Critical Democracy Infrastructure

Protecting American Elections in the Digital Age

Threats, Vulnerabilities, and Countermeasures as a National Security Agenda

OSET INSTITUTE

September 2017

About the OSET Institute

The Open Source Election Technology ("OSET") Institute is a 501(c)(3) tax-exempt nonpartisan, nonprofit election technology research corporation chartered with research, development, and education in election technology innovation.

The Institute's flagship effort, the TrustTheVote™ Project is developing **Elect**OS™ a next generation higher integrity, lower cost, easier to use election administration and voting technology framework freely available for any election jurisdiction to adopt, and have professionally adapted and deployed. ElectOS and all open source election technology is being designed and engineered per the requirements and specifications of election officials, administrators, and operators through a Request For Comment (RFC) process.

As part of our research, development and education mission, from time to time, the Institute produces Briefings and other content to inform stakeholders, supporters, and the public about issues of election technology innovation and integrity.

Threats to our election administration technology infrastructure are inherently threats to our democracy

© 2017. All Rights Reserved. This Briefing document may be reproduced in its entirety, so long as the OSET Institute is credited, a link to the Institute's web site is provided (use: www.osetfoundation.org), and no charge is imposed on any recipient of the reprint or reproduction. This Briefing document may not be reproduced in part or altered form, or if a fee is charged, without the OSET Institute's written permission. The OSET visual mark, TrustTheVote, ElectOS, VoteStream, Satori, and "Code Causes Change" are all trademarks, service marks or registered trademarks of the OSET Institute.

© 2017 OSET Institute, Inc. All Rights Reserved

Acknowledgements

OSET Institute Board member **Peter F. Harter** provided instrumental guidance and advice in the development of this work. Several Board Advisors contributed key advice and input on the subject matter, including **Cameron Quinn**, a lifelong election administration executive and lawyer now with the Department of Homeland Security; **Aneesh Chopra**, former U.S. CTO; **Bryan Sivak** former CTO for DHS, the state of Maryland, and the District of Columbia; **Simon Rosenberg**, President of the New Policy Institute, and **Theresa Swinehart**, Senior Vice President, Multistakeholder Strategy And Strategic Initiatives at ICANN.

We gratefully acknowledge and thank **Dr. R. David Edelman**, who was Special Assistant to President Obama for Economic & Technology Policy (*and previously served on President Obama's National Security Council staff as Director for International Cyber Policy and in the Office of Science & Technology Policy*), and currently directs the Project on Technology, the Economy, and National Security (TENS) at the Massachusetts Institute of Technology. Dr. Edelman was the principal catalyst for the development of this Critical Democracy Infrastructure Briefing during his White House tenure in August of 2016.

We also are grateful to a list of over 100 elections experts and officials who, over the course of more than a year from time to time, provided insights, knowledge, and opinions through informal conversations, interviews, articles, postings, and replies in digital media, and/or other exchanges of mindshare that helped shape this Briefing. We wanted to include anyone we spoke with or participated in digital communications with including: **Robert Adams**, Former Deputy County Clerk, Bernalillo County NM; **Kim Alexander**, Executive Director, California Voter Foundation; **William Anthony**, Director, Franklin County Ohio Board of Elections; **Andrew Appel**, Professor of Computer Science, Princeton University; **Ron Bandes**, Network Security Analyst, Software Engineering Institute, CERT Division; **David Becker**, Executive Director and Founder, Center for Election Innovation & Research; **Josh Benaloh**, Research Scientist, Microsoft Research; **Kenneth Bennett**, Office of Registrar-Recorder/County Clerk, Los Angeles County, CA; **Matt Bishop**, Professor of Computer Science, University of California Davis; **Kimball Brace**, Election Data Services, Inc.; **Harvey Branscomb**, Coloradans for Voting Integrity; **Doug Chapin**, Director of the Program for Excellence in Election Administration, Humphrey School of Public Affairs, University of Minnesota; **Matthew Caufield**, Ph.D Cnd., Wharton School; **Dana Chisnell**, Co-Director, Center for Civic Design; **Thomas E. Connolly**, Deputy Director of Public Information, New York State Board of Elections; **Dr. Andrew Coopersmith**, Managing Director, Penn-Wharton Public Policy Institute; **Edgardo Cortes**, Commissioner, Virginia Department of Elections; **Matt Damschroder**, Assistant Secretary of State and Chief of Staff, Office of the Secretary of State, Ohio; **Matthew Davis**, Chief Information Officer, Virginia Department of Elections; **Dana DeBeauvoir**, Clerk, Travis County Texas; **David Dill**, Professor of Computer Science, Stanford University; **Caitlin Dirkovich**, Assistant Secretary for Infrastructure Protection, Department of Homeland Security, now Toffler Associates; **Susan Dzieduszycka-Suinat**, President and CEO, Overseas Vote Foundation; **John Dziurlaj**, former IT Data Architect, Office of Secretary of State, Ohio; **Mark Earley**, Voting Systems Manager, Leon County Florida Board of Elections; **Jeremy Epstein**, Deputy Division Director, Computer & Network Systems Division, National Science Foundation; **Efrain Escobedo**, VP Civic Engagement and Public Policy, California Community Foundation; **Edward Felten**, Professor of Computer Science, Princeton University; **Judy Flaig**, Election Manager, Fairfax County, Virginia; **Christopher Fowler**, Chief Innovation Officer and Director of IT, Rhode Island Department of State; **Josh Franklin**, National Institute of Standards and Technology; **Susannah Goodman**, Director for Corporate Accountability, Common Cause; **Susan Greenhalgh**, Elections Specialist, Verified Voting; **Ericka Haas**, Systems Engineer and Technical Liaison, Electronic Registration Information Center, Inc.; **Alex Halderman**, Director, Center for Computer Security and Society, University of Michigan; **Thomas Hicks**, Commissioner, U.S. Election Assistance Commission; **Candice Hoke**, Professor, Cleveland State University and Center for Election Excellence; **Stuart Holmes**, Voting Information System Manager, Secretary of State, Washington; **Gema Howell**, National Institute of Standards and Technology; **Harri Hursti**, Independent Consultant; **Waldo Jaquith**, U.S. Open Data Institute; **David Jefferson**, Visiting Scientist Retired, Lawrence Livermore National Laboratory; **Neil Jenkins**, Chief of Policy and Planning, Department of Homeland Security, National Protection and Programs Directorate, Office of Cybersecurity & Communications.; **Chris Jerdonek**, former President San Francisco Elections Commission; **Douglas Jones**, Professor of Computer Science, University of Iowa; **Arthur Keller**, former Senior Research Scientist,

Stanford University; **Neal Kelley**, Registrar, Orange County California; **Doug Kellner**, Co-Chair, New York State Board of Elections; **Merle King**, Executive Director, Center for Election Systems at Kennesaw State University; **Joe Kiniry**, Chief Scientist, Galois Inc. and Free and Fair Inc.; **Ronald L. Rivest**, Vannevar Bush Professor of Electrical Engineering and Computer Science, Massachusetts Institute of Technology; **Sharon Laskowski**, National Institute of Standards and Technology; **Dean Logan**, Registrar-Recorder/County Clerk, Los Angeles County California; **Joseph Lorenzo Hall**, Chief Technologist, Center for Democracy and Technology; **Paul Lux**, Supervisor of Elections, Okaloosa County FL; **Ryan Macias**, Certification Program Specialist, U.S. Elections Assistance Commission; **Elaine Manlove**, Delaware Election Commissioner; **Matthew Masterson**, Commissioner, U.S. Election Assistance Commission; **Neal McBurnett**, Consultant, Data Science; **John McCarthy**, Computer Scientist, Verified Voting; **Christy McCormick**, Commissioner, U.S. Election Assistance Commission; **Amber McReynolds**, Director of Elections, Denver Clerk and Recorder Colorado; **Justin Moore**, Computer Scientist, Google, Inc.; **Brad Nelson**, Elections Director, Pima County Arizona Elections Department; **Peter G. Neumann**, Senior Principal Scientist, SRI International; **Brian Newby**, Executive Director, U.S. Election Assistance Commission; **Lawrence Norden**, Deputy Director, Democracy Program at Brennan Center for Justice, NYU School of Law; **Wendy Noren**, County Clerk, Boone County Missouri; **Katy Owens Hubler**, Senior Policy Specialist, National Conference of State Legislatures; **Don Palmer**, Fellow, Democracy Project, Bipartisan Policy Center; **Tammy Patrick**, Senior Advisor, Bipartisan Policy Center; **Eddie Perez**, Director of Product Management, Hart InterCivic; **Noah Praetz**, Director of Elections, Cook County, IL; **Whitney Quesenbery**, Co-Director, Center for Civic Design; **Peggy Reeves**, Assistant to the Secretary of State for Elections, Connecticut Secretary of State; **Andrew Regenscheid**, National Institute of Standards and Technology; **Joe Rozell**, Director of Elections, Oakland County Michigan Elections Commission; **Ion Sancho**, Supervisor of Elections, Leon County, Florida; **Marian Schneider**, Special Advisor to the Governor on Election Policy, Pennsylvania; **Jim Silrum**, Deputy Secretary of State of North Dakota; **Barbara Simons**, Voting Technology Expert, and Past President, Association for Computing Machinery; **Pamela Smith**, former President, Verified Voting; **Tom Stanionis**, Office of Yolo County Registrar of Voters, California; **Philip Stark**, Professor of Statistics, University of California Davis; **Paul Stenbjorn**, Director of Election Administration, Virginia Department of Elections; **Anthony Stevens**, New Hampshire Office of Secretary of State; **Warren Stewart**, Communications Director, Verified Voting; **Charles Stewart III**, Professor of Political Science, MIT; **Paul Stokes**, United Voters of New Mexico; **Rokey Suleman**, former Elections Official Fairfax County Virginia and District of Columbia; **Vanessa Teague**, Senior Lecturer, Computing Information Systems, University of Melbourne; **Ken Terry**, Director of Allen County Ohio Board of Elections; **Chris Thomas**, former Director of Elections, Michigan; **Maggie Toulouse Oliver**, Secretary State, New Mexico; **Wendy Underhill**, Program Manager, Elections, National Conference of State Legislatures; **Poorvi Vora**, Professor, Computer Science, George Washington University; **John Wack**, National Institute of Standards and Technology; **David Wagner**, Professor, Electrical Engineering & Computer Sciences, University of California, Berkeley; **Dan Wallach**, Professor of Computer Science, Rice University; **Sarah Whitt**, Wisconsin Elections Commission; **Dawn Williams**, Elections Director, Iowa Secretary of State; **Michael Winn**, Director of Elections, Travis County Texas; **Rebecca Wright**, Professor of Computer Science at Rutgers University and Director of the Center for Discrete Mathematics and Theoretical Computer Science; **Alec Yasinsac**, Dean of School of Computing, University of South Alabama; **Paul Ziriax**, Secretary of the State Election Board of Oklahoma.

OSET Institute Supporter Acknowledgement

The OSET Institute deeply appreciates the **John S. and James L. Knight Foundation**, the **Democracy Fund**, the **Frost Foundation**, the **James H. Clarke Foundation**, the **Chris Kelly & Jennifer Carrico Family**, the **Barbara Coll Family**, the **Michael L. Henry Family**, **Matt Mullenweg**, the **Frank J. Santoro Family**, and the **Alec Totic Family** for their generous support of our work to increase integrity, lower cost, and improve usability of election technology infrastructure in the U.S. and abroad.

Foreword

By **William P. Crowell**
Former Deputy Director, National Security Agency; Partner, Alsop Louie Partners

In 2016 we witnessed an unprecedented election cycle wherein at least one foreign state adversary launched successful attacks on our election processes and technology. One clear outcome is that U.S. election infrastructure is now a matter of national security. Arguably, that makes election technology part of the assets of critical infrastructure. Unless we protect this infrastructure against future attacks, the potential for damage recognized in 2016 could be realized as soon as next year's 2018 Midterm Election.

Russian state sponsored activities in 2016 are now a recipe for refined capabilities to inflict even greater damage by themselves and others. As a former Deputy Director of the National Security Agency years ago, fortified by my engagement in breakthrough information security innovations ever since, I can say with confidence that in order to combat the threat of growing foreign adversarial attack capabilities, election machinery must be re-designed with a security-centric engineering approach in order to address this mounting cyber-threat.

Protecting against this threat requires a new mindset and a new infrastructure to ensure that election administration can occur with minimal to no disruption. We know our current election technology is obsolete, and relies on an untrusted dwindling supply chain of replacement parts. We also know there is a challenging and difficult reality regarding an inherently insecure underlying architecture of current voting and election administration technology. Like it or not, polling places are now pop-up data centers, and the fact that no Internet connectivity is involved is irrelevant to their integrity and security. Moreover, elections workers cannot be expected to match wits and resources with increasingly capable cyber adversaries. Unless there is a reset of the priorities for resourcing election organizations across the nation with better protocols, policies and platforms, our electoral process will continue to be at greater risk of chaos, uncertainty and upheaval. Proper protection of our election infrastructure is the basis for trust in the results of its operation: declared and accepted election winners and losers, and the orderly transfer of power.

So, what must be done? This Briefing presents the basis on which to work toward a comprehensive solution: adopting and adapting the principles of critical infrastructure protection to America's election technology infrastructure—as distributed and diffuse as it is, obsolete as its becoming, and re-invented as it must be.

Unfortunately, partisan polarization has made this topic and conversation on how to protect our election infrastructure difficult, if not nearly impossible. This must change. I've said it before and it bears worth repeating, *the earlier you make the decision to bank on the future at some present cost, the better off you are*. Our adversaries have no partisan preference; they are opportunists. Therefore, a patriotic approach must prevail. I believe this Briefing, thoroughly researched and thought-through, offers a non-partisan basis to help understand the questions, and seek good answers to securing this imperative aspect of our sovereignty. I hope you agree.

© 2017 OSET Institute, Inc. All Rights Reserved

Table of Contents

Foreword by William P. Crowell, *Former Deputy Director, National Security Agency* 5

Executive Summary 9

1. Increasing Risks and Critical Infrastructure 12
   - 1.1 The Mission 12
   - 1.2 Mission Critical 13
   - 1.3 Scope 14
   - 1.4 Central Questions 17
   - 1.5 Briefing Outline 18

2. The Scope & State of Critical Democracy Infrastructure 19
   - 2.1 Overview of the U.S. Electoral Process 19
   - 2.2 The Current State of EI Assets and Operation 21
   - 2.3 The Current State of Risk to EI and CDI 26
   - 2.4 The Challenge of Protecting Election Infrastructure 35
   - 2.5 Compensating Risk Factors for Current Risks 39
   - 2.6 Summary 41

3. Why Critical Infrastructure? 42
   - 3.1 The Rationale for CI Designation 42
   - 3.2 Concerns About the CI Designation 42
   - 3.3 Comparing EI to Other CI 46
   - 3.4 Administrative Intent 47
   - 3.5 Suggested Objectives for CDI Uplift 48

4. Organizational Development for CDI Protection 50
   - 4.1 Institutions for Voluntary Cooperation and Sharing 51
   - 4.2 Public-Private Partnerships 52
   - 4.3 Private Sector Roles 52
   - 4.4 Costs and Benefits 53

5. Findings and Recommendations 54
   - 5.1 Operations of an Elections CI Sector 55
   - 5.2 Architectural Innovation 55
   - 5.3 Short-Term Cyber Risk Reduction 56
   - 5.4 Supply Chain Risk Reduction 60

6. Summary 61

Citations 64

Glossary of Terms 69

© 2017 OSET Institute, Inc. All Rights Reserved

Authors

Gregory A. Miller co-founded the Open Source Election Technology (OSET) Institute in November 2006. He leads all aspects of the Institute's resource development, corporate partner R&D alliances, public outreach, election official stakeholder relations, and government and legal affairs. Gregory has been a volunteer subject matter expert in elections technology integrity and security to the U.S. Department of Homeland Security (DHS), the National Security Council (NSC) and continues to advise committees and members of Congress on the same. Mr. Miller has 30+ years of technical and business experience in computer and information technology with Internet and technology pioneers such as Netscape Communications. He is a trained computer scientist and software engineer, with graduate business education, and his law degree focused on intellectual property, technology law, and public policy. Greg has also been active in the American Bar Association focused on technology law and public policy issues, including Cyber-law, Information Privacy & Security, and Internet Governance. Mr. Miller participated in initial reviews of technology public policy components of the first National Infrastructure Protection Plan in the early 2000. Greg is also a member of the Congressional Internet Caucus Advisory Committee, and a sustaining member of the Internet Society. Mr. Miller also served on the San Francisco Voting Systems Task Force, 2010-2012.

E. John Sebes is one of the two original co-founders and Chief Technology Officer ("CTO") for the U.S. based OSET Institute, a nonprofit, nonpartisan election technology research and development organization. He leads all aspects of technology strategy, vision, architecture, engineering and development for the TrustTheVote Project, which is developing ElectOS™ a publicly available, open source election operating system. For over three decades, John has been a software engineer, technical consultant, and CTO, working in several areas—network infrastructure, application frameworks, embedded systems, critical infrastructure, and data center operations — with strong common themes of risk management, security, privacy, and reliability. Innovation and technology transfer have been another consistent theme, in settings as varied as government-funded R&D, venture-backed start-ups, professional services, academia, and non-profits. John has been a Principal Investigator in R&D projects, ranging from DARPA projects performed in the pre-web era, to recent work with the Department of Homeland Security on open source security technology. John's involvement with cyber critical infrastructure protection dates back to 2000, when Mr. Sebes was a member of the group who reviewed the first-ever *National Infrastructure Protection Plan* (NIPP), and contributed to the first revision of it, focusing on the infrastructure sectors containing cyber-physical system risks. John is a co-author of 12 patents and 20+ publications.

Joy London is Associate General Counsel of the OSET Institute, focused on election law, public policy and government relations. Ms. London earned her JD from Temple University School of Law, is licensed to practice in the State of New York and has held several private practice positions. Joy also earned her Master of Professional Studies in Cyber Policy & Risk Analysis from Utica College, and published a Capstone research paper: *The Threat of Nation-State Hacking of State Voter Registration Databases in U.S. Presidential Elections*. Ms. London is also currently a member of the New York Democratic Lawyers Council, Subcommittee on Election Integrity & Technology and National Security Working Group; and was a member of the Cybersecurity Policy Working Group on the Hillary for America campaign.

OSET Institute Team Acknowledgement

The authors gratefully acknowledge several colleagues that collaborated and contributed to preparing this Briefing, primarily the extensive research, fact-checking, and initial drafting efforts of **Sergio Valente**, *Election Infrastructure Policy Analyst* in the office of CTO for the OSET Institute, and student at American University in International Relations and Economics.

Similarly, we gratefully acknowledge the assistance during the year this Briefing has been in development from **Patrick Reed**, *Sr. Policy Analyst* in the office of CTO for the OSET Institute, the operational support of **Shoshanna Israel**, Chief of Staff in the office of COO for the OSET Institute, and the editorial support of several Institute and TrustTheVote Project staff, including **Meegan Gregg**, **Ali Tweedt**, **Alisa Zwanger**, and **Max Mirho**.

© 2017 OSET Institute, Inc. All Rights Reserved

Executive Summary

Free and fair elections are an essential ingredient to the administration of American democracy. American elections have a core mission: select political leadership in a manner that ensures a constitutionally mandated orderly transfer of power. Accordingly, election infrastructure is critical to our democracy and the administration of U.S. elections. Elections are an element of U.S. sovereignty and therefore, the technology of election administration is an asset of national security.

Attempts to interfere with or disrupt our elections are threats to our national security, and an infringement to our national sovereignty. As the 2016 election cycle revealed, our nation-state adversaries are even more empowered in the digital age to carry out their long-established desire to disrupt our elections. Although attempts to disrupt our elections are not new, adversaries' capabilities now include a synergistic combination of social engineering, information operations, and cyber operations, to exploit well-documented vulnerabilities in the cyber elements of election technology infrastructure, which include the "*storage facilities, polling places, and centralized vote tabulations locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments*." [1] The threats to election infrastructure range from disruption of election operations, to subversion of infrastructure, to potentially altering outcomes, to reputational attacks that undermine the American public's trust in free and fair elections.

The clear and present threats to the integrity of U.S. elections created by election infrastructure vulnerabilities are now broadly understood. This acute awareness has emerged at a pivotal time when local U.S. election administration offices across the country are facing the prospect of an underfunded replacement of election and voting systems. This is a result of the well-documented decay in election and voting systems[2] including obsolete voting machines, with replacements that offer no improvements in terms of vulnerabilities at all levels: hardware supply chain, fundamental system and software vulnerabilities, and lack of support for the essential information assurance mission of U.S. election officials. That mission is to provide the public with the evidence that elections results are derived solely from the legitimate ballots of authorized voters, acting freely without constraint or coercion.

---

1 Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," *Department of Homeland Security*, January 6, 2017, https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical

2 Lawrence Norden and Christopher Famighetti, "America's Voting Machines at Risk," *Brennan Center for Justice*, September 15, 2015, www.brennancenter.org/publication/americas-voting-machines-risk. The authors identify three (3) main problems facing voting machines: 1) they won't work properly (*or reliably*), 2) they will be incompatible with new and emerging technology, and 3) there is an increased difficulty in finding replacement (*spare*) parts.

It is difficult to find a national security mission, requiring government operated critical infrastructure, with a greater mismatch to the capabilities of our nation's adversaries. American election infrastructure was *never* designed for the current threats, nor intended to be operated by local government organizations with little or no critical infrastructure operator capacity, yet face security threats from nation-state adversaries.

The need for risk reduction is clear, but the broad scope for action is less so; both are catalyzed and clouded by concerns over the recent, formal designation of election infrastructure as a CI subsector.[3] There are varying viewpoints about the advisability and significance of that designation, which might help uplift the level of protection of election infrastructure. These views must cooperate within the existing administrative structure of U.S. elections that are administered by state and local elections jurisdictions by U.S. constitutional mandate. Unfortunately, policy discussions and concrete actions toward risk reduction are impaired by a broad lack of clarity on exactly what election infrastructure consists of, what might be designated as critical infrastructure, and hence a lack of clarity on how an official designation will foster constructive action in practice.

The objectives of this OSET Institute Briefing are to 1) clarify these issues and 2) provide recommendations in several areas for action toward risk reduction. Our vantage point for this Briefing is a decade of in-depth understanding of the processes and platforms of election administration—the underlying mechanics and technology of elections, with a strong appreciation for the policy issues. Thus, a goal of this Briefing is to provide actionable input into the policy-making aspects of protecting our nation's election infrastructure.

Our motivation for this Briefing is twofold: 1) the clear and present threats to the operational continuity of our democracy in the digital age, which resolving is core to our mission;[4] and 2) the increasing public attention to the vulnerabilities, which is giving rise to confusion, misperceptions, and even distortions of the threats, and the required solutions.

We start this Briefing by defining election infrastructure—the components of election administration technology, as well as the broader set of elements comprising critical democracy infrastructure. We then apply these definitions together with a current situation assessment to make recommendations on how to fortify and improve critical democracy infrastructure protection.

---

[3] "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," *Department of Homeland Security*, January 6, 2017, www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

[4] The mission of the OSET Institute is to increase confidence in elections and their outcomes in order to preserve our democracy by researching and developing innovations in election technology that will increase verifiability, accuracy, security, and trustworthiness in the processes and platform of election administration and operation.

Our cornerstone observation is that many valuable critical democracy infrastructure uplift activities can be undertaken with or without an official designation of election infrastructure as critical infrastructure, in two essential areas: 1) evolution of election operation toward norms of operation of national security assets, and 2) creation of the information technology base for election infrastructure that meets appropriate requirements for national security assets. In terms of scope for this Briefing, these recommendations include:

- Establishing and operating information sharing organizations and activities;
- Increasing voluntary use of federal assistance in cybersecurity assessment and protection by local election administration offices;
- Expanding the role of state and interstate election bodies to define guidance for critical democracy infrastructure uplift operations;
- Defining local initiatives to uplift critical democracy infrastructure protections as part of the broader election technology replacement wave now in progress;
- Accelerating existing activities on standards, interoperability, and especially cybersecurity requirements for election technology; and
- Accelerating existing activities of innovative election technology development.

This Briefing is not intended to be comprehensive on the many nuanced issues of these recommendations. The goal of this Briefing is to raise awareness and increase understanding of the criticality of election infrastructure for those readers less familiar with this topic. For those more familiar, we imagine this as a "living document" in that it will (*and should*) evolve as requirements and realities change.

Deeper policy thinking is outside the scope of this work. We prefer to collaborate with other policy research organizations, contributing our domain expertise on election technology.[5]

Accordingly, we hope this Briefing provides a solid foundation of information based on a decade of research, study, and technology development by the experienced technology and digital security professionals of the OSET Institute. Key contributors of the OSET Institute team bring years of experience in critical infrastructure and national defense technology. Thus, the OSET Institute is deeply committed to credible, pragmatic, and innovative research and development of high assurance technology to protect this most vital aspect of our democracy.

[5] To be sure, the Institute is increasing its technology public policy expertise, primarily to stay abreast of developments and thinking, and to complement an already sizable allocation of resources for government relations.

© 2017 OSET Institute, Inc. All Rights Reserved

1. Increasing Risks and Critical Infrastructure

Never has the potential for disrupted elections been higher, with multiple risk factors: nation-state adversaries with advanced capabilities to attack our election processes; greater distrust in those election processes; heightened suspicion of both electoral irregularities and voter fraud; increased tension between potential voter fraud versus voter access; and the ability of social media to spread inflammatory disinformation to millions in moments. The integrity, security, and trust of our election infrastructure—the processes, services, and technology that enable election administration—have never been more important, and more at risk. This Briefing is intended to provide a foundation of information based on a decade of research, study, and technology development by the experienced technology and digital security professionals of the OSET Institute.

For those familiar with the topic, this Briefing will hopefully provide perspective on how to fortify our election infrastructure ("EI") to ensure the operational continuity of this aspect of our democracy; you should be able to move quickly through the content, focusing on the sections of most interest. For those just turning their attention to this matter, we attempt to provide a basic, and to the best of our ability, non-technical appreciation for the importance and urgency of this topic to the extent that it can inform administrative, leadership, and/or public policy interests and responsibilities.

1.1 The Mission

United States elections are *critical* to our democracy, with a twofold mission: 1) to select political leadership and resolve questions of public interest (e.g., referenda), and 2) to ensure a timely and orderly transfer of power, which is in turn based on two critical election outcomes: the electorate's consensus belief in the legitimacy of election results, and concession of defeat by those not elected, based on the legitimate evidence of election results.

Consider the impact on national stability if there were a major election in which a candidate did not concede, the public was not patient, and the massive echo chamber of social media (*in infancy in 2000*) amplified both real and spurious concerns and incidents, enabling organized unrest. Any lack of clarity on election outcomes can create dire threats not only to the orderly transfer of political power, but even to public safety.

Basic consideration of a failed election process and consequent civil unrest indicates that the integrity of the election process is critical. At the national scale, threats to election integrity are threats to national security, particularly where nation-state actors may be engaging in operations to destabilize election processes or public trust of election results.[6]

---

[6] Max Bergmann and Carolyn Kenney. "War by Other Means." *Center for American Progress*, June 6, 2017,www.americanprogress.org/issues/security/reports/2017/06/06/433345/war-by-other-means/. Russia and other nation-state actors can use disinformation campaigns to sway the minds of individuals and destabilize America. While this has been done in the past, the advent of social media has increased its potency.

Where threats to elections involve EI, infrastructure for a critical function of our democracy, managing those threats and their risks is also a matter of homeland security.

1.2 Mission Critical

EI then, is indeed *critical infrastructure*. It is critical democracy infrastructure that is as important in its own way as critical power infrastructure, critical transportation infrastructure, and several other officially designated CI sectors that the Department of Homeland Security ("DHS") is tasked to provide assistance to as a result of Presidential Decision Directive 63 ("PDD-63"). And in terms of formal definitions, EI meets the basic definition when considered in terms of the basic mission stated above. According to DHS, critical infrastructure ("CI") is comprised of the: *"assets, systems, and networks, whether physical or virtual, considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."*[7]

President Clinton created the designation of CI in the 1998-issued PDD-63, but it gained new significance three years after the attacks of 9/11. It established that some parts of society were critical to the well-being of society and needed to be protected by the United States government as an extension of America's sovereignty.[8]

With that definition in mind, EI may be considered "*critical democracy infrastructure*" in a fundamental sense, explicitly linking election administration to specific branches of government that have the responsibility to *"strengthen the security and resilience of its own critical infrastructure, for the continuity of national essential functions,*[9] *and to organize itself to partner effectively with and add value to the security and resilience efforts of critical infrastructure owners and operators."*[10]

This responsibility was a major part of the rationale for the recent designation of elections as a new subsector of CI. As Jeh Johnson, the former Secretary of Homeland Security who designated EI as *CI*, wrote: "*given the vital role elections play in this country, it is clear*

---

7 "What Is Critical Infrastructure?" *Department of Homeland Security*, July 12, 2017, www.dhs.gov/what-critical-infrastructure.

8 "Presidential Decision Directive 63," *Clinton Digital Library*, May 20, 1998, clinton.presidentiallibraries.us/items/show/12762.

9 National Continuity Policy Implementation Plan Homeland Security Council, August, 2007, http://bit.ly/FEMncpip. On May 4, 2007, President George W. Bush issued "the National Continuity Policy, an updated, integrated approach to maintaining a comprehensive and effective continuity capability to ensure the preservation of our constitutional form of government and the continuing performance of National Essential Functions [NEFs] under all conditions." NEFs include "the eight functions the President and national leadership will focus on to lead and sustain the Nation during a catastrophic emergency."

10 Barack Obama, "Presidential Policy Directive — Critical Infrastructure Security and Resilience," *The White House President Barack Obama*, February 12, 2013, obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

that certain systems and assets of election infrastructure meet the definition of critical infrastructure, in fact and in law."[11]

Regardless of the official designation, there can be no doubt that election operation is an essential national function. Elections are a foundational exercise of our very sovereignty as a nation through our ability to express self-determination. Attacks against them are nothing less than an affront to America's sovereignty and as such an issue of national security. It would be a mistake to view any CI designation as merely a bureaucratic shift for DHS that makes available more funding for EI. EI is CI in a broader sense; it is composed of national security systems.

Before describing the current state of and challenges to our democracy infrastructure, we first describe its scope and extent, starting with some important definitions.

1.3 Scope: Critical Infrastructure, Election Infrastructure, and Critical Democracy Infrastructure

Since the first national Critical Infrastructure Plan established in 1998,[12] CI has expanded to cover 16 sectors: 1) Chemical, 2) Commercial Facilities, 3) Communications, 4) Critical Manufacturing, 5) Dams, 6) Defense Industrial Base, 7) Emergency Services, 8) Energy, 9) Financial Services, 10) Food and Agriculture, 11) Government Facilities, 12) Healthcare and Public Health, 13) Information Technology, 14) Nuclear Reactors, Materials, and Waste, 15) Transportation Systems and 16) Water and Wastewater Systems.[13]

Within any sector, a "*CI operator*" is the organization that operates critical assets that if compromised, whether by physical method or by "*cyber*" means (*i.e., via computers, networks, and other information technology*) could result in significant national impact. That impact is significant regardless of whether the harm is accidental or intentional.[14]

---

11 "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," *Department of Homeland Security*, January 6, 2017, www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

12 "Presidential Decision Directive 63." *Clinton Digital Library*, May 20, 1998, clinton.presidentiallibraries.us/items/show/12762.

13 "Presidential Policy Directive—Critical Infrastructure Security and Resilience (Presidential Policy Directive/PPD-21)," February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

14 Throughout this Briefing, nuanced distinctions like this are called out because of an overarching requirement to support "*uplift*" of CI. By "uplift," we mean more than concrete demonstrative actions. Uplift also includes the incorporation of personnel attitude, mindset, and "*modus operandi*." In this case for example, the intent, whether nonfeasance or malfeasance, should not alter the approach, protocols, processes, or (*best*) practices in assessing, responding, and handling any incident impacting a CI asset. In other words, an accident that harms a CI asset should be treated no differently than a willful malicious attack on that asset. Indeed, this will be new thinking to election administrators now tasked as "CI operators" (*in addition to their duties in managing an election*.) The notion of "*not taking it seriously, it's simply one of those things*" is no longer an acceptable attitude. Uniform application of practices becomes a CI operator's mindset, and even removes potential partisanship concerns by treating everything uniformly.

CI operators include public corporations, private corporations, public utilities, and government organizations ranging from federal (*e.g., air traffic control*) to locally operated utilities. In addition, several kinds of government organizations are designated as first responders in some cases of CI incidents or outages.

CI operators are responsible for operation of a *critical asset*. Assets can be critical for several reasons. One familiar reason is *continuity*: we expect the power grid and the global financial transaction processing systems to be "*always on*" and resilient to significant disruptions. Other assets may not always be on, but are safety critical; serious harm could result from malfunctioning of control systems at hazardous materials factories or water treatment facilities. Other assets, such as dams and bridges, constitute direct threats to public harm if targeted by adversaries.

EI consists of all the assets necessary to successfully administer and operate an election. Disruption of EI can lead to a failed election—one that lacks conceding losers, consensus winners, and legitimacy for the transfer of power—which alone could be a failure of a "*national essential function*," ("NEF") but also could have consequent effects on national security and public safety.

EI shares a characteristic with another important CI sector: finance. In both sectors, a critical part of the mission is maintaining *public confidence* in the correct operation of the assets. If there is significant loss of public confidence—regardless of actual malfunction or the degree to which malfunction affects outcomes—the mission of U.S. elections may be in danger. For both kinds of "*transactions*"—election votes and financial payments—the underlying CI must be able to sustain public confidence that the transactions are performed legitimately and accurately. Unlike power utilities distribution or air traffic safety, adequate transaction fraud prevention and detection are key parts of the mission; even further, these protections must be *demonstrably* adequate. The public requires a basis for the belief that the protections for elections are performed diligently, not the mere assertion by responsible parties that protection is in place.

1.3.1 EI: Core Assets and More

Core assets of EI are those involved in managing the critical physical items and data items that are central to the outcome of an election. These are:

1. Voter records ("VRs"), including voter registration records, voter data in databases, VRs exported for pollbook or electronic pollbook ("e-pollbook" or "EPB") preparation, and the IT systems that handle voter data in these and other forms and formats;
2. Voting system components involved in casting and counting ballots into tallies, aggregating tallies and producing vote totals; and
3. Back-office systems, including, but not limited to, Election Management Systems ("EMS"), which election officials ("EOs") use to prepare for an election, and create data for and otherwise prepare the devices that cast and count ballots.

Beyond these core assets, there is a broader definition of assets, corresponding to a broader definition of the mission of EI, which is much more than simply counting ballots.

EI includes corresponding physical and cyber-assets like paper ballots, removable memory devices that contain votes, personal computers ("PCs") running the back-office software for managing voting systems, PCs and tablets that act as pollbooks, and the whole panoply of "big IT" for managing VRs: databases, servers, data center physical infrastructure, data continuity systems, operational continuity systems, and more.

But EI also includes the infrastructure for protecting and operating these assets. For example, the physical chain of custody of ballots and ballot boxes is important not merely as a process that must be performed, but a process that must be *documented* as having been performed correctly. In cases of dispute over election results or election operations, records of proper physical access control and custody are essential. Similar or analogous types of controls are relevant for all physical assets, such as transportation and storage of voting machines, as well as for digital controls like proper use of digital access controls, authentication, proper use of encryption for data authenticity, and proper encryption key management.

1.3.2 From EI to Critical Democracy Infrastructure

To encompass a broad scope beyond core EI assets and related CI assets, the term *critical democracy infrastructure* ("CDI") may be used to encompass not only the EI that meets the traditional CI definition of physical and cyber-assets, but also the broader set of practices and procedures, the documentation of how they are to be performed, and the records of them having been performed properly.

With CDI, there is a useful distinction of the "5 P's" of the elections ecosystem—the people that are critical to election operations; the processes that they perform to conduct elections that meet their objectives; the platform for doing so (*physical and cyber-assets of EI as CI*); the policies that govern the responsibilities of the people, the requirements for the processes, and the required characteristics of the elements of the platform. Finally, the 5th P, politics, dictates the design and development of governing legislation and rulemaking that direct, guide, and impact the entire ecosystem.

A complete understanding of CDI includes both breadth and transparency. The broad understanding of CDI includes people, processes, and platform, as well as an understanding of how these are shaped by policies, and politics. In each, some degree of transparency is essential for public confidence in election results. By contrast, opaque election administration processes breed distrust of fair access to the ballot, opaque election technology leads to a lack of trust in accurate vote counting, and opaque rulemaking breeds distrust that policies are equitably defined.

1.3.3 Beyond CDI: the Democracy Infrastructure Ecosystem

Core EI assets and CDI more broadly are operated by EOs—either state election officials ("SEOs") or local election officials ("LEOs"), or by the contractors and service providers that support them—a broad range of goods and services that includes IT service providers and the physical storage and transportation services required to transport voting machines from storage to testing facilities, to polling places, to canvass facilities, and more.

However, beyond elections offices and the CDI that they operate, there are other organizations and assets that have significant roles in the democratic process, and which may be targets for adversaries attempting to disrupt the election process or influence outcomes rather than subvert outcomes. These include:

- Political party IT systems both internal and public facing, where internal information leakage or public defacement can be considered tampering with the campaign process.
- Candidate and cause campaigns, PACs, and similar institutions' IT systems—logical next targets after the recent attacks on party systems.
- Third-party voter registration organizations' IT systems that supplement the services of SEO's and LEOs' voter registration functions.
- Mainstream media and new media news outlets IT systems, especially for coverage of election operations on Election Day, and results reporting on Election Night.
- EOs' online and other publishing methods for unofficial results—like media outlets, in no way connected to real EI assets, but easily mistaken for them.

As we consider CI status for EI, we must recognize the extension of "infrastructure" viewed through the "5 Ps" and into a penumbra of non-government and/or non-EI assets and organizations. While these may not be EI in the sense described above, these non-government organizations, and their IT assets, have been shown to be targets for adversaries attempting to disrupt elections. Just as homeland and national security policy must address protection of government operated critical assets, there is also the issue of the broader ecosystem of our democracy's privately operated infrastructure, and how to mitigate threats to election integrity that arise from attacks on organizations and assets as part of the broader democracy infrastructure ecosystem. Fair and deserving consideration of this aspect of protecting the broader ecosystem as part of preserving our nation's sovereignty is beyond the scope of this Briefing and the domain expertise of the OSET Institute.

1.4 Central Questions

However, even basic consideration of strengthening EI's security and resilience raises several questions central to the considerations of CI. For instance:

1. What are the basic components of EI; that is, those assets referred to in the policy definition?
2. Which of those components are *core* technology for national security?
3. Of those core components, who is responsible for ensuring and delivering their fault tolerance in design and performance?
4. Who are the CI owners and operators, and what are their responsibilities?
5. How does the CI operator role fit within the role of elections organizations of many kinds?

6. How must DHS partner with election CI operators—as the agency has effectively partnered with CI operators in other sectors—to adapt to election administration, without running afoul of the reserved powers clause of the Constitution's Tenth Amendment that delegates the responsibility of administering federal, as well as state and local, elections to the states?
7. How is election administration and the election process itself affected by a CI designation, and in particular, what might be the costs, benefits, and trade-offs?
8. How can election administration be improved regardless of a CI designation? What might be those costs, benefits, and trade-offs?

1.5 Briefing Outline

The balance of this Briefing, then, covers the following:

- Section 2 provides background in several areas: the current state of EI operations; their risks and compensating factors; a brief overview of the electoral process; and the challenges of ensuring the integrity of that process.
- Section 3 describes the issues of administrative designation of EI as CI, and the impact that designation has had on other sectors that might be appropriate for election administration.
- Section 4 provides organizational recommendations for CI-based activities in election administration, and the related costs and benefits.
- Section 5 provides our findings and summarizes recommendations into four areas: 1) CI sector operations; 2) short-term technical risk remediation; 3) redesign of core EI technology; and 4) supply chain integrity. Recommendations are guided by four principles: organizing, mitigating, redesigning, and securing.

© 2017 OSET Institute, Inc. All Rights Reserved

2. The Scope & State of Critical Democracy Infrastructure

2.1 Overview of the U.S. Electoral Process

With the scope of this document and some definitions laid out in Section 1, the next step is laying out a more detailed account of EI's assets, their operation, and the current state of risks and threats to them. Discussion of these assets requires some familiarity with the process of elections. For those with less familiarity, this Section offers an overview.

2.1.1 Roles and Responsibilities

American election administration is collectively performed by an elections organization for each state and territory—often part of the office of its secretary of state—in conjunction with 6,467 local elections organizations,[15] each a part of a county or township government. The Tenth Amendment of the U.S. Constitution implicitly delegates elections as a matter for states to conduct, with considerable latitude for state decisions about how to do so. Among each state's individual policies for elections are policies for how election operation and administration are delegated to local governments.

The most significant change to the minimal structure for elections was the Seventeenth Amendment to the Constitution, which removed the states' right to define their own method for electing U.S. senators (*often as an election within the state legislature*), and created a national mandate for senators to be popularly elected in every state.

The most recent significant structural change in federal election operations occurred in 2002, when Congress passed the Help America Vote Act ("HAVA"). Among other things, Congress mandated that each state implement, manage and administer a "*uniform, official, centralized, interactive, computerized statewide voter registration list.*"[16] Previously, each state could make its own policy ranging from state level administration of voter registration, to purely local administration with no consolidated statewide voter list at all—and several points in between.

Other aspects of federal-state interplay on elections have stemmed from the Voter Rights Act of 1964 and subsequent related legislation and jurisprudence. In these matters, the federal government asserted the right to constrain or oversee election administration within a state (*often with respect to voter list management, ballot composition, and access to the voting process including early voting*). However, such oversight did not

---

15 "U.S. Election Commission Administration, The Election Administration and Voting Survey 2016 Comprehensive Report," https://www.eac.gov/assets/1/6/2016_EAVS_Comprehensive_Report.pdf. For sake of accuracy, given there are a couple of different ways in which this is calculated, we opt for the EAC definition. In fact, the number ranges from 6,400 to 10,000 depending on how certain outlying jurisdictions are considered.

16 Help America Vote Act of 2002, 42 U.S.C. §§101-906, §303(a)(1)(A) (2002). https://www.eac.gov/assets/1/6/HAVA41.PDF

mandate any diminution in state and local level operational responsibilities for election administration.

Likewise, other federal involvement in elections has been regulatory—as with the Federal Election Commission ("FEC")—or advisory, as with the Election Assistance Commission ("EAC"), and more recently some states' voluntary acceptance of cybersecurity support from DHS. The FEC's campaign finance mandate has been a major focus of regulation and legislation, but again, these matters have had little or no effect on how states choose to divide elections operations responsibilities between the state and its localities.

2.1.2 Activities and Operations

In terms of elections operations—that is, operating the process of casting and counting ballots, as opposed to a variety of pre- and post-election administrative functions—localities have operations responsibility in every state. The degree to which each state offers funding or operations resources and support to its localities' election offices varies.

More broadly, the majority of election administration is composed of these parts, each with the participation of local election offices (LEOs) or state election offices (SEOs).

- Registration. Voter registration, where a SEO has responsibility for the overall system, but LEOs provide the critical function of reviewing voter registration requests (and related requests), to approve or deny them. Varying by state, LEOs and/or SEOs perform other critical functions such as voter list maintenance, which includes removing ineligible voters.
- Candidate Management. Candidate management is the process of qualifying candidates for a specific contest, and overseeing the compliance process that is largely focused on campaign finance disclosures. SEOs perform this function for state and federal contests, while LEOs do this for local contests. There is also an analogous process for ballot questions, including, but not limited to, referenda.
- Voter Rolls. LEOs prepare and print paper pollbooks, and configure EPBs, using voter list data extracted from the voter registration system.
- Election Definition. Election definition is the process of compiling the final list of all contests, candidates, and questions for a specific election in a specific jurisdiction. SEOs provide to LEOs the master ballot specification for state and federal contests and questions. LEOs, working in parallel with SEOs, conduct their own processes, and fold in the information from the state, to create the master ballot specification for the local jurisdiction.
- Ballot Preparation. LEO election management processes include election definition, the creation of ballot specifications for each individual ballot, layout and printing of paper ballots, layout of screen ballots, and preparation of election-specific configurations for each component of a voting system, such as a direct-record election device ("DRE"), ballot marking device ("BMD"), or an optical scanner.
- Logistics Planning. LEOs perform a considerable amount of logistics to convey voting equipment from a storage facility to a testing facility (*often the LEO headquarters*),

configure the equipment with data from an EMS, perform logic and accuracy testing, and other testing, prepare them for use (*including tamper detection sealing*), and convey them to polling locations. Closely related, LEOs prepare and distribute a variety of materials to be used in polling places, including paper and EPBs.

- Poll Worker Training. LEOs train poll workers, arrange for the use of polling places, and provide support for the operation of polling places.
- Absentee Balloting. In some states, LEOs conduct the vote-by-mail process.
- Tabulation. LEOs perform the tabulation process of counting the ballots, creating a data set of tallies that are then combined and tabulated to create vote totals for the local jurisdictions.
- Canvassing. Canvassing is the process that begins on Election Night and ends with certification of the election after the polls close. LEOs canvass their local contests and questions for which the vote totals comprise an election result. LEOs submit vote totals for state and federal elections to SEOs, who are responsible for combining vote totals and certifying the election results.

These activities and operations are the major parts of the election operations process. Development of a more complete lifecycle is an ongoing part of the process of National Institute of Standards and Technology's ("NIST") election data standardization, which includes work in progress on creating a complete business process model for election operations. Even NIST's work product will be mainly a common denominator that omits many localities' or states' specific election activities. Nevertheless, the above overview provides enough background on the use of EI assets for an assessment of the current state of EI activities and operations in practice.

2.2 The Current State of EI Assets and Operation

With EI considered as CI, there are thousands of organizations that can now be recognized as potential "CI operators"—that is, every local public elections organization in the 6,467 localities that collectively operate all of the states' election processes, together with the SEOs that support them and also provide critical state-level operations such as voter records management ("VRM"). Before addressing risks, we describe the current state of EI and its operation, broken down into distinct types of EI assets.

2.2.1 State-Managed EI: Voter Records

There has been long-standing and well understood recognition of the importance of the accuracy of voter records ("VRs"), and the propriety of operations including voter registration and list management in voter registration databases ("VRDBs"). This recognition attests to a clear understanding of each of the following assets related to VRs:

- VRs as critical data stored in VRDBs.
- VRDBs as infrastructure for storing VRs and making them accessible to other infrastructure.

- Voter registration systems that EOs use to process voter registration requests and make updates to VR databases.
- VRM systems that EOs use to manage VRs via support of list management processes, for example, identifying those records that match records of people who have died, who have been released from prison as felons, or who can claim a right to vote outside the U.S.—all reasons for offloading VRs from VRDBs.
- Voter lists created from VRDBs for any of a variety of purposes, including records requests, support for periodic reporting such as Election Administration and Voting Survey ("EAVS"),[17] and most notably the preparation of pollbooks for an election.
- Systems that use voter lists to create paper pollbooks or to prepare election specific data for EPBs.
- Systems that acquire pollbook records for voter checking (*including data entry or data capture from paper pollbooks, and data offloading from EPBs*).
- Systems that combine acquired pollbook records with VR data to record checked-in voters and aid in the process of absentee and provisional ballot processing, to ensure that each voter has no more than one ballot counted.

All of these forms of data and systems that manage that data are critical (*cyber*) assets; these and the people and processes of VRM comprise CDI that has a central role in public trust in elections: the assurance that ballots are cast only by authorized voters, that only legitimate ballots are counted, and that the voter lists that help provide that assurance are based on accurate data that is managed in accordance with relevant state election law, regulations, and processes.

With increased public awareness that nation-state adversaries target VRs in cyber operations, there is (*or should be*) a clearly higher standard of care in operating the systems that manage VR data. Recently, some states have begun to fortify their VR systems' professional IT operations, with voluntary acceptance of cybersecurity and critical infrastructure operational assistance offered by DHS.

With these recent developments, it is already becoming apparent how state-managed VRs are affected by the CI designation, at least with reference to one of two critical aspects of VRM: the typical closed IT system operation of a VR database, the software for managing it, and the systems that provide both SEO and LEOs with controlled access to VRs. These are typical IT operations, where practices from other CI sectors can be relevant, and federal assistance can take the form of similar assistance to other sectors.

---

[17] 2016 "Election Administration & Voting Survey," *Election Assistance Committee*, accessed August 2017, www.eac.gov/research-and-data/election-administration-voting-survey/. The Election Administration and Voting Survey is a biennial survey administered by the EAC that collects election administration data from states.

© 2017 OSET Institute, Inc. All Rights Reserved

2.2.2 State-Managed EI: Online Voter Registration

The second of two critical aspects of VRM is the more recent addition in several states of an Internet-facing interface for public access to *online voter registration* ("OVR"). OVR is a bit of a misnomer, however: properly described, OVR is a method for digital submission of the same voter registration request that voters can submit by paper. Digital submission has many advantages, but does not change the basic voter registration process: citizens submit requests, and LEOs review these requests together with other records, to accept or reject each request – regardless of whether the request arrived digitally, or arrived on paper.

There are two challenges to VR integrity and security that result from OVR, one specific and one general. The more general challenge of OVR is simply that of all Internet-connected systems, are vulnerable to cyber attack from the global communities of cyber-criminals and nation-state adversaries. Conventional cybersecurity operations must be applied to cyber-defense and recovery from successful attacks that in today's threat environment cannot be categorically prevented. However, public confidence in these public systems is crucial, cybersecurity operations, at a very high level of capability, are warranted, which is probably not typical in today's first generation OVR systems. Originally envisioned as a "Web form" analogous to a paper voter registration form, these systems were not developed with consideration for CI.

The specific challenge is *separation*; that is, the operation of a new (*Web-based*) OVR system for *submitting* requests, as separate from the legacy (*back-office*) system for *reviewing* requests and *managing* the actual VRs. The former, by definition, is an Internet-connected system, while the latter must continue to be a closed, tightly controlled system without general access from the Internet. Typical IT security technology and operations methods must be carefully used to control the back-office system so that threats to the OVR system are not threats to the actual VRs. Fortunately, this form of separation is not unusual in cyber-CI, and existing methods can be applied to meet this challenge.

As with VRM discussed above, practices from other CI sectors can be relevant, and federal assistance can take the form of similar assistance in other CI sectors.

2.2.3 Locally Managed EI: Organizations and Assets

By contrast to state operations, the majority of local election operations are small organizations without a dedicated data center, professional IT organization, or dedicated funding for technical security or security operations management. Large or small, these town or township, municipal, or county elections organizations manage a variety of technical EI, and a corresponding variety of people, roles, and processes for managing each kind of asset.

For a single LEO, the technical EI and related physical EI often consists of a variety of assets, including, but not limited to, the notable assets common to many election operations:

- PC workstations and/or servers running voting system application software, EMS, for functions including: election definition, ballot layout, voting device preparation, tabulation management, and reporting.
- PC workstations and/or servers running non-voting system application software for functions such as candidate filing and campaign finance compliance, physical asset inventory management, and personnel management including election-time temporary workers and volunteers.
- Voting system components that includes high-capacity scanners with software for central count optical scanning (CCOS) of paper ballots.
- Similar lower-capacity components for precinct count optical scanners (PCOS).
- Voting system components, such as BMDs, that serve voters who have enhanced access needs or preferences.
- Paper ballots.
- Physical infrastructure for absentee/mail ballot mail-out, and for receipt and access control after receipt.
- DREs including those to provide voters with enhanced access.
- Paper record accessories for DREs that create a voter-verified paper audit trail (VVPAT).
- Removable digital storage media that contain vote tally data from PCOS and DREs.
- PCs or tablets running software for an EPB, sometimes with separate peripherals for signature capture.
- Paper pollbooks and the IT systems that produce them from data from a VRM system, and that capture information recorded in pollbooks.
- Tamper-evident, physical integrity seals applied to voting system components before use.
- Tamper-evident, physical integrity seals applied to equipment, ballot boxes, and other election evidence containers, after polls close.
- Poll worker work sheets for logging setup and teardown activity, recording the ballot reconciliation process, tamper-evident seal checks and application events, and other required logging or tracking activities as required by state election law, regulations, and local election practices.
- Physical chain of custody records.
- Local VRM systems used, among other purposes, for adjudicating absentee ballots and provisional ballots.

© 2017 OSET Institute, Inc. All Rights Reserved

Each LEO operates a substantial but locally varying subset of the above and related EI assets. The level of complexity of the assets and the asset management processes is evident from the above "highlights" list.

These assets and processes play a role in elections at every level of government: federal, statewide, state-level (e.g., counties, townships, municipalities), and a host of local special districts, and must be protected. Protection functions are applied to uphold the integrity of the process as a whole, but election operations are fundamentally a local matter, ordinarily conceived of as a county or township government function—*not as a national security matter that is delegated locally*. The resources and expertise applied to LEOs' operations are those generally conceived of as appropriate to local government operation, albeit an important and visible one.

And in the majority of locales, LEO services are a periodic, part-time function of an office that also provides local-level services such as deed recording and business licensing.

2.2.4 Locally Managed EI: Critical Democracy Infrastructure

In the current threat environment, it may be evident in hindsight that the above assets, and the people and process for managing them, are CDI that if successfully attacked—or even successfully discredited regardless of actual attack—can have national consequences.

However, as U.S. LEO organizations have evolved since the 1998-issued PDD-63 (*when the national CI planning began, and then became subsumed by DHS post-9/11*), CI was not a common organizing principle. A LEO today, considering herself a CI operator, may well be taken aback, much as some other local-level CI operators were 15 or so years ago, upon learning that they operated CI such as local utilities, transportation authorities, and first-responder facilities.

In addition, the full scope of CDI includes elements that are often outsourced in a way that has a potential for loss of control by CI operators that would not be typical in other CI sectors. For example, EI physical assets, such as voting machines, require storage and transportation that is typically outsourced.

Especially for small LEOs, a portion of election management itself is outsourced to a voting system vendor or a third-party service provider. For example, an LEO might specify the contents of an election's ballots, but provide those to a service provider that creates the election-specific datasets that must be configured into each type of voting machine.

Furthermore, LEOs as CI operators may have a somewhat larger role than CI operators in other sectors, taking into account a) the full scope of CDI, not just the primary assets but also the people and processes for managing them, and b) the election-specific requirements for CDI that include record-keeping for evidence that demonstrates compliance with laws, regulations, processes, and procedures—and sufficient to enable adversarial situations such as recount and litigation.

© 2017 OSET Institute, Inc. All Rights Reserved

2.3 The Current State of Risk to EI and CDI

With scope, definitions, election process overview, and an account of EI assets and their use, the next step of situation assessment is to focus on the risks to core EI assets and CDI more broadly.

Core EI technical assets are many years behind current technology, and were not developed with protections against the current threat environment. All are subject to tampering and other threats based on physical access, theft, or abuse of insider privilege. There is ample evidence of vulnerability of voting machines,[18] EMS, EPBs, and VR systems. This Section describes the scope of risk, avenues of attack, possible outcomes, and the sources of technical risk.

While the basis of physical and social attack vectors may be evident to those familiar with election processes, there are several aspects of the current technology platform that require a more detailed explanation for two reasons: an understanding of deficiencies of the current technology platform and recommended requirements for the next generation of election technology. The current deficiencies include problems with verifiability, validation, immutability, assurance, and other desirable properties of trustworthy voting systems that were not specifically required by HAVA (*or other post-HAVA laws*), and hence, are not part of current voting systems.

2.3.1 Scope of Risk: Cyber-Physical and Cyber-Social

Avenues of attack on election integrity go beyond direct attacks on election technology to subtly change the result of a specific contest in an election. They can be sophisticated attacks on assets that use local networking and/or connection to the public network, including:

- OVR systems, EPBs and the back-office systems that manage them;
- Statewide real-time voter check-in systems, eMail ballot return systems, Web-upload ballot return systems, digital blank ballot distribution systems; and
- Voting system components with features for digital communication of unofficial Election Night vote tallies.

Regardless of the avenues of attack, the range of threats can be broken down into three (3) kinds of outcomes that adversaries might seek to create:

1. Subversion - manipulation of cyber-assets to undetectably change an election result
2. Defamation - disinformation attacks with supporting cyber operations, that dramatically impact public confidence in the legitimacy of election results
3. Disruption - cyber-availability attacks and disinformation attacks that impeded voters' ability to vote

---

[18] Robert Schlesinger, "Hack the Vote: a reminder of how insecure our ballots can be," *U.S. News & World Report*, July 31, 2017, www.usnews.com/opinion/thomas-jefferson-street/articles/2017-07-31/hackers-demonstrate-how-vulnerable-voting-machines-are. Individuals and organizations have repeatedly demonstrated, on request, the vulnerability of voting machines to manipulation by compromising the machines themselves.

Subversion is the most commonly discussed form of election attack, but by no means should it be the only one protected against; any of these three methods can compromise an election. For subversion to work effectively an election must already be close, but it is worth noting that a targeted attack on specific precincts in battleground swing-states could alter the result of an election with surprisingly few votes being changed.[19]

Defamation offers an easier, and perhaps even more powerful route for America's adversaries. In most cases other nation-states may not have a strong preference for which presidential candidate wins the election, but sowing political chaos across the country serves the interests of any American (democracy) adversary. For example, if a large, and perhaps poorly executed attack on an American election were discovered, it would cause questions and doubts about whether other attacks evaded detection. A foreign country could then use disinformation campaigns to tarnish the legitimacy of the election results, leading to political chaos on a national scale.

Adversaries can use disruption to achieve results similar to subversion or defamation. By manipulating VRDBs, either locally or remotely, a malicious actor could alter a voter's address, party affiliation, or other information to prevent them from voting in the upcoming election. This could take the form of an absentee ballot never arriving or even an inability to vote at the polls. While these issues might eventually be remedied, they can result in voters becoming frustrated with the government and either changing the way they vote or not voting at all. As prospective voters are denied from voting at poll booths and struggle to determine the reasons for denial, the waiting time at the polls will increase, leading others who were not directly targeted to not vote. Such disruption, if targeted correctly, could change the result of an election the same way a subversion attack would, or, especially if amplified by a disinformation campaign, could create the perception that a specific demographic was being disenfranchised, leading to the same result as a defamation attack.

Subversion attacks have higher costs and risks, and lower payoff than defamation or disruption attacks, which have a different goal: destabilizing the election process and reducing the public credibility of the process and its results—in other words, a direct attack on the basic objective of an election: yielding consensus results and an orderly transfer of power.

2.3.2 Sources of Technical Risks: Hardware

One fundamental source of technical risk to core EI cyber-assets is at the hardware level, via threats from untrustworthy hardware components sourced from an open supply chain with no controls or provenance on acquired components.

---

[19] Tim Meko, Denise Lu, Lazaro Gamio. "How Trump won the presidency with razor-thin margins in swing states," *The Washington Post*, November 11, 2016. www.washingtonpost.com/graphics/politics/2016-election/swing-state-margins/. Due to the way the Electoral College works, margins of victory that appear large can result from only a small number of individual votes. A few thousand votes can carry with them a large amount of electoral votes and thus, an entire election.

This risk is particularly notable for voting system components, certainly during the manufacturing process, but more notably for EO operator maintenance in the use of replacement parts over the system components' extended life cycle. This practice has increased over time, due to the effect of market forces on the vendors, and to the effect of EO's reduced capacity for capital expenditures.

Since the passage of HAVA, the number of voting system vendors in the U.S. has shrunk from six to three vendors who together serve nearly all (approximately 85%) of the U.S. market, including two vendors who support the products of other now dissolved vendors. At the same time, the ability of U.S. election jurisdictions to pay for voting system products has shrunk as well, with HAVA funds exhausted and many state legislatures unable (*or unwilling*) to appropriate funds for localities to replace ageing-out voting system components.

One result of this ossified market is that the maintenance of existing voting system devices depends on obtaining replacement hardware components from the global market in which components are sourced from supply chains dominated by vendors in nations that in other contexts are considered threats to national security.

As a result, U.S. voting system products have a *supply chain risk*, defined by 48 CFR 239.7301 (2) of Title 48 of the Code of Federal Regulations:

> "*Supply chain risk means the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a national security system (as that term is defined at 44 U.S.C. 3542(b)) so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system*."

Although some may deem the likelihood of attack via supply chain to be low, the vulnerabilities in voting systems are pervasive, broad, and deep. Fortunately, experience in military supply chain risk reduction can be applied quite feasibly to voting systems. For critical military and/or classified information processing systems, concerted efforts have yielded, for some critical national security systems, a significant reduction in supply chain risk by the creation and maintenance of a closed supply chain limited to trustworthy component providers either U.S. based or based in definitively non-adversarial nations such as the I5 nations.

While this approach can be challenging for national security systems that have complex or domain-specific hardware requirements, the same is definitely *not* the case for the critical devices of voting systems. These devices' required functionality is quite simple compared to, say, a heterogeneous remote sensing array as part of a Command, Control, Communications, Computers, and Intelligence ("C4I") system. By contrast, critical voting system devices' functionality can be supported entirely by hardware composed of components that are completely common in ordinary PCs and scanners. As a result, a *trustworthy closed supply chain* may be more feasible to set up and maintain for future voting systems, compared to more complex national security systems requiring supply chain risk reduction.

2.3.3 Sources of Technical Risks: System and Software Modification

The current generation of U.S. voting system technology is massively mismatched for the current threat environment of cyber operations by state-sponsored adversaries with advanced capabilities. The mismatch arises from a core defect, where the post-HAVA voting system products were based on ordinary 1990's PC technology, where the entire software base is modifiable, and every system is capable of running any new software consistent with the hardware, whether the new software (*or modification of existing software*) is legitimate or malicious. This two-edged sword is typical for commercial computing in which flexibility is prized, and the consequently required defensive security arms race is an acceptable cost for the flexibility. However, flexibility is *antithetical* to voting systems.

The fundamental risk is not merely generally vulnerable legacy computing platforms as the basis of both ballot casting/counting devices, and back-office election administration software. With this underlying technology base, voting system components have a well-known range of vulnerabilities of legacy PC technology stemming from their design as general-purpose platforms.[20] As a result, these systems are not able to protect themselves in the current threat environment.

- Failure to Meet System Control Requirements

  Actually, the fundamental risk stems from the very basic flexibility of the underlying platform. Every voting system used by a locality's EOs must be certified by their state, and may not be modified. Prior to each use, every system must be revalidated to ensure that it remains in the certified configuration. The ability for a system to be arbitrarily modified, while useful for PCs, is completely *counter-productive* in voting systems.

  The risk is not limited to legacy systems. Even the most up-to-date general-purpose platforms are *fundamentally inappropriate* for ballot casting and counting devices and critical back-office components of voting systems. General purpose computing platforms have a fundamental requirement to be able to be patched, updated, have new applications added to them, have applications that update themselves, and so on. These are *malleable* systems by design, which accounts also for their vulnerability to run malicious software. By contrast, critical voting systems have a fundamental requirement to run exactly one set of software, to not be able to modify that software, and to not be able to run any other software. Voting system components' requirements are exactly the opposite of a general-purpose platform.

  Yet, with this antithetical technology foundation, current voting systems are just as vulnerable to attack as the ordinary PC technology they are based on. Years of experience in commercial computing have shown that the fundamental risk cannot be

[20] "Computer Security Resource Center National Vulnerability Database." *National Institute of Standards and Technology*, accessed August 22, 2017, http://bit.ly/NVDsearch. The same Windows operating systems used by American election systems have long lists of *common vulnerabilities and exposures* (CVEs) that have been documented over the years and are publicly accessible.

contained, only mitigated in an ongoing arms race between adversaries, and defensive technology creators and asset owners attempting to use the latest defensive technology.

The basic system control requirements come directly from the federal and state regulations on voting systems. A local election office cannot use a voting system unless the state has certified it as fit for use, often based on the federal process of voting system testing and certification. Certified voting systems must not be modified or extended; that would amount to the use of an uncertified system. Any needed changes must be made to the base hardware or software, and the resulting modified base must be recertified. Then existing fielded systems can have the older certified software replaced by the newer certified software—which again must not be changed in the field.

- No Support for Feasible Validation

Another closely related property of certified voting systems is validation: the ability for an EO to inspect each individual device and ensure that it consists of hardware and software in the certified configuration, with no modifications. Because voting machinery is based on general-purpose computing platforms, there is no basis for EOs to validate each device. Instead, they generally must take on faith that there have been no changes (*accidental or malicious*) since its last use, and conduct pre-election testing to ensure that each device behaves like a device in the certified configuration.

EOs do have methods to attempt to work around the fundamental malleability of systems. For example, they can use techniques for rule-based "check summing"[21] of a selected subset of a computer's file system. These approaches for system integrity self-checking have essential limitations, from the original "*tripwire*" technology[22] to all modern derivatives for file integrity monitoring and intrusion detection.

First, years of experience have shown that these techniques are only as useful as the accuracy of the inputs.[23] Such inputs are complex and system-specific rules, file system subset definitions and checksum baselines. Any error or omission in these inputs can produce false negatives (*failure to detect an attack*) or false positives; the latter can be specifically harmful for public trust in election outcomes.

Secondly, these techniques also have the basic limitation of any software self-check technique: an adversary who has gained the ability to tamper with a target system can also tamper with the self-checking software to prevent detection of the primary tampering. As these techniques have been applied to current malleable voting system components, the effectiveness is limited to accidental modification, which can cause a certified voting system to operate form an uncertified software base—an important

---

21 See: https://en.wikipedia.org/wiki/Checksum

22 See: https://en.wikipedia.org/wiki/Open_Source_Tripwire

23 Gene H. Kim, Eugene H. Spafford, "Experiences With Tripwire: Using Integrity Checkers for Intrusion Detection," Computer Science Technical Report, Department of Computer Science, Purdue University, 1994 http://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=2114&context=cstech

situation to detect. However, these techniques are powerless against malicious modification by advanced adversaries, who can modify the system's self-checking code to provide inaccurate reports.

As a result, today's limited approaches to meeting validation requirements are approaches that are also unsuited to the current environment. These systems were simply *not* designed for validation in a hostile threat environment.

- Redesign not Remediation

The resulting vulnerabilities can be remediated to an extent with compensating personnel, procedural, and physical controls. To various degrees, and with varying success in compliance, U.S. EOs do use compensating measures. However, the root cause can *only* be addressed with fundamental changes to the underlying system design, including avoiding the use of general-purpose platforms.

Current voting systems were based on general purpose computing platforms as a matter of expediency for time to market in the early 2000s when HAVA made available billions in federal funding to replace older election technology suffering from defects such as hanging chads, and lack of accessibility support for disabled voters. There is no technology currently in use in voting systems to support the requirement for fielded voting system components that can be validated and immutable.

However, there are ample examples of available technologies in use outside of elections, for systems that do meet similar requirements. Generations of aerospace, communications, and defense systems have been built with an expanding toolkit of technologies for fixed-function embedded or dedicated systems designed to operate in hostile environments. The lack of application of these techniques to voting system component design is not an indicator of inapplicability, but rather of a lack of market impetus to redesign election technology in a major departure from the early 20th century approach that was driven in large part by time-to-market, cost-of-goods-sold, market pricing, return-on-investment, and market share preservation considerations.

2.3.4 Sources of Technical Risks: Data Integrity for Information Assurance

EOs' mission includes significant components of information assurance ("IA"). EOs manage a process that yields critical information: the winners of a set of contests and questions in an election, together with all the supporting details like voter check-in records, precinct level vote tallies, residual vote records, and more.

The IA mission is to provide assurance that this information is derived entirely and only from the legitimate voting of authorized voters. This IA mission depends on underlying data that is at risk both *as stored*, and *in transit*. Integrity and authenticity measures are essential to protect the underlying data so that as it is received and used, it can be validated as being from a legitimate source, and not tampered with since creation at that source

Both voting system ("VS") and EPB technologies have requirements for data protection. VS components generate vote tally data from ballot casting and counting operations. These must be securely stored with *proof of origin*, and protected with *tamper detection*.

The risks of modification of tally data clearly include the risk of a modification changing an election result. The same is true of the voter check-in records created by EPBs. Since this data is an important input to the absentee ballot process, tampering of EPB data could result in disenfranchisement or fraud. Disenfranchisement could result from rejecting a specific voter's legitimate absentee ballot based on a spurious voter check-in record for that voter. After a specific voter casts a ballot in-person, deletion of the EPB record could enable counting of an illegitimate absentee ballot.

Both VS and EPB systems have similar requirements for legitimacy of their input data. For a VS component, tampered or illegitimate ballot data could result in voters created invalid ballots. For an EPB, tampered or illegitimate voter list data could result in admission of illegitimate voters, or barring of legitimate voters. In addition to such election *subversion attacks*, both attack vectors serve equally well or better for *disruption attacks* and *defamation attacks*.

As a result of these IA requirements, VS and EPB systems have fundamental requirements for validation of integrity and provenance of input data, as well as creation of output data for which other systems can validate integrity and provenance. For these IA requirements, VS and EPB systems have data security functional requirements that include:

- Cryptographic key generation, distribution, and backup;
- Key ignition and key protection in fielded VS components;
- Use of keys for output data protection; and
- Use of keys for input data validation.

Current VS and EPB technologies are not capable of performing high assurance operation of these critical data protection measures. Current EPB products run on commodity PC or tablet platforms, with application software that was not subject to uniform security requirements, security review, or certification.[24] VS products, though certified, have also been demonstrated to lack effective data security measures. Every independent source code review or red team test has uncovered deficiency in data security implementations (*e.g., hardcoded or otherwise shared keys, rather than key distribution*).

Finally, these current products, being based on general-purpose system platforms, are unable to protect key data and cryptographic functions from the full array of malware threats that have been demonstrated for these platforms.

As a result, future VS and EPB technology must be designed and implemented specifically for high assurance operation to meet data security functional requirements, including those identified above.

[24] A notable exception is an effort in Indiana to develop certification methods for EPBs. The EPB software is fundamentally vulnerable to tampering that could result in compromise of cryptographic key data. No security review demonstrated effective measures to counter these data integrity threats, or even to validate that security functions are properly implemented.

© 2017 OSET Institute, Inc. All Rights Reserved

2.3.5 Sources of Technical Risks: Limited Support for Evidence-Based Election Results

Verifiability is a basic requirement for the election results produced by a voting system. A voting system must produce not only vote totals, but must also produce evidence that those vote totals comprise a valid election result. Risk-limiting ballot audits are current best practice for cross-checking the work of ballot counting technology by comparing machine counts of a subset of ballots with human counts of those same ballots.

For evidence-based verifiability of a voting system's results, the cornerstone is the basis in durable paper ballots of record that support two basic forms of election results: 1) rapidly produced machine counts by devices that support ballot audits; and 2) human conducted ballot audits. There is no single point of trust because there is no sole reliance on either a) humans to produce rapid, accurate, demonstrably impartial vote counts; or b) machines to function flawlessly in terms of accuracy or reliability. Machines can produce results impartially, rapidly, and usually accurately, while humans cross check the results to detect and correct inaccuracy.

For this cornerstone to be effective, a voting system must not only produce ballots, but also must support ballot audits with specific evidence-related functions. These include creation of *cast vote records* ("CVRs"), and the effective use of cryptography to demonstrate "*data provenance*" of these records. This specific evidence enables LEOs to effectively use ballot audit techniques that are much more feasible in terms of scope and cost than today's common and unnecessarily labor-intensive process of flat X% ballot audits, where "X" is specified by law or regulation (and *where audits are possible and funded*).

In order for audits to be demonstrably adequate to verify results, the scope of audits needs to be carefully chosen for a process that is both feasible and transparent. A voting system must retain a CVR for each ballot, to support the most effective and least effort ballot audit procedure: risk-limiting audits, based on sound statistical principles, using minimum size ballot batches randomly selected with constraints.

Current voting technology has limited support for verifiability. These limits include:

- Paperless DREs: Early attempts at accessibility in the polling place led to DREs, many still in use, that unnecessarily combine the functions of accessible ballot marking, and tabulation of voters' choices. This combination created several issues: no support for verifiability; risks to vote tally data stored only digitally; and unequal risks, because paper ballot voters' ballots are verifiable, while DRE users' votes are at greater risk. Although being phased out in many jurisdictions, paperless DREs are still used.
- Limited Tally Data: Many currently used voting systems that do support a voter verified paper ballot nevertheless lack support for risk-limiting audits, because of lack of single ballot CVRs or other requirements for such audits. As a result, audit batches are limited to machine counts batches (*such as an entire precinct*) and hence create a trade-off between significantly increased personnel and costs vs. less statistical confidence in election results. This seemingly technical defect also pits confidence against limited resources for the local election offices that conduct audits.

- Proprietary Data Formats: Even where CVRs are available, they are stored in proprietary data formats (rather than an open data standard format) that can impede public access to ballot audit records. Ultimately, a risk-limiting ballot audit process is only effective if independent watchdogs can view the evidence of an audit, and determine that it was performed adequately.
- Lack of Data Security: As described above, many current voting systems lack effective data security measures. As a result, CVRs (*if available*) and tally data *cannot* be demonstrated to be the legitimate, un-tampered basis for verification of machine tallies.

Progress on all the above issues will be required to create the conditions for truly verifiable evidence-based elections, including: phase-out of paperless DREs; adoption of BMDs; support for CVRs; and development of a national standard common data format for CVRs are positive developments.

Yet all of these factors still require high-assurance voting system technology that can both provide required data security measures, and provide system-level protections against subversion that can undermine data security measures. Further, the administration of voting systems, including cryptographic key management, must be feasible for ordinary EOs to perform.

2.3.6 Synergies of Technical Risks

Taken together, several of these sources of technical risk have a synergistic effect. The following list comprises the omissions or defects of current voting system and EPB technology that work together to create very significant technical risk:

1. Inability to categorically prevent unauthorized modification.
2. Not providing EOs with an ability to feasibly validate systems as not having been modified.
3. Inability to make appropriate use of cryptography for tamper detection of critical data.
4. Not providing EOs with an ability to feasibly perform required cryptographic key management and protection.
5. When modifications to software are required, reliance on patching (*modification-in-place*) to systems that might have been modified and are incompatible with patches; rather than relying on authenticated, controlled, wholesale replacement of the software base with a new instance that was tested in totality and certified.
6. Lack of full support for data retention that is required to support risk-limiting post-election ballot audits, the only process available to EOs to detect cases where erroneous system behavior (*regardless of origin*) has created vote tallies that are sufficiently at variance with human counts, to have changed an election result.
7. Lack of support for forensic IT audit to assess possible malfeasance.
8. Lack of any use of high-assurance system development or validation practices.

9. Lack of separation of a voting system into a trusted computing base ("TCB") distinct from untrusted functions, and separation of the TCB into distinct components amenable to feasibly addressing each of the above defects.

The length of this list, the synergy between these issues, and the resulting high risk in the current threat environment, all combine to create our finding that *remediation of existing technology is not feasible*, and that redesign and reimplementation is *required* for meaningful integrity of election results.

2.4 The Challenge of Protecting Election Infrastructure

In addition to the technical risks, there are several other challenges to EI protection, many of which have a common root cause: election operations in the U.S. have grown organically, locally, and (*until HAVA*) with largely state and local funding. Such funding was oriented toward operations rather than treating the technical infrastructure as critical infrastructure. With HAVA, the main goals for election technology reform were speed, ease, and confidence of vote counts; accessibility of voting technology; speed of voting technology refresh; and a new mandate for states to centralize voter registration operations.

For the most part, criticality, security, and integrity were not fundamental requirements, and were entirely subsidiary to the goal of quickly replacing punch card and lever type voting machines.

One notable exception was the mandate for central state VRDBs. This mandate essentially moved VRs processing technology into the state datacenter (*for states where that was not already the case*), with central control, and the opportunity (*though not requirement*) to uniformly apply large government IT best practices to the protection and control of VRs.

However, as the remainder of this Section explains, locally operated EI still faces many challenges.

2.4.1 Challenges for Cyber-Assets

Challenges to cyber-assets fall into two categories: 1) long-standing systemic challenges and 2) more recent challenges.

The long-standing challenges to voting systems stem from the sources of technical risks outlined above. The consequence is the necessity for LEOs to provide additional safeguards that compensate for the fundamental deficiencies of current voting technology. The net result is an increase in the complexity of physical and procedural security on the cyber-physical assets of voting systems components.

CI operators in other sectors have faced similar challenges in applying complex physical and procedural controls to compensate for weakness in critical systems, notably legacy industrial control systems and supervisory control and data acquisition ("SCADA") devices that were designed and deployed without any concern of an adversarial threat environment. With the formation of an election CI sector, and learning from other sectors, there is reason to expect these challenges to be met with a higher regard for criticality.

More recent challenges stem from recent changes in U.S. election practice and will require either or both increased cybersecurity efforts and procedural controls. In other words, the technical complexity of election technology continues to grow, even as the stakes for protection increase, while, hitherto, there has not been a corresponding increase in CI protection efforts.

A small selection of recent additions includes:

- Online voter registration (OVR) systems, which create new vectors of attack on VRs databases, if the Internet-connected OVR servers are improperly isolated from the database systems that manage the VRs. There are recently documented nation-state-actor cyber-operations targeted at OVR systems. As described above, there is significant scope for improvement via better use of typical government datacenter IT best practices. However, robust defense against nation-state actors may require use of cyber-defense skills that are not common in state IT organizations. Recent recognition of the criticality of these assets, and their vulnerability to nation-state adversaries, has resulted (*perhaps with some fortification from the formal CI designation*) in new efforts in cybersecurity, with some states voluntarily obtaining assistance from DHS.
- Internet-based ballot return, which exposes "digital ballots" to the full range of Internet-based security threats, and likewise the Internet-connected IT systems that facilitate digital ballot return. These practices create fundamental challenges, given the current inability to completely secure Internet-connected transaction processes systems of all kinds. Continuing policy discussions include a focus on in-theater military staff and the benefit to them of digital ballot return in situations where physical ballot return may not occur in a timely manner, even with the use of digital blank ballot delivery. With the possibility of nation-state actors, advanced cyber-defense expertise will be needed for a balanced analysis of costs, risks, and potential detriment and benefit of these digital ballots.
- Electronic Pollbooks (EPBs or e-pollbooks), which comprise another recent addition to election technology. EPBs manage critical election data: lists of authorized voters and records of which voters have already cast a ballot. Manipulation of this data can both affect voters' access to their ballot, as well as enable fraud via blocking counting of legitimate absentee ballots or enabling counting of illegitimate absentee ballots. Yet this data is not rigorously protected in current EPB systems, because EPB's face the same types of challenges as voting machine components that use commodity platforms and were not designed for the current threat environment.
- Internet-based voter check-in systems, such as that pioneered in Colorado, which use public networks to connect polling-place check-in terminals to a central voter check-in management system. The challenges are essentially the same as for any Internet-connected system, but the current bar of protection may be slightly higher, due to control of both endpoints. But again, with nation-state threats, advanced cyber-defenses may not be present in state-level IT organizations.

© 2017 OSET Institute, Inc. All Rights Reserved

2.4.2 Challenges with Physical Assets

Physical assets face many challenges, especially for EI assets managed by local elections organizations. In a nutshell, each local elections organization has quite a substantial logistics operation to move, test, manage, distribute, and protect a variety of physical assets, including, but not limited to, the many types of assets listed above in Section 2.2.3 as Locally Managed EI: Organizations and Assets, and involved in the local level activities and operations listed above.

These base logistical challenges are substantial not only in scope and extent, but also in the responsibility for clearly stated policies and procedures for physical security, and adequate training for all relevant staff, including contractors and volunteers. These base challenges are further magnified by the responsibility for meticulous records-keeping to demonstrate that the procedures were properly performed and evidence maintained.

In other words, not only do EOs have to properly *perform* a number of controls, but they also have to *prove* that they did so, with evidence that can withstand an adversarial challenge to the propriety of election operations or the legitimacy of election results.

Given the recent unfortunate change in American political discourse to include widespread concern over the possibility election "rigging," the importance of these challenges may in some cases be larger than the typical local election office's assumptions based on previous election cycles.

CI operators in other sectors have faced similar challenges in standing up rigorous and evident protection of physical assets. With the formation of an election CI sector, and learning from other sectors, there is reason to expect these challenges to be met with a higher regard for criticality.

EAC and DHS are working together on an essential response to the CI challenge of elections: formation of sector-specific organizations that are described in Section 3 and Section 4 below, and are the topic of one of our four major areas of findings and recommendations. One significant advantage that the elections sector has over some other sectors in the formational phase is that elections already have strong institutions for collaboration, including NASS, NASED, IAOGO, and several States' association of LEOs. As likely co-SSAs (co-*sector specific agencies*), EAC and DHS have convened organizational workshops with these stakeholder organizations, and leaders from representative state and local elections offices. The combination of existing sector institutions and an existing possible SSA organization, or organizations, with expertise in elections promises the sector formation activities might proceed in a timely manner.

2.4.3 Challenges for Personnel

As with any operation with physical controls, personnel security is a central pillar of protection. In the few large local election jurisdictions that comprise perhaps a quarter or more of the voting population, a local election office may have the ability to rely largely on employees. As a result, such organizations may be able to leverage a large local government's capacity for background checks, fine-grained employee-based physical

access controls (*e.g., badge-based controls*), and other bread-and-butter personnel security measures.

However, even a large elections organization still relies on service providers of physical services (*transportation, storage*) and personnel services (*temporary clerical workers for peak times*), as well as a large number of volunteer or slightly compensated poll-workers. Personnel security is essentially absent in these cases.

For the majority of the many small elections organizations in the 6,467 plus localities in the U.S., personnel security capability can be limited or entirely absent, while the organizations must depend more on outsourced IT service providers and services contracted to a voting system vendor. In very small locales, the choice of service providers may be limited. Elections organizations are then essentially dependent on the personnel security measures of their vendors and of their service providers.

2.4.4 Challenges from Regulatory and Market Factors

Mitigation of these risks is hindered by some overarching factors related to the voting system test and certification process.

- There is no explicit definition of a voting system, but the de facto definition is the entirety of a product sold by a vendor; this can include numerous components or feature sets that are not critical to the creation of a verifiable election result. As a result, the scope of the test and certification process can be unnecessarily broad.
- The process is oriented toward testing of an entire monolithic voting system product, consisting of several inter-related and interdependent components (*e.g., EMS, ballot casting and counting devices*). Recertification of an updated voting system product requires retesting and recertification of the entire product, even if the update affected only a small part of the product.

Because of these and related issues, the voting system recertification process is slow and expensive for vendors, creating unintended market disincentive to provide incremental releases to EOs based on their feedback and new requirements for security and other characteristics.

As a result, there are significant hurdles to innovation that could address the shortcomings described above. Vendors have little or no commercial incentive to innovate their products with respect to security and assurance issues that were described above, and which are not explicitly required by their customers. Other innovators may have an improved voting system component (*e.g., a ballot scanner with features to specifically support risk-limiting audits*) but that cannot be certified unless it is part of an entire voting system product.

Partly as a consequence of these market forces and regulatory constraints, the sources of technical risk have not been systematically addressed. When the HAVA was passed in 2002, policy makers were not focused on cyber threats to voting machines. Election system vendors did not enter the market as vendors of national security systems, and many, if not all, are not equipped to become such vendors. Even if vendors were equipped to sell the level of security appropriate for a proper election system, they lack the economic

motivation to do so. Most counties don't have the budgets for election systems to justify the innovation and costs associated with designing and selling a proper election system; short of another HAVA, which is highly unlikely in the current political climate, it is unlikely sufficient funds will ever appear.

Many jurisdictions across the nation must replace their aging-out voting systems soon. However, the current options presented to them all lack adequate improvements. While they will certainly make voting systems more reliable and marginally more secure, they do not solve the fundamental problems of a modifiable system. If counties choose to acquire these systems, due to lack of a better option, it will be years, perhaps even over a decade, before they can afford to buy a different system that is not fundamentally insecure.

2.5 Compensating Factors for Current Risks

The current status of election technology also includes activities that can enable the sources of technical risk to be much more readily addressed.

2.5.1 Efforts of EAC and NIST

The EAC, working in conjunction with NIST, has recently been developing new standards and requirements for voting systems. The standards and requirements are *prerequisite* to changing the voting system certification process, to mitigate the market and regulatory factors described above. EAC and NIST's work in tandem is focused on a recently reinvigorated set of open public processes for developing of requirements and standards that can better enable both election technology innovation and reform of the regulatory hurdles to adoption.

The work described below is proceeding, but with relatively few resources, and plenty of scope for acceleration. One beneficial aspect of a possible CI designation would be reprioritization that could accelerate the work and deliver its public benefits more quickly. The pace is relevant, because of a desire of many parties to effect significant improvements during the 2018 to 2020 election cycle.

In terms of CDI assets, the EAC/NIST work is most focused on voting systems, but also addresses elements of e-pollbooks and VRs technology.

- Open Data Standards

  An open data standard consists of a technical specification of a common data format ("CDF"), together with explanatory documentation and examples. A CDF helps with inter-operability and data exchange by defining a common "language" to systems to communicate effectively with one another.

  A recent example is a CDF for election definitions and election results. Early adopters of the CDF use it by converting from a variety of legacy data formats to the CDF, and publishing the resulting dataset as raw election results for general consumption. Based on the standard CDF, a variety of data consumers (*news organizations, data scientists, academics, and other researchers*) use the CDF in tools to obtain and interpret the data, where a single tool serves this function for any number of standards-based sources.

In the EAC/NIST election standards development effort, NIST publishes CDF definition documentation as guideline documents. In order for the CDF to become a true open data standard, the EAC needs to add a design guideline that certified voting systems must support the data standards for interoperability.

- Certification Reform

  Open data standards provide the basis for innovation in the architecture and operational model of voting systems. Currently, certification is based on a model of a large, monolithic, complex, low assurance system. The most potentially transformative type of data interoperability is interoperability between voting system components. Component interoperation provides the basis for a single component to be certified, which would be a major departure from the current certification program. This departure would enable some technology providers to focus on what they do best (*e.g., handicapped-voter physical access to a voting machine, digital image processing software, or hardware integration*), and would enable EOs to choose individual voting system components that meet their needs best.

  As a result, there would be markedly lower barriers to delivery to EOs of CDI technology with innovations that lack the defects leading to the many technical risk challenges outlined above.

- New Voting System Guidelines

  New voting system guidelines are another important aspect of EAC's work. New guidelines are needed for the component-based certification described above. Critically, new guidelines can also specify new requirements for voting technology that currently are not required, such as evidence-based tabulation, support for risk-limiting audits,[25] supporting component validation, preventing unauthorized modifications, proper use of cryptography for data provenance, and others described above.

  Support for component certification would not be limited to data standards and new requirements. New guidelines could also define, for the first time ever, the functional requirements for each component, requiring that each certified component conform to the standard product definition, and requiring the test labs perform conformance testing. This approach would be a major improvement to the current model, where each vendor defines each component in its own way, requiring the test process to be entirely customized every time.

- Current Efforts and Resources

  All of the efforts described above are part of an ongoing set of projects and working groups that are comprised largely of volunteers, and coordinated by a small number of staff and contractors at EAC and NIST, who also have other duties. The total funded

[25] Mark Lindeman and Philip B. Stark, "A Gentle Introduction to Risk-limiting Audits," *IEEE Security and Privacy*, March 16, 2012, www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf. Risk-limiting audits, in the context of elections, are a method that EOs can employ to ensure that the results of an election are accurate.

level of effort might be as little as 2.5 full-time-equivalent staff. While the contributions of many volunteers are required to perform the work, the volunteer nature of the teams means that work progresses at an irregular pace. Taking the common data formats work, which now has over half a dozen active subgroups, the overseeing EAC commissioner aimed for a calendar year for substantial completion; yet efforts are well into the third year, albeit with notable deliverables such as a national standard data format for election results. The work on new cybersecurity requirements for voting system began even more recently; notable progress has been made, but there is no complete project scope or timeline.

At the time, the decade-plus old certification program can't be significantly updated until new guidelines and requirements are complete and promulgated. If there are to be substantial improvements in voting system technology as certified by EAC and by states, and put into fielded use for the next presidential election, then at least two missing factors are needed for acceleration. First, additional resources are needed both for project managing these efforts to a timeline for specific impact, and also to bolster the efforts of volunteers. Second, such additional leadership and participation needs to inject national security and CI protection principles into the process.

2.5.2 Specific Government Efforts to Meet the CI Challenge

The EAC and DHS are working together on an essential response to the CI challenge of elections: formation of sector-specific organizations that are described in Section 3 and Section 4 below, and are the topic of one of our four major areas of findings and recommendations.

One significant advantage that the elections sector has over some other sector in the formational phase is that elections already have strong institutions for collaboration, including NASS, NASED, IAOGO, and several states' association of LEOs. As likely co-SSAs (*sector specific agencies*), EAC and DHS have convened organizational workshops with these stakeholder organizations, and leaders from representative SEOs and LEOs. The combination of existing sector institutions and an existing possible SSA organization with expertise in elections, promises the sector formation activities might proceed in a timely manner.

2.6 Summary

In this section, we have surveyed the present CDI, with definitions of terms and descriptions of assets, the current state of election operations using those assets, the current state of risks to them, the sources of those risks, and current activities to mitigate the risk as election technology progresses.

Based on this survey, we can now address the issue of the critical infrastructure designation for EI, which could range from EI core assets narrowly considered, or to CDI more broadly.

© 2017 OSET Institute, Inc. All Rights Reserved

3. Why Critical Infrastructure?

3.1 The Rationale for a CI Designation

Given the criticality of our democracy infrastructure described earlier, it will be clear to many that EI meets the formal definitions for critical infrastructure (CI), including the roles of various government organizations as either CI operators or as operating in a supporting role.

With respect to formal designation, EI operators are in some sense in a situation similar to other CI sectors at the outset of their designation. Unlike the more obvious CI assets (e.g., power grid, financial clearing systems, air traffic control), some CI was not as obvious at the outset of CI policy making. But once asset identification and risk analysis began, for example, a hydro dam's digital control systems, it became obvious that a cyber attacker could use that to interrupt service, or harm people and property by opening floodgates.

The same may be true of EI given the recent significant reassessment of the threat environment including nation-state actors, and the possibility of election dysfunction leading to civil unrest. Put another way, there is a recently increased understanding of elections as being a *critical function* that have *significant threats*. If elections are a critical function (to the operational continuity of our democracy as a sovereign act), and there are credible threats to the conduct of elections, then elections' infrastructure must be considered critical infrastructure, whether or not the official designation remains or evolves.

3.2 Concerns About the CI Designation

Of course, there are several relevant concerns about the advisability of the formal CI designation. Any discussion about the value of a CI designation must be balanced by an assessment of concerns. We describe the more important ones here.

- Undue Federal Influence in Elections

  Perhaps foremost is the concern, as voiced by Georgia Secretary of State Brian Kemp, about undue federal government influence or involvement in state and local election administration and operation.[26] It is important to note that any relationship between CI operators and DHS is *voluntary*. EOs can determine the scope and duration of their interactions with the DHS; the designation merely makes EI a priority for resources and assistance should an EO want them. Regarding Homeland Security, the actual history of DHS's role in other CI sectors does *not* suggest DHS intrusion, or potential thereof, into election operations.

  Nevertheless, federal overreach is conceivable. While primary authority over elections rests with the states constitutionally (*i.e., Tenth Amendment*), the federal government does retain (*little used*) authority over elections for federal offices (*i.e., Congress and*

[26] Tim Starks. "DHS labels elections as 'critical infrastructure'". *Politico*, January 6, 2017, www.politico.com/story/2017/01/elections-critical-infrastructure-homeland-security-233304.

the President), so reasonable legal experts can argue over what this could mean. Thus, we regard it as a fixed point for any effective federal role, by DHS or otherwise, with or without an official designation, that the existing administrative structure of U.S. elections be left unchanged and untouched.

- The Scope of EI Designation

  Lack of clarity on the scope of EI designation has also created concern over federal overreach.[27] To be clear, the existing subsector designation applies strictly to the EI operated by state and local elections organizations, but does *not* extend to the infrastructure of the many non-government organizations involved in the larger political process outside of administering elections. For example, as Christy McCormick, an EAC commissioner, rightly points out, issues such as "*what happens on or to the eMail systems of political parties or their committees, purported influence campaigns, and celebrations for one candidate or another have no impact on the security and integrity of our election infrastructure.*"[28] Political parties and their eMail may be a part of a broader democracy *ecosystem* but they are certainly *not* a part of EI. As EI sector formation activities evolve, it is important that the scope of sector activity not be misconstrued as extending beyond government-operated EI.

- Federal Regulations of Elections

  There is a fear that the designation makes it politically expedient for the federal government to regulate elections for national security purposes.[29] However, an increase in political expediency, if present, would not change the fact that today, there is no part of the executive branch that has rule-making authority over elections, other than the FEC's oversight of campaign finance. Any future increase in federal regulation would require Congressional legislation to grant some rule-making powers. To date, the existing designation seems to have had little if any impact on the desire of Congress to provide greater regulatory authority beyond that already granted to the FEC. Indeed, currently there remains on-going Congressional effort to terminate the U.S. Elections Assistance Commission.

---

27 "Securing Elections as Critical Infrastructure." *National Association of Secretaries of State*, www.nass.org/index.php/nass-initiatives/nass-cybersecurity-elections-critical-infrastructure/. Accessed on August 17, 2017

28 Hans Spakovsky. "DHS' Election Power-Grab Raises Huge Questions and Red Flags." *The Heritage Foundation*, January 13, 2017. www.heritage.org/election-integrity/commentary/dhs-election-power-grab-raises-huge-questions-and-red-flags.

29 Pam Fessler. "State And Local Officials Wary Of Federal Government's Election Security Efforts." *National Public Radio*, April 5, 2017, www.npr.org/2017/04/05/522732036/state-and-local-officials-wary-of-federal-governments-election-security-efforts.

- Congress Creating Permanent Designation

  This leads to another concern: that Congress will legislate that elections be permanently classified as critical infrastructure, as H.R. 1562 seeks to do.[30] It is unlikely that DHS's designation will affect Congress's views on critical infrastructure, but even if Congress were to create a permanent designation it could never interfere with State's constitutional right to administer elections. The states have hundreds of years of experience running elections that the federal government lacks; there is no evidence that critical infrastructure designation is any attempt to limit or remove states from that role, but all indications so far are that it is an attempt to increase the capacity for voluntary assistance to states. We offer no opinion on the value of legislatively making such a designation permanent other than to catalog it here as a valid concern. However, this Briefing is intended to inform that conversation and any such initiative.

- Designation Doesn't Provide Reaction for Cyber-Attacks

  Critics also point out that the act of designation does not address how the United States would or should react to foreign cyber-attacks.[31] This is true. But designation does help prepare for those attacks by reprioritizing DHS's cybersecurity resources to help EOs should they request it.

- No Change in DHS Assistance

  Some have correctly observed that since the subsector designation occurred, DHS has offered no assistance other than what it has always offered to the states.[32] However, states have accepted more voluntary aid from DHS and DHS has been more successful at supplying it since the designation, although it is possible that this was not a result of designation.

- Conditions on DHS Assistance

  DHS assistance based on voluntary requests from states is a new and unfamiliar relationship. Some EOs have expressed concern that such assistance might 1) become contingent on compliance with DHS guidance or conformance to DHS security requirements; or 2) be performed with a scope that is defined by DHS not scoped and constrained by the state requesting assistance.[33] If such adverse situations were to

---

30 "H.R.1562 - SAFE Act." *congress.gov*, accessed August 16, 2017. www.congress.gov/bill/115th-congress/house-bill/1562/all-actions.

HR 1562 is a bill that seeks to make the designation of election as CI permanent by act of Congress, among other things.

31 Pam Fessler. "State And Local Officials Wary Of Federal Government's Election Security Efforts." *National Public Radio*, April 5, 2017, www.npr.org/2017/04/05/522732036/state-and-local-officials-wary-of-federal-governments-election-security-efforts.

32 Lily Newman. "Securing Elections Remains Surprisingly Controversial." *Wired*, July 13, 2017. www.wired.com/story/election-security-critical-infrastructure/.

33 Hans A. von Spakovsky. "Why Does DHS Want to Designate Election Booths 'Critical Infrastructure?' *The Heritage Foundation*, Aug. 17, 2016, www.heritage.org/election-integrity/commentary/why-does-dhs-want-designate-election-booths-critical-infrastructure.

arise, they would definitely be cases of both overreach of DHS's assistive function and departure from the existing experiences of DHS engagement with other CI sectors. However, the concern is legitimate, not because of past experience, but because elections are a unique government function, and DHS is part of the government that is served by elections. As a result, DHS's relationship with election CI operators might have less clarity than relationships with CI operators in other sectors. Perhaps the best way for states to address such concerns and maintain vigilance over DHS's role is for states to voluntarily participate in information sharing organizations, sharing experiences pro and con from engagement with DHS.

- Designation is Unconstitutional

  Another criticism of designation is, as some EOs have argued, that the federal government has no constitutional legal authority to classify elections systems as critical infrastructure.[34] It is possible that this is the case, but regardless, it is a constitutional law issue to be dealt with separately from the continuing upsurge in engagement among local, state, and federal government on improving protections to EI.

- Disapproval of States

  Another concern, as pointed out by Hans A. von Spakovsky is that "the formal designation itself admitted that 'many [state and local election officials] are opposed to this designation.'"[35] Yet, many find it concerning that a designation claiming to give more resources to states, would be opposed by those same states. This fear likely ties into concern of federal overreach, which can, at least partially, be allayed by the voluntary nature of DHS assistance. It is also important that as the CI sector develops, new processes, platforms, and policies are put in place to prevent DHS from using its resources as leverage to manipulate elections—that is, appropriate checks and balances.

- Designation is Unnecessary

  A final concern, also expressed by von Spakovsky, is that "*nothing prevents DHS from making recommendations now —no 'critical infrastructure' designation is required.*"[36] It is true that assistance can be provided to states without the critical infrastructure designation, but the designation increases the capacity for voluntary information sharing organizations, and prioritizes DHS cybersecurity resources for EI.

---

[34] Mark Rockwell. "Critical infrastructure designation for voting goes too far, says state official." *FCW*, September 13, 2016. fcw.com/articles/2016/09/13/election-hack-hearing-rockwell.aspx.

[35] Hans A. von Spakovsky. "DHS' Election Power-Grab Raises Huge Questions and Red Flags." *The Heritage Foundation*, Jan. 13, 2017. www.heritage.org/election-integrity/commentary/dhs-election-power-grab-raises-huge-questions-and-red-flags.

[36] Hans A. von Spakovsky. "Why Does DHS Want to Designate Election Booths 'Critical Infrastructure?' *The Heritage Foundation*, Aug. 17, 2016, www.heritage.org/election-integrity/commentary/why-does-dhs-want-designate-election-booths-critical-infrastructure.

© 2017 OSET Institute, Inc. All Rights Reserved

Another significant concern about designation is the observation that EI appears to be very different from other existing officially designated CI, in sectors such as transportation, finance, telecom, and others. This is also a reasonable assertion; however, there are important similarities to existing CI sectors as well, which can provide a valuable model for *uplift* of CDI protection, and specific measures that are relevant with or without an official designation.

Therefore, before discussing the basic goals for CDI protection uplift, we compare and contrast EI with other CI.

3.3 Comparing EI to Other CI

Although EI is different from types CI in that it is not "*always on*," such as power distribution or air-traffic control, EI is similar to other CI sectors. For example, EI is similar to CI for finance, in that elections are essentially composed of *transactions* of ballots—of a voter indicating their votes for candidates and referenda. To be sure, there are critical differences, such as that ballots must be anonymous, and the transaction of counting a ballot cannot be reversed. But some parallels exist, because there is process defined by law, available to any citizen, consisting of personal actions that must be approved and recorded. Indeed, by a quirk of history, EOs are often also in the transaction-processing business as much as the NYSE or NASDAQ—being county EOs on the one hand, but also having responsibilities as recorders of real estate transactions.

EI also has similarities to other CI sectors that have locally operated assets, or government-operated assets. After all, we might reasonably expect stock exchanges and financial services companies to be able to operate critical systems, both because of organizational capacity, and because of the organizations' own self-interest in continuity of operation and in public trust in the legitimacy of transactions. Likewise, government operated air traffic control is safety critical and funded to meet stringent continuity requirements.

But do we expect state and local governments to exercise similar responsibility? *Yes*. Elections organizations have a *fiduciary responsibility* that is as imperative as that of financial services, and on election days has as much continuity responsibility as air traffic control.

But could we reasonably expect these state and local governments to develop similar capabilities for CI operation? *Yes*. Some CI operators are local government organizations, and the same is true of many first responders whose infrastructure is critical for public service and safety. Local government organizations operate water services, bridges and tunnels, and other assets essential to public service and safety. As CI operations practices have developed and extended to multiple sectors, state and local government organizations have evolved to conduct CI operations. There is every reason to believe Elections organizations can do so as well.

3.4 Administrative Intent

The administrative intent of designating EI as CI need not be significantly different from similar designations in other sectors, especially those sectors where some CI operators are state and/or local government organizations. Although designation may not be, strictly speaking, required for any benefit, the major benefits would include prioritization, voluntary assistance, and voluntary sharing.

The administrative intent of CI designation should be a major re-prioritization intended to have a positive effect particularly on local elections offices' ability to gain assistance and resources. At present, election operations are rarely treated as a top priority with national implications.[37] One possible parallel example is the positive impact that CI designation had on local first responder organizations to upgrade equipment and test response processes.

Other benefits are largely those of voluntary assistance and participation in sector-specific activities such as Information Sharing and Analysis Centers ("ISACs"). Again, an instructive analogy may be local water board operations, classified post-9/11 as public safety critical, and a very broad scale vector of attack for homeland adversaries. From the first impact of CI designation up to the present day, the fundamentals of local water and sanitation operations have changed little. There is no DHS role in the operation of local utilities. There is no national regulation for required standard water treatment processes. There has been assistance to local organizations in performing asset classification, risk analysis, cost-benefit analysis, and other typical risk management activities that local utilities typically lack expertise in – particularly with respect to cyber-assets.

Specifically, with respect to elections organizations, constraints on change are more powerful and explicit than any other CI sector, including: Article 1 Section 4 of the U.S. Constitution, Article 2 Section 1, and Amendments 12, 15, 17, 19, 23, 26.[38] Likewise, historically elections have been notably free of directive federal legislation, with literally a handful of federal acts in many decades, and a near absence of federal regulation. With the notable exception of the FEC's role for campaign finance, Congress has not provided rule-making authority regarding elections to any federal agency.

Not only does designation not change the federal government's limited regulatory powers, designation also does not create any new powers. For elections, as in every other sector, and with each designation of a new sector, the federal role has been as outlined above. CI designation in no way enables the federal government to have any new direct *operational*

---

[37] Many localities have been unsuccessful in seeking financial and other resources to improve election operations. A major exception has been innovation grants from EAC and DoD/FVAP, but the aggregate nationwide funding in a decade is perhaps a few million dollars.

[38] "The Constitution of the United States: A Transcription." *National Archives,* June 26, 2017. www.archives.gov/founding-docs/constitution-transcript. The Constitution of the United States delegates the elections largely to the states and restricts the influence the federal government can have over them. Through multiple amendments it also dictates certain characteristics of elections.

role in election administration, the operation of elections, or indeed any role in SEOs and LEOs.

3.5 Suggested Objectives for CDI Uplift

There are three primary objectives for new activity to bring CI practices to CDI operations and dramatically raise the level of protection of CDI assets and activities—or, for short, "*CDI uplift*." Regardless of official designation, the immediate objectives for CDI uplift would be to:

1. Identify those elections organizations that are CI operators;
2. Provide support for a re-prioritization of the their functions and resources; and
3. Foster beginning the transition of elections organizations toward operating as a CI provider – much as was done in each case of adding a new CI sector in the past, especially for CI operators that were locally operated and/or government operated.

In the case of elections organizations, however, there are election-specific requirements for CI operation. Secondary objectives include:

1. Identify the sector-independent CI operations requirements that apply to the elections sector.
2. Define election sector-specific requirements for CDI operators, and
3. Enabling EOs to evolve their organizations to meet these requirements.

As elections organizations may be expected to become CI operators, with potentially significant organizational changes being necessary, there are still CI issues specific to elections. Some of the most important such election sector specific issues are related to *feasibility* and *transparency*. Unlike many CI sectors, the public has a fundamental right to observe election operations, and to derive trust in election results from transparency of election administration. While the general public might also have a basis in trust of power reliability, that's not based in the ability to observe the operations of power generation facilities, or to hold power distribution operators to a demonstrable standard of care. By contrast, with elections, the public does require transparency for trust.

As EOs become CI operators, the transparency and trust requirements are even higher. EOs are accountable to the public to be custodians of EI, and proper protection of EI is the basis for trust in the results of EI operation: declared and accepted election winners and losers, and the orderly transfer of power. With more explicitly recognized CI responsibility, EOs will also have greater responsibility for demonstrating to the public that they carried out their CI protection duties properly, and that election results are genuine.

At the same time, many EOs have a narrower base of expertise to start from as new CI operators. Unlike other CI sectors where operator staff have professional degrees or certification (*e.g., industrial engineering in the power sector, IT in the finance and telecom sectors*), many EOs have little or no formal training in election operations, much less the application of CI protection principles to the operation of EI.

© 2017 OSET Institute, Inc. All Rights Reserved

As a result, a practical approach to CDI uplift must emphasize *feasibility*. The new CI duties of EOs must be feasible for them to carry out, feasible for staff to be trained on, feasible for auditing compliance with defined CI protection practices, and feasible for compliance to be evident to the public, with the operational transparency that's needed for election results to be trustworthy.

In other words, *organizational transformation* will be necessary. A major objective of CDI uplift is to prioritize two kinds of resources:

1. The resources needed to define specific types of transformation as *feasible* for today's EOs, and
2. The additional types and level of resources that EOs would require to operate effectively as a CI operator.

Similar to experiences of other sectors' CI operators, one goal for transformation is that it cannot impact the existing responsibilities and duties of elections offices. However, the standard of care and the expected operational integrity will be higher, and initially some elections organizations may not have the resources or the skills for "*elevating their game*." However, by recognizing its role as being like any CI operator, an elections organization can make use of many new resources and sources of support to help uplift their organizations to become solid CI operators. The same process that has occurred with other local and/or government CI operators can and should happen with CDI operators. Indeed, we've already seen the beginnings of this change, as several state elections organizations have made use of voluntary assistance from DHS on cybersecurity of state-managed VRs systems.

To be sure, it will be challenging due to the sheer number of thousands of county or local EOs with these additional responsibilities, and the fact that most are small operations with little to zero local funding, and several other responsibilities in between elections. But the good news is that unlike, for example, local utility operators, every local elections organization is also part of the responsibility of full-time state elections organizations.

As a result, states can offer significant structure for assisting localities in a uniform way statewide. Similarly, states can help conduct pilots of CI operations uplift, and facilitate the spread of improvements across states. States have the ability and responsibility to expend state funding for election integrity (*as some have already done by funding county election technology upgrades*) including funding and resources for expanding state and local elections organizations' capability to become CI operators.

© 2017 OSET Institute, Inc. All Rights Reserved

4. Organizational Development for CDI Protection

To protect not only core EI, but also the full range of government operated CDI, one broad area of required activity is the formation and operation of sector-specific CI organizations for information sharing, guidelines definition, incident response support, and other typical functions of a CI sector. At present, the election operations CI subsector has begun organization formation,[39] with EAC proposed as a co-SSA with DHS,[40] and working with state and local elections leaders, professional organization such as NASS and NASED, and other local, state, and federal stakeholders.

Our specific recommendations amplify some of the details of the ongoing sector formation activities, and the continuing activities after formation. Many such activities follow the CI practices of other existing CI sectors. Some will be specific to elections, as will the range of organizations involved:

- LEOs as CI operators for election operations;
- SEOs both as CI operators of voter lists, and as supervisory bodies for LEOs;
- Other state-level organizations such as national guard cyber protection units;
- EAC and/or DHS as Sector-Specific Agencies;
- Law enforcement;
- Liaison with national security;
- Other federal organizations such as NIST;
- Technology vendors, IT service providers, and other organizations that support state and local elections organizations.

Most or all of the sector formation activities can be undertaken with or without designation, but might benefit from the current designation in terms of mindset (*prioritization*), resources allocation, or speed of execution. Few or none of these activities need be affected by a change in designation. All of these activities can and must be undertaken within the existing administrative structure of U.S. election operations. The remainder of this Section provides additional background on sector formation activities.

---

39 "EAC Meeting Moves Election Cybersecurity Protections Forward" *Elections Assistance Commission,* July 27, 2017, www.eac.gov/news/2017/07/27/eac-meeting-moves-election-cybersecurity-protections-forward/. In late July the EAC held a meeting with national security and election stakeholders to begin the steps of organizing EI into a CI sector.

40 "U.S. Election Systems as Critical Infrastructure." *Election Assistance Commission*. www.eac.gov/assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf. Co-Sector Specific Agencies are used to help fill the knowledge gaps that arise from DHS lacking knowledge relevant to a specific CI sector.

© 2017 OSET Institute, Inc. All Rights Reserved

4.1. Institutions for Voluntary Cooperation and Sharing

Information sharing and advisory institutions are central features of existing CI sectors. Formation of one or more Information Sharing and Analysis Organizations (ISAOs) or similar organizations is an essential part of work toward the creation of a fully functioning CI sector for elections.[41] [42] The precise nature, functioning, and benefits of an ISAO for elections would be determined during the formation process, by the formation participants. However, some of the functions of other sectors might apply, and might apply in an election-specific way.

One critical function of an ISAO is to operate as a private space for participants to share information, in some cases with exceptions from regulation that would otherwise stifle communication (*e.g., antitrust collusion constraints*). In other cases, the communication is protected from disclosure with provisions that remove participants' fiduciary responsibilities (*e.g., disclosing information that might destroy trade secrets, harm one's own reputation, or influence equities or commodities trading that is relevant to the sector*).

In the case of elections, many of these concerns would not apply to elections organizations, but might well apply to their vendors, whose participation in an ISAO would likely be very beneficial to EOs. Privacy may also make it easier for EOs to share information that might in some cases be more closely held out of concern for public response or misunderstanding, and/or have political implications.[43]

Private ISAO collaboration can also be helpful to industry self-regulation or standardization, in the sense of creating recommended or quasi-standard practices that help participants benefit from one another's experience, without necessarily creating a real or perceived method of comparing CI operators for degrees of compliance. For the many personnel and procedural aspects of EI operation and protection noted above, such collaboration may enable cross-training and operational improvements.

Another benefit of government/operator partnership is the ability of DHS and other sector-relevant government organizations to offer expertise and assistance to operators, including those that may be more palatable if performed without public visibility.

And not least among the benefits would be a controlled environment for information sharing from intelligence and law enforcement to elections organizations, and vice versa.

---

41 "National Council of ISACs," *National Council of ISACs*. www.nationalisacs.org/. ISACs are Information Sharing and Analysis Centers. They help CI owners and operators share information to improve the security of their infrastructure.

42 "Frequently Asked Questions About Information Sharing and Analysis Organizations (ISAOs)" *Department of Homeland Security*, Oct. 6, 2016, www.dhs.gov/isao-faq. ISAOs are self-organized and not necessarily part of CI, but, similar to ISACs, they facilitate information sharing.

43 "U.S. Election Systems as Critical Infrastructure." *Election Assistance Commission*. www.eac.gov/assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf. CI sectors are allowed to have information sharing with federal and state governments that are free from FOIA requests (*and their state counterparts*). This assuages fears that sensitive information could be exposed to the public.

The world of election administration already includes strong structures for collaboration in the form of national organizations such as NASS, NASED, and IAOGO, and within most states, an association of county registrars or other LEOs. Consequently, it is already clear which organizations would be eligible as voluntary participants to support EOs in a new role as CI operators.

4.2 Public-Private Partnerships

Public-private partnership is a term used in homeland security to describe processes and institutions of assistance and sharing of relevant federal agencies with operators in a sector, and between operators. In the case of CDI, public-private partnerships would operate slightly differently than in other CI sectors. None of the assets in EI are privately owned; CI operators are state and local government organizations; private sector roles do exist, but as vendors of products or services procured by state or local elections organizations.

Regardless of this difference, the same types of sharing and assistance that are essential to other sectors also have potential for significant benefit in the CDI ecosystem. Partnership between election CI operators and federal government organizations and state government organizations (*e.g., state-level homeland security fusion centers*) is an essential part of a fully functioning election CI sector. As with all such partnerships, the involvement of a particular elections organization, and the types of engagement with specific partners, is entirely voluntary to the elections organization.

4.3 Private Sector Roles

Private sector organizations also have a key role to play in the formation and operation of election sector institutions. Private sector companies have several key roles at both the state and local levels.

At the state-level, private sector companies have roles in supporting or providing services to a state elections organization, including, but not limited to, the elections organization that operates a state's central VRs system. Roles include: software vendor, IT services and technical support, supplying or supporting government-operated datacenters, outsourced operation of such datacenters, and data hosting and cloud computing services.

In each of these and other existing roles, private sector organizations have vital experience in supporting the operation of critical EI assets—experience that makes them valuable contributors to information sharing activities, as well as important recipients of benefits from them. For example, IT services providers might have a role in independent cybersecurity assessment both before and after activities to strengthen cyber defense of voter record-related IT systems.

At the local level, vendor roles include: voting system product vendors, the product service and support arm of these vendors, third party voting system support vendors, county-level IT services that support local elections offices, either provided by the county, outsourced by the county, or outsourced by the elections office, and warehousing, transportation, storage and related services for physical assets of voting systems. As at the state-level,

these organizations have critical expertise that is needed by information sharing organizations, and also may have operational roles that benefit from sharing activities.

4.4 Costs and Benefits

We only briefly address this topic as it could easily consume another entire paper of this size or greater. It is certainly fiscally responsible to ask about, and analyze the costs and benefits of designating and protecting America's CDI. Such an analysis must, by definition, examine the cost of *not* seeking such protective measures, let alone the costs of not developing a CI attitude and mindset. While a detailed analysis is beyond the scope of this Briefing, for effort of completeness, we offer a summary comment, and refer readers to detailed DHS documentation on CI.

There is little doubt that the government and the private sector have a shared interest in ensuring the viability of CI and the provision of essential services, under all conditions. CI owners and operators are usually the greatest beneficiaries of investing in their own security and resilience, and are influenced by a social responsibility to adopt such practices. Yet, it is reasonable for the private sector, as well as the public sector in the case of EI, to be concerned about returns on investment in security and resilience initiatives, including the cost and benefit of services, systems and tools. This is especially true when such investments may not yield demonstrative and immediate measurable benefits (i.e., *returns on investment).*

It is possible that effective incentives can facilitate cost justification of improved security and resilience by balancing short-term costs of additional investment with short-term benefits. The fact is, the risk of failing to properly protect the critical assets of election administration is too great and the cost of such failures (*e.g., a compromised election*) may be imponderable.

We believe, as alluded to elsewhere in this Briefing that redesign of the underlying architecture of election technology will be required in the near term. And that can result in financial benefit itself. Forward-thinking security-centric design and engineering practices can actually lower costs—not only of initial investment but also costs of potential incidents and recovery therefrom. Therefore, factoring security and resilience measures into design decisions can result in systems better able to mitigate physical and cyber vulnerabilities at lower cost. In fact, over the long run, investments in more fault-tolerant, high assurance election equipment design should result in lower costs than the expenses of maintaining obsolete equipment on a dwindling supply of spare parts.

Nevertheless, assessing the cost and benefit of each individual security initiative including capital and annual expense commitments is an important exercise in prioritizing budgets, and making trade-off decisions where they must be made. We imagine this is an important exercise as part of determining the costs to improve America's EI in general, and perhaps an assignment for the Congressional General Accounting Office at the federal level, and states' equivalent offices of management and budget.

© 2017 OSET Institute, Inc. All Rights Reserved

5. Findings and Recommendations

Our findings and recommendations fall into four groups:

1. CI sector operations;
2. Short-term technical risk remediation;
3. Redesign of core EI technology; and
4. A trustworthy supply chain.

5.1 Operation of an Elections CI Sector

Findings

Our first set of Findings relates to the current situation in which state election officials and local election official (*SEOs and LEOs*) are responsible to acting as CI operators, but lack nearly all the support that CI operators have in other sectors.

Our Recommendations in this area are all oriented to the activities of these CI operators and other election sector stakeholders, to form the institutions and practices typical of other CI sectors, and to use them to support the election CI operators' organizational change to gain capacity in CI operations security.

The detailed findings for these recommendations are provided above in Section 4.

Recommendations

1. Short-term collaboration among sector stakeholders to identify the scope for needed information sharing organizations, and to identify the election CI sector players that could have a role in them. Such collaboration is underway in early stages; for example, the EAC is convening of exploratory meetings with leaders from state and local elections organizations, and industry organizations including NASS and NASED.
2. Based on short-term collaboration, establish information-sharing organizations with specific scope. For instance, form an ISAO for states' VRM organizations to develop and share sector-specific cybersecurity practices, and experiences with voluntary use of assistance from other organizations (*e.g., DHS, state cyber national guard*).
3. In information sharing organizations and/or industry organizations, define the elements of general CI operations and CI security guidance[44] that are applicable to specific types of EI asset operation, and share experiences in applying them to strengthen the protection of EI assets in ways that smaller or elections organizations with fewer resources can learn from the experience of larger or earlier-acting elections organizations.

[44] "Framework for Improving Critical Infrastructure Cybersecurity." *National Institute of Standards and Technology*. Jan 10, 2017. www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf

4. Within state elections organizations, existing interstate organizations, and new information sharing organizations, develop sector-wide recommendations for methods to create, in existing local elections organizations, the skills and resources to act as a CI operator.
5. Contribute to the acceleration of existing activities on standards, interoperability, and especially cybersecurity requirements for election technology. This work is underway, but needs additional focus on CI security that can be effectively supported by information sharing organizations. The current resources of NIST, EAC, with Technical Guidelines Development Committee ("TGDC") and other volunteers, must be supplemented to make rapid progress possible.

5.2 Architectural Innovation

Findings

One of the most critical findings primarily concerns existing voting system technology, and to a lesser degree, other kinds of EI technology assets. Section 2.4 describes the current state of risk to and vulnerability of our current voting systems technology.

Our principal finding is that the base technology for voting systems does not fit the current threat environment, is insufficiently robust for a national security system, and insuperably difficult for U.S. elections organizations to operate and protect as CI given both the technologies' fundamental weakness, and the decentralized nature of the U.S. election system, which consists of thousands of state and localities with varying budget, resources and capabilities.

Additional near-term efforts on mitigation of risks is essential (see Section 5.3) but cannot remove the fundamental vulnerabilities because they are "built-in" as a result of design decisions made over a decade ago—to base voting systems on personal computing (PC) technology that was specifically designed to be easily modifiable. The results for consumer computing have been an indefinite arms race of security exploits and countermeasures to further modify systems in reaction to exploits.

Finding that the existing election technology base is fundamentally inappropriate for critical systems, the core observation is that it *must be replaced*. Our recommendations are objectives and courses of action toward that replacement, starting with fortification of existing R&D to pursue the goal of new voting system base technology and fielded systems built upon it; systems with a base that is specifically designed for the security requirements of national security systems and designed for feasible CI protection by U.S. EOs.

Further, we recommend an approach that is based on proven technology in use for many years in other areas of computing that are familiar to DoD, NASA, and other organizations that require high assurance: fixed function embedded systems. The objective:

> *New Infrastructure*
> *Rapidly redesign and reengineer the underlying technology base for voting systems in an application specific componentized architecture for fixed-function components that are fault-tolerant to withstand digital compromise*.

There are currently half a dozen major research and development projects contained in academic, public, and private sector organizations to produce the kind of fault-tolerant, verifiable, accurate, secure, and trustworthy election and voting systems technology required to achieving the objective above.

These projects should have immediate (*as soon as possible*) access to research and development funding grants on the condition that what results from this funding is publicly owned technology readily available to be incorporated into new election and voting systems that achieve the mandates as outlined in this Briefing. That is an obvious outcome given that said research and development dollars, regardless of the agency dispensing them, amount to taxpayer funding. There is a worked example for this: This is the model that relied upon DARPA (Defense Advanced Research Projects Agency) and NSF (National Science Foundation) to develop the foundations of what today is the commercial and global Internet.

The following are specific recommendations of initial steps toward the above objective.

Recommendations

1. Rapidly survey the existing work on next-generation voting system technology, in government election organizations, academia, and non-government organizations.
2. Design rapid funding vehicles for fortifying these efforts, as well as an agile Program Management Office ("PMO") to coordinate them.
3. Task the PMO with designing technology transfer vehicles that meet the varying needs of the thousands of U.S. localities, their vendors, and their technology services providers.
4. Create a vehicle for accelerating the existing standards and requirements work particularly on cybersecurity, but with a *new* focus: requirements for the subset of voting system components that must meet the most stringent challenges in the current threat environment.
5. Explore alternative certification and accreditation ("C&A") methods that can incorporate proven methods of security-specific C&A programs for security-critical Department of Defense ("DoD") systems.
6. Engage with policy analysis and development organizations to identify any policy challenges for technology transfer and commercialization.

5.3 Short-Term Cyber Risk Reduction

Findings

Our key finding about risk reduction is that core EI cyber-assets have significant scope for risk reduction by the application of established cybersecurity practices and technical remediation. This significant scope exists not because these core assets have been poorly managed, but rather because hitherto, the security management of these assets was not performed in the framework of CI security for national security systems. With a shift to

that framework, EI operators have a new opportunity to apply numerous proven cybersecurity methods.

There are three primary sources of support for short-term cyber risk reduction.

1. The first and most immediate one is DHS's cybersecurity assessment services and remediation support services, which over 30 states and localities have made voluntary use of. Use of these services can quickly identify cybersecurity posture improvements.
2. A second source of support is the extensive cybersecurity guidance and best practices provided from numerous sources, but most notably NIST and DHS. NIST created a cybersecurity framework with recommendations for CI owners and operators to apply in order to evaluate and improve the cybersecurity of their systems.[45] The framework is divided into five categories: 1) Identify, 2) Protect, 3) Detect, 4) Respond, and 5) Recover. These categories represent vital activities for evolving existing EI asset management to include modern security management practices. Further, CI-specific guidance is available from NIST and DHS.[46]

   However, this second category is thorough and broad. Extensive use of these resources by a state or local elections organization is a process that amounts to the development of a complete security management program—appropriate to their role as a CI operator, but not a short-term undertaking, and one beyond the short-term internal resources and capabilities of many organizations. EOs need to make best use of their current internal resources to make the highest impact improvements based on thorough and broad guidance.[47]
3. To this end, a third resource has significant potential: use of the information sharing organizations, for EOs to learn from one another which of the methods of cybersecurity improvement were the most effective as well as time and cost effective.

A closing point applies to the use of all these resources: a focus on the core EI cyber-assets of state-managed VRs systems and locally managed voting system components (described in more detail in Section 2.3).

A final Finding is a bipartisan effort that would directly address short-term cyber risk reduction. On the 27th of July 2017 Senator Amy Klobuchar (for herself and Senator Graham) introduced the *Graham-Klobuchar Amendment* (SA 656)[48] to H.R. 2810, the *2018 National Defense Authorization Act*.

---

45 "Cybersecurity Framework." *National Institute of Standards and Technology.* Jan 10, 2017. www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf

46 "Framework for Improving Critical Infrastructure Cybersecurity." *National Institute of Standards and Technology.* Jan 10, 2017. www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf

47 "Security and Privacy Controls for Federal Information Systems and Organizations." *National Institute of Standards and Technology*. April 2013. nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

48 The complete text of the proposed amendment can be downloaded from: http://bit.ly/GKA656

This amendment would provide states with funding necessary to improve and secure election systems, provided that grantee states meet certain administrative, technical, and transparency requirements set forth by the Amendment and a commission of stakeholders to be established by the legislation. Specifically, the Graham-Klobuchar legislation would amend the *Help America Vote Act of 2002* (HAVA) with a new section for federal funding to states in the form of "*Election Technology Improvement Grants*" that could be used to improve security of existing voting systems, provided that certain best practices and conditions set forth in the amendment were followed. To receive funding once an appropriation is made, states would be required to develop, submit and publish a plan that detailed how these federal funds would be applied toward improving voting systems.

States would be eligible for a grant only if their election systems survive a "*Security Risk and Vulnerability Assessment*" from the Department of Homeland Security, including correcting detected vulnerabilities. Grants would have to be applied to satisfying the cyber-security and cyber-hygiene recommendations of the to-be-formed federal-state commission. The good news here is that this legislation properly considers all stakeholders for this commission including (but not limited to) the:

- National Association of Secretaries of State (NASS)
- National Association of State Election Directors (NASED)
- National Association of Election Officials (NAEO)
- International Association of Government Officials (IAOGO)
- National Association of State Chief Information Officers (NASCIO)
- Secretary of the Department of Homeland Security
- EAC Technical Guidelines Development Committee
- EAC Standards Board
- EAC Board of Advisors
- National Institute of Standards and Technology (NIST)
- Multi-State Information Sharing and Analysis Center

There is considerable detail in the proposed Amendment that addresses qualifications, applications for grants, reporting processes, and the like. Those details are deserving of a separate analysis, beyond the scope of this Briefing; however, a paper has already been published by the *Institute for Critical infrastructure Technology* and is worth a read.[49]

Recommendations

1. State EOs should make voluntary use of DHS cyber-security services to assess and improve controls over core VRs databases and internal systems used to manage the data. Included in the scope of work should be an assessment of attack surface to VRs from external but non-public systems such as motor records IT systems.
2. For states with online voter services registration or OVR, with such assistance determine whether the core voter database is any way accessible to public-facing

[49] http://icitech.org/wp-content/uploads/2017/08/ICIT-Analysis-The-Graham-Klobuchar-Amendment-Can-Secure-Election-Infrastructure.pdf

systems, and if so, at least plan (*and ideally execute*) a redesign effort shift to the proven practices of other states that have OVR systems that are limited in access to a read-only copy of VRs, and a segregated system for storing OVR requests for later processing.

3. State EOs should leverage these short-term assessment and remediation activities to begin the process of instituting (*if not already present*) a complete security management program for all IT systems related to VRM, using resources including those noted above. Included in the scope should be documentation and testing of data recovery plans to be used to recover from security incidents that may include data tampering.
4. Local EOs should make voluntary use of DHS cybersecurity services to assess and improve controls over all local IT systems involved in election administration and election management, starting with a complete review and inventory of any system that handles pre-election election-management data, preparation of systems for ballot casting and counting and post-election tally data.
5. Local EOs should leverage these short-term assessment and remediation activities to begin the process of instituting (*if not already present*) a complete security management program, starting with independent assessment of documentation (*e.g., compliance documents, training materials, product administration guides*) of the complete set of physical, personnel, and procedural controls intended to mitigate risks of tampering with any components of the voting system, or systems on which they depend.
6. The U.S. Senate should pass the Graham-Klobuchar amendment to H.R. 2810,[50] the *National Defense Authorization Act for fiscal 2018*.[51] This legislation is one (*but certainly not the only*) means to assist states with triage efforts to reduce cyber-security risks in existing election and voting systems. The major objectives are to secure voter registration logs; upgrade election auditing processes; promote information sharing to stymie emerging threats; and strengthen transparency, intergovernmental communications, and oversight. All of these elements are within the objective to reduce short-term cyber-security risks, and this amendment is a perfect complement to our aforementioned recommendations.

Finally, it is important to observe that these recommendations are needed to mitigate risks, and although they are not a substitute for longer-term security-centric redesign of core EI cyber-assets, they are necessary stopgap measures that can serve as important guidance to redesign efforts.

---

[50] Graham-Klobuchar Amendment, S. 656, 115th Cong. (2017). https://www.congress.gov/amendment/115th-congress/senate-amendment/656/text

[51] National Defense Authorization Act for Fiscal Year 2018, H.R.2810, 115th Cong. (2017). https://www.congress.gov/bill/115th-congress/house-bill/2810/text

© 2017 OSET Institute, Inc. All Rights Reserved

5.4 Supply Chain Risk Reduction

Findings

Our findings on hardware-level vulnerabilities are focused on voting system components. Described in Section 2.4.2, these have substantial supply chain risk, including in manufacturing, but especially in the common situation of voting system operators (local elections offices—LEOs) extending the lifespan of failing voting system components by replacing faulty hardware with replacement parts sourced from an uncontrolled supply chain.

We also note, looking ahead to future voting system technology developed for high assurance, that the higher-level assurance characteristics must be supported by trustworthy hardware, including hardware components with strong provenance, derived from a trustworthy supply chain.

Recommendations

For both these findings, we recommend the following steps toward the creation and operation of a trustworthy, closed supply chain for hardware for all EI cyber assets.

1. Identify applicable proven examples of hardware component supply chain risk management ("SCRM"), particularly for common PC components, that might provide a model for SCRM for voting systems.
2. Identify existing government organizations that have set up and/or that operate an SCRM program and/or a closed supply chain.[52]
3. Designate an agency with requisite regulatory authority to administer and manage the supply chain, in this case, perhaps the DHS.
4. Require an accreditation and certification process for participating vendors to attest to sources of materials, as part of that SCRM program.
5. Develop guidelines whereby states can preserve certification of hardware-modified voting systems only when the replacement hardware components come from an accredited supplier.
6. Develop similar guidelines for original equipment manufacture.

---

[52] Heath Ferry and Van Poindexter, "Supply Chain Risk Management: An Introduction to the Credible Threat," *Defense Acquisition University, accessed August 22, 2017.* http://dau.dodlive.mil/2016/06/13/supply-chain-risk-management-an-introduction-to-the-credible-threat/. SCRM is a process for identifying susceptibilities, vulnerabilities, and threats throughout a supply chain. The DoD uses SCRM to ensure the security of its supply chains.

© 2017 OSET Institute, Inc. All Rights Reserved

6. Summary

In this Briefing, we have applied to U.S. election administration and operations, all of the CI policy of the relevant presidential decision directives ("PDDs"), presidential policy directives ("PPDs") and the CI practice of DHS and other government organizations in their support of CI operators of many different CI sectors. We identified those assets that are either core EI assets, or broader CDI that is operated by or supported by U.S. EOs and their various contractors and service providers.

Starting from CI first principles, we observe seven maxims:

1. Elections are an essential government function necessary for the orderly operation of our government and nation.
2. The core assets of elections are critical for this essential function; therefore, EI is CI.
3. Elections are fundamental to our national sovereignty, and hence the integrity of our elections is a national security matter, in addition to matters of homeland security and CI protection.
4. The core assets of EI are largely the physical and digital resources related to voters, voting, and ballots.
5. The operators of these core assets are CI operators: specifically, EOs (SEOs and LEOs) and their staffs and in some cases volunteers (*e.g., some poll workers*).
6. CDI also includes all the assets and resources that EOs depend on to execute the election mission: supporting physical and IT assets of EOs; and supporting services of contractors, other service providers, and their service providers in a complete service/supply chain.
7. Required CI protections are broad and decentralized: including all the cyber, physical, personnel, and procedural controls that EOs and supporting organizations must apply to core assets or supporting assets.

We note as *beyond the scope* of this Briefing, those assets that comprise a *broader* Democracy Infrastructure Ecosystem, where primary asset owners are *not* government organizations, and yet play important roles in the election process, outside of the administration and operations of U.S. elections. Though outside the full range of CDI targets for election disruption, these other assets and organizations may be targets as well. These targets are *not* CI in the sense of the current CI designation: government operated EI as a subsector of the existing multi-state CI sector. However, attacks on these targets may nevertheless be attacks on national sovereignty, or otherwise a national security matter, based on doctrines or policies outside traditional CI policy. Such broader doctrines or policies are beyond the scope of this Briefing and the Institute.

Based on the above scope, and the above reasoning from first principles, we've provided extensive background, definition, and examples of core EI assets; CDI more broadly; and

typical U.S. election practices, roles, and responsibilities. A large portion of the background presented is analysis of the sources of technical risk to EI, including risks to hardware, software, system integrity, data integrity, and other technical security properties of EI.

We've also provided background on the nature of current challenges, technical and otherwise, to containing these risks, together with current activities to mitigate these challenges.

We've also provided background and supporting references for the nature of the CI designation as applied to elections, and the promise of several activities for CI sector formation activities.

One essential finding in this background is that CI designation is *not* strictly needed for the various activities now underway as CI sector formation, though designation may or may not have helped with motivation or prioritization of efforts on those organizations involved.

Based on these background descriptions, our situation assessment yielded an essential observation and four areas of findings and recommendations. An essential observation is that EI and CDI are both very weak considered in the context of nation-state adversaries with proven desire to disrupt our nation's operations, including elections, and advanced capabilities to do so. Core EI assets were *not* designed as national security assets, or to be operated with CI protections that are typical of other CI sectors. CDI includes many supporting assets, services, and organizations that have never operated or protected CI, and have never operated in an environment with national security threats.

Based on our situation assessment, we presented these four areas of findings and recommendations:

1. There are several organizations and formative activities that are currently underway, including ISAOs, EAC and DHS as co-SSAs and conveners, and DHS cybersecurity outreach and assistance to EOs. All these and others should be accelerated, because they are essential to support both operations as a typical CI sector, and also what we call "*CDI uplift*": the development of new capacity and additional resources for EOs to function as fully functional CI operators.
2. Among these current activities are several technical and procedural security assessment and remediation activities being conducted by EOs, particularly with a focus on cyber risk remediation. These are all essential short-term measures that should be accelerated, though there are substantial challenges given the diversity between states, the large number of local elections organizations, and the hitherto typically low level of resources devoted to elections administration and operation.
3. One of the risks that cannot be contained with short-term security practices improvement is the risk to elections from election machinery that is manufactured with hardware parts from an unsecured global supply chain, and, worse, is maintained by LEOs with replacement parts with no source control. Therefore, we recommend the use of proven SCRM methods to election technology. The benefits would be not only in

quantifying and containing current risks, but also in creating a trustworthy hardware substrate required to support our fourth area of recommendation, immediately below.

4. Though required for risk reduction, these short-term tactical measures are insufficient. Much of the technical EI currently in use has foundational weaknesses than cannot be remediated, which we discussed at length in Section 2.4. Further, these structural weaknesses in election technology also have the effect of requiring significant CDI and efforts to contain risks that are typical of commodity computing, but antithetical to CI operation of national security assets.

   Therefore, we recommend the acceleration of existing efforts in developing innovative election technology, particularly those that apply security design and implementation methods already proven in IT for national security systems. There are half a dozen such election infrastructure innovation research and development projects underway around the nation today. These projects will produce public technology that can be adopted, adapted, and deployed by commercial vendors or jurisdictions themselves to produce higher integrity, lower cost systems that are more verifiable, accurate, secure, and transparent in composition than anything available today. Those projects need proper funding to be finished and made available as soon as is practical.

The integrity of our electoral process is at risk, with clear and present dangers from proven adversaries. Currently, these risks are not contained using the methods typical of CI and of national security. We believe that by recognizing the current threat and risk environment, and shifting to a *national security perspective* and *mindset*, the broad range of election stakeholders can make rapid progress toward reducing risk, both short-term tactical reduction – *the proverbial low-hanging fruit* – as well as longer-term structural changes.

In four essential areas, with several specific recommendations, individual stakeholders can continue existing or nascent activities in risk reduction. For rapid progress to be possible, however, substantial acceleration will need to be enabled.

In all these areas of activity noted in this Briefing, the methods have been proven in prior use. The challenge ahead is to apply these methods, proven in other areas in CI protection and national security, to both elections administration and elections operation.

© 2017 OSET Institute, Inc. All Rights Reserved

Citations

1. Bergmann, Max and Carolyn Kenney. "War by Other Means." *Center for American Progress*. June 6, 2017. www.americanprogress.org/issues/security/reports/2017/06/06/433345/war-by-other-means/. Bergmann and Kenney explain how Russia and other nation-states have used disinformation campaigns to sway American public opinion and destabilize the U.S. The article focuses on the increased effectiveness of these disinformation campaigns on social media.

2. Breitenbach, Sarah. "Aging Voting Machines Cost Local, State Governments." *The PEW Charitable Trust*. March 2, 2016. www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2016/03/02/aging-voting-machines-cost-local-state-governments. Breitenbach explains how paperless voting systems are not only considered to be less secure than paper voting systems, but they can also be costlier for counties.

3. "Checklist for Securing Voter Registration Data." *Election Assistance Commission*. www.eac.gov/assets/1/28/Checklist_Securing_VR_Data_FINAL_5.19.16.pdf. This EAC checklist outlines basic security measures for voter registration data, and provides additional sources for improving the security of VRDBs.

4. "Computer Security Resource Center National Vulnerability Database." *National Institute of Standards and Technology*. nvd.nist.gov/vuln/search/results?adv_search=true&form_type=advanced&cpe_version=cpe:/o:microsoft:windows_2003_server. The National Vulnerability Database (NVD) provides a list of CVEs for operating systems. This specific search shows CVEs for windows operating systems, including those our current voting systems use.

5. "Critical Infrastructure Sector Partnerships." *Department of Homeland Security*. www.dhs.gov/critical-infrastructure-sector-partnerships. This DHS page explains how sector partnerships for CI function. While EI differs from other sectors in that it is largely within the public sector, the same framework used for other CI sectors will apply to EI.

6. "EAC Meeting Moves Election Cybersecurity Protections Forward." *Elections Assistance Commission*. July 27, 2017. www.eac.gov/news/2017/07/27/eac-meeting-moves-election-cybersecurity-protections-forward/. This EAC press release summarizes improvements in information sharing within the EI and how the sector will be managed. The release shows the EI sector is organizing and emphasizing the EAC's role in that process.

7. Ferry, Heath and Van Poindexter. "Supply Chain Risk Management: An Introduction to the Credible Threat." *Defense Acquisition University*. dau.dodlive.mil/2016/06/13/supply-chain-risk-management-an-introduction-to-the-credible-threat/. Heath and Poindexter's article explains how SCRM functions and why it is important.

8. Fessler, Pam. "State And Local Officials Wary Of Federal Government's Election Security Efforts." *National Public Radio*. April 5, 2017. www.npr.org/2017/04/05/522732036/state-and-local-officials-wary-of-federal-governments-election-security-efforts. This NPR story examines EOs' concerns about DHS's choice to designate EI as CI. The source provides evidence that EOs are concerned that designation will lead to federal regulation of elections and that it does not provide for a response to attacks.

9. "Framework for Improving Critical Infrastructure Cybersecurity." *National Institute of Standards and Technology*. January 10, 2017. www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf. This page references the NIST Framework for Improving Critical Infrastructure. The framework outlines different ways that CI operators can try to improve the cybersecurity of their systems. This source helps to provide examples of short-term fixes for EI, as well as a resource for those who seek more information about what actions to take to improve the cybersecurity of CI.

10. "H.R.1562 - SAFE Act." *congress.gov*. www.congress.gov/bill/115th-congress/house-bill/1562/all-actions. Congress.gov is a website that provides a place to view congressional bills. It tracks the bill's progress through Congress as well as showing its text and other relevant information. This specific page shows HR 1562 and the relevant text regarding the bill's intention of permanently legislating EI as CI. The site illustrates why some might fear that DHS's designation might lead to a permanent designation from Congress.

11. Lindeman, Mark and Philip B. Stark. "A Gentle Introduction to Risk-limiting Audits." *IEEE Security and Privacy*. March 16, 2012. www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf. Mr. Lindeman and Mr. Stark's work offers an explanation of how risk-limiting audits work and why they are important. The article offers a way for interested readers to learn more about RLAs.

12. Tim Meko, Denise Lu, Lazaro Gamio. "How Trump won the presidency with razor-thin margins in swing states." *The Washington Post*. November 11, 2016. www.washingtonpost.com/graphics/politics/2016-election/swing-state-margins/. This article analyzes the Electoral College and popular vote results of the 2016 presidential election. It explains how thin victories in valuable swing-states translated into a victory in the Electoral College. The article helps to make the point that only targeted attacks, not widespread attacks, are necessary to derail an election, and such attacks need only change a small number of votes to change a relatively close election.

13. Obama, Barack. "Presidential Policy Directive—Critical Infrastructure Security and Resilience." *The White House President Barack Obama*. Feb. 12, 2013. obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. The Obama White House Archives provide a record of all the presidential policy directives issued by former President Barack Obama. This PPD-21 established policy regarding CI security and clarified CI functions and responsibilities.

14. Newman, Lily. "Securing Elections Remains Surprisingly Controversial." *Wired*. July 13, 2017. www.wired.com/story/election-security-critical-infrastructure/. Newman's article seeks to explain why the designation of elections as CI is controversial. It examines both sides of the debate, providing some of the common concerns of EOs and the rationales for DHS's actions. The article provides evidence that some EOs believe that the designation will lead to no change in DHS assistance.

15. Norden, Lawrence and Christopher Famighetti. "America's Voting Machines at Risk." *Brennan Center for Justice*. September 15, 2015. www.brennancenter.org/publication/americas-voting-machines-risk. Nordon and Famighetti's analyze the predicament of current voting machines and offers recommendations to improve them. They review case studies of counties and technologies that offer potential for improvement.

16. Norden, Lawrence and Ian Vandewalker. "Securing Elections from Foreign Interference." *Brennan Center for Justice*. June 29, 2017. www.brennancenter.org/sites/default/files/publications/Securing_Elections_From_Foreign_Interference_0.pdf. Norden and Vandewalker's extensive and well-researched white paper provides the issues and challenges facing the American election system, specifically voting machines and VRDBs. The Brennan Center offers an assessment of the current protections and vulnerabilities of voting machines and VRDBs, along with recommendations for remediating them. OSET has written a more in-depth analysis of the Norden and Vandewalker's work in a three part blog series, which can be found here.

17. Norden, Lawrence. "Opinion: Protect Our Voting Machines From Hackers." *NBC News*. August 12, 2016. www.nbcnews.com/news/us-news/opinion-protect-our-voting-machines-hackers-n628441. Norden's analyzes the integrity of America's current election system and offers ideas as to what kinds of improvements can be made. Importantly, Norden explains some of the problems with antiquated operating systems such as Windows XP.

18. Rockwell, Mark. "Critical infrastructure designation for voting goes too far, says state official." *FCW*. September 13, 2016. fcw.com/articles/2016/09/13/election-hack-hearing-rockwell.aspx. Rockwell's article shares EOs concerns, including federal overreach, and concomitant unconstitutionality, with the designation of EI as CI.

19. Root, Danielle and Liz Kennedy. "9 Solutions to Secure America's Elections." *Center for American Progress*. August 16, 2017. www.americanprogress.org/issues/democracy/reports/2017/08/16/437390/9-solutions-secure-americas-elections/. Root and Kennedy's *Center for American Progress* white paper outlines a list of solutions to improve the integrity of America's elections. Many of the solutions proposed in the white paper are reiterated in this Briefing, and reflect the consensus of the American election community. The OSET Institute has written a more in-depth analysis of Root and Kennedy's work, which can be found here.

20. Schlesinger, Robert. "Hack the Vote: a reminder of how insecure our ballots can be." *U.S. News & World Report*. July 31, 2017. www.usnews.com/opinion/thomas-jefferson-street/articles/2017-07-31/hackers-demonstrate-how-vulnerable-voting-machines-are. Demonstrations by hackers show the ease with which a technically capable adversary can compromise the integrity of a voting machine.

21. "Securing Elections as Critical Infrastructure." *National Association of Secretaries of State*. Accessed August 17, 2017. www.nass.org/index.php/nass-initiatives/nass-cybersecurity-elections-critical-infrastructure/. NASS rejects the designation of EI as CI. The organization of secretaries of state argues that the scope of the CI designation remains unclear.

22. "Security and Privacy Controls for Federal Information Systems and Organizations." *National Institute of Standards and Technology*. April 2013. nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. This NIST document provides cybersecurity guidelines for federal information systems and offers analysis of specific security systems and methods. The document provides concrete examples of recommended actions that EOs and policy makers should take in the short-term to improve the security of elections.

23. von Spakovsky, Hans. "DHS' Election Power-Grab Raises Huge Questions and Red Flags." *The Heritage Foundation*. January 13, 2017. www.heritage.org/election-integrity/commentary/dhs-election-power-grab-raises-huge-questions-and-red-flags. von Spakovsky offers a critical view of the designation of EI as CI. He relies heavily on EAC Commissioner Christy McCormick's views of the designation. The article raises the question of the necessity of the designation, and the fact that many state EOs disapprove of the designation.

24. von Spakovsky, Hans. "Why Does DHS Want to Designate Election Booths 'Critical Infrastructure?' *The Heritage Foundation*. August 17, 2016. www.heritage.org/election-integrity/commentary/why-does-dhs-want-designate-election-booths-critical-infrastructure. von Spakovsky is critical of the CI designation. The designation would allow public officials to play a malicious role in elections. The article provides a voice to concerns that the designation is unnecessary and that DHS's assistance, while "voluntary," will, in effect, be compulsory.

25. Starks, Tim. "DHS labels elections as 'critical infrastructure." *Politico*, January 6, 2017. www.politico.com/story/2017/01/elections-critical-infrastructure-homeland-security-233304. Starks describes the designation of EI as CI and the criticisms that come with the designation. The article references Georgia Secretary of State Brian Kemp's disagreement with the designation.

26. "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector." *Department of Homeland Security*. January 6, 2017. www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical. Former Secretary of Homeland Security Jeh Johnson's statement regarding the designation of EI as CI.

27. "The Constitution of the United States: A Transcription." *National Archives*. June 26, 2017. www.archives.gov/founding-docs/constitution-transcript. This website offers a full transcript of the U.S. Constitution. Certain articles and amendments to the Constitution describe the laws regarding federal elections and they are referenced in this Briefing.

28. "U.S. Election Systems as Critical Infrastructure." *Election Assistance Commission*. www.eac.gov/assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf. This briefing, published by the EAC, explains how CI sectors function with a focus on information sharing. It explains how Co-SSAs, GCCs, ISAOs and ISACs work. This source is useful for its explanation of these important terms of the art and for its collection of relevant information to how the critical infrastructure designation will likely affect EI.

29. "What Is Critical Infrastructure?" *Department of Homeland Security*. July 12, 2017. www.dhs.gov/what-critical-infrastructure. This page is part of the official website for the Department of Homeland Security. It explains, in the eyes of the department, the definition of critical infrastructure, which this Briefing adopts.

30. Wolff, Josephine. "Great, Now Malware Can Jump the 'Air Gap' Between Computers." *Slate*. December 3, 2013. www.slate.com/blogs/future_tense/2013/12/03/researchers_michael_hanspach_michael_goetz_prove_malware_can_jump_air_gap.html. Wolff's article explains how non-networked ("air-gapped) computer systems can be compromised and manipulated by skilled adversaries. The article references the Stuxnet worm, that wriggled its way into the air-gapped industrial computer systems that commanded and controlled the flow and speed of thousands of uranium gas centrifuges at Iran's Netanz nuclear enrichment facility.

31. Windrem, Robert, William M. Arkin, and Ken Dilanian. "Russians Hacked Two U.S. Voter Databases, Officials Say." *NBC News*. August 30, 2016. www.nbcnews.com/news/us-news/russians-hacked-two-u-s-voter-databases-say-officials-n639551. This article reports Russian attempts to manipulate U.S. VRDBs. These attempts highlight both the vulnerability and importance of VRDBs to the integrity of American elections.

32. "2016 Election Administration & Voting Survey." *Election Assistance Committee*. Accessed August 22, 2017. www.eac.gov/research-and-data/election-administration-voting-survey/. This page offers the 2016 Election Administration & Voting Survey conducted by EAC.

© 2017 OSET Institute, Inc. All Rights Reserved

Glossary of Terms

The definitions in this Glossary for terms appearing in this Briefing were derived from language enacted in federal laws and/or included in National Plans, including:

- Homeland Security Act of 2002
- USA PATRIOT Act of 2001
- 2013 NIPP (*heavily relied upon for this Briefing*)
- Presidential Policy Directive #8 (PPD-8), National Preparedness
- Presidential Policy Directive #21 (PPD-21), Critical Infrastructure Security and Resilience

Additional definitions come from the DHS Lexicon. The source for each entry below follows each definition. Terms appearing in the Briefing that appear below have the meaning as defined hereunder unless otherwise attributed or explained by footnote.

Asset. A person, structure, facility, information, material, or process that has value. (*Source: DHS Lexicon, 2010*)

Business Continuity. Activities performed by an organization to ensure that during and after a disaster the organization's essential functions are maintained uninterrupted, or are resumed with minimal disruption. (*Source: 2013 NIPP*)

Consequence. The effect of an event, incident, or occurrence, including the number of deaths, injuries, and other human health impacts along with economic impacts both direct and indirect and other negative outcomes to society. (*Source: DHS Lexicon, 2010*)

Control Systems. Computer-based systems used within many infrastructure and industries to monitor and control sensitive processes and physical functions. These systems typically collect measurement and operational data from the field, process and display the information, and relay control commands to local or remote equipment or human-machine interfaces (*operators*). Examples of types of control systems include SCADA systems, Process Control Systems, and Distributed Control Systems. (*Source: 2013 NIPP*)

Critical Infrastructure. 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. (*Source: §1016(e) of the USA Patriot Act of 2001 (42 U.S.C. §5195c(e))*

Critical Infrastructure Community. Critical infrastructure owners and operators, both public and private; Federal departments and agencies; regional entities; SLTT governments; and other organizations from the private and nonprofit sectors with a role in securing and strengthening the resilience of the Nation's critical infrastructure and/or promoting practices and ideas for doing so. (*Source: 2013 NIPP*)

Critical Infrastructure Information (CII). Information that is not customarily in the public domain and is related to the security of critical infrastructure or protected systems. CII consists of records and information concerning any of the following:

- Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law; harms the interstate commerce of the United States; or threatens public health or safety.
- The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation, risk management planning, or risk audit.
- Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, insurance, or continuity, to the extent that it is related to such interference, compromise, or incapacitation. (*Source: CII Act of 2002, 6 U.S.C. § 131*)

Critical Infrastructure Owners and Operators. Those entities responsible for day-to-day operation and investment of a particular critical infrastructure entity. (*Source: 2013 NIPP*)

Critical Infrastructure Partner. Those Federal and SLTT governmental entities, public and private sector owners and opera- tors and representative organizations, regional organizations and coalitions, academic and professional entities, and certain not-for-pro t and private volunteer organizations that share responsibility for securing and strengthening the resilience of the Nation's critical infrastructure. (*Source: 2013 NIPP*)

Critical Infrastructure Partnership Advisory Council (CIPAC). Council established by DHS under 6 U.S.C. §451 to facilitate effective interaction and coordination of critical infrastructure activities among the Federal Government; the private sector; and SLTT governments. (*Source: CIPAC Charter*)

Critical Infrastructure Risk Management Framework. A planning and decision-making framework that outlines the process for setting goals and objectives, identifying infrastructure, assessing risks, implementing risk management activities, and measuring effectiveness to inform continuous improvement in critical infrastructure security and resilience. (*Source: 2013 NIPP*)

Cybersecurity. The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability; includes protection and restoration, when needed, of information networks and wire-line, wireless, satellite, public safety answering points, and 911 communications systems and control systems. (*Source: 2013 NIPP*)

© 2017 OSET Institute, Inc. All Rights Reserved

Cyber System. Any combination of facilities, equipment, personnel, procedures, and communications integrated to pro- vide cyber services; examples include business systems, control systems, and access control systems. (*Source: 2013 NIPP*)

Dependency. The one-directional reliance of an asset, system, network, or collection thereof—within or across sectors—on an input, interaction, or other requirement from other sources to function properly. (*Source: 2013 NIPP*)

Executive Order 13636. Executive Order that calls for the Federal Government to closely coordinate with critical infrastructure owners and operators to improve cybersecurity information sharing; develop a technology-neutral cybersecurity framework; and promote and incentivize the adoption of strong cybersecurity practices. (*Executive Order 13636, Improving Critical Infrastructure Cybersecurity, February 2013, Executive Order 13636, www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf*)

Emergency Support Functions (ESF). The primary, but not exclusive, Federal coordinating structures for building, sustaining, and delivering the response core capabilities. ESFs are vital for responding to Stafford Act incidents but also may be used for other incidents. (*Source: National Response Framework, 2013*)

Federal Departments and Agencies. Any authority of the United States that is an "agency" under 44 U.S.C. §3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. §3502(5). (*Source: PPD-21, 2013*)

Incident. An occurrence, caused by either human action or natural phenomenon, that may cause harm and require action, which can include major disasters, emergencies, terrorist attacks, terrorist threats, attacks, cyber failure or accident, and other occurrences requiring an emergency response. (*Source: DHS Lexicon, 2010*)

Information Sharing and Analysis Centers (ISACs). Operational entities formed by critical infrastructure owners and operators to gather, analyze, appropriately sanitize, and disseminate intelligence and information related to critical infrastructure. ISACs provide 24x7 threat warning and incident reporting capabilities and have the ability to reach and share information within their sectors, between sectors, and among government and private sector stakeholders. (*Source: PDD-63, 1998*)

Information Sharing and Analysis Organization. Any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of:

(a) Gathering and analyzing critical infrastructure information to better understand security problems and interdependencies related to critical infrastructure and protected systems, so as to ensure the availability, integrity, and reliability thereof;

(b) Communicating or disclosing critical infrastructure information to help prevent, detect, mitigate, or recover from the effects of an interference, compromise, or an incapacitation problem related to critical infrastructure or protected systems; and

(c) Voluntarily disseminating critical infrastructure information to its members, State,

local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (a) and (b). (*Source: Homeland Security Act of 2002, 6 U.S.C. § 131*)

Infrastructure. The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole; consistent with the definition in the Homeland Security Act, infrastructure includes physical, cyber, and/or human elements. (*Source: DHS Lexicon, 2010*)

Interdependency. Mutually reliant relationship between entities (objects, individuals, or groups); the degree of interdependency does not need to be equal in both directions. (*Source: DHS Lexicon, 2010*)

Joint Terrorism Task Forces (JTTFs). FBI-led local task forces of highly trained Federal, State, and local law enforcement and intelligence agencies established to collect terrorism-related intelligence and conduct investigations. The local FBI JTTFs receive and resolve reports of possible terrorism activity submitted by private industry partners and the public. (*Source: FBI Website, www.fbi.gov*)

Mitigation. Capabilities necessary to reduce loss of life and property by lessening the impact of disasters. (*Source: PPD-8, 2011*)

National Cyber Investigative Joint Task Force. The multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations, with representation from Federal agencies, including DHS, and from State, local, and international law enforcement partners. (*Source: FBI Website, www.fbi.gov*)

National Cybersecurity and Communications Integration Center. The national cyber critical infrastructure center, as designated by the Secretary of Homeland Security, which secures Federal civilian agencies in cyberspace; provides support and expertise to private sector partners and SLTT entities; coordinates with international partners; and coordinates the Federal Government mitigation and recovery efforts for significant cyber and communications incidents. (*Source: DHS Website, www.dhs.gov*)

National Infrastructure Coordinating Center. The national physical critical infrastructure center, as designated by the Secretary of Homeland Security, which coordinates a national network dedicated to the security and resilience of critical infrastructure of the United States by providing 24/7 situational awareness through information sharing, and fostering a unity of effort. (*Source: DHS Website, www.dhs.gov*)

National Operations Center. A DHS 24x7 operations center responsible for providing real-time situational awareness and monitoring of the homeland, coordinating incident response activities, and, in conjunction with the Office of Intelligence and Analysis, issuing advisories and bulletins concerning threats to homeland security, as well as specific protective measures. (*Source: DHS Website, www.dhs.gov*)

© 2017 OSET Institute, Inc. All Rights Reserved

National Preparedness. The actions taken to plan, organize, equip, train, and exercise to build and sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the Nation. (*Source: PPD-8, 2011*)

Network. A group of components that share information or interact with each other to perform a function. (*Source: 2013 NIPP*)

Partnership. Close cooperation between parties having common interests in achieving a shared vision. (*Source: 2013 NIPP*)

Presidential Policy Directive 8 (PPD-8). Facilitates an integrated, all-of-Nation approach to national preparedness for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, attacks, pandemics, and catastrophic natural disasters; directs the Federal Government to develop a national preparedness system to build and improve the capabilities necessary to maintain national preparedness across the five mission areas covered in the PPD: prevention, protection, mitigation, response, and recovery. (*Source: PPD-8, 2011*)

Presidential Policy Directive 21 (PPD-21). Aims to clarify roles and responsibilities across the Federal Government and establish a more effective partnership with owners and operators and SLTT entities to enhance the security and resilience of critical infrastructure. (*Source: The White House, Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience, www.whitehouse.gov/the-press-office/2013/02/12/ presidential-policy-directive-critical-infrastructure-security-and-resil, 2013*)

Prevention. Those capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism. (*Source: PPD-8, 2011*)

Protected Critical Infrastructure Information (PCII). All critical infrastructure information that has been properly submitted and validated pursuant to the Critical Infrastructure Information Act and implementing directive; all information submit- ted to the PCII Program Office or designee with an express statement is presumed to be PCII until the PCII Program Office determines otherwise. (*Source: CII Act of 2002, 6 U.S.C. § 131*)

Protection. Those capabilities necessary to secure the homeland against acts of terrorism and manmade or natural disasters. (*Source: PPD-8, 2011*)

Recovery. Those capabilities necessary to assist communities affected by an incident to recover effectively, including, but not limited to, rebuilding infrastructure systems; providing adequate interim and long-term housing for survivors; restoring health, social, and community services; promoting economic development; and restoring natural and cultural resources. (*Source: PPD-8, 2011*)

© 2017 OSET Institute, Inc. All Rights Reserved

Recovery Support Functions (RSF). Coordinating structures for key functional areas of assistance during recovery operations; RSFs support local governments by facilitating problem solving, improving access to resources, and fostering coordination among State and Federal agencies, nongovernmental partners, and stakeholders. (*Source: National Disaster Recovery Framework, 2011*)

Resilience. The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions; includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. (*Source: PPD-21, 2013*)

Response. Capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred. (*Source: PPD-8, 2011*)

Risk. The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. (*Source: DHS Lexicon, 2010*)

Risk-Informed Decision Making. The determination of a course of action predicated on the assessment of risk, the expected impact of that course of action on that risk, and other relevant factors. (*Source: 2013 NIPP*)

Sector. A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society; the *National Plan* addresses 16 critical infrastructure sectors, as identified in PPD-21. (*Source: 2013 NIPP*)

Sector Coordinating Council (SCC). The private sector counterpart to the GCC, these councils are self-organized, self-run, and self-governed organizations that are representative of a spectrum of key stakeholders within a sector; serve as principal entry points for the government to collaborate with each sector for developing and coordinating a wide range of critical infrastructure security and resilience activities and issues. (*Source: 2013 NIPP*)

Sector-Specific Agency (SSA). A federal department or agency designated by PPD-21 with responsibility for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment. (*Source: PPD-21, 2013*)

Sector-Specific Plans (SSP). Planning documents that complement and tailor application of the *National Plan* to the specific characteristics and risk landscape of each critical infrastructure sector; developed by the SSAs in close collaboration with the SCCs and other sector partners. (*Source: Adapted from the 2013 NIPP*)

Secure/Security. Reducing the risk to critical infrastructure by physical means or defensive cyber measures to intrusions, attacks, or the effects of natural or manmade disasters. (*Source: PPD-21, 2013*)

Steady State. The posture for routine, normal, day-to-day operations as contrasted with temporary periods of heightened alert or real-time response to threats or incidents. (*Source: DHS Lexicon, 2010*)

System. Any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose. (*Source: DHS Lexicon, 2010*)

Terrorism. Premeditated threat or act of violence against noncombatant persons, property, and environmental or economic tar- gets to induce fear, intimidate, coerce, or affect a government, the civilian population, or any segment thereof, in furtherance of political, social, ideological, or religious objectives. (*Source: DHS Lexicon, 2010*)

Threat. A natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. (*Source: DHS Lexicon, 2010*)

Threat and Hazard Identification and Risk Assessment (THIRA). A tool that allows a regional, State, or urban area jurisdiction to understand its threats and hazards and how the impacts may vary according to time of occurrence, season, location, and other community factors. This knowledge helps a jurisdiction establish informed and defensible capability targets for prepared- ness. (*Source: www.fema.gov*)

Value Proposition. A statement that outlines the business and national interest in critical infrastructure security and resilience actions and articulates the benefits gained by partners through collaborating in the mechanisms described in the *National Plan*. (*Source: 2013 NIPP*)

Vulnerability. A physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. (*Source: DHS Lexicon, 2010*)

The OSET Institute and TrustTheVote Project are supported by grant making organizations, philanthropists, and individual supporters like you. Financial support of the OSET Institute is tax-deductible (Fed. Tax ID: 20-8743186).

10 Years of dedication to improving election technology integrity

530 Lytton Avenue
2nd Floor
Palo Alto, California 94301 USA
650.600.1450
www.osetfoundation.org