(U) ELECTION INFRASTRUCTURE CYBER RISK CHARACTERIZATION

(U) September 2016

NATIONAL PROTECTION AND PROGRAMS DIRECTORATE

OFFICE OF CYBER AND INFRASTRUCTURE ANALYSIS

/

(U) This page intentionally left blank.

(U) KEY FINDINGS

- **(U//FOUO) The Office of Cyber and Infrastructure Analysis (OCIA) assesses that voter registration databases are vulnerable to cyber intrusions, but in 2016 the likely impacts of such intrusions are generally limited to personally identifiable information being released. From a systemic perspective, voter registration databases are resilient to cyber intrusions because of the diverse systems and security measures surrounding them.**
- **(U//FOUO) OCIA assesses that voter registration databases could be vulnerable to the manipulation of voter data or disruptions to their availability, which may impact voter's ability to vote on Election Day. However, most jurisdictions still rely on paper voter rolls or electronic pollbooks that are not connected in real-time to voter registration databases, limiting the possible impacts in 2016.**
- **(U//FOUO) OCIA assesses that successfully mounting a widespread attack on voting machines, enough to affect a national election, would require a multiyear effort with significant human and information technology resources available only to a nation-state, but the level of effort required would make it nearly impossible to avoid detection. OCIA bases this assessment on the diversity of systems, the need for physical access to compromise nearly all voting machines, and the security and pre-election testing employed by State and local officials.**
- **(U//FOUO) OCIA assesses that smaller-scale manipulation of votes could be accomplished, as has been demonstrated by security researchers with physical access to machines in controlled environments. However, such manipulations would likely not affect the outcome of the election because of existing safeguards in the post-election process, including audits and paper backup systems.**
- **(U//FOUO) OCIA assesses that systems used to tabulate votes on or after Election Day are vulnerable to cyber intrusions, which could undermine public confidence in the election process. The impacts of such intrusions would likely be contained to the manipulation of unofficial Election Night reporting results, which would not impact the outcome of an election but would significantly undermine public confidence in the results.**
- **(U//FOUO) OCIA assesses that the introduction of new technologies into the voting process will increase vulnerabilities to the election system in the future. These technologies include cloud-based information technology infrastructure, electronic pollbooks, ballot-on-demand printers, and online voting systems.**

(U) Contents

(U) Figures

(U) SCOPE

(U) This assessment provides a characterization of the election process and election infrastructure in the United States and identifies potential cyber vulnerabilities. The product was developed by the Office of Cyber and Infrastructure Analysis (OCIA) to support U.S. Department of Homeland Security's (DHS) planning efforts as it considers activities to enhance the security of election infrastructure in the United States. The product is focused on cyber vulnerabilities that could impact the integrity and confidentiality of information on election systems. The analysis does not consider cyber vulnerabilities to nongovernmental-owned or -operated systems used by partisan organizations to drive voter targeting, get out the vote efforts, and other election activities. The analysis was developed on a short timeline to best support efforts in advance of the 2016 election. A more exhaustive analysis of election infrastructure risks is expected to be undertaken following the 2016 election.

(U) This assessment was coordinated with the DHS/Office of Infrastructure Protection and Office of Cybersecurity and Communications, Pacific Northwest National Laboratory, the United States Election Assistance Commission (EAC), and the National Institute of Standards and Technology, and the Executive Director of the National Association of Secretaries of State.

(U) CHARACTERIZATION OF VOTING PROCESS

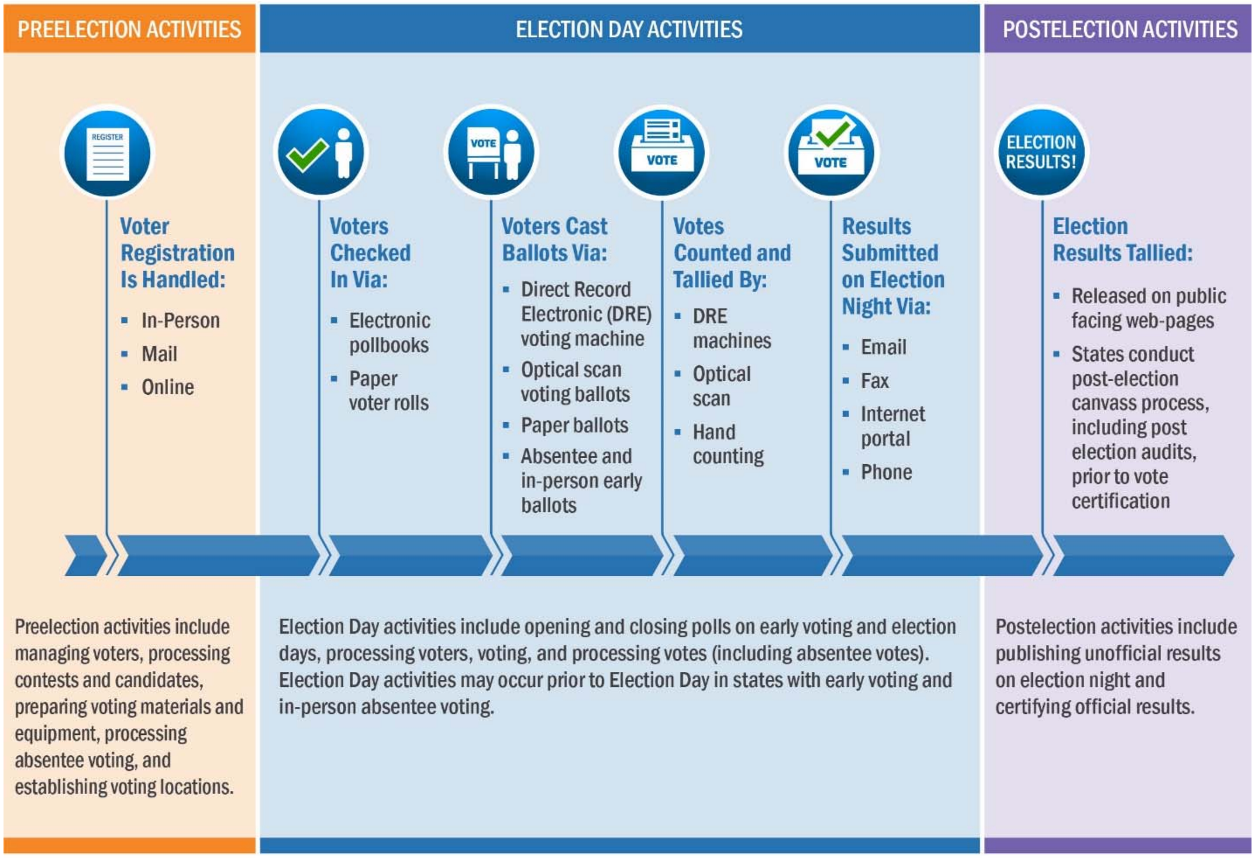
(U) The 2016 Presidential election is scheduled to be held on Tuesday, November 8, 2016. The casting and counting of votes through Election Day are multiple-month processes that include registration of voters, the casting and counting of ballots, announcement of results on election night, and certification at the State and Federal levels of the results and the victor. Elections are managed and administered at the State and local levels, although numerous Federal agencies have roles in the process.

(U) States must design their processes to comply with the U.S. Constitution and Federal law; however, States are granted the authority to develop their own processes and procedures to manage elections and determine voters eligible to participate in elections. Laws governing U.S. elections date back to Article 1 of the Constitution, which gave States the responsibility of overseeing Federal elections. This has resulted in 51 unique election workflows, although some commonalities exist across the States and the District of Columbia.

(U) The election process comprises three general phases: preelection, Election Day, and postelection activities (figure1).

- (U) Preelection activities include managing voters, processing contests and candidates, preparing voting materials and equipment, processing absentee voting, and establishing voting locations.
- (U) Election Day activities include opening and closing polls on early voting and election days, processing voters, voting, and processing votes (including absentee votes).
- (U) Postelection activities include publishing unofficial results and certifying official results.

(U) The contents of this figure are UNCLASSIFIED.



PREELECTION ACTIVITIES

ELECTION DAY ACTIVITIES

POSTELECTION ACTIVITIES

Voter Registration Is Handled:

- In-Person
- Mail
- Online

Voters Checked In Via:

- Electronic pollbooks
- Paper voter rolls

Voters Cast Ballots Via:

- Direct Record Electronic (DRE) voting machine
- Optical scan voting ballots
- Paper ballots
- Absentee and in-person early ballots

Votes Counted and Tallied By:

- DRE machines
- Optical scan
- Hand counting

Results Submitted on Election Night Via:

- Email
- Fax
- Internet portal
- Phone

Election Results Tallied:

- Released on public facing web-pages
- States conduct post-election canvass process, including post election audits, prior to vote certification

Preelection activities include managing voters, processing contests and candidates, preparing voting materials and equipment, processing absentee voting, and establishing voting locations.

Election Day activities include opening and closing polls on early voting and election days, processing voters, voting, and processing votes (including absentee votes). Election Day activities may occur prior to Election Day in states with early voting and in-person absentee voting.

Postelection activities include publishing unofficial results on election night and certifying official results.

(U) FIGURE 1—ELECTION PROCESS PHASES

(U) PREELECTION ACTIVITIES

(U) Before Election Day, officials focus on logistic concerns to enable the successful execution of the election. Managing voters is a significant responsibility in this phase, centered on the voter registration process. Election officials are responsible for managing processes to add voters to the rolls or edit their records, as well as conduct processes to ensure the integrity of voter rolls (e.g., remove ineligible voters from voter registration lists or identify voters who may have moved out of their district). The Help America Vote Act of 2002 (HAVA) required each State to have a computerized voter registration database.[1] States manage these databases in three ways:

1. (U) Top-down systems owned or operated by the State.
2. (U) Bottom-up systems for which localities are responsible for maintaining voter rolls.
3. (U) Hybrid systems in which management responsibilities are shared between States and localities.

(U) In advance of elections, officials must also process contests and candidates; candidates for office are required to meet certain criteria and reporting requirements. Election officials perform a number of tasks including finding and securing polling places, recruiting poll workers, and preparing voting materials and equipment by producing election materials that meet accessibility requirements and other criteria to make races competitive (e.g., alternate the order in which candidates are listed on ballots). Officials must also perform absentee voting processing so that

[1] (U) H.R. 3295 – Help America Vote Act of 2002. Public Law 107-252. https://www.congress.gov/bill/107th-congress/house-bill/3295. Accessed 23 August 2016.

voters who cannot vote in person on Election Day are enabled to cast their ballots. Finally, voting locations are established to enable in-person voting (during early voting and on Election Day).

(U) VOTING ACTIVITIES

(U) Not all voting activities occur on Election Day. In 37 States and the District of Columbia, any qualified voter may cast a ballot in person before Election Day.[2] During early voting and on Election Day, officials are responsible for opening and closing polling locations and processing voters to ensure they are eligible and voting in the proper location. HAVA requires that voters whose names are not shown on voter rolls (or if their eligibility is challenged at the polling place) are provided with a provisional ballot.

(U) After voters have been processed and deemed eligible, they are allowed to vote. Three primary means exist in the United States by which voters cast ballots—direct record electronic (DRE) voting machines, optical scan voting ballots, and paper ballots. DRE voting machines are voting machines where voting data is captured directly into electronic memory. DRE voting machines may or may not come equipped with a voter verified paper audit trail (VVPAT) feature, a machine feature that provides a printout, verified by voters, to ensure their votes are correctly captured. Optical scan systems use machine-readable paper ballots that are marked by voters, whereas paper ballots are not intended to be machine-readable. Three states (Colorado, Oregon, and Washington) are the exception to these three means, and allow all voters to cast their ballots via postal mail.[3] Ballots submitted via postal mail are normally then counted and tallied using optical scanning machines.

(U) POSTELECTION ACTIVITIES

(U) After the polls close on election night, officials focus on two primary activities: publishing unofficial results and certifying official results. The news media and voting public rely on unofficial election results to determine who the victor is after an election, as these results become available on election night. However, these results are unofficial, and most likely do not include the counts of provisional ballots.

(U) States use canvassing processes to certify the official results of the election. Although election night reporting is focused on providing results as quickly as possible, canvassing processes are focused on ensuring every valid vote is included in election totals. In 29 States and the District of Columbia, the canvas process includes a postelection audit to compare a sample of voting records against the reported results to verify systems accurately recorded and counted votes.[4] In the remaining 21 voting jurisdictions, audits of some nature may be conducted based on specific circumstances.[5]

(U) ANALYSIS OF ELECTION SYSTEM RISKS

(U) ELECTION INFRASTRUCTURE

(U) Elections involve a diverse set of assets, systems, and networks, both public and private. Based on analysis of each phase of the election process, OCIA assesses that the following election infrastructure represent the assets, systems, and networks most critical to the security and resilience of the election process:

- (U) Storage facilities, which may be located on public or private property that may be used to store election and voting system infrastructure before Election Day.

[2] (U) National Conference of State Legislatures, "Absentee and Early Voting" May 26, 2016, http://www.ncsl.org/research/elections-and-campaigns/absentee-and-early-voting.aspx. Accessed 23 August 2016.

[3] (U) National Conference of State Legislatures, "All-Mail Elections (aka Vote-By-Mail)," March 8, 2016, http://www.ncsl.org/research/elections-and-campaigns/all-mail-elections.aspx. Accessed 23 August 2016.

[4] (U) "Post-Election Audits," National Conference of State Legislatures, June 14, 2016. http://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx. Accessed 23 August 2016.

[5] (U) bid.

- (U) Polling places (including early voting locations), which may be physically located on public or private property, and may face physical and cyber threats to their normal operations on Election Day.
- (U) Centralized vote tabulation locations, which are used by some States and localities to process absentee and Election Day voting materials.
- (U) Information technology infrastructure and systems used to maintain voter registration databases.
- (U) Voting systems and associated infrastructure, which are generally held in storage but are located at polling places during early voting and on Election Day.
- (U) Information technology infrastructure and systems used to manage elections, which may include systems that count, audit, and display election results on election night on behalf of State governments, as well as for postelection reporting used to certify and validate results.

(U) PREELECTION ACTIVITIES

(U//FOUO) The Office of Cyber and Infrastructure Analysis (OCIA) assesses that voter registration databases are vulnerable to cyber intrusions, but in 2016 the likely impacts of such intrusions are generally limited to personally identifiable information being released. From a systemic perspective, voter registration databases are resilient to cyber intrusions because of the diverse systems and security measures surrounding them.

(U) Compromises of voter registration databases have resulted in the potential release of personally identifiable information, but not the modification of records. The exposure of voters' information does not threaten the integrity of the election process, but could undermine confidence in the system.

- (U) In June 2016, the Arizona voter registration system was taken offline after the Federal Bureau of Investigation warned it may have been compromised, although no evidence of a compromise was ultimately found.[6]
- (U) In November 2012, personal information for 1,200 voters in Chicago was inadvertently exposed online for a week.[7]
- (U) In August 2011, Maine's voter registration database was breached because of a malware infection at a town clerk's office. No personal information was believed to be compromised during the breach.[8]

(U//FOUO) From a national perspective, voter registration databases are resilient to widespread cyber intrusions because of the diversity of systems and security measures surrounding them. Diversity is a recommended strategy for secure and resilient information technology security architecture.[9]

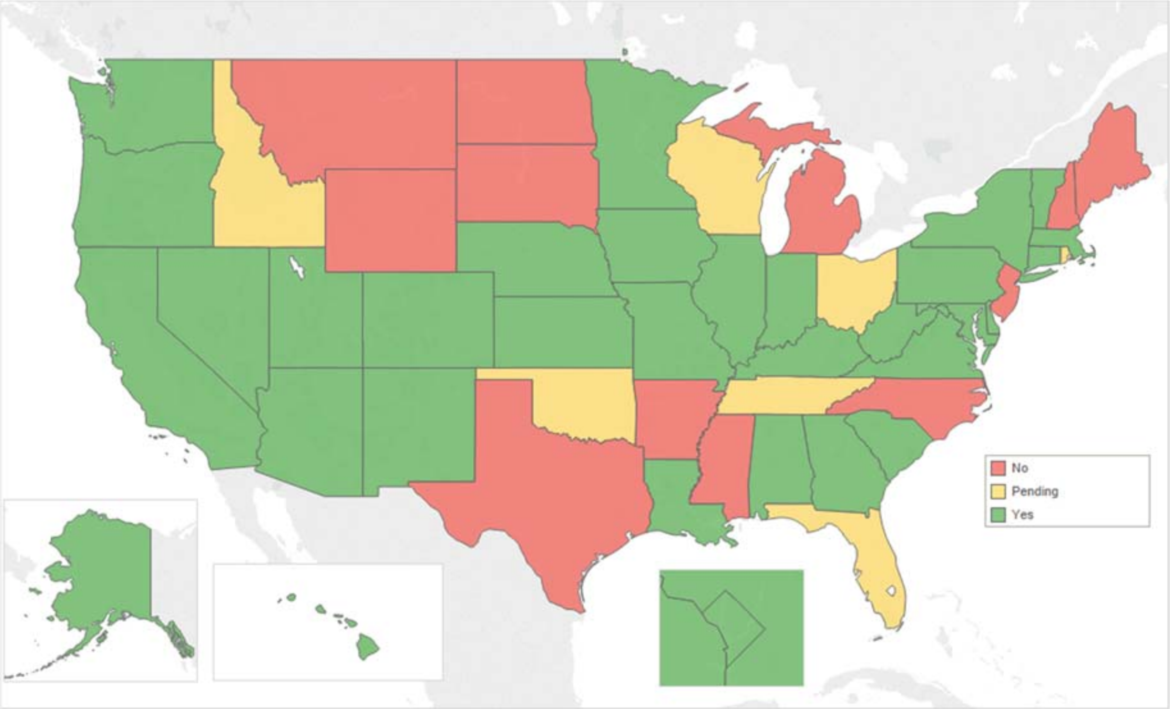
- (U//FOUO) Discussions with State Election Officials, the U.S. Election Assistance Commission, and subject matter experts indicate that each State's voter registration system and associated information technology system is unique and customized to the State's processes and procedures for maintaining the current list of registered, eligible voters.

(U//FOUO) Online voter registration systems provide an additional point of vulnerability to enable cyber actors to gain illicit access to voter registration databases. These portals have been exploited by hackers in the past to gain illicit access to voter information.

[6] (U) Pam Fessler, "Hacking an Election: Why It's Not As Far-Fetched As You Might Think," National Public Radio, August 1, 2016, http://www.npr.org/2016/08/01/488264073/hacking-an-election-why-its-not-as-far-fetched-as-you-might-think. Accessed 23 August 2016.
[7] (U) John Byrne and Hal Dardick, "Chicago election site exposed personal information," Chicago Tribune, November 13, 2012, http://www.chicagotribune.com/news/local/breaking/chi-chicago-election-site-exposed-personal-information-20121113-story.html. Accessed 23 August 2016.
[8] (U) Eric Russell, "Voter database breach came from Millinocket, no information compromised," Bangor Daily News, August 25, 2011, http://bangordailynews.com/2011/08/25/politics/voter-database-breach-came-from-millinocket-no-information-compromised.
[9] (U) Harriet G. Goldman, "Building Secure, Resilient Architectures for Cyber Mission Assurance," MITRE Corporation, 2010, page 9.

- (U) Thirty-one States and the District of Columbia offer online voter registration according to data from the National Council of State Legislatures (figure 2).[10] These systems may also have connections to other State databases, such as motor vehicle records.
- (U) In July 2016, the Illinois online voter registration system was hacked, leading the State to shut down the system temporarily. Voter records were potentially exposed to hackers in the attack, but State authorities said they believed hackers did not add, edit, or delete any records.[11]
- (U//FOUO) Some States with online voter registration employ safeguards to segregate the online system from the State voter registration database.[12]

(U) The contents of this figure are UNCLASSIFIED.



(U) FIGURE 2—ONLINE VOTER REGISTRATION IN THE UNITED STATES[13]

(U//FOUO) OCIA assesses that voter registration databases could be vulnerable to the manipulation of voter data or disruptions to their availability, which may impact voter's ability to vote on Election Day. However, most jurisdictions still rely on paper voter rolls or electronic pollbooks that are not connected in real-time to voter registration databases, limiting the possible impacts in 2016.

(U) Top-down voter registration databases are the most common type of voter registration system used by States. The failure or disruption of a single, top-down voter registration system on Election Day that is used as a real-time feed by local governments to determine the eligibility of voters to vote, could reduce public confidence in the voting system using that real-time feed.

[10] (U) National Conference of State Legislatures, "Online Voter Registration," June 14, 2016, http://www.ncsl.org/research/elections-and-campaigns/electronic-or-online-voter-registration.aspx.

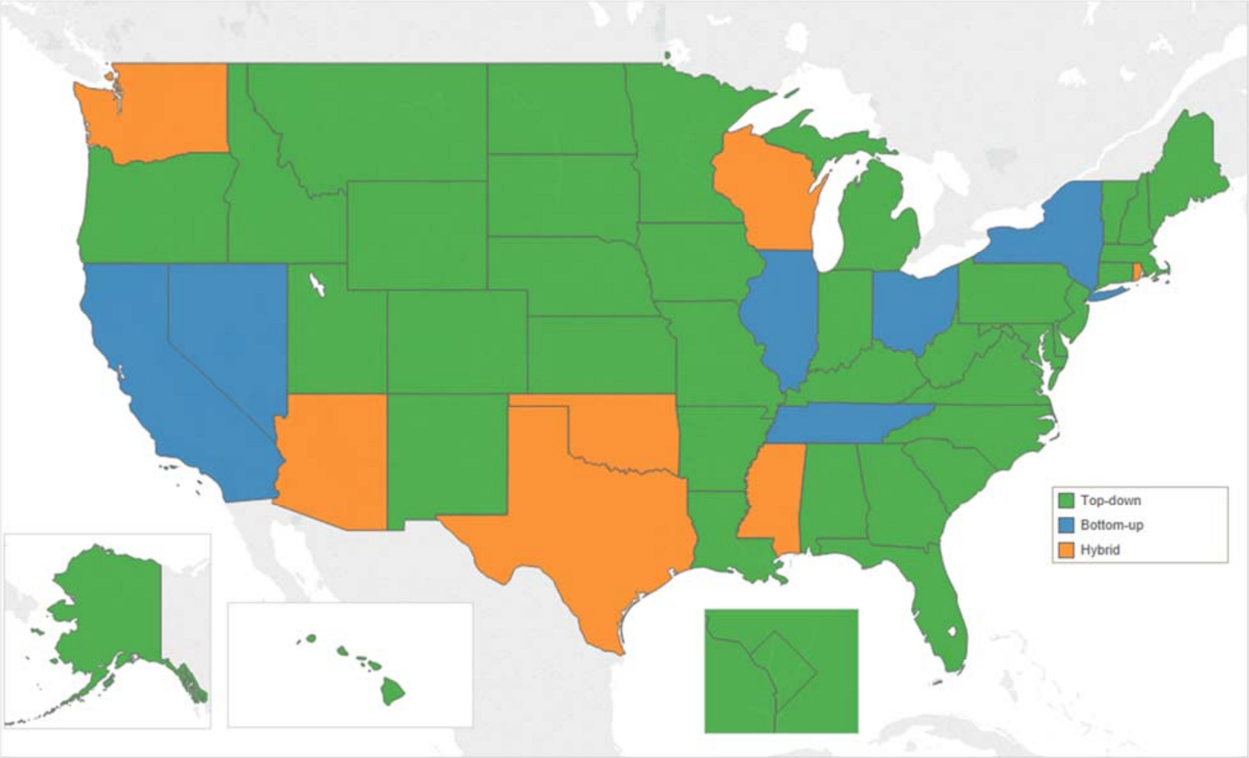
[11] (U) "Voter Records Copied Off Compromised Ilinois Voter Registry," Nextgov, July 2016.

[12] (U) Judd Choate and Trevor Timmons, "DHS Questions on Election Systems," Colorado Secretary of State's office (teleconference, Department of Homeland Security, August 24, 2016).

[13] (U) National Conference of State Legislatures. Online Voter Registration. June 14, 2016. http://www.ncsl.org/research/elections-and-campaigns/electronic-or-online-voter-registration.aspx. Accessed 23 August 2016.

- (U) Thirty-seven States and the District of Columbia maintain top-down voter registration systems, whereas six States maintain bottom-up systems, and seven States maintain hybrid systems according to data from the U.S. Election Assistance Commission (figure 3).[14]
- (U//FOUO) States with top-down voter registration systems present attackers with a single system that if compromised could disrupt the voting process. Since top-down voter registration systems maintain the entire voter registration database for a State, it presents an attack surface that could disrupt many more voters than contained in a bottom-up or hybrid system, which would require the compromise of a diverse number of systems across a State to achieve similar results.
- (U//FOUO) The security of top-down systems, maintained by States, is likely to be stronger than bottom-up systems, based on a review of overall State and local cybersecurity efforts.[15]

(U) The contents of this figure are UNCLASSIFIED.



(U) FIGURE 3—VOTER REGISTRATION BY SYSTEM TYPE[16]

(U) Cyber intrusions to voter registration databases and their supporting information technology could undermine confidence in the election process by demonstrating the capability to alter voter records, leading the American public to question the integrity of the election process. Cyber vulnerabilities to State voter registration databases have already been either identified by security researchers or exploited.

- (U) In June 2016, the District Attorney in Riverside County, CA, said hackers had changed voter registrations before its presidential primary.[17]

[14] (U) U.S. Election Assistance Commission, 2014 Statutory Overview, January 2015, pages 17-23. http://www.eac.gov/assets/1/Page/2014_Statutory_Overview_Final-2015-03-09.pdf. Accessed 23 August 2016.

[15] (U) The 2014 Nationwide Cyber Security Review Executive Summary found that "Local governments face the same cyber security threats as states face, but often have added challenges, and are lagging significantly in security maturity compared to state governments." Multi-State Information Sharing & Analysis Center, 2014 Nationwide Cyber Security Review: Executive Summary, page 4.

[16] (U) U.S. Election Assistance Commission. Election Administration and Voting Survey. 2014. http://www.eac.gov/research/election_administration_and_voting_survey.aspx. Accessed 23 August 2016.

[17] (U) Jacob Preal, "DA confirms hackers are culprit of voter registration changes," Valley News, June 12, 2016, http://myvalleynews.com/most-relevant/voting-irregularities-disenfranchises-many-riverside-county. Accessed 23 August 2016.

- (U) In September 2012, computer researchers alerted the State of Maryland that its online voter registration system was vulnerable to "large-scale, automated fraud" that could either affect voters' ability to legitimately vote or enable voter fraud.[18]

(U//FOUO) Many States continue to rely on paper backups or voter registration lists downloaded directly to electronic devices, limiting the impact of cyber intrusions that would manipulate data or make databases inaccessible on Election Day.

- (U) Several States specifically stipulate that electronic pollbooks may not be connected to a network, requiring that data be directly downloaded to the pollbook before Election Day.[19]
- (U) Eighteen States and the District of Columbia do not use electronic pollbooks, and in the remaining States the pollbooks are only used in some jurisdictions.[20]
- (U//FOUO) Most jurisdictions finalize voter lists long before Election Day, limiting the impact of intrusions that manipulate data or deny access to the database on or near Election Day.[21]

(U) VOTING ACTIVITIES

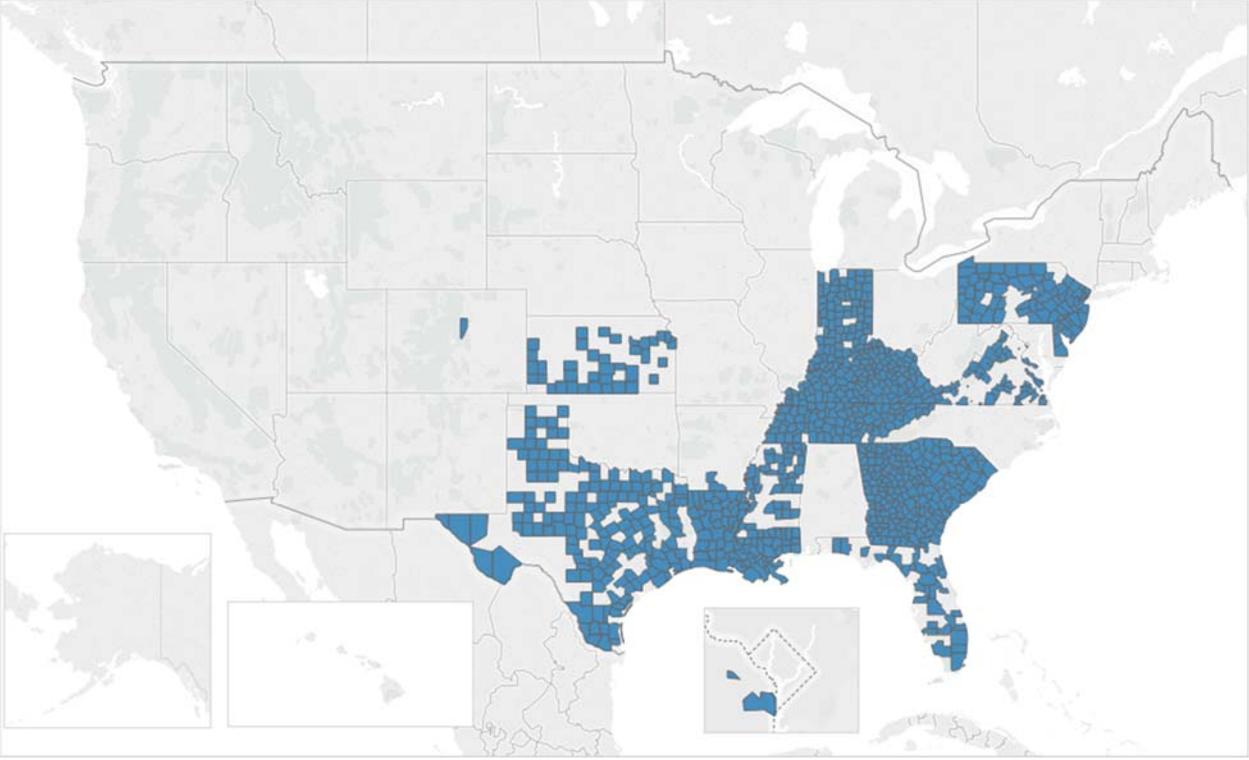
(U//FOUO) OCIA assesses that successfully mounting a widespread attack on voting machines, enough to affect a national election, would require a multiyear effort with significant human and information technology resources available only to a nation-state, but the level of effort required would make it nearly impossible to avoid detection. This assessment is based on the diversity of systems, the need for physical access to compromise voting machines, and the security and preelection testing employed by State and local officials.

- (U) According to data compiled by the Verified Voting Foundation, voting precincts in more than 3,100 counties across the United States use nearly 50 different types of voting machines produced by 14 different manufacturers.[22] The diversity in voting systems and versions of voting software provides significant security by complicating attack planning.
- (U//FOUO) Most voting machines do not have active connections to the Internet.[23,24] Compromising non-networked voting machines would require physical access to potentially hundreds of locations to affect a national election, because even small States will store voting equipment in 50 or more locations.
- (U) Some jurisdictions may use voting systems that have the ability to wirelessly connect to networks, such as the Advanced Voting System WINVote device, which security researchers have found vulnerable.[25] These connections can be exploited to remotely modify votes; in the case of the WINVote vulnerability, this would be done using a device wirelessly connected to the machine (as opposed to via the Internet).[26] However, available data indicates that the use of these devices appears to be limited.

[18] (U) J. Alex Halderman, David Jefferson, and Barbara Simons, Letter to the Maryland State Board of Elections, September 25, 2012. https://www.verifiedvoting.org/wp-content/uploads/2013/04/maryland-online-voting-concerns.pdf. Accessed 23 August 2016.
[19] (U) National Conference of State Legislatures, "Electronic Poll Books | E-Poll Books," May 31, 2016, http://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx. Accessed August 30, 2016.
[20] (U) Ibid.
[21] (U) Matt Masterson and Brian Newby, "DHS Election Questions Follow Up", U.S. Election Assistance Commission (teleconference, Department of Homeland Security, August 25, 2016).
[22] (U) Verified Voting Foundation, derived from "The Verifier" dataset, 2016. https://www.verifiedvoting.org/verifier/. Accessed 23 August 2016.
[23] (U) Matt Masterson and Brian Newby, "Election Infrastructure and Voting Systems Discussion," U.S. Election Assistance Commission (meeting, Department of Homeland Security, Arlington, VA, August 12, 2016).
[24] (U) Alex Schwartzmann, Alex Russell, and Laurent Michele, "DHS Questions on Voting Systems Security," University of Connecticut Center for Voting Technology Research (teleconference, Department of Homeland Security, August 26, 2016).
[25] (U) State of Virginia, Security Assessment of Winvote Voting Equipment for Department of Elections, April 14, 2015, http://elections.virginia.gov/WebDocs/VotingEquipReport/WINVote-final.pdf. Access 23 August 2016.
[26] (U) Ibid.

- (U) To receive Election Assistance Commission certification, election systems must meet voluntary cybersecurity standards established by the National Institute for Standards and Technology.[27] Forty-seven States and the District of Columbia use some aspect of the Election Assistance Commission.[28]
- (U) The vast majority of localities engage in logic and accuracy testing, which work to ensure voting machines operate and tabulate as expected before, during, and after the election.[29] For example, the State of New York engages in a comprehensive preelection testing program, where voting systems are tested against multiple scenarios to ensure the system can tabulate votes correctly.[30] Similar preelection testing programs can be found throughout the United States.
- (U//FOUO) DRE voting machines without a VVPAT are employed in only sixteen States according to data from the Verified Voting Foundation, meaning the vast majority of votes in the United States have a verifiable paper backup (figure 4).[31] In the sixteen States that use DRE without VVPAT, other election safeguards have been put into place, including audits and additional election security procedures to ensure the accuracy of election processes and results.[32]

(U) The contents of this figure are UNCLASSIFIED.



(U) FIGURE 4—COUNTIES USING DRE SYSTEMS WITHOUT VVPAT[33]

[27] (U) U.S. Election Assistance Commission, 2015 Voluntary Voting System Guidelines. http://www.eac.gov/testing_and_certification/voluntary_voting_system_guidelines.aspx. Accessed 23 August 2016.

[28] (U) Tammy Patrick, Bipartisan Policy Center, "Where Do We Go From Here" (presentation, U.S. Election Assistant Commission Technical Guidelines Development Committee, 20 July 2015).

[29] (U) U.S. Election Assistance Commission, Election Management Guidelines. http://www.eac.gov/election_management_resources/election_management_guidelines.aspx. Accessed 23 August 2016.

[30] (U) State of New York. Voting System Pre-Election Logic and Accuracy Testing. 2009. http://www.elections.ny.gov/NYSBOE/hava/Voting_Machines/EACPreLATGrantReport.pdf. Accessed 23 August 2016.

[31] (U) Verified Voting Foundation, derived from "The Verifier" dataset, 2016.

[32] (U) Statement of Kathy Rogers, Director of Election Administration, Georgia Office of Secretary of State regarding Electronic Voting To the Election Assistance Commission. May 5, 2004. http://www.eac.gov/assets/1/AssetManager/testimony%20kathy%20rogers%20director%20of%20elections%20georgia%20public%20meeting%20may%205%202004.pdf. Accessed 24 August 2016.

[33] (U) Verified Voting Foundation, derived from "The Verifier" dataset, 2016. https://www.verifiedvoting.org/verifier/. Accessed 23 August 2016.

(U//FOUO) Security researchers have repeatedly demonstrated in laboratory testing environments that voting machines are vulnerable to compromise usually with physical access, and such compromises could result in the manipulation of vote totals. If such manipulations were made public, it could undermine public confidence in the election system.

- (U//FOUO) Researchers at the University of Connecticut believe most voting machines to be vulnerable, although they believe these vulnerabilities can be mitigated through chain of custody and auditing procedures that many localities employ.[34] Many of these vulnerabilities require physical access to the voting machines or the removable media used to store information on the machines, but can also include the infection of removable media with malware.[35]
- (U) As part of a 2007 voting study sponsored by the Ohio Secretary of State, security researchers were able to compromise every voting system they were given access to, often in ways that could result in the undetectable manipulation of election results.[36]
- (U) A team from Argonne National Laboratory demonstrated that electronics could be introduced to voting machines to manipulate vote results.[37] Argonne researchers showed how a Diebold Accuvote TS touch screen voting machine can be compromised by inserting a man-in-the-middle electronic component to intercept the vote cast by a voter and change it before it is recorded by the system.[38]
- (U) Voting machines could be compromised by a sophisticated supply chain attack, where an individual gains insider access in the manufacturing chain, supply chain, or services and support companies, to modify equipment and software to install malicious code or media that would disrupt the normal operations of the machine.[39] This can be mitigated by election officials by establishing a chain of custody and system and services acquisition controls.

(U) POSTELECTION ACTIVITIES

(U//FOUO) OCIA assesses that smaller-scale manipulation of votes could be accomplished, as has been demonstrated by security researchers with physical access to machines in controlled environments. However, such manipulations would likely not affect the outcome of the election because of existing safeguards in the post-election process, including audits and paper backup systems.

- (U) Election officials are generally aware of the risks of cyber intrusions to the systems used to register official vote totals and employ security practices such as not connecting those systems to the Internet and barring the use of removable media that has been inserted in a computer connected to the Internet.[40,41]
- (U) Twenty-nine States and the District of Columbia use postelection audit processes to compare a sample of voting records against the reported results to verify systems accurately recorded and counted votes, which would identify irregularities.[42] In the remaining 21 voting jurisdictions, audits of some nature may be conducted based on specific circumstances.[43]

[34] (U) Alex Schwartzmann, Alex Russell, and Laurent Michele, “DHS Questions on Voting Systems Security,” University of Connecticut Center for Voting Technology Research (teleconference, Department of Homeland Security, August 26, 2016).

[35] bid.

[36] (U) Pennsylvania State University, University of Pennsylvania, and WebWise Security, Inc., EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing, December 7, 2007. http://siis.cse.psu.edu/everest.html. Accessed 23 August 2016.

[37] (U) Brad Friedman, “Diebold voting machines can be hacked by remote control,” Salon, September 27, 2011, http://www.salon.com/2011/09/27/votinghack. Accessed 23 August 2016.

[38] (U) Computerworld. Argonne researchers 'hack' Diebold e-voting system. September 28, 2011. http://www.computerworld.com/article/2511508/security0/argonne-researchers--hack--diebold-e-voting-system.html. Accessed 23 August 2016.

[39] (U) Election Assistance Commission. Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA). December 23, 2009.http://www.eac.gov/assets/1/Page/Election%20Operations%20Assessment%20Threat%20Trees%20and%20Matrices%20and%20Threat%20Instance%20Risk%20Analyzer%20%28TIRA%29.pdf.

[40] (U) Matt Masterson and Brian Newby, “Election Infrastructure and Voting Systems Discussion,” U.S. Election Assistance Commission (meeting, Department of Homeland Security, Arlington, VA, August 12, 2016).

[41] (U) Beth Ann Surber, Layna Brown, and Sheryl Webb, “Election Security Discussion,” West Virginia Secretary of State’s office (teleconference, West Virginia Secretary of State’s office, August 23, 2016).

[42] (U) National Conference of State Legislatures, “Post-Election Audits,” June 14, 2016. http://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx. Accessed 23 August 2016.

[43] (U) Ibid.

- (U) Forty-six States and the District of Columbia allow partisan election observers to monitor post-election activities, which provides an additional layer that could identify irregularities in vote counting.[44] These observers are highly incentivized to identify issues that could affect the outcome of a race.
- (U) California employs a number of manual steps in its post-election canvas process, such as an inspection of all materials and supplies returned by poll workers, with central counting locations appointing not less than three deputies to open the envelopes or containers with the materials returned from the precincts.[45] Texas employs similar manual methods in post-election canvass processes to ensure voting results. [46]
- (U) The diversity of information technology systems used by State and local governments to perform election system processes also provides safeguards against widespread cyber intrusions.[47]

(U//FOUO) OCIA assesses that systems used to tabulate votes on or after Election Day are vulnerable to cyber intrusions, which could undermine public confidence in the election process. The impacts of such intrusions would likely be contained to the manipulation of unofficial Election Night reporting results, which would not impact the outcome of an election but would significantly undermine public confidence in the results.

- (U) States use different information technology solutions to tabulate election results, some of which are commercial off the shelf solutions while others were developed by States as purpose built systems.[48]
- (U) State government information technology solutions generally include a public-facing Internet connected portion that is used to report election results to the general public and media, which some States have begun migrating to the cloud due to Election Day demand.[49,50] The public-facing, internet portion provides some vulnerability to cyber intrusion that could be used to manipulate vote results, even if only those results that are displayed to the public and media. Election Day results are not the official results of the State or local jurisdiction.
- (U//FOUO) The compromise or disruption of election night reporting functions, to include the disruption of public-facing Web pages that display general election results, could generate significant media attention and could affect public confidence in election results. This is true especially if combined with claims of further election manipulation—even if such claims are ultimately proven false.

(U) EMERGING RISKS

(U//FOUO) OCIA assesses that the introduction of new technologies into the voting process will increase vulnerabilities to the election system in the future. These technologies include cloud-based information technology infrastructure, electronic pollbooks, ballot-on-demand printers, and online voting systems.

(U//FOUO) States and localities are likely to acquire new or updated election systems over the next four years, which will introduce new technologies and potentially add to the number of potential vulnerabilities in election systems.

[44] (U) National Conference of State Legislatures, Policies for Election Observers, August 18, 2016, http://www.ncsl.org/research/elections-and-campaigns/policies-for-election-observers.aspx. Accessed 23 August 2016.

[45] (U) State of California. California Election Code - Division 15. Semifinal Official Canvass, Official Canvass, Recount, and Tie Vote Procedures. http://leginfo.legislature.ca.gov/faces/codes_displayexpandedbranch.xhtml?tocCode=ELEC&division=15.&title=&part=&chapter=&article=. Accessed 23 August 2016.

[46] (U) State of Texas. Election Code – Title 6 Conduct of Elections, Chapter 67 Canvassing Elections. http://www.statutes.legis.state.tx.us/Docs/EL/pdf/EL.67.pdf. Accessed 23 August 2016.

[47] (U) Harriet G. Goldman, "Building Secure, Resilient Architectures for Cyber Mission Assurance," MITRE Corporation, 2010, page 9.

[48] (U) Matt Masterson and Brian Newby, "Election Infrastructure and Voting Systems Discussion," U.S. Election Assistance Commission (meeting, Department of Homeland Security, Arlington, VA, August 12, 2016).

[49] (U) Beth Ann Surber, Layna Brown, and Sheryl Webb, "Election Security Discussion," West Virginia Secretary of State's office (teleconference, West Virginia Secretary of State's office, August 23, 2016).

[50] (U) Eyragon Eidam, "Is Your Election Night Reporting System Ready for 2016?," Government Technology, December 21, 2015, http://www.govtech.com/state/Is-Your-Election-Night-Reporting-System-Ready-for-2016.html. Accessed 23 August 2016.

- (U) A significant number of voting machines were purchased immediately following the passage of HAVA and are expected to require replacement by 2020.[51] One company is projecting that 35 percent of voting machines will be replaced before the 2018 election and 70 percent of voting machines will be replaced before the 2020 election.[52]
- (U//FOUO) States will also move to make upgrades to their other election systems, including voter registration databases, many of which were also initially procured after the passage of HAVA and have not seen significant investments since.[53]
- (U) A number of States are either studying or beginning to adopt cloud computing solutions more widely.[54] This includes some State Secretary of State offices exploring wider adoption of cloud computing for their election systems.[55]
- (U//FOUO) A software-as-a-service electronic voting solution was certified by a test laboratory accredited by the EAC in August 2016, meaning that it will be available for adoption in a number of States for future elections.[56]

(U//FOUO) Electronic pollbooks, which are laptops or tablets containing a list of eligible voters at a precinct, could provide another means to electronically disrupt elections or collect personally identifiable information. However, the technology is still in the early adoption phase and paper backups are available or would be readily available should they be disrupted in 2016.

- (U//FOUO) Thirty-two States have jurisdictions that use electronic pollbooks.[57] At least one State, New Mexico, requires polling locations to have an Internet connection and real-time access to the State-wide voter registration system.[58] The State of Colorado is reliant on the use of electronic pollbooks because it allows same-day voter registration.[59]
- (U) Electronic pollbooks can allow poll workers to look up voters across the State, scan driver's licenses to pull up voter records, notify poll workers if a voter voted during early voting or as an absentee, produce turnout numbers, and receive immediate updates if voters vote in other voting centers.[60]
- (U//FOUO) The State of Connecticut has delayed procuring and employing electronic pollbooks due to concerns raised by University of Connecticut security researchers.[61] The researchers found that electronic pollbooks can be used to intercept personally identifiable information and alter voting records.[62]
- (U//FOUO) A widespread cyber intrusion or disruption of an electronic pollbook could delay the orderly processing of voters at polling locations on Election Day and draw significant media attention. Jurisdictions with e-poll books generally have numerous backup procedures including having paper pollbooks available to election officials if necessary due to machine or system unavailability or failure.[63] However, a systemic

[51] (U) "The American Voting Experience," Presidential Commission on Election Administration, January 2014, page 4.
[52] (U) Lori Steele, "Meeting with 'Everyone Counts,'" Everyone Counts (meeting, Department of Homeland Security, August 26, 2016).
[53] (U) Matt Masterson and Brian Newby, "DHS Election Questions Follow Up", U.S. Election Assistance Commission (teleconference, Department of Homeland Security, August 25, 2016).
[54] (U) Kevin Desouza and Gregory Dawson, "Getting IT Right? How State Governments are Approaching Cloud Computing," TechTank, The Brookings Institution, https://www.brookings.edu/blog/techtank/2015/01/20/getting-it-right-how-state-governments-are-approaching-cloud-computing/. Accessed 26 August 2016.
[55] (U) Beth Ann Surber, Layna Brown, and Sheryl Webb, "Election Security Discussion," West Virginia Secretary of State's office (teleconference, West Virginia Secretary of State's office, August 23, 2016).
[56] (U) Lori Steele, "Meeting with 'Everyone Counts,'" Everyone Counts (meeting, Department of Homeland Security, August 26, 2016).
[57] (U) National Conference of State Legislatures. All about e-poll books. February 2014. http://www.ncsl.org/research/elections-and-campaigns/the-canvass-february-2014.aspx#Poll%20Books. Accessed 23 August 2016.
[58] (U) Ibid.
[59] (U) Judd Choate and Trevor Timmons, "DHS Questions on Election Systems," Colorado Secretary of State's office (teleconference, Department of Homeland Security, August 24, 2016).
[60] (U) Ibid.
[61] (U) Peggy Reeves, Thomas Miano, and Ted Bromley, "DHS Questions on Election Systems," Connecticut Secretary of State's office (teleconference, Department of Homeland Security, August 24, 2016).
[62] (U) Alex Schwartzmann, Alex Russell, and Laurent Michele, "DHS Questions on Voting Systems Security," University of Connecticut Center for Voting Technology Research (teleconference, Department of Homeland Security, August 26, 2016).
[63] (U) Matt Masterson and Brian Newby, "DHS Election Questions Follow Up", U.S. Election Assistance Commission (teleconference, Department of Homeland Security, August 25, 2016).

loss of access to electronic pollbooks in the middle of Election Day may result in localities being unable to determine which voters already cast ballots before the system became unavailable.[64]

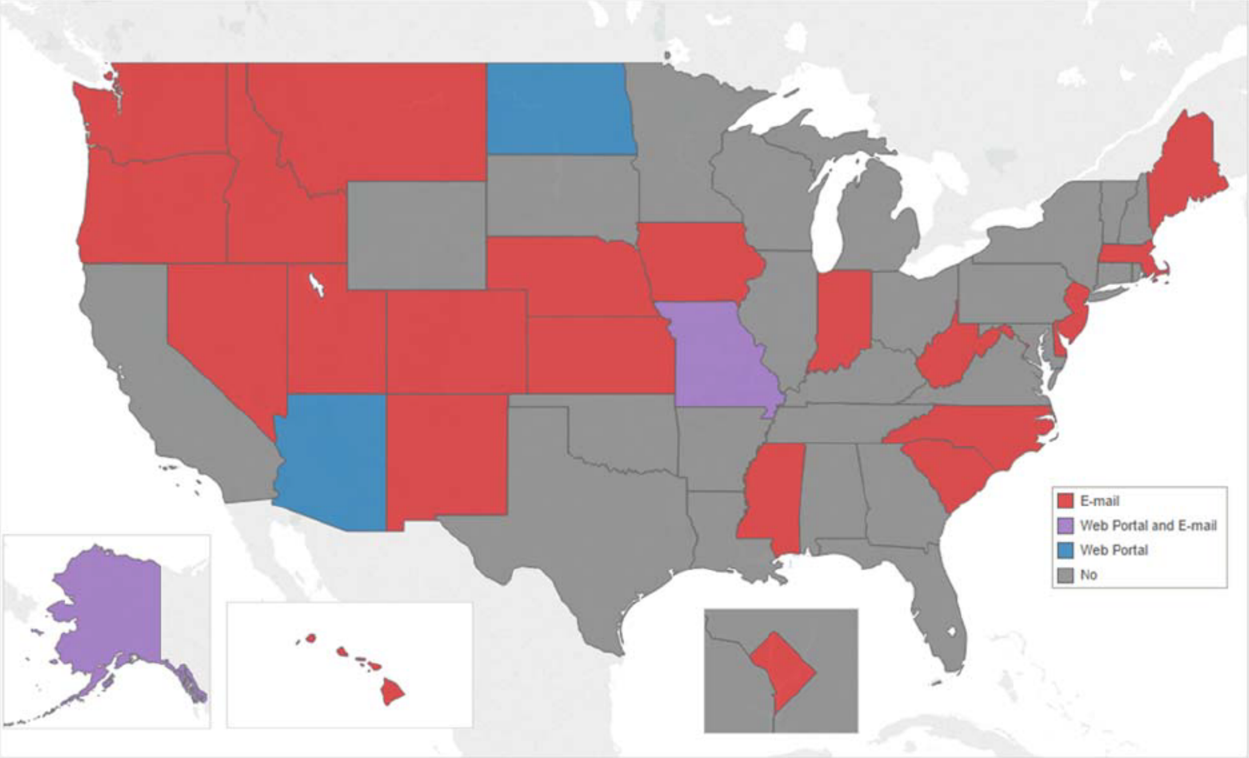
- (U) Some States are adopting ballot-on-demand printers, which allow jurisdictions to print paper ballots that are correct for a voter based on their jurisdiction.[65] These printers can be connected to voter registration technologies, such as electronic pollbooks.[66]

(U//FOUO) The submission of ballots electronically (both through Internet portals or via email) add additional vulnerabilities that could be used to tamper with ballots or identify who voters selected. However, these will account for a small fraction of total ballots cast in 2016; and, other security safeguards exist.

- (U) Alaska allows widespread submission of absentee ballots through an Internet portal; an additional 24 States and the District of Columbia allow the submission of absentee ballots in limited circumstances either through an Internet portal or email (figure 5).[67]
- (U) Other than Alaska, ballots submitted online are largely associated with members of the military and U.S. citizens living abroad, which is governed by the Uniformed and Overseas Absentee Voting Act (UOCAVA).[68]
- (U) Many States that allow the electronic submission of UOCAVA votes have other security safeguards or restrictions including requiring the submission of paper ballots in addition to electronic submission or restricting electronic submission to individuals in combat zones.[69]
- (U//FOUO) Although only four States specifically authorize voting via web portal for UOCAVA voters, jurisdictions in at least 12 states are leveraging electronic voting software provided by Everyone Counts for those voters.[70]
- (U//FOUO) In the 2012 election, UOCAVA votes accounted for only 0.5 percent of all votes.[71] The Department of Defense estimates that roughly 154,000 UOCAVA ballots will be submitted electronically (including Internet portal, email, and fax) in 2016, which would be 0.1 percent of the nearly 130 million voters who participated in the 2012 Presidential election.[72,73]

[64] (U) Alex Schwartzmann, Alex Russell, and Laurent Michele, "DHS Questions on Voting Systems Security," University of Connecticut Center for Voting Technology Research (teleconference, Department of Homeland Security, August 26, 2016).
[65] (U) National Conference of State Legislatures, "Elections Technology Toolkit | Voting Machines and Beyond," March 7, 2016. http://www.ncsl.org/research/elections-and-campaigns/elections-technology-toolkit.aspx. Accessed 25 August 2016.
[66] (U) Wyle Laboratories, "Testing Considerations for Ballot on Demand and ePollBook Systems,"
[67] (U) National Conference of State Legislatures, "Electronic Transmission of Ballots," July 29, 2016. http://www.ncsl.org/research/elections-and-campaigns/internet-voting.aspx. Accessed 23 August 2016.
[68] (U) Ibid.
[69] (U) Ibid.
[70] (U) Lori Steele, "Meeting with 'Everyone Counts,'" Everyone Counts (meeting, Department of Homeland Security, August 26, 2016).
[71] (U) Election Assistance Commission. 2012 Election Administration and Voting Survey - A Summary of Key Findings. September 2013. http://www.eac.gov/assets/1/Page/990-050%20EAC%20VoterSurvey_508Compliant.pdf. Accessed 23 August 2016.
[72] (U) U.S. Department of Defense. Federal Voting Assistance Program projection of e-ballots in 2016, August 22, 2016.
[73] (U) Election Assistance Commission. 2012 Election Administration and Voting Survey - A Summary of Key Findings. September 2013. http://www.eac.gov/assets/1/Page/990-050%20EAC%20VoterSurvey_508Compliant.pdf. Accessed 23 August 2016.

(U) The contents of this figure are UNCLASSIFIED.



(U) FIGURE 5—ADOPTION OF INTERNET VOTING[74]

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.G. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

[74] (U) National Conference of State Legislatures. Electronic Transmission of Ballots. July 29, 2016. http://www.ncsl.org/research/elections-and-campaigns/internet-voting.aspx. Accessed 23 August 2016.