiently disclosed; whether existing law provides sufficient regulation of issue-oriented ads about the political process but that do not trigger campaign finance law/regulation; whether additional disclosure requirements would produce sufficient information to warrant additional compliance burden	Maintain status quo; increase donor disclosure; add disclaimer requirements through campaign finance law or other federal statutes; require platforms to disclose content or targeting data
Protecting voter information and records	States vary on voter registration database (VRDB) cybersecurity practices and policies for obtaining voter lists.	Whether or how to utilize other sources of information (e.g., agency records; other states) to update voter data; how individuals can update or access their own information without hampering election administration or enabling unauthorized access to voter data; whether existing (primarily state-level) processes to verify data accuracy, or update data, are sufficient	Maintain status quo; require security standards for VRDB access; specifying permissible uses for voter data; require or encourage opportunity to update information at the time of voting

Policy Issue	Status Quo	Selected Areas of Policy Debate	Selected Policy Options
Relationship between campaign and election security and voter access	States determine registration and voting requirements. NVRA and VRA prohibit intimidation, threats, or coercion in registration, voting, and elections (in addition to other provisions that are beyond the scope of this report)	Whether or how to alter federal role in the relationship between security and access; whether voter access should be pursued as a component of campaign and election security or as a separate policy debate Note: Much debate in this area occurs at the state level (e.g., over voter-identification requirements; the issue of voter fraud; access to absentee ballots, etc.)	Maintain status quo; make changes to the federal role or federal policy regarding election security that would have implications for voter access; pursue voter access as separate policy area from campaign and election security
Verifying election results	2018 EAVS report notes 29.6% of states used direct-recording electronic (DRE) voting machines with no voter-verified paper trail in at least one jurisdiction during the 2018 election. A majority of states require some type of post-election audit to ensure that votes are counted correctly, but there is no federal requirement. EAC provides guidance and VVSG that states may use addressing certain voting system features.	Whether current state-level verification processes are sufficient; what equipment or standards help voters ensure their ballot is cast correctly and help election officials ensure that vote results are complete and accurate; whether states have sufficient resources to purchase voting machines or other equipment that would help meet these standards	Maintain status quo; encourage or require auditing standards, such as risk-limiting audits; provide additional (or less) funding for states to implement audits; require paper ballots and/or voter-verified paper ballot trails
Voter registration databases (VRDBs)	HAVA requires states with voter registration to have a "centralized, interactive computerized statewide voter registration list" containing certain information. NVRA provides some circumstances for removing an individual from a VRDB, but states vary on other list maintenance practices.	Whether cybersecurity standards or guidelines are needed to protect database access, contents, storage, or information sharing; how to ensure information remains accurate for eligible voters; how to ensure ineligible voters cannot vote and are removed from VRDB	Maintain status quo; provide funding to states for upgraded equipment; resources for VRDB threat assessments; require information-sharing requirements if a vulnerability is detected; require VRDB access logs or offline backups; require or encourage: automatic voter registration, list maintenance requirements, or criteria for removing ineligible voters from lists

Source: CRS analysis of recent legislation and policy debates.

Notes: The table reflects recent policy debates, but is not intended to be exhaustive. Some observers might consider other issues not reflected here to be relevant for campaign and election security.

Concluding Observations

Campaign and election security are developing fields that cross policy and disciplinary boundaries. This complexity is reflected in the various statutes, agencies, and congressional committees that share responsibility for policymaking and administrative matters relevant for security U.S. campaigns and elections. Questions such as those that follow reflect themes discussed throughout this report. These and other questions could help congressional readers decide whether they want to maintain the status quo, appropriate funds, or pursue oversight or legislation.

- **Federal Role.** A key question for Congress is whether, where, and how it chooses to be involved in campaign and election security. Most broadly, this potentially includes how to define this rapidly developing policy area, and in so doing, considering which issues are most appropriately addressed at the federal level versus at the state or local levels. This report has emphasized the federal role because those topics are most relevant for Congress. As the report also explains, states, localities, and territories are responsible for making many of their own election security decisions—just as political campaigns, parties, and PACs are responsible for their own security. Therefore, there are important debates about what campaign and election security includes that the federal government can influence, but that are primarily addressed below the federal level, in the private sector, or both. Examples include, but are not limited to, how election security might affect voter access, and vice versa; whether states require voter identification at the polls and whether or to what extent alleged vote fraud exists; how much and on what jurisdictions choose to spend available funds; and whether states, localities, or political campaigns and parties have sufficient resources to secure their elections or organizations.
- **Communication.** Does Congress want to encourage or require additional information sharing about campaign and election security matters between the federal government and nonfederal elections agencies? Similarly, do state, territorial, and local elections officials feel that they have or need clear points of contact within federal agencies, and do they know which agencies to contact in various circumstances? If it determines that the status quo is inadequate, does Congress want to encourage or require different reporting protocols, agency outreach, etc.?
- **Coordination.** Various agencies have reported to Congress that they have improved coordination among themselves, particularly through working groups or task forces.[73] Less clear, at least from publicly available information, is

[73] For an overview, see, for example, U.S. Congress, Senate Committee on Rules and Administration, *Oversight of the U.S. Election Assistance Commission*, 116th Cong., 1st sess., May 15, 2019, S. Hrg. 116-74 (Washington: GPO, 2019); U.S. Congress, House Committee on Homeland Security, *Defending Our Democracy: Building Partnerships to Protect America's Elections*, 116th Cong., 1st sess., February 13, 2019, Serial No. 116-1 (Washington: GPO, 2019); and U.S. Congress, House Committee on Oversight and Reform, Subcommittee on National Security, *Securing U.S. Election Infrastructure and Protecting Political Discourse*, 116th Cong., 1st sess., February 13, 2019, Serial no. 116-28 (Washington: GPO, 2019). See also discussion and witness testimony presented during an October 22, 2019, House Judiciary Committee oversight hearing, "Security America's Elections Part II: Oversight of Government Agencies." As of this writing, the hearing record does not appear to have been published. Video and written materials are available on the committee website, https://judiciary.house.gov/legislation/hearings/securing-america-s-elections-part-ii-oversight-government-agencies. See also, for example, Martin Matishak, "NSA, Cyber Command Reveal New Election Security Task Force Leaders," *Politico Pro*, November 7, 2019, accessed via CRS subscription.

specifically how such coordination works and whether current coordinating mechanisms are sufficient or whether agencies need additional resources or mechanisms to improve coordination. If it determines that the status quo is inadequate, does Congress want to exercise oversight in this area, provide additional information-sharing authorities, funding, etc., or does it consider current coordination authorities and mechanisms sufficient?

- **Sectors.** Much of the federal government's attention to campaign and election security appears to emphasize outreach to election administrators in states, territories, and localities. With respect to the private sector (such as political campaigns and equipment manufacturers), is federal agency support sufficient? To what extent are information-sharing practices among federal agencies and the private sector (or voters) similar to or different from those that shape communication between federal agencies and state, territorial, or local governments? If it determines that the status quo is inadequate, does Congress want to encourage or require additional federal agency support for nongovernmental entities in campaign and election security, or reporting requirements for those entities to the federal government?
- **Voters.** Some federal public education campaigns, such as those to counter disinformation in elections, are aimed at individual voters. Overall, however, much of the federal role in campaign and election security emphasizes communication among government agencies or, in some cases, the private sector. If it determines that the status quo is inadequate, does Congress want to task federal agencies—and if so, which ones—with additional responsibility for educating voters about campaign and election security; to provide funding for nongovernmental organizations to do so, etc.?

The scope of potential campaign and election security threats, and the federal government's role in responding to those threats, has changed substantially in less than five years. The foreign interference revealed during the 2016 cycle—and widely reported to be an ongoing threat—has renewed congressional attention to campaign and election security and raised new questions. Whatever Congress determines about whether these or other questions are relevant for its consideration of campaign and election security policy, the issue is likely to remain prominent for the foreseeable future.

Appendix. Legislation Related to Campaign and Election Security That Has Advanced Beyond Introduction, 116th Congress

See the "Scope of the Report" section for additional detail.

Bill Number	Sponsor	Short Title	Committee Referral	Brief Summary of Security-Related Provisions	Latest Major Action
H.R. 1	Sarbanes	For the People Act of 2019	House Administration; Intelligence; Judiciary; Oversight and Reform; Science, Space, and Technology; Education and Labor; Ways and Means; Financial Services; Ethics; Homeland Security	Codify DHS "critical infrastructure" designation; authorize federal funding to assist states to upgrade election equipment or otherwise enhance security, including by implementing risk-limiting audits; include electronic poll books in HAVA voting systems standards; require paper ballots in federal elections; require election-threat reports among federal and state governments; require developing a national strategy to safeguard democratic institutions; expedite security clearances for election officials; amend FECA foreign national prohibition to include state and local ballot initiatives; and require FEC reporting to Congress on foreign funds in federal elections	Passed House (234-193), 03/08/2019
H.R. 753	Castro	Global Electoral Exchange Act of 2019	Foreign Affairs	Direct Secretary of State to establish a Global Electoral Exchange Program to promote and exchange international best election practices (including, among other practices, cybersecurity; transmitting results; data transparency; election dispute resolution)	Passed House (voice vote), 05/20/2019
H.R. 1158	McCaul	Consolidated Appropriations Act, 2020	Appropriations	In addition to providing some relevant agency appropriations, appropriate funds (Title V) to EAC for disbursement to states to	Became P.L. 116-93, 12/20/2019

Bill Number	Sponsor	Short Title	Committee Referral	Brief Summary of Security-Related Provisions	Latest Major Action
				"improve the administration of elections for Federal office, including to enhance election technology and make election security improvements"	
H.R. 2500	Smith (WA)	National Defense Authorization Act for Fiscal Year 2020	Armed Services	Among other provisions, require DNI, in consultation with FBI, NSA, and CIA directors, to report to Congress on Russian interference with U.S. elections (§1240B)	Passed House (220-197), 07/12/2019 See also S. 1790.
H.R. 2722	Lofgren	Securing America's Federal Elections (SAFE) Act	House Administration; Space, Science, and Technology	Among other provisions, amend HAVA to authorize grants to states for upgrading election equipment cybersecurity, and risk-limiting audits; require use of voter-verified paper ballots; specify ballot printing and accessibility requirements; and require states to "seek to ensure" that voting equipment is manufactured in the United States	Passed House (225-184), 06/27/2019
H.R. 3351	Quigley	Financial Services and General Government Appropriations Act, 2020	Appropriations	In addition to providing some relevant agency appropriations, appropriate funds (Title V) to EAC for disbursement to obtain "qualified" election equipment (including voter-verified paper audit trail)	Passed House (224-196), 06/26/2019 See also H.R. 1158.
H.R. 3494	Schiff	Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020	Intelligence	Among other provisions, require (Title XXV) development of national strategy for countering Russian interference in U.S. election; require DNI designation of counterintelligence officer to coordinate election security counterintelligence; specify various reporting and congressional briefing requirements concerning election interference	Passed House (397-31), 07/17/2019 See also S. 1790.

Bill Number	Sponsor	Short Title	Committee Referral	Brief Summary of Security-Related Provisions	Latest Major Action
H.R. 3501	Engel	Safeguard our Elections and Combat Unlawful Interference in Our Democracy Act (SECURE Our Democracy Act)	Foreign Affairs; Judiciary; Financial Services	Impose financial and immigration sanctions on all foreign individuals who have engaged in U.S. election interference since January 2015; State Department would identify individuals who have engaged or assisted in interference efforts to appropriate congressional committees	Foreign Affairs Committee ordered to be reported, 07/17/2019
H.R. 4617	Lofgren	Stopping Harmful Interference in Elections for a Lasting Democracy Act (SHIELD Act)	House Administration; Judiciary	Among other provisions, require political committees to report to the FBI and FEC offered or proposed contributions, coordination, or collaboration with foreign nationals; require political committees to establish foreign contact reporting compliance system; require FBI reporting to Congress of foreign interference; contains Honest Ads Act provisions extending certain disclaimer requirements to online political advertising, and requiring online platforms to maintain publicly available advertising data; clarify various aspects of FECA foreign-national prohibition; require FEC independent report on "media literacy" and "online political content" consumption; amend FECA foreign national prohibition to include providing or offering nonpublic campaign material; contains Deceptive Practices and Voter Intimidation Prevention Act of 2019 provisions prohibiting providing false elections information or interference with registration; amend Immigration and	Passed House (227-181), 10/23/2019

Bill Number	Sponsor	Short Title	Committee Referral	Brief Summary of Security-Related Provisions	Latest Major Action
				Nationality Act to prohibit U.S. admission for persons believed to have interfered with elections; require FEC to notify states of foreign national disinformation campaigns; amend FECA to prohibit "materially deceptive media" (including "deepfakes") 60 days before elections, unless media contains a disclaimer noting such manipulation	
H.R. 4782	Thompson (MS)	National Commission on Online Platforms and Homeland Security Act	Homeland Security; Energy and Commerce	Establish National Commission on Online Platforms and Homeland Security to examine how or whether online platforms have been used to promote violence, terrorism, or foreign influence campaigns (including in elections); require DHS Under Secretary for Science and Technology to conduct research on such topics	Homeland Security Committee ordered to be reported, 10/23/2019
H.R. 4990	Sherrill	Election Technology Research Act of 2019	Science, Space, and Technology; House Administration	Direct NIST, in collaboration with National Science Foundation, to carry out a research program on voting systems, including cybersecurity, end-to-end verifiable systems; accessibility and human-technology interface; voter privacy and data protections; and audit methods; direct NIST, in collaboration with the EAC, to update the HAVA voting system certification process; amend HAVA voting systems definition to include other elements of election system; and for other purposes.	Science, Space, and Technology Committee ordered to be reported, 11/14/2019
S. 482	Graham	Defending American Security from Kremlin	Foreign Relations	Among other provisions, prohibit damaging a critical infrastructure computer, including those	Reported, 12/18/2019

Bill Number	Sponsor	Short Title	Committee Referral	Brief Summary of Security-Related Provisions	Latest Major Action
		Aggression Act of 2019 (DASKA)		related to voter registration and voting machines; impose immigration restrictions and financial restrictions for foreign interference in U.S. elections; require Secretary of State and DNI to report to Congress on Russian election interference	
S. 1060	Van Hollen	Defending Elections from Threats by Establishing Redlines Act of 2019	Banking, Housing, and Urban Affairs	Among other provisions, require regular federal government assessments of foreign interference in U.S. elections, and require imposing sanctions in such cases	Hearing held, 07/18/2019
S. 1321	Blumenthal	Defending the Integrity of Voting Systems Act	Judiciary	Amend Computer Fraud and Abuse Act (CFAA) to add voting systems and elections	Passed Senate (unanimous consent), 07/17/2019
S. 1328	Durbin	Defending Elections against Trolls from Enemy Regimes (DETER) Act	Judiciary	Designate foreign persons as ineligible for entry to the United States, or subject to deportation, if those persons are believed to have interfered with U.S. elections or to be seeking entry to interfere in U.S. elections	Passed Senate (unanimous consent), 06/03/2019
S. 1589	Burr	Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020	Intelligence	Require (Title IV) assessments by DNI of foreign interference in elections (§ 408) and (Title V) reports to Congress from (1) Under Secretary of Homeland Security for Intelligence and Analysis on cyberattacks on election infrastructure during 2016 U.S. presidential election foreign interference and anticipated future attacks (§ 501); (2) DNI on Intelligence Community posture and analytical capabilities during 2016 election interference (§502); (3) and DNI, in consultation with various other agency heads, pre-	Reported (S.Rept. 116-47), 06/11/2019 See also S. 1790.

Bill Number	Sponsor	Short Title	Committee Referral	Brief Summary of Security-Related Provisions	Latest Major Action
				election foreign intelligence threats (§503); DNI, in consultation with various other agency heads, on Russian influence campaigns directed at non-U.S. elections (§505); require DNI, in consultation with various other agency heads, to develop "whole-of-government" strategy for protecting U.S. "electoral systems and processes" from Russian interference (§504); require DNI in consultation with various other agency heads, to make publicly available pre-election reports on counterintelligence and cyber threats to federal campaigns (§506); require DNI to assist DHS in providing security clearances and share information with state election officials (§507); require DNI, FBI Director, and Secretary of Homeland Security to brief Congress if they jointly determine that "significant cyber intrusion or active measures campaigns" intended to influence federal elections (§508); require DNI designation of counterintelligence officer to coordinate election security counterintelligence (§509)	
S. 1790	Inhofe	National Defense Authorization Act for Fiscal Year 2020	Armed Services	Among other provisions, require reports to Congress from (1) Under Secretary of Homeland Security for Intelligence and Analysis on cyberattacks on election infrastructure during 2016 U.S. presidential election foreign interference and anticipated future attacks (§6501); (2) DNI on	Became P.L. 116-92, 12/20/2019

Bill Number	Sponsor	Short Title	Committee Referral	Brief Summary of Security-Related Provisions	Latest Major Action
				Intelligence Community posture and analytical capabilities during 2016 election interference (§6502); (3) DNI, in consultation with various other agency heads, on pre-election foreign intelligence threats (§6503); and DNI in consultation with various other agency heads, on Russian influence campaigns directed at non-U.S. elections (§6505); require DNI, in consultation with various other agency heads, to develop "whole-of-government" strategy for protecting U.S. "electoral systems and processes" from Russian interference (§6504); require DNI to assist DHS in providing security clearances and share information with state election officials (§6506); require DNI, FBI Director, and Secretary of Homeland Security to brief Congress if they jointly determine that "significant cyber intrusion or active measures campaigns" intended to influence federal elections (§6507); require DNI designation of counterintelligence officer within National Counterintelligence and Security Center to coordinate election security counterintelligence (§6508)	
S. 1846	Peters	State and Local Government Cybersecurity Act of 2019	Homeland Security and Governmental Affairs	Among other provisions, add "entit[ies]" that collaborate with state and local "election officials" as permissible participants in DHS National Cybersecurity and Counterintelligence Center (NCCIC)	Passed Senate (unanimous consent), 11/21/2019

Bill Number	Sponsor	Short Title	Committee Referral	Brief Summary of Security-Related Provisions	Latest Major Action
S. 2065	Portman	Deepfake Report Act of 2019	Homeland Security and Governmental Affairs	Require reports from Secretary of Homeland Security about the state of "digital content forgery technology"	Passed Senate (unanimous consent), 10/24/2019
S. 2524	Kennedy	Financial Services and General Government Appropriations Act, 2020	Appropriations	In addition to providing some relevant agency appropriations, appropriate funds (Title V) to EAC for disbursement to states to "improve the administration of elections for Federal office, including to enhance election technology and make election security improvements"	Reported (S.Rept. 116-111, 09/19/2019) See also H.R. 1158.

Source: CRS analysis of bill texts.

Notes: Bills in the table specifically reference campaigns or elections and security. Other legislation not included in the table could be relevant for campaign or election security once implemented or in practice. See the "Scope of the Report" section for additional detail. The table excludes resolutions (e.g., proposed constitutional amendments) and routine appropriations bills that propose funding for agencies such as the Election Assistance Commission or Federal Election Commission, unless the appropriations bill also contains additional provisions specifically addressing campaign and election security.

Author Information

R. Sam Garrett, Coordinator
Specialist in American National Government

Karen L. Shanton
Analyst in American National Government

Sarah J. Eckman
Analyst in American National Government

Disclaimer