2017

Protecting America's Elections from Foreign Tampering: Realizing the Benefits of Classifying Election Infrastructure as Critical Infrastructure under the United States Code

Allaire M. Monticollo
University of Richmond

PROTECTING AMERICA'S ELECTIONS FROM FOREIGN TAMPERING: REALIZING THE BENEFITS OF CLASSIFYING ELECTION INFRASTRUCTURE AS "CRITICAL INFRASTRUCTURE" UNDER THE UNITED STATES CODE

In just the past five years, the United States has suffered numerous hacks into important entities and institutions across the country by ill-intentioned actors. Private companies and government agencies alike have felt the negative impacts of security breaches by hackers infiltrating proprietary and protected systems.[1] Even the United States political landscape has proven vulnerable to bad actors in the realm of cyber security.[2] Furthermore, analysts have attributed some of the most recent highly publicized hacks to state-sponsored groups.[3] As cyber security threats and opportunities for foreign hackers to infiltrate critical systems become more prevalent, it is natural to wonder where the next hack will occur, when it will happen, and whom it will affect.[4]

Many experts believe the next frontier for state-sponsored hackers could be election processes.[5] While some have maintained

1. *See generally* Michael Cieply & Brooks Barnes, *Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm*, N.Y. TIMES (Dec. 30, 2014), http://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html?_r=0; Julie Hirscheld Davis, *Hacking of Government Computers Exposed 21.5 Million People*, N.Y. TIMES (July 9, 2015), http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html?_r=0.

2. *See* Wesley Bruer & Evan Perez, *Officials: Hackers Breach Election Systems in Illinois, Arizona*, CNN (Aug. 30, 2016), http://www.cnn.com/2016/08/29/politics/hackers-breach-illinois-arizona-election-systems/; Tal Kopan, *DNC Hack: What You Need To Know*, CNN (June 21, 2016), http://www.cnn.com/2016/06/21/politics/dnc-hack-russians-guccifer-claims/.

3. *See, e.g.*, Cieply & Barnes, *supra* note 1 (attributing the Sony hack to North Korea); Kopan, *supra* note 2 (attributing the Democratic National Committee ("DNC") hack to Russia).

4. *See, e.g.*, Amanda Taub, *D.N.C. Hack Raises a Frightening Question: What's Next?*, N.Y. TIMES (July 29, 2016), http://www.nytimes.com/2016/07/30/world/europe/dnc-hack-russia.html.

5. *NSA Chief Says Spy Agencies Are Concerned Over Possible U.S. Election Hacks*, FORTUNE.COM (Sept. 13, 2016), http://fortune.com/2016/09/13/nsa-chief-election-hack/; *see*

that a large-scale hack on election systems would be difficult because many voting machines are not directly connected to the internet,[6] others have noted that "the machines . . . Americans use at the polls are less secure than the iPhones they use to navigate their way there."[7] Additionally, the mere potential for disrupting election infrastructure threatens the general public's faith in the democratic process.[8] Wavering faith in the democratic election process can call into question the legitimacy of American government, harm the United States' reputation abroad, and threaten the peaceful transition of power after Election Day.

Scholars point out that there is "no singular national body that regulates the security or even execution of what happens on Election Day."[9] Article I of the United States Constitution gives individual states the power to control the "Times, Places and Manner" of congressional elections.[10] Article II and the Twelfth Amendment set forth a bare bones procedure by which members of the Electoral College are appointed within individual states for presidential elections.[11] Overall, both election processes and presidential election processes are administered primarily by the states and are largely state controlled.[12] With the exception of some measured federal intervention, when issues of voting rights and election integrity are implicated,[13] Congress has taken a diminished role in regulating elections in the United States.[14] As a result, state-controlled election processes and infrastructures have created a disjointed electoral system across America that is ill-prepared to respond to a hack or state-sponsored attempt to influence the outcome of an American election.

Members of the Aspen Institute Homeland Security Group Issue Statement on DNC Hack, PRNEWSWIRE.COM (July 28, 2016), http://www.prnewswire.com/news-releases/members-of-the-aspen-institute-homeland-security-group-issue-statement-on-dnc-hack-300306004.html.

6. Massimo Calabresi, *Hacking the Voter*, TIME, Oct. 10, 2016, at 30.

7. Ben Wofford, *How to Hack an Election in 7 Minutes*, POLITICO (Aug. 5, 2016), http://www.politico.com/magazine/story/2016/08/2016-elections-russia-hack-how-to-hack-an-election-in-seven-minutes-214144.

8. Calabresi, *supra* note 6.

9. Wofford, *supra* note 7.

10. U.S. CONST. art. I, § 4, cl. 1.

11. U.S. CONST. art II., § 1, cl. 2; U.S. CONST. amend. XII.

12. *See* Joshua A. Douglas, *(Mis)trusting States to Run Elections*, 92 WASH. U.L. REV. 553, 553 (2015).

13. *See* Justin Weinstein-Tull, *Election Law Federalism*, 114 MICH. L. REV. 747, 755 (2016).

14. Douglas, *supra* note 12.

The disjointed nature of states' election processes—together with the primitive nature of voting machine data security technology and the rising ubiquity of cyber security hacks—suggests that the United States' voting apparatus may be vulnerable to foreign tampering. In August 2016, Secretary of Homeland Security Jeh Johnson proposed a potential solution to this vulnerability.[15] He suggested that the federal government should seriously consider classifying voting processes as "critical infrastructure" under the United States Code.[16] On January 6, 2017, Johnson formally implemented this policy change by announcing the designation of election infrastructure as critical infrastructure within the Department of Homeland Security ("DHS").[17]

DHS regulates and oversees the country's critical infrastructure to ensure that it is protected.[18] The nation depends on the safety of critical infrastructure industries to ensure physical and economic security. DHS has classified sixteen industries as critical infrastructure sectors, including the transportation systems sector, the chemical sector, the emergency management sector, the government facilities sector, and others.[19] These sectors are comprised of private infrastructure owners who utilize DHS's resources and information sharing network to thwart potential attacks on their security.[20] The classification of election infrastructure as critical infrastructure opens up an avenue for DHS to step in and regulate election processes. Such regulation will result in

15. *See Christian Science Monitor Breakfast with Jeh Johnson*, C-SPAN (Aug. 3, 2016), https://www.c-span.org/video/?413496-1/homeland-security-secretary-jeh-johnson-speaks-christian-science-monitor-breakfast ("I do think that we should carefully consider whether our election system . . . is critical infrastructure like the financial sector [and] like the power grid.").

16. *Id.* Critical infrastructure is defined in the U.S. Code as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." 42 U.S.C. § 5195c(e) (2012).

17. Press Release, U.S. Dep't Homeland Sec., Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector (Jan. 6, 2017), https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical [hereinafter Press Release, Secretary Jeh Johnson].

18. *Critical Infrastructure Sectors*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/critical-infrastructure-sectors (last visited Apr. 5, 2017); *Office of Infrastructure Protection*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/office-infrastructure-protection (last visited Apr. 5, 2017).

19. *Critical Infrastructure Sectors*, *supra* note 18.

20. *See Critical Infrastructure Sector Partnerships*, DEP'T OF HOMELAND SEC, https://www.dhs.gov/critical-infrastructure-sector-partnerships# (last visited Apr. 5, 2017).

much needed information sharing across states with regard to their voting systems and procedures, increase federal resources for state election administration, and restore the general public's faith in the democratic process of American elections.[21]

Advocating for increased federal supervision over elections is not a new concept,[22] but the manner and scope of proposed federal oversight has been an issue of considerable debate.[23] DHS's recent classification of voting systems as "critical infrastructure" has prompted even more disagreement as to whether this is the correct classification and what federal regulation in this space should attempt to accomplish.[24] This comment argues that DHS is right to classify election infrastructure as "critical infrastructure" and takes the position that federal supervision over elections should accordingly increase. Part I discusses state control of election administration, the creation and development of DHS, and the critical infrastructure framework in general. Part II argues that DHS is correct in its classification and asserts that voting processes are properly understood as critical infrastructure. It highlights states' current problems in ensuring the security of elections. Finally, it posits that a critical infrastructure designation for election processes allows DHS to promulgate regulations in the election space to help secure the integrity of elections. Part III explains the benefits that DHS regulations have had on other critical infrastructure industries. It suggests that similar regulations in the election sphere could benefit election processes now that they too are classified as critical infrastructure. This comment concludes that the critical infrastructure classification for election infrastructure will help thwart potential state-sponsored threats to American election legitimacy.

---

21. The potential federalism concerns regarding federal executive branch supervision over state-administered elections is beyond the scope of this comment.

22. *See, e.g.*, Dan T. Coenen & Edward J. Larson, *Congressional Power Over Presidential Elections: Lessons from the Past and Reforms for the Future*, 43 WM. & MARY L. REV. 851, 853 (2002) (stating that "[p]residential election controversies are nothing new").

23. *See, e.g.*, Richard H. Pildes, *Judging "New Law" in Election Disputes*, 29 FLA. ST. U. L. REV. 691, 694–95 (2001) (advocating for a more "aggressively 'centralizing'" approach to federal oversight in state election law).

24. Press Release, Jeh Johnson, *supra* note 17 ("I have determined that election infrastructure in this country should be designated as a subsector of the existing Government Facilities critical infrastructure sector. Given the vital role elections play in this country, it is clear that certain systems and assets of election infrastructure meet the definition of critical infrastructure, in fact and in law.").

I. TRADITIONAL STATE CONTROL OVER ELECTION ADMINISTRATION AND FEDERAL SUPERVISION OVER CRITICAL INFRASTRUCTURE INDUSTRIES

A. *States Largely Control Election Administration*

The states, rather than the federal government, are the primary administrators of elections across the country. Towns, counties, and cities oversee and administrate federal elections.[25] Each state's Secretary of State usually serves as its chief election officer who leads the voting administration apparatus within the state.[26] Below the Secretary of State are state election officials, who are responsible for preparing ballots, organizing polling places, training poll officials, and counting votes.[27] They also help register voters and maintain voters' personally identifiable information.[28] Finally, these state election officials manage the maintenance and use of voting machinery and equipment.[29] They monitor voting machinery and help voters utilize it on Election Day.[30] After Election Day, states retain auditing power over the election results.[31] However, auditing procedures vary from state to state.[32]

Many sources of legal authority underpin state primacy over election administration. The United States Constitution gives the states the power to prescribe the "[t]imes, [p]laces and [m]anner of holding [congressional] [e]lections"[33] and "appoint, in such [m]anner as the [l]egislature thereof may direct, a [n]umber of [e]lectors" for presidential elections.[34] Additionally, Congress enacted only a limited number of federal statutes in the area,[35] and "federal courts are increasingly likely to defer to a state's interest

25. *See* Robert S. Montjoy, *The Public Administration of Elections*, 68 PUB. ADMIN. REV. 788, 788 (2008).

26. Jocelyn Friedrichs Benson, *Democracy and the Secretary: The Crucial Role of State Election Administrators in Promoting Accuracy and Access to Democracy*, 27 ST. LOUIS U. PUB. L. REV. 343, 359–60 (2008); *see also* Montjoy, *supra* note 25, at 788–89.

27. Montjoy, *supra* note 25, at 789.

28. *Id.*

29. *Id.*

30. *See id.* at 790.

31. *See id.*

32. *See id.* at 790, 794.

33. U.S. CONST. art. I, § 4, cl. 1.

34. U.S. CONST. art II, § 1, cl. 2.

35. *See* Douglas, *supra* note 12, at 553.

in a particular policy [regarding election administration] unless it is blatantly unconstitutional or discriminatory."[36]

B. *Hacking Elections Presents a Unique National Security Concern That States are Unable to Address Alone*

Even though states largely control almost all election administration-related endeavors, they are unable to adequately address the current threat of foreign actors hacking into United States elections. Hackers present a unique threat to elections because states do not maintain the resources or means to prevent, identify, or quash potential hacks from foreign actors. The fragmented nature of the United States' election process, the characteristic that grants individual states autonomy over elections administered within the state, contributes to the issues states have in responding to threats from hackers. State control over elections has created a system of unique local practices for election administration. Such "[d]ecentralization and fragmentation affect the uniformity of administration and the capacity of systems to implement top-down mandates."[37] When administration issues arise, such as hackers infiltrating voter registration databases,[38] states struggle with troubleshooting measures because each locality's voting processes and procedures are different.

State election officials are responsible for preparing ballots, organizing polling places, training poll officials, and counting votes.[39] These tasks already present formidable challenges for state election officials, and the added threat of hackers infiltrating voting infrastructure is not something states currently have the resources to address. Quality of training for polling officials varies widely from state to state,[40] but none are trained on how to identify, respond to, or neutralize a threat in the form of a foreign hack into an election administration system. Scholars suggest that the quality of training for these state officials matters.[41] When election officials are better trained and understand the

36. Benson, *supra* note 26, at 344.

37. Montjoy, *supra* note 25, at 789.

38. *See* Bruer & Perez, *supra* note 2.

39. Montjoy, *supra* note 25, at 789.

40. J. MIJIN CHA & LIZ KENNEDY, MILLIONS TO THE POLLS: PRACTICAL POLICIES TO FULFILL THE FREEDOM TO VOTE FOR ALL AMERICANS 2 (2014).

41. Montjoy, *supra* note 25, at 791.

procedures put in place to rectify particular voting administration problems, elections run much more smoothly. However, not all state election officials have access to adequate training opportunities before Election Day.[42]

Additionally, the voting machine technology used by many states is acutely vulnerable to threats by hackers. Federal law mandates the availability of computerized state voter registration systems and promotes the use of electronic voting machinery.[43] One might believe that this federal mandate and stamp of approval would increase uniformity throughout states' election procedures, reliability in election results, and safety from tampering. However, "those systems, especially the kinds that record votes directly into a computer's memory (DREs), raise concerns about security and reliability."[44] Due to the lack of security and reliability of DREs, hackers are able to infiltrate the machinery and alter vote inputs.[45] At least thirty-two states used DREs at polling places during the presidential election on November 8, 2016.[46] Despite the widespread use of these machines, experts continuously note security concerns and general usage problems with using DREs during elections.[47]

C. *History of Federal Supervision Over Critical Infrastructure*

While states largely control election administration, the federal government is the main supervisory body over the United States' critical infrastructure. The United States Code defines "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[48] Many of the individual entities that directly deal with critical infrastructure are

42. Weinstein-Tull, *supra* note 13, at 779.

43. Help America Vote Act of 2002, 52 U.S.C. §§ 20901–21145 (2012 & Supp. II. 2015).

44. ARTHUR L. BURRIS & ERIC A. FISCHER, CONG. RESEARCH SERV., RS20898, THE HELP AMERICA VOTE ACT AND ELECTION ADMINISTRATION: OVERVIEW AND SELECTED ISSUES FOR THE 2016 ELECTION x (2016).

45. *See id.* at 13–14.

46. *The Verifier—Polling Place Equipment—2016*, VERIFIED VOTING, https://www.verifiedvoting.org/verifier/# (last visited Apr. 5, 2017).

47. *See, e.g.*, BURRIS & FISCHER, *supra* note 44.

48. 42 U.S.C. § 5195c(e) (2012).

private companies.[49] The federal government created DHS with the particular aim of consolidating its supervisory role over the nation's critical infrastructure.[50] DHS streamlined the federal government's capability to thwart and respond to potential attacks on critical infrastructure industries. However, from its inception, DHS was required to cooperate with private sector critical infrastructure companies to achieve its goals.[51] The critical infrastructure framework is specifically structured to ensure the autonomy of critical infrastructure controllers while simultaneously encouraging communication and information sharing amongst controllers within each critical infrastructure sector.

Prior to the creation of DHS, critical infrastructure considerations and "homeland security activities were spread across more than 40 federal agencies and an estimated 2,000 separate Congressional appropriations accounts."[52] Congress' efforts to protect critical infrastructure by legislation began more than a hundred years ago.[53] However, the more modern move by the executive branch to create a streamlined system of control over the nation's critical infrastructure began with the Clinton administration.

In July 1996, President Bill Clinton established the President's Commission on Critical Infrastructure Protection ("PCCIP") via an executive order, which recognized the need for "a comprehensive national policy and implementation strategy for protecting critical infrastructures from physical and cyber threats and assuring their continued operation."[54] President Clinton's initial executive order set forth the following critical infrastructure sectors: telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation,

---

49. *Critical Infrastructure Sector Partnerships*, *supra* note 20.

50. PRESIDENT GEORGE W. BUSH, PROPOSAL TO CREATE THE DEPARTMENT OF HOMELAND SECURITY 3 (2002), https://www.dhs.gov/sites/default/files/publications/book_0.pdf ("The Department would be responsible for comprehensively evaluating the vulnerabilities of America's critical infrastructure. . . .").

51. *Id.*

52. ELIZABETH C. BORJA, DEP'T OF HOMELAND SEC., HISTORY OFFICE, BRIEF DOCUMENTARY HISTORY OF THE DEPARTMENT OF HOMELAND SECURITY: 2001–2008 3 (2008).

53. *Critical Infrastructure Protection Oral History Project and Digital Archive*, GEORGE MASON UNIV., http://chnm.gmu.edu/cipdigitalarchive/timeline.php?century=19&decade=2&year=1916 (last visited Apr. 5, 2017) (noting that in 1916, prior to the United States joining the allies in World War I, Congress created the Council of National Defense as part of the Army Appropriations Act).

54. Exec. Order No. 13,010, 61 Fed. Reg. 37,347, 37,348 (July 17, 1996).

water supply systems, emergency services, and continuity of government.[55]

The PCCIP produced a report in October of 1997, which advocated for sharing information among infrastructure owners, establishing awareness of critical infrastructure vulnerabilities, and creating education programs to better help infrastructure owners secure critical infrastructures from potential threats.[56] After the PCCIP's recommendations underwent interagency review, President Clinton issued Presidential Decision Directive No. 63 ("PDD-63") in 1998.[57] PDD-63 set forth a national goal to protect the United States' critical infrastructure from threats that would diminish the abilities of the federal government, state and local governments, and the private sector.[58] Additionally, PDD-63 identified particular sectors whose critical infrastructures should be protected and assigned a "Lead Agency" to each sector.[59] These Lead Agencies were in charge of running the critical infrastructure protection plan with regard to their individual critical infrastructure industries.[60] At that point in 1998, the federal government's plan to protect its critical infrastructure spanned multiple different agencies, legal frameworks, and stakeholders.

After the September 11, 2001 terrorist attacks, the Bush Administration moved to consolidate the critical infrastructure organizational schema by creating a cabinet department primarily dedicated to securing the nation's critical infrastructure from foreign threats. The federal government realized the dangers of decentralized supervision over critical infrastructure and quickly consolidated its effort to protect it. Congress passed the Homeland Security Act of 2002 ("the HSA"), which created DHS.[61] The HSA set forth DHS's mission, which included preventing terrorist attacks, reducing the United States' vulnerability to terrorism, and minimizing the damage of terrorist attacks if and when they

55. *Id.* at 37,347.

56. PRESIDENT'S COMM'N ON CRITICAL INFRASTRUCTURE PROTECTION, CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURES xi (1997).

57. THE WHITE HOUSE: PRESIDENTIAL DECISION DIRECTIVE/NSC-63, CRITICAL INFRASTRUCTURE PROTECTION (1998), https://fas.org/irp/offdocs/pdd=63.pdf.

58. *Id.* at 2–3.

59. *Id.* at 3.

60. *Id.*

61. *See generally* Homeland Security Act of 2002, Pub L. No. 107-296, 116 Stat. 2135 (codified as amended at 6 U.S.C. § 111 (2012 & Supp. 2016)).

are carried out in the country.[62] By March 1, 2003, the Federal Emergency Management Agency, the Transportation Security Administration, the Coast Guard, the Customs Service, the United States Secret Service, and various other agencies were brought within DHS's control.[63]

On December 17, 2003, the Bush Administration issued Homeland Security Presidential Directive 7 ("HSPD-7").[64] HSPD-7 established a "national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks."[65] It also assessed the new critical infrastructure landscape after the HSA. HSPD-7 clarified the Secretary of Homeland Security's role in coordinating the unified national goal to ensure the security of critical infrastructure and the relationship between DHS and other agencies that maintained direct regulatory powers over critical infrastructure sectors.[66] Additionally, it required Lead Agencies "to report annually to the Secretary of Homeland Security on their efforts in working with the private sector."[67]

Organizationally, the Homeland Security Council remains an interagency group for coordinating policy across departments and for informing the White House.[68] Other agencies that previously operated autonomously were brought within DHS's control and were instructed to utilize their resources to protect critical infrastructure industry sectors. Private entities within critical infrastructure industry sectors were asked "to organize themselves to assist in coordination of effort and information sharing."[69] Certain operational units outside of DHS's critical infrastructure framework (for example, the FBI's National Infrastructure Protection

62. *Id.* § 101(b)(1), 116 Stat. 2142.

63. THE PRESIDENCY A–Z 283 (Gerhard Peters & John T. Woolley eds., 5th ed. 2013).

64. *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/homeland-security-presidential-directive-7 (last visited Apr. 5, 2017) [hereinafter *Homeland Security Presidential Directive* 7]; *see also* JOHN D. MOTEFF, CONG. RESEARCH SERV., RL30153, CRITICAL INFRASTRUCTURES: BACKGROUND, POLICY AND IMPLEMENTATION 10 (2015).

65. *Homeland Security Presidential Directive* 7, *supra* note 64.

66. MOTEFF, *supra* note 64, at 10–11.

67. *Id.* at 11.

68. *Id.*

69. *Id.*

Center) were initially left in place, though later moved to and restructured within DHS.[70]

II. VOTING PROCESSES AS CRITICAL INFRASTRUCTURE

State primacy over election administration has resulted in a number of widely publicized election administration issues.[71] These election administration issues have prompted a national conversation about the legitimacy of elections in America and have highlighted weaknesses in states' abilities to administer elections.[72] It follows that state election procedures may be vulnerable in other ways. The 2016 presidential campaigns emphasized the potential vulnerability of American elections to foreign tampering through hacking.[73] As the system currently stands, states have no clearly identified avenue for communicating with one another about potential threats to election processes on Election Day.

This part argues first in Part II.A that DHS currently has the power to regulate critical infrastructure industries in response to national security concerns. It also notes that the Obama administration was acutely focused on thwarting attacks on United States critical infrastructure via cyber mechanisms. Part II.B then argues that voting processes fit well within this plain text definition of critical infrastructure and the intent of the classification. Now that election processes are classified as critical infrastructure, the federal government can promulgate regulations through DHS to protect the integrity of elections from foreign hacker threats. This section also details federal legislation in other circumstances where states had problems administering elections. Finally, Part II.B concludes by stating that a critical infra-

70. *Id.* at 12.

71. *See, e.g.*, Shapiro v. McManus, 136 S. Ct. 450, 453, 456 (2015) (denying Maryland's motion to dismiss a case brought by voters alleging that the state used gerrymandering tactics with an intent to dilute and burden voters' political expression); Bush v. Gore, 531 U.S. 98, 100 (2000) (per curiam) (describing an election tabulation discrepancy in Florida during the 2000 presidential election that prompted a hand recount of 9000 "undervotes" in Miami-Dade County); *see also Structuring Judicial Review of Election Administration: Explanations and Opportunities*, 156 U. PA. L. REV. 313, 314–17 (2007) (describing the increase in litigation concerning voter participation and electoral mechanics issues).

72. *See* Andrew Gumbel, *The History Of 'Rigged' US Elections: From Bush v Gore To Trump v Clinton*, THE GUARDIAN (Oct. 25, 2016, 6:00 PM), https://www.theguardian.com /us-news/ 2016/oct/25/donald-trump-rigged-election-bush-gore-florida-voter-fraud.

73. Cory Bennett, *U.S. Elections are More Vulnerable Than Ever to Hacking*, POLITICO (Dec. 29, 2016, 5:07 AM), www.politico.com/story/2016/12/election-hacking-vulnera bilities-233024.

structure classification for voting processes allows the executive branch to effectively regulate elections in ways that federal congressional legislation has failed to do in the past.

A. *DHS Can Regulate Critical Infrastructure in Response to National Security Risks*

Congress has given DHS broad power to exercise discretion when regulating critical infrastructure sectors in response to national security concerns. The Homeland Security Act of 2002 directly addressed DHS's ability to issue regulations in the critical infrastructure arena.[74] DHS's regulatory capabilities flow from the Administrative Procedure Act.[75] The Homeland Security Act of 2002 also took precautionary measures to ensure that it did not vest any novel regulatory authority in the newly created DHS. For instance, the Act only gave DHS the regulatory power already vested in other federal agencies on the day it was passed.[76] Additionally, DHS assumed the ability to regulate on behalf of all of the agencies consolidated under its umbrella.

Though Congress vested DHS with broad power to regulate critical infrastructure, the agency still must abide by other laws that limit the scope of its regulatory capabilities. For example, DHS abides by the mandates of the Regulatory Flexibility Act and various executive orders that issue guidance for federal agency regulations.[77] The Regulatory Flexibility Act commands federal agencies to thoroughly consider the impact of potential rules and regulations on entities of varying sizes before implementing such rules and regulations.[78] Executive Orders 12866 and 13563 direct federal agencies to follow particular principles and practices when issuing rules and regulations.[79] These principles require agencies to carefully consider possible alternatives before proposing a regulation. An agency must thoroughly analyze the costs

74. Homeland Security Act of 2002, Pub. L. No. 107-206, § 102(e), 116 Stat. 2135 (codified as amended at 6 U.S.C. § 111 (2012 & Supp. 2016)).

75. *Id.*

76. *Id.* § 877, 116 Stat. at 2244–45.

77. *DHS Rulemaking*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/dhs-rulemaking (last visited Apr. 5, 2017).

78. Regulatory Flexibility Act, Pub. L. 96-354, 94 Stat. 1164 (1980) (codified as amended at 5 U.S.C. §§ 601–12 (2012)).

79. Exec. Order 13,563, 3 C.F.R 215 (2012); Exec. Order 12,866, 3. C.F.R. 638–39 (1994).

and benefits of a proposed regulatory action, publish regulatory flexibility agendas in the Federal Register, and work with the Office of Information and Regulatory Affairs when proposing regulations under the federal rulemaking process.[80]

The Obama administration carried forward many of the Bush administration's policies with respect to critical infrastructure protection.[81] However, the Obama administration took a larger interest in protecting critical infrastructure from cyber threats.[82] The security community, the Obama administration, and Congress have debated the need to legislate and increase regulation of cyber security as critical infrastructure.[83] However, passing legislation in Congress has proven difficult. Interest groups are concerned about the costs of additional regulations and the potential for over-burdensome reporting requirements associated with regulations.[84] As a general statement of policy, owners and operators of critical infrastructure work with the federal government on a voluntary basis.[85]

Today, the Undersecretary for National Protection and Programs, a DHS official, is responsible for implementing critical infrastructure regulatory policies and coordinating programs with infrastructure owners.[86] The National Protection and Programs Directorate's mission is to make the nation's critical infrastructure as secure and resilient as possible, and to work against physical and cyber risk.[87] The Directorate strives to develop partner-

80. *See, e.g.*, 5 U.S.C. § 602 (2012) (requiring agencies to file biannual regulatory impact assessments regarding the effects on small businesses); Exec. Order 13,563, 3 C.F.R. 215, 217 (2012) (requiring agencies to consider alternatives, perform cost-benefit analysis, and consult with the Office of Information and Regulatory Affairs).

81. MOTEFF, *supra* note 64, at 12.

82. Dustin Volz & Mark Hosenball, *Concerned by Cyber Threat, Obama Seeks Big Increase in Funding*, REUTERS (Feb. 10, 2016, 6:45 AM), http://www.reuters.com/article/us-obama-budget-cyber-idUSKCN0VI0R1.

83. *See* MOTEFF, *supra* note 64, at 12–14.

84. *See* EDWARD C. LIU ET AL., CONG. RESEARCH SERV., R42409, CYBERSECURITY: SELECTED LEGAL ISSUES 2 (2013).

85. *See* MOTEFF *supra* note 64, at 11. For example, sharing information with the federal government about risk assessments, vulnerability calculations, and taking additional protective actions is meant to be entirely voluntary.

86. *See Suzanne E. Spaulding*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/person/under-secretary-nppd-suzanne-e-spaulding (last visited Apr. 5, 2017).

87. DEP'T OF HOMELAND SEC., PRESIDENTIAL POLICY DIRECTIVE 21—CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE, (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil; *see also* DEP'T HOMELAND SEC., NPPD AT A GLANCE (2014), https://www.dhs.gov/sites/default/files/publications/nppd-at-a-glance-071614.pdf.

ships with critical infrastructure owners and operators as well as federal, state, and local officials. DHS takes a much more active role in identifying critical assets, assessing vulnerabilities, and recommending and supporting protective measures than did earlier organizational structures.[88] Also, the "manpower and resources devoted to these activities have greatly increased" since DHS's inception.[89]

In many cases, DHS effectuates its core mission to thwart acts of terrorism through the promulgation of regulations that affect critical infrastructure. There are six operational components under DHS's wing with regulatory responsibilities: the United States Citizenship and Immigration Services, the United States Coast Guard, the United States Customs and Border Protection, the Federal Emergency Management Agency, the United States Immigration and Customs Enforcement, and the Transportation Security Administration.[90] Additionally, DHS regulates through the National Protection and Programs Directorate.[91]

B. *Federal Regulation via DHS in the Election Arena is a Viable Option to Respond to National Security Concerns over Election Hacks*

Voting processes fit within the plain text definition of critical infrastructure and the federal government's intent in creating the critical infrastructure framework. The definition of critical infrastructure suggests that election processes fall within its proposed scope.[92] Disruption of election systems by ill-intentioned actors, whether actual (through a carried out hack) or theoretical (through threats that undermine faith in election legitimacy),[93]

88. DEP'T OF HOMELAND SEC., PRESIDENTIAL POLICY DIRECTIVE 21—CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE, (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

89. MOTEFF, *supra* note 64, at 12.

90. *DHS Rulemaking*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/dhs-rulemaking (last visited Apr. 5, 2017).

91. *Id.*

92. 42 U.S.C. § 5195c(e) (2012).

93. *See, e.g.*, Greg Miller & Adam Entous, *Declassified Report Says Putin 'Ordered' Effort to Undermine Faith in U.S. Election and Help Trump*, WASH. POST (Jan. 6, 2017), https://www.washingtonpost.com/world/national-security/intelligence-chiefs-expected-in-new-york-to-brief-trump-on-russian-hacking/2017/01/06/5f591416-d41a-11e6-9cb0-54ab630851e8_story.html?utm_term=.534f0fb1ddbb.

has a debilitating impact on national security. Additionally, the federal government intended the critical infrastructure classification to protect systems and infrastructures that are vital to the national security of the United States.[94] Ensuring the integrity of voting processes is imperative to further continuity of government and public faith in elections.[95] In this way, election infrastructure is uniquely suited to fit within the intended nature of the critical infrastructure framework.

Even though the United States Constitution gives states a large amount of control over election administration, Congress has enacted substantial federal statutes in this area, which proves the federal government is not averse to asserting some level of supervision over election administration. The federal government has enacted a number of statutes largely to protect individuals' right to vote and ensure the integrity of elections.[96] This legislation addresses the timing of voter registration,[97] absentee voting rules,[98] and prohibitions on discriminatory practices.[99] Together, these federal statutes direct the administration of elections to some degree. However, these laws do not provide any concrete mechanisms for states to communicate about their election administration practices or receive federally supported training and education for effective administration practices.

The National Voter Registration Act of 1993 ("NVRA") is a federal statute enacted to regulate the timing of voter registration.[100] The NVRA "requires all states to adopt the federal voter registration procedures detailed in the Act, except for those states that have no registration requirements or that permit election-day

94. 42 U.S.C. § 5195c(e) (2012); MOTEFF, *supra* note 64, at 2.

95. *See generally Cybersecurity: Ensuring the Integrity of the Ballot Box: Hearing Before the Comm. on House Oversight and Gov't Reform, Subcomm. on Info. Tech.*, 114th Cong. (2016) (statement of Lawrence D. Norden, Deputy Director of the Democracy Program at the Brennan Center for Justice, NYU School of Law) (acknowledging the largest threats to the integrity of elections "are attempts to undermine public confidence in the reliability of that system.")

96. *See generally* Weinstein-Tull, *supra* note 13 (providing a comprehensive account of non-Voting Rights Act federal voting laws).

97. *See, e.g.*, National Voter Registration Act of 1993, Pub. L. 103-31, 107 Stat. 77 (codified at 52 U.S.C. §§ 20501–11 (2012 & Supp. 2015)).

98. *See, e.g.*, Uniformed and Overseas Citizens Absentee Voting Act of 1986, Pub. L. 99-410, 100 Stat. 924 (codified at 52 U.S.C. §§ 20301–11 (2012 & Supp. 2015)).

99. *See, e.g.*, Voting Rights Act of 1965, Pub. L. 89-110, 79 Stat. 437.

100. Pub. L. 103-31, 107 Stat. 77 (codified at 52 U.S.C. §§ 20501–11 (2012)).

registration with respect to federal elections."[101] In this way, the federal statute allows for states to escape its reach by permitting registration until and throughout Election Day. By exempting states that have no registration requirements and states that allow election-day registration from the statute, the NVRA substantially defers to state discretion. Therefore, though the federal government has chosen to control voter registration at some level, it still allows states a large amount of discretion to opt out of federal requirements.

Congress has also enacted federal statutes imposing requirements on the states with respect to absentee voting procedures. For example, Congress has enacted statutes to protect the absentee voting rights of military personnel stationed overseas. The Uniformed and Overseas Citizens Absentee Voting Act of 1986[102] ("UOCAVA") "requires states to permit (1) uniformed services voters and all other voters living overseas, and (2) uniformed services voters and their dependents within the U.S., but living out of their voting jurisdictions, to vote by absentee ballot in federal elections."[103] Interestingly, the UOCAVA places the onus of carrying out the Act on the executive branch by way of the Secretary of Defense.[104] Accordingly, the UOCAVA suggests that there is room for the executive branch of government to play a role in regulating the administration of elections in the United States.

Federal statutes have also been enacted to quash state voting administration procedures that had a discriminatory effect on particular groups of individuals. The Voting Rights Act of 1965, for example, protects the right to vote for persons of color and individuals who speak English as a second language.[105] Section 202 of the Voting Rights Act prohibits all states and localities from using any test or device to establish voter eligibility.[106] The expansive nature of the Voting Rights Act of 1965 suggests that the

101. U.S. GOV'T ACCOUNTING OFFICE, GAO-01-470, ELECTIONS: THE SCOPE OF CONGRESSIONAL AUTHORITY IN ELECTION ADMINISTRATION 12 (2001) [hereinafter U.S. GOV'T ACCOUNTING OFFICE, ELECTIONS: THE SCOPE OF CONGRESSIONAL AUTHORITY].

102. Pub. L. No. 99-410, 101 Stat. 924 (codified at 52 U.S.C. § 203 (2012)).

103. U.S. GOV'T ACCOUNTING OFFICE, ELECTIONS: THE SCOPE OF CONGRESSIONAL AUTHORITY, *supra* note 101, at 13.

104. Pub. L. No. 99-410, § 101(a), 100 Stat. 924; Exec. Order No. 12642, 53 Fed. Reg. 21975 (June 10, 1988).

105. Voting Rights Act of 1965, Pub. L. No. 89-110, 79 Stat. 437, 439 (codified at 52 U.S.C. §§ 10101–02 (2012)).

106. *Id.* § 202; *see also* JOCELYN F. BENSON, STATE SECRETARIES OF STATE 4 (Routledge ed., 2016).

federal government is in no way averse to recognizing problems in state-run election administration procedures and implementing measured responses to rectify the issues states cannot fix themselves.

In 2002, Congress enacted the Help America Vote Act[107] ("HAVA") in response to the "dimple" and "chad" ballot issues of the 2000 presidential election.[108] Congress enacted HAVA to rectify election administration issues caused by faulty state procedures.[109] While HAVA provided federal funding to update voting machines and train state administrators, these improvements were not made mandatory upon the states.[110] HAVA created the Election Assistance Commission (the "EAC"), which established *voluntary* election standards for the states.[111] The EAC also set forth *voluntary* certification standards for voting systems.[112] Additionally, the Act could not and did not prohibit states from using the voting equipment used in the presidential election of 2000.[113] As a result, though well intentioned, HAVA essentially "pave[d] the way for the continued use of the very voting systems associated with many of the problems plaguing Florida in 2000."[114]

DHS's ability to regulate is one of the main reasons it is the most optimal organizational structure for protecting election systems as opposed to prior efforts made by Congress through federal legislation. Specifically, because election processes are now classified as critical infrastructure, DHS's ability to regulate such processes will be more effective than HAVA. Though Congress enacted HAVA to bolster the integrity of American elections,[115] HAVA did not grant the EAC any regulatory power.[116] Section 209 of the Act prohibits the EAC from "issu[ing] any rule, promul-

107. Pub. L. No. 107-252, 116 Stat. 1666 (codified at 52 U.S.C. §§ 20901–21145 (2012)).

108. Steven Ramirez & Aliza Organick, *Taking Voting Rights Seriously: Race and the Integrity of Democracy in America*, 27 N. ILL. U.L. REV. 427, 428, 434–35 (2007); Brandon Fail, Comment, *HAVA's Unintended Consequences: A Lesson for Next Time*, 116 Yale L.J. 493, 493 (2006).

109. Pub. L. No. 107-252, 116 Stat. 1666 (2002); Ramirez & Organick, *supra* note 107, at 435.

110. Ramirez & Organick, *supra* note 108, at 435–36.

111. *Id.* at 436.

112. *Id.*

113. Help America Vote Act § 102.

114. Ramirez & Organick, *supra* note 108, at 436.

115. Weinstein-Tull, *supra* note 13, at 757–59.

116. Leonard M. Shambon, *Implementing the Help America Vote Act*, 3 ELECTION L.J. 424, 428 (2004).

gat[ing] any regulation, or tak[ing] any other action."[117] This has caused many scholars to note that HAVA's attempt at centralizing voting processes and increasing standards for voting infrastructure is ineffective.[118] In contrast, DHS's ability to regulate allows it to effectuate its goals in a way HAVA did not authorize the EAC to do. Classifying election infrastructure as critical infrastructure affords DHS regulatory power over the industry. This regulatory power could help increase communication across states with respect to election practices, increase federal resources for state administered elections, and promote the populace's faith in elections by legitimizing voting processes.

III. BENEFITS OF A CRITICAL INFRASTRUCTURE CLASSIFICATION

DHS's current oversight of critical infrastructure sectors focuses on information sharing, training and education, partnerships with local entities and private companies, assessments, analysis, and regulatory compliance.[119] If this general oversight structure expands to election processes by way of election infrastructure's critical infrastructure designation under the United States Code, states will be better able to communicate about potential threats from foreign actors to election integrity.[120] Involving DHS in elections will also help states gain federal resources to train state election administrators. Finally, DHS involvement in the election sphere will promote greater faith in electoral legitimacy.[121]

---

117. Pub. L No. 107-252, § 209, 116 Stat. 1678.

118. *See, e.g.*, Herbert E. Cihak, *The Help America Vote Act: Unmet Expectations?*, 29 U. ARK. LITTLE ROCK L. REV. 679, 684 (2007) ("It is not apparent that the EAC . . . fully understood the nation-wide ramifications of replacing punch card voting machines, lever voting machines, and paper ballots with electronic touch screen voting equipment. As early as 1969, studies . . . indicated that computerized voting presented a whole host of security issues."); Fail, *supra* note 108, at 494 (noting "HAVA might also ensure that future upgrades [to voting machinery] occur only infrequently and at great cost to state and local election agencies").

119. OFFICE OF INFRA. PROT., DEP'T OF HOMELAND SEC., IP FACT SHEET, https://www.dhs.gov/sites/default/files/publications/ip-fact-sheet-508.pdf (last visited Apr. 5, 2017).

120. *See* Letter from Tom Carper, U.S. Senator, to Jeh Johnson, Sec'y, Dep't of Homeland Sec., (Aug. 8, 2016), https://www.hsgac.senate.gov/media/minority-media/carper-urges-dhs-to-protect-the-us-election-systems-from-cyberattacks (discussing how classifying election systems as critical infrastructure would help to prevent and respond to potential cyberattacks from inside and outside of the country).

121. *See, e.g.*, Katie Bo Williams, *DHS Designates Election System 'Critical Infrastructure'*, THE HILL (Jan. 6, 2017), http://thehill.com/policy/national-security/313132-dhs-designates-election-systems-as-critical-infrastructure (quoting Representative Bennie Thompson, stating that the designation "will put our electoral systems on a more secure footing

Simply by focusing on the goals of sharing information, increasing federal resources, and ensuring popular faith in election legitimacy, states can still be given wide latitude to determine the time, place, and manner of elections. A critical infrastructure designation by DHS allows the federal government to tailor its oversight policies to the specific industry—election infrastructure. As a result, the executive branch could certainly adopt a hands-off approach to regulating voting processes while simultaneously helping to promote election security on Election Day. Alternatively, DHS could step in and regulate election processes if and when the agency foresees vulnerability. DHS would be able to play a vital role in information sharing, provide training for election officers, and increase faith in American election administration procedures by conducting assessments of election infrastructure.

DHS already brings these benefits to other critical infrastructure industries through its regulatory capabilities. DHS regulations on these industries have helped foster information sharing among critical infrastructure owners, increase federal resources given to these industries to thwart potential vulnerabilities, and bolster public faith in the security of these industries.[122] The positive benefits enjoyed by the critical infrastructure sectors through DHS regulation can be duplicated in the election sphere now that election infrastructure has been designated as critical infrastructure under the United States Code.

A. *Election Infrastructure Can Benefit from DHS Regulations Intended to Increase Information Sharing Within the Industry Similar to Those Already Enacted in the Transportation Systems Critical Infrastructure Sector*

In 2005, DHS promulgated a regulation requiring commercial vessels and aircrafts to share passenger manifest information before arrival in and departure from the United States.[123] The goal of this regulation, called the "Electronic Transmission of Passenger and Crew Manifests for Vessels and Aircraft," was to alleviate "the increased terrorist threat facing the United States and in-

---

and maintain public confidence in our elections").

122. *See generally Critical Infrastructure Resources*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/critical-infrastructure-resources (last visited Apr. 5, 2017) (listing resources available to critical infrastructure industries).

123. 19 C.F.R. §§ 4.7b, 4.64, 1.2249a, 1.2275a (2005).

ternational trade and transportation industries, particularly the commercial air and vessel carrier industries, since the September 11, 2001 terrorist attacks."[124] The regulation increased information sharing by requiring aircrafts and commercial vessels to communicate about passenger manifest information before a threat to the aviation industry could be effectively carried out.

Election infrastructure could benefit from a regulation similar in spirit to DHS's Electronic Transmission of Passenger and Crew Manifests for Vessels and Aircraft regulation. Increased communication across states regarding election administration procedures could help states identify common vulnerabilities. Then, these states could work together to fix the vulnerabilities in their processes. The 2016 hack of Illinois and Arizona's voter registration databases is an apt example of how a lack of information sharing can affect more than one infrastructure owner.[125] DHS estimates that since the hacks into Illinois and Arizona's voter registration databases, at least eighteen other states' voter registration systems have also been targeted.[126] After becoming aware of this threat to election system security, DHS "stepped up its outreach to states and localities . . . [by] encouraging them to implement existing technical recommendations to secure their election systems and ensure that electronic voting machines are not connected to the internet."[127] However, the way the current system is structured, the onus is on the states to reach out to DHS for help in implementing these recommendations.[128] Despite this burden on the states to affirmatively reach out to federal agencies for help in securing their elections, states have noted the vulnerabilities in their own systems and asked DHS to step in to some degree.[129] At least nineteen of the twenty targeted states "expressed interest in a general 'cyber hygiene' scan of key [voter registration] websites" from DHS.[130]

Still, even if DHS could have helped states secure their registration websites for the 2016 election, any lasting protection of

124. *Id.*

125. Bruer & Perez, *supra* note 2.

126. *U.S. Official: Hackers Targeted Voter Registration Systems of 20 States,* CHI. TRIB. (Sept. 30, 2016, 4:42 PM), http://www.chicagotribune.com/news/nationworld/ct-hackers-target-election-systems-20160930-story.html.

127. *Id.*

128. *Id.*

129. *See id.*

130. *Id.*

voter registration sites by DHS would be impossible without a critical infrastructure designation or specific congressional legislation addressing the matter directly. Because election infrastructure has been classified as critical infrastructure, DHS can now provide information to all states about the nature of the hacks into Arizona's and Illinois' voter registration databases. States can learn from the vulnerabilities in Arizona's and Illinois' voter registration websites to better ensure that their own websites do not suffer from the same weaknesses.

B. *Voting Processes Could Benefit from DHS Regulations Intended to Increase Federal Funding to the Industry Similar to Those Already Enacted in the Emergency Services Critical Infrastructure Sector*

In 2006, DHS promulgated a regulation that expanded upon an already established federal loan program.[131] The loan program provided funding to state and local governments that suffered losses in revenue after large natural disasters.[132] This loan program, called the Special Community Disaster Loans Program, was created in response to Hurricanes Katrina and Rita, which devastated Mississippi, Florida, Alabama, and Louisiana.[133] Specifically, the 2006 regulation proposed "procedures and requirements for governments who received Special Community Disaster Loans to apply for cancellation of loan obligations as authorized by the U.S. Troop Readiness, Veterans' Care, Katrina Recovery, and Iraq Accountability Appropriations Act, 2007."[134] Removing the burden on state and local governments to repay the disaster loans allowed them to utilize the full potential of the federal funding they received.

The Special Community Disaster Loans Program represents DHS's willingness to offer resources to critical infrastructure sectors in need. A critical infrastructure designation creates an avenue for increased federal funding to reach a particular industry

131. 44 C.F.R. § 206.377 (2006); DEP'T OF HOMELAND SEC., NOTICE OF PROPOSED RULEMAKING: SPECIAL COMMUNITY DISASTER LOANS PROGRAM 1, 6, https://www.dhs.gov/xlibrary/assets/nprm_fema_scdlp_2009-03-30.pdf.

132. DEP'T OF HOMELAND SEC., NOTICE OF PROPOSED RULEMAKING: SPECIAL COMMUNITY DISASTER LOANS PROGRAM 1, 3, https://www.dhs.gov/xlibrary/assets/nprm_fema_scdlp_2009-03-30.pdf.

133. *Id.* at 3–4.

134. *Id.* at 1.

sector.[135] For fiscal year 2016, the Obama administration requested $1.3 billion from Congress for critical infrastructure protection.[136] This amount was calculated to encompass all of DHS's infrastructure protection and information security concerns for the fiscal year.[137] DHS now has the ability to contribute part of the billion dollar appropriation it receives from Congress to state election infrastructure. The additional monetary resources could lead to advancements that would help thwart potential hacks by foreign actors on election systems. The funding may go toward shoring up registration websites, purchasing more secure election machinery, or training election administration officials to respond appropriately in the case of a hack on voting systems.

C. *Voting Infrastructure Could Benefit from DHS Regulations Intended to Increase Public Perception of the Industry's Integrity Similar to Those Already Promulgated in the Chemical Critical Infrastructure Sector*

In 2007, DHS promulgated regulations to "to enhance the security of our Nation by . . . lowering the risk posed by certain chemical facilities."[138] These Chemical Facility Anti-Terrorism Standards ("CFATS") marked the beginning of a comprehensive regulatory program that placed policies, standards, and certification requirements onto many of the country's largest chemical producers and refiners.[139] Prior to the enactment of these DHS regulations, chemical safety had become an issue of widespread concern for the United States population.[140] As a result, legislators made concerted attempts to lower the risk of chemical accidents in the country.[141] A highly publicized gas leak at an American pesticide facility in Bhopal, India, in 1984, prompted Congress to enact an amendment to the Clean Air Act in 1990,

135. *See* MOTEFF, *supra* note 64, at 27.

136. *Id.* at 32.

137. *See id.*

138. Chemical Facility Anti-Terrorism Standards, 6 C.F.R. § 27.100 (2010).

139. Scott Goodman, *Recent Development: Department of Homeland Security's Chemical Facility Anti-Terrorism Standards and the Program's Immediate Effect on American Industry*, 6 ENVTL. & ENERGY L. & POL'Y J. 104, 104 (2011).

140. *See, e.g.*, JESSICA ZUCKERMAN, HERITAGE FOUND., CHEMICAL SECURITY IN THE U.S.: CFATS REGULATION TOO COMPLEX, OVERLY BURDENSOME 2 (Aug. 14, 2012), http://thf_media.s3.amazonaws.com/2012/pdf/bg2718.pdf.

141. *Id.*

commonly known as the Bhopal Amendment.[142] This amendment responded to prevalent public concern over the security of chemical plants after the Bhopal disaster.[143] The legislation placed additional obligations and requirements on chemical facility critical infrastructure owners to handle chemicals carefully in order to prevent disasters.[144]

In addition to recognizing the risk for potential chemical accidents, the United States simultaneously recognized the risks of insecure chemical facilities with respect to potential terrorist activities or infiltration by foreign actors. A Congressional Research Service report on chemical facility security in 2006 noted that prior to the enactment of the CFATS regulations, evidence existed to suggest that terrorists could gain access to chemical weapons inside the United States by orchestrating an attack on the chemical facilities critical infrastructure.[145] DHS's CFATS regulations represented an effort to quell the public's concern about chemical industry critical infrastructure vulnerabilities to potential terrorist threats.

Similar to the public's concern in the early 2000s about potential foreign attacks on chemical critical infrastructure, the 2016 presidential election has highlighted a general American fear that state-sponsored actors could attempt to influence the outcome of election results.[146] This fear threatens the legitimacy of American elections and the continuity of government.[147] Some commentators have pointed out that a hack on an American elec-

142. *Id.*

143. *See* Nehal A. Patel & Ksenia Petlakh, *Gandi's Nightmare: Bhopal and the Need for a Mindful Jurisprudence*, 30 HARV. J. RACIAL & ETHNIC JUST. 151, 153–54 (2014) (describing the December 3, 1984, Bhopal Disaster in India, when an American-owned pesticide plant caused tens of thousands of deaths by leaking methyl isocyanate into the atmosphere).

144. Philip Radford, *Protecting Our Communities From a Chemical Disaster*, HUFFINGTON POST BLOG (July 1, 2012), http://www.huffingtonpost.com/philip-radford/protecting-our-communitie_b_1465680.html.

145. LINDA-JO SCHIEROW, CONG. RESEARCH SERV., RL31530, CHEMICAL FACILITY SECURITY CRS-4 (2006).

146. NAT'L INTELLIGENCE COUNCIL, OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, INTELLIGENCE COMMUNITY ASSESSMENT: ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS 1 (2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf; Cory Bennett & Eric Geller, *FBI Alert Sparks Fears That State Voting Systems Are Under Digital Assault*, POLITICO (Aug. 29, 2016, 7:25 PM), http://www.politico.com/story/2016/08/fbi-states-voting-systems-digital-assualt-227523.

147. NAT'L INTELLIGENCE COUNCIL, OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, INTELLIGENCE COMMUNITY ASSESSMENT: ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS 2 (2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf.

tion could be appealing to state-sponsored actors "because they can succeed, especially if they find willing accomplices in the targeted country."[148] Citing a long history of state-sponsored attempts to influence elections all over the world, certain scholars believe that Americans should have expected a certain level of interference in election administration from foreign actors on Election Day.[149]

Regulation in the election sphere similar to DHS's CFATS regulations could help Americans regain faith in election legitimacy. CFATS proposed standards for chemical facilities in order to shore up the sector's critical infrastructure and secure it from the risk of foreign attack.[150] CFATS also represented DHS's willingness to insert itself into a potentially vulnerable critical infrastructure sector. Now that DHS has the ability to regulate in the election space by virtue of a critical infrastructure designation for election infrastructure, public perception of the legitimacy of election outcomes will likely increase.[151] Just as CFATS quelled the public's concern over weaknesses in the chemical industry's critical infrastructure security, DHS regulation of election infrastructure could quell the current public concern over weaknesses in state-run election administration security.

CONCLUSION

As technology advances, new opportunities for hackers to infiltrate critical systems will only continue to grow. State-sponsored hackers have already shown that they are capable of infiltrating the United States' political systems by hacking into voter registration databases and accessing the confidential information of at least one major political party.[152] Election systems may prove especially vulnerable to state-sponsored threats from hackers in the future due to the generally insecure nature of current election

148. Paul Musgrave, *Why Would Russia Interfere In the U.S. Election? Because It Sometimes Works*, WASH. POST (July 26, 2016), https://www.washingtonpost.com/posteverything/wp/2016/07/26/why-would-russia-interfere-in-the-u-s-election-because-it-usually-works/.

149. *Id.* (discussing examples including KGB conspiracy theories regarding Dr. Martin Luther King Jr.'s death).

150. *See* SCHIEROW, *supra* note 145, at CRS 27–32.

151. *See supra* Part II.B.

152. *See* Bruer & Perez, *supra* note 2; Tal Kopan, *DNC Hack: What You Need To Know*, CNN (June 21, 2016), http://www.cnn.com/2016/06/21/politics/dnc-hack-russians-guccifer-claims/.

machinery and registration procedures, the lack of federal oversight in the election sphere, and the intrinsic connection between democratic legitimacy and successfully administered elections.

Elections are largely state-administered events. However, the federal government has the constitutional power to supervise the state-level administration.[153] HAVA represented a federal attempt to do so, but this federal legislation lacked any practical ability to impose requirements on state election procedures. HAVA, therefore, became more of a suggestion to states regarding election practices rather than an enforceable law. As a result, states were able to opt out of the beneficial effects HAVA could have had on election practices.

The classification of election infrastructure as critical infrastructure under the United States Code is one possible way to better protect our elections from state sponsored threats. Classifying voting procedures as critical infrastructure puts elections within DHS's regulatory reach. As a result, DHS can exercise its regulatory power to increase information sharing among the states with respect to election processes, increase federal resources for state election administration, and increase faith in the democratic process of voting by playing an active role in the election space. DHS has already successfully achieved these goals via regulation in other critical infrastructure sectors. If DHS can duplicate the success it had in encouraging information sharing, increasing federal resources, and restoring public faith in the security of other critical infrastructures in election systems, it will go a long way to help prevent a future state-sponsored threat to United States election systems.

Allaire M. Monticollo *

153. *See supra* Part II.B.

* J.D. Candidate, 2018, University of Richmond School of Law. B.A., 2012, University of Virginia. I would like to thank the University of Richmond Law Review staff and editors for their diligent work in preparing this comment for publication; my final editor, Rachel Willer, for her excellent feedback and guidance; and Professor Christopher Cotropia for being an incredible mentor and writing advisor throughout this process. Finally, I would like to thank my parents and my brother for all of their encouragement, love, and support.

***