Democracy Live Inc.
Technical Response to:

Request for Proposal
West Virginia Secretary of State
CRFP SOS2200000001

For: Election E-Ballot Delivery Technology

Event	Date	Time
Bid Submission Date	November 22, 2021	1:30 PM EST

RFP Issued By:
State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130

Bidder: Democracy Live, Inc.
Bryan Finney, President/CEO
(206) 465-5636
bryan@democracylive.com

Submitted on November 22, 2021

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Centralized Request for Proposals
Info Technology

Proc Folder: 957044

Doc Description: Addendum No. 1 WVSOS Election Division E-Ballot Delivery Technology

Proc Type: Central Contract - Fixed Amt

Reason for Modification:

Addendum No. 1 is issued to publish questions and answers, and to extend opening date.

Date Issued	Solicitation Closes	Solicitation No	Version
2021-11-02	2021-11-22 13:30	CRFP 1600 SOS2200000001	2

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Customer Code: VS0000026409

Vendor Name Democracy Live, Inc.

Address: 2900 NE Blakeley Street

Street:

City: Seattle

State: WA **Country:** USA **Zip:** 98105

Principal Contact: Bryan Finney, President

Vendor Contact Phone: 206-465-5636 **Extension:**

FOR INFORMATION CONTACT THE BUYER
Toby L Welch
(304) 558-8802
toby.l.welch@wv.gov

Vendor Signature X **FEIN# 45-4826119** **DATE 11-18-2021**

All offers subject to all terms and conditions contained in this solicitation

ADDITIONAL INFORMATION

Addendum No. 1 is issued for the following reasons:

1) To publish a copy of vendor's questions with the answers/responses.

2) To extend the technical opening date to Monday, November 22, 2021 @ 1:30 to allow vendors more time to prepare and submit bids as per attached:

--no other changes--

Request for Proposal (CRFP)

As Authorized by W.V. Code 5A-3-10b,The West Virginia Purchasing Division is soliciting proposals for the agency, the West Virginia Secretary of State - Election Division, to provide Professional Services for Election E-Ballot Delivery Technology and expert technical assistance as per the attached documentation.

**** Online responses has been prohibited for this solicitation, if you have questions contact the Buyer - Toby Welch @ toby.l.welch@wv.gov

See attached instructions for requirements for responding.

INVOICE TO	SHIP TO
SECRETARY OF STATE BLDG 1 STE 157K 1900 KANAWHA BLVD E CHARLESTON WV 25305-0770 Us	SECRETARY OF STATE BLDG 1 STE 157K 1900 KANAWHA BLVD E CHARLESTON WV 25305-0770 US

Line	Comm Ln Desc	Qty	Unit of Measure	Unit Price	Total Price
	Election E-Ballot Delivery Technology system	1.00000	EA		

Comm Code	Manufacturer	Specification	Model#
81112200			

Extended Description:

Vendors must fill out Cost Sheet included as an attachment.
ONLINE SUBMISSIONS OF REQUESTS FOR PROPOSAL ARE PROHIBITED

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Questions are due by 4:00 p.m.	2021-11-08

	Document Phase	**Document Description**	**Page 3**
SOS2200000001	Draft	WVSOS Election Division E-Ballot Delivery Technology	
SOS2200000001	Draft	Addendum No. 1 WVSOS Election Division E-Ballot Delivery Technology	

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

REQUEST FOR PROPOSAL

West Virginia Secretary of State
CRFP SOS2200000001
Election E-Ballot Delivery Technology

Table of Contents

DEMOCRACYLIVE
VOTER INFORMATION TECHNOLOGIES

In partnership with aws

November 18, 2021

Toby L. Welch
toby.l.welch@wv.gov
Bid Clerk
Department of Administration
Purchasing Division
2019 Washington St E
Charleston, WV 25305

Reference: **Cover Letter – Request for Proposal # CRFP SOS2200000001**
Election E-Ballot Delivery Technology
Bid Response

Dear Bid Clerk:

Thank you for the opportunity to respond to your RFP for a secure, accessible remote ballot delivery and return system. Over the last decade, Democracy Live has delivered secure, remote balloting solutions in over 2,500 elections to more than 2,00 jurisdictions across the U.S. Democracy Live, in partnership with Amazon (AWS), has the proven experience and background to ensure West Virginia's requirements and expectations for a secure ballot delivery and return system are fully met.

Launched in 2008, Democracy Live has more experience deploying and supporting secure remote balloting solutions than any other provider in the market. Democracy Live developed and deployed the first remote absentee balloting system in 2009. To date, the Democracy Live OmniBallot system has been reviewed, selected and deployed in more elections than all the other remote balloting solutions combined in the U.S.

Democracy Live partners with Amazon AWS, the largest secure cloud provider in the U.S. AWS has been approved by the Department of Defense, CIA, NSA, FBI and Department of Homeland Security. AWS and Democracy Live team together to offer state and local governments the most deployed, secure electronic balloting platform in the U.S.

Over the last decade, UOCAVA and voters with a full range of physical and cognitive disabilities have used Democracy Live accessible remote balloting technologies. In the 2020 Presidential Election, U.S. voters in 24 states and 96 countries used Democracy Live for either accessible absentee, UOCAVA and/or accessible sample ballots.

As a founding member of the Department of Homeland Security Elections Sector Executive Committee (SCC) and Chair of the SCC Emergency Response Task Force, I understand security is our key priority at Democracy Live. Deployed in over 2,000 elections in nearly half the states, the Democracy Live OmniBallot system has never been compromised. In partnership with AWS, Democracy Live is confident the State of West Virginia will receive a best-of-breed team that offers the most experience, stability, scalability and security for West Virginia's UOCAVA and accessible remote electronic balloting needs.

Sincerely,

Bryan D. Finney
President/CEO
Democracy Live

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

Bryan Finney, President

2900 NE Blakeley Street, Seattle, WA 98105
Main (855) 655-VOTE (8683)
Mobile (206) 465-5636
bryan@democracylive.com

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through wvOASIS, I certify that: I have reviewed this Solicitation in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that I am authorized by the vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

By signing below, I further certify that I understand this Contract is subiect to the provisions of West Virginia Code§ 5A-3-62, which automatically voids certain contract clauses that violate State law.

Democracy Live, Inc.
(Company)

(Authorized Signature) (Representative Name, Title)

Bryan Finney, President
(Printed Name and Title of Authorized Representative)

11-18-2021
(Date)

206-465-5636
(Phone Number) (Fax Number)

REQUEST FOR PROPOSAL

West Virginia Secretary of StateCRFP SOS2200000001 Election E-Ballot Delivery Technology

SECTION 4: PROJECT SPECIFICATIONS

Background and Current Operating Environment:

Following the passage of SB 94 (2020), the Agency is statutorily required to prescribe an electronic ballot transmission and marking tool for the 2022 West Virginia primary and general elections for use by registered West Virginia voter who are eligible for the option of participating in the election(s) via electronic absentee voting under the W. Va. Code§ 3-3-1 *et seq.* (eligible absentee voters living with a physical disability which prevents them from voting independently) as well as the Uniformed and Overseas Citizens Absentee Voting Act ("UOCAVA") set forth in 52 U.S.C.A. §20301 *et seq.* and W. Va. Code§ 3-3-2.

Elections systems and associated technology have been classified by the Department of Homeland Security as Critical Infrastructure since 2017. Electronic voting systems are currently certified and uniform standards created by the United States Election Assistance Commission. However, currently, electronic ballot delivery technologies have no such uniform security standards.

Due to the supreme importance of protecting Critical Infrastructure, rapidly changing elections technology landscape, and regularly evolving federal standards for systems used in Critical Infrastructure sectors, the Agency collaborated with a federal security and compliance company with specialized services and expertise with implementing federally approved cybersecurity controlsfor Critical Infrastructure technology, evaluating acquisition documents and contracts for such technologies, and auditing compliance with such standards for government agencies in Critical Infrastructure sectors.

4.1. Project Goals and Mandatory Requirements:

The electronic absentee ballot transmission and marking tool shall be prescribed for use by all 55 West Virginia counties. The Agency will serve in an administrative capacity by ensuring uniformity,providing support, and assisting with issue resolution when necessary. The tool shall comport with all goals and objectives set forth herein and as required by applicable West Virginia and federal laws.

Vendor should describe its approach and methodology to providing the service or solving the problem described by meet the goals/objectives identified below. Vendor's response should includeany information about how the proposed approach is superior or inferior to other possible approaches.

4.1.1. Goals and Objectives

4.1.1.1 The Vendor provides an electronic ballot delivery and marking tool to all 55 WestVirginia Counties in the State. The tool shall be ready for go-live use by no later than the statutory absentee ballot mailing deadline on March 26, 2022. All development, proofing, training, and other necessary actions shall be complete prior to that date.

Democracy Live Response:

OmniBallot is the most deployed accessible remote balloting technology in the United States. Pioneering the first accessible absentee technology in 2009, Democracy Live has implemented secure, accessible remote balloting in more elections and jurisdictions than all other providers combined. As the industry leader in accessible absentee balloting,OmniBallot has deployed and supported more elections than any other technology in this category. Democracy Live remote accessible balloting technologies have been deployed in over 2,500 jurisdiction, across 24 States, available to over 10 million voters over the last decade.

Democracy Live is the only voting technology provider to have been approved for funding by four federal agencies. Two of which were for our work on accessible voting, and one was specific to serving military and overseas voters. The four federal agencies are:

- U.S. Department of Health and Human Services (accessibility funding)
- U.S. Department of Defense
- Elections Assistance Commission (accessibility funding)
- U.S. State Department

Democracy Live has over a decade providing secure, accessible remote balloting technologies to over 2,000 elections in 24 States. Democracy Live had the honor to support the State of West Virginia in the State's Primary and General 2020 election. Each of the over 2,000 jurisdictions went live on time in the 2020 Presidential election cycle. Democracy Live has a 99% on-time Go Live success rate over the last 10 years.

With our industry-leading experience developing, deploying and supporting accessible, remote balloting technologies, West Virginia can be assured all development, proofing, training, and other necessary actions will be completed by the State's March 26th, 2022 absentee ballot mailing deadline.

4.1.1.2 The tool satisfies all West Virginia and federal requirements for electronic absentee voting, including but not limited to W. Va. Code§ 3-3-1 *et seq.,* the Uniformed and Overseas Absentee Voting Act, the Military and Overseas Voter Empowerment Act, and the Americans with Disabilities Act.

Democracy Live Response:

Democracy Love has a long history supporting UOCAVA voters. Democracy Live was the first firm selected by the U.S. Department of Defense in the 2012 UOCAVA MOVE Act funding program. Democracy Live ended up being selected for more states, jurisdictions and funding than any other recipient of DoD funding under the FVAP grant program. In 2009, Democracy Live pioneered the first fully accessible, ADA-compliant absentee balloting technology in the U.S. The system has now been deployed in over 2,000 elections to meet the remote, accessible balloting needs of UOCAVA and voters with disabilities. Democracy Live won the 2019 Accessibility in Voting Award presented at the United Nations, while our customers have won national accessibility awards for deploying our accessible balloting technologies.

OmniBallot satisfies all West Virginia and federal requirements for electronic absentee voting, including but not limited to W. Va. Code§ 3-3-1 et seq., the Uniformed and Overseas Absentee Voting Act, the Military and Overseas Voter Empowerment Act, and the Americans with Disabilities Act.

4.1.1.3. The tool's functionality allows convenient confirmation of voter eligibility, voteridentity, and accessibility.

Democracy Live Response:

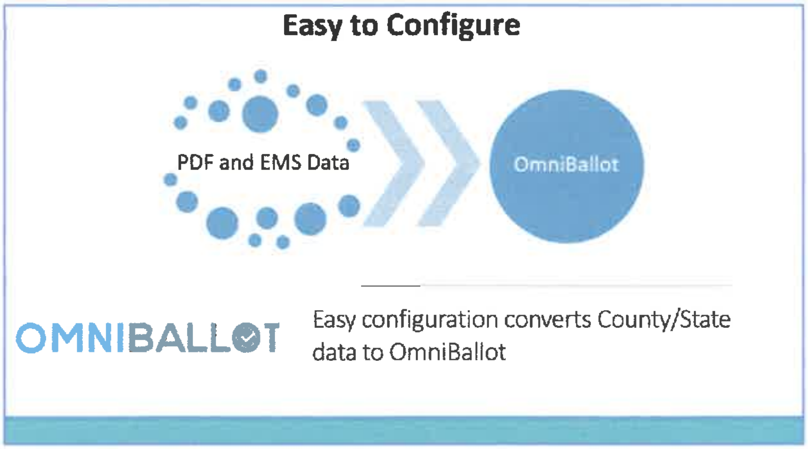
Democracy Live has an easy-to-use voter look-up tool to ensure all eligible voters, whether domestic or abroad can conveniently and securely confirm their eligibility without delay. Since 2009, over 10 million voters have had access to the Democracy Live voter look-up tool. Only eligible voters have access to the OmniBallot portal, as only those voters eligible are entered into the system.

4.1.2. Mandatory Project Requirements -The following mandatory requirements relate to the goals and objectives and must be met by the Vendor as a part of its submitted proposal. Vendor should describe how it will comply with the mandatory requirements and include any areas whereits proposed solution exceeds the mandatory requirement. Failure to comply with mandatory requirements will lead to disqualification, but the approach/methodology that the vendor uses to comply, and areas where the mandatory requirements are exceeded, will be included in technical scores where appropriate. The mandatory project requirements are listed below.

4.1.2.1 The tool is capable of recognizing and reading each ballot style based on the"Ballot Design" files in the format provided by the Agency, a county, or a county's ballot programming vender.

Democracy Live Response:

In collaboration with ES&S, OmniBallot has a proven and well-established ES&S data importing tool, specifically developed for the State of West Virginia. Democracy Live has been importing ballot data from a wide range of tabulation and ballot data systems, including ES&S, for over a decade. The OmniBallot ES&S Ballot Data Importer ensures ballot data can be easily, securely and accurately imported to ensure 100% on-time implementations for every election.



Easy to Configure

Easy configuration converts County/State data to OmniBallot

4.1.2.2 The tool includes a cloud server or equivalent backend which securely processes each electronic absentee ballot submission into a cast vote record (CVR) format, stores the records in a tamper-resistant manner, and enables all participating counties to access the CVRs as requiredby the election schedule and process for in-county tallying.

Democracy Live Response:

OmniBallot is hosted in Amazon Web Services (AWS) which is the largest provider to Federal, state and local governments in the U.S. OmniBallot processes each electronic absentee ballot submission into a cast vote record (CVR) format, stores the records in a federally approved, Fedramp cloud environment, and enables all participating counties to access the CVRs. Ballots securely stored in AWS, are then printed directly onto paper ballots and processed.

The OmniBallot cloud partner, AWS, was recently selected by the National Security Agency (NSA) to securely host and secure some of the nation's most critical and classified documents. Like the NSA, OmniBallot leverages AWS to securely store digital versions of documents (ballots), before printing and processing.

Voter's using OmniBallot are able to login to the secure balloting portal, hosted in the federally approved, AWS cloud to access, review, mark, return and confirm their ballot submission. All OmniBallot logs, activity and reporting is available to fully and transparently audit and review each election.

4.1.2.3 The tool includes a web-based or equivalent administration console for reporting and tracking voter participation.

Democracy Live Response:

The OmniBallot Admin Console is a Web-based console that allows state and local account users to test, view, QA and approve ballots in OmniBallot. In the OmniBallot Admin Console approved administrators can download and print approved ballots and other required return materials directly from the portal. From the Admin console, administrators can run an array of reports on voter activity and site usage.

4.1.2.4 The tool permits a voter to mark a ballot independently and without assistance.

Democracy Live Response:

The OmniBallot ballot marking portal has been designed to meet the highest levels of accessibility, while working with over 90 combinations of screen readers, browsers, operating systems and devices. Over the last decade, OmniBallot has been used by voters representing the full array of disabilities. Voters with Parkinson's, palsy, paralysis, vision loss, cognitive challenges and others can all use OmniBallot to privately, independently and securely access their absentee ballot. Working in collaboration with the Center on Technology and Disabilities, Democracy Live pioneered the nation's first accessible absentee system in 2009.

4.1.2.5 The tool provides a voter the option to transmit a marked ballot, along with a return packet that includes the requisite forms and disclosures, to the county clerk electronically, or alternatively to print a voted ballot with the aforementioned return packet for return via other approved means to the county clerk.

Democracy Live Response:

All voter's using OmniBallot have the option of either printing their ballot and all required return materials, or electronically returning the ballot and return materials, including the signature page. If electing to electronically return the ballot and return materials, the Clerk's office will be notified a ballot packet has been submitted and is ready to be downloaded and printed. All OmniBallot related actions and activities are logged and tracked for auditing and review purposes. If an elections office has a Ballot on Demand printer, they could print a fully tabulatable ES&S ballot directly from the OmniBallot portal.

Includes All Required Return Materials

The ballot and all required absentee return materials are printed by the voter, or at the Elections office

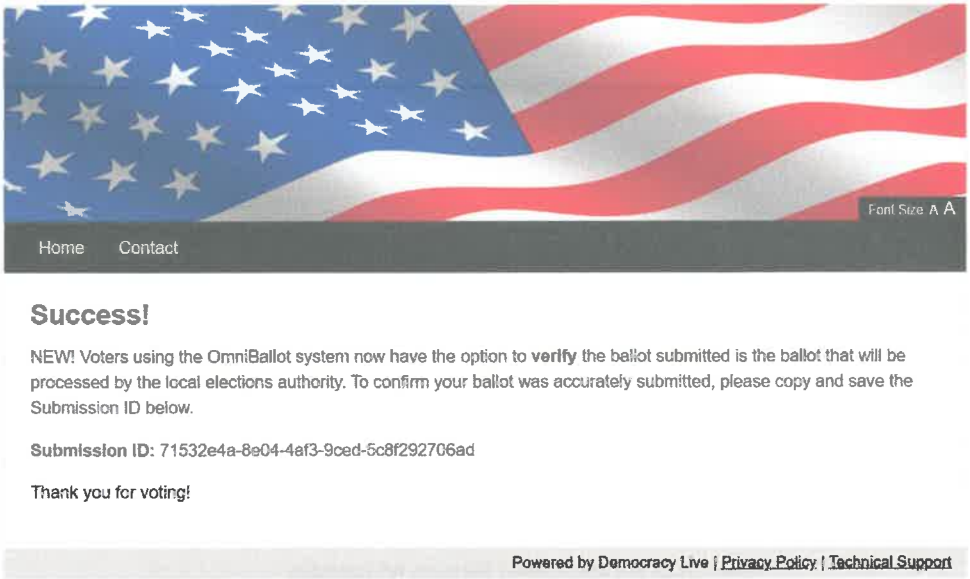
OMNIBALLOT

4.1.2.6 The tool includes a verification portal that permits a voter to review their marked,submitted ballot, in a secure and anonymous manner, and in a read-only format, affording the voter with the ability to confirm the ballot cast is the ballot received by the county.

Democracy Live Response:

Democracy Live offers a portal that permits a voter to review their marked, submitted ballot ensuring the voter can confirm the ballot submitted was the ballot received by the county. Democracy Live deployed a ballot verification portal in Arlington, VA in 2021 which offered voters the ability to confirm from any device the ballot submitted to the elections office was the ballot received. As shown below, the Ballot Verification Portal allows a voter to confirm the ballot they submitted was the ballot received by the election's office.

Step 1. *Voter receives ballot verification code after submitting ballot through OmniBallot*



Success!

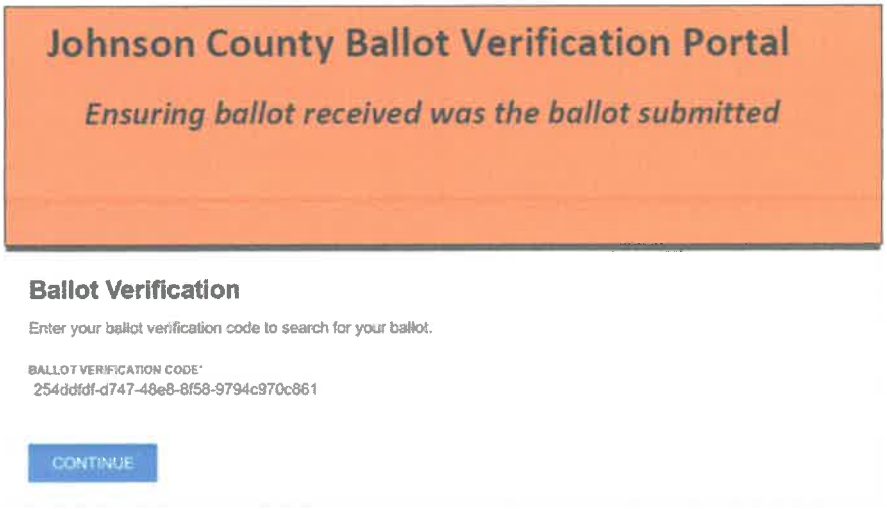
NEW! Voters using the OmniBallot system now have the option to **verify** the ballot submitted is the ballot that will be processed by the local elections authority. To confirm your ballot was accurately submitted, please copy and save the Submission ID below.

Submission ID: 71532e4a-8e04-4af3-9ced-5c8f292706ad

Thank you for voting!

Powered by Democracy Live | Privacy Policy | Technical Support

Step 2. *Voter enters Verification Code into the Verification Portal*



Johnson County Ballot Verification Portal

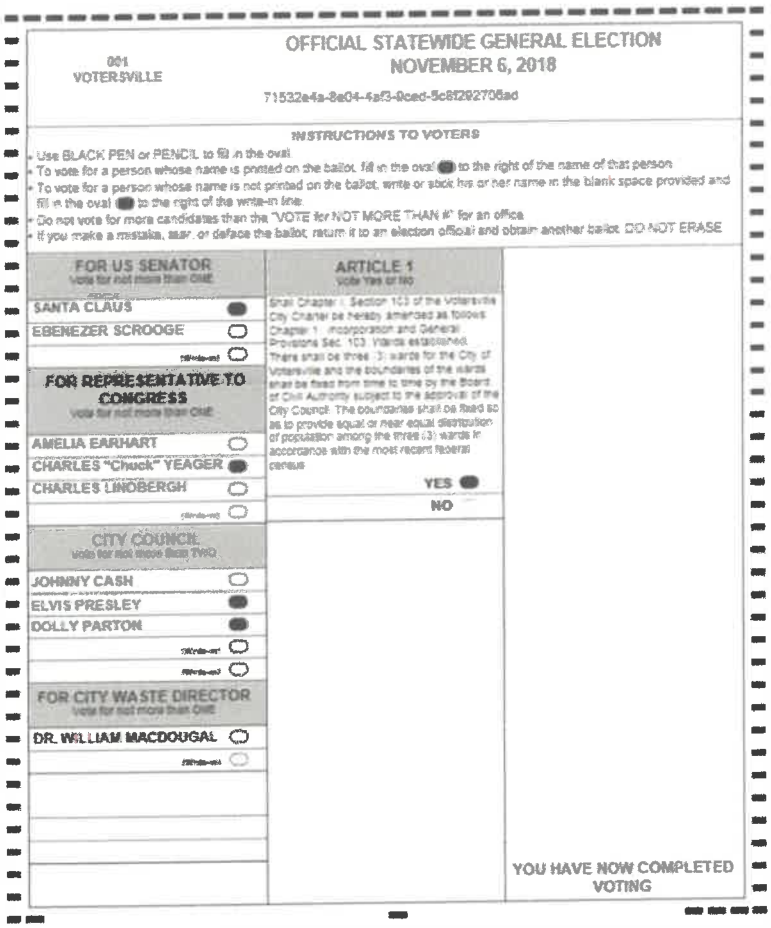
Ensuring ballot received was the ballot submitted

Ballot Verification

Enter your ballot verification code to search for your ballot.

BALLOT VERIFICATION CODE*
254ddfdf-d747-48e8-8f58-9794c970c861

Step 3. *Voter views the ballot that was submitted and received by the Elections office.*



001
VOTERSVILLE

OFFICIAL STATEWIDE GENERAL ELECTION
NOVEMBER 6, 2018

71532e4a-8e04-4af3-0ced-5c8f292706ad

INSTRUCTIONS TO VOTERS

- Use BLACK PEN or PENCIL to fill in the oval.
- To vote for a person whose name is printed on the ballot, fill in the oval ● to the right of the name of that person.
- To vote for a person whose name is not printed on the ballot, write or stick his or her name in the blank space provided and fill in the oval ● to the right of the write-in line.
- Do not vote for more candidates than the "VOTE for NOT MORE THAN #" for an office.
- If you make a mistake, tear, or deface the ballot, return it to an election official and obtain another ballot. DO NOT ERASE

FOR US SENATOR
Vote for not more than ONE

SANTA CLAUS ●
EBENEZER SCROOGE ○
(Write-in) ○

FOR REPRESENTATIVE TO CONGRESS
Vote for not more than ONE

AMELIA EARHART ○
CHARLES "Chuck" YEAGER ●
CHARLES LINDBERGH ○
(Write-in) ○

CITY COUNCIL
Vote for not more than TWO

JOHNNY CASH ○
ELVIS PRESLEY ●
DOLLY PARTON ●
(Write-in) ○
(Write-in) ○

FOR CITY WASTE DIRECTOR
Vote for not more than ONE

DR. WILLIAM MACDOUGAL ○
(Write-in) ○

ARTICLE 1
Vote Yes or No

Shall Chapter 1, Section 103 of the Votersville City Charter be hereby amended as follows: Chapter 1 - Incorporation and General Provisions Sec. 103 - Wards established. There shall be three (3) wards for the City of Votersville and the boundaries of the wards shall be fixed from time to time by the Board of Civil Authority subject to the approval of the City Council. The boundaries shall be fixed so as to provide equal or near equal distribution of population among the three (3) wards in accordance with the most recent federal census

YES ●
NO

YOU HAVE NOW COMPLETED VOTING

4.1.2.7 The Vendor provides training and support to the Agency and counties during theduration of the contract.

Democracy Live Response:

Democracy Live staff have over 100 years of combined elections industry expertise delivering and supporting elections in over 2,000 elections in 24 states in the U.S. Our CEO, Bryan Finney has over 20 years in the elections space and has imparted the importance of thorough training, reliable support and 24/7 availability to every customer. All Democracy Live customers receive training and 24/7 support during elections periods. All 2,500 jurisdictions that had access to OmniBallot in the 2020 General election went live on time.

Democracy Live has a well-established and tested and proven project planning process that ensures delivery of a turn-key fully deployed ADA and MOVE Act compliant Electronic Blank Ballot Delivery and Return System to the State of West Virginia, meeting all stated deadlines.

Deliverable dates will be specified in collaboration with county leadership and stakeholders as suggested in the below Work Plan.

Milestone	Typical Duration	Comments
Complete Contracting Process	Start	Democracy Live will ensure that we are available to the State of West Virginia procurement staff to ensure a smooth and efficient contracting process.
Project Kickoff	Week 1	Initial Meeting to introduce principal stakeholders from the State of West Virginia and Democracy Live. Primary contacts will be established, and a high-level review of the project and West Virginia expectations will be reviewed.
Complete Preliminary Project Plan	Week 2	Based on initial input from the State of West Virginia, the Democracy Live Project Manager will develop a preliminary scope statement, and initial project management plan.
Complete Detailed Project Plan	Week 3 Week 3 (cont'd)	This plan will include a full description of the project's scope, deliverables, resources, and budget. Plans will include: • Scope • Team Responsibilities • Communication Plan • Deliverables and Limitations • Work Breakdown Schedule • Schedule • Budget • Quality Management Plan • Scope Management Plan • Customer Acceptance Plan • Operational Training Plan • Operational Implementation Plan • Operational Maintenance Plan
First Customer Product Review	Week 5	Based on our prior experience, we expect that we will rapidly configure a first demonstration of the system for end-end testing.
Customer Acceptance		Assuming that there may be adjustments that

	Week 7	need to be made to the Week 5 deliverable, we allow another two weeks for any iterations
Customer Training	Week 9	Training for Key Stakeholders.
Customer Training	As Requested	We will accommodate the schedule that best suits the West Virginia County Elections Staff.
Operational Handoff	As Requested	We will accommodate the schedule that best suits the West Virginia County Elections Staff.

Sample Timeline for OmniBallot Deployment (will be adjusted to meet the state's needs)

E60* - Upload ES&S import data and Ballot PDFs of all ballot return materials to the secure data transfer site provided by your Democracy Live Project Manager

E60 - Upload initial voter registration data for qualified voters

E50 (or earlier) - Fully configured data will be provided to you by Democracy Live

E47 - System approval and activation. Democracy Live provides the link that may be emailed to voters.

E45 – State posts and/or emails the link to the OmniBallot System to voters

Ongoing – State may add additional qualified voters as applications are received and approved

***E60** indicates 60 days before Election Day

Note: *This timeline may be adjusted for an earlier activation date by adjusting all listed activities by the corresponding amount of time.*

4.1.2.8 Section 508 Compliance
Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use Information and Communication Technology (ICT), it shall be accessible to people living with disabilities. Federal employees and members of the public who have disabilitiesmust have access to, and use of, information and data that is comparable to people withoutdisabilities.

Products, platforms and services delivered as part of this work statement that are ICT, or contain ICT, must conform to the Revised 508 Standards, which are located at 36 C.F.R. §1194.1 & Apps. A, C & D, and available at https://www.access-board.gov/guidelines- andstandards/communications-and-it/about-the-ict-refresh/final-rule/text-of-the- standardsand-guidelines

Democracy Live Response:

Democracy Live deployed the nation's first WCAG, Section 508 compliant remote accessible absentee ballot in 2009. Since that launch over a decade ago and through our engagement with leading disability groups and organizations, Democracy Live continues to ensure that OmniBallot meets the highest levels of accessibility. The OmniBallot Portal (ICT) conforms to the revised Section 508 and WCAG 2.0AA (and where applicable AAA).

4.1.2.8.1 Provide list of item(s) that contains ICT. For each item, the followingrequirements apply:

Democracy Live Response:

The OmniBallot Balloting Portal contains ICT.

4.1.2.8.2 All functional performance criteria apply when using an alternative design or technology that achieves substantially equivalent or greater accessibility and usability by individuals with disabilities, than would be provided by conformance to one or more of the requirements in Chapters 4-6 of the Revised 508 Standards, or when Chapters 4-6 do not address one or more functions of ICT.

Democracy Live Response:

OmniBallot has been developed to meet WCAG 2.0 AA (and AAA where possible) accessibility guidelines.

4.1.2.8.2 Software features and components: All WCAG Level AA SuccessCriteria, 502 Interoperability with Assistive Technology, 503 Application.

Democracy Live Response:

OmniBallot has been developed to meet WCAG 2.0 AA (and AAA where possible) accessibility guidelines.

4.1.2.8.3 Hardware features and components: All requirements apply

Democracy Live Response: N/A

4.1.2.8.4 Applicable support services and documentation: All requirements apply.

Democracy Live Response:

OmniBallot has fully accessible instructions in the portal that provides instruction on how to navigate through the balloting process. This workflow has been developed in collaboration with dozens of members of the disability community, representing many of the major disability advocacy organizations.

4.1.2.8.2 Provide an Accessibility Conformance Report (ACR) for each commercially available ICT item offered through this contract. Create the ACR using the Voluntary Product Accessibility Template Version 2.1 or later, located at https://www.itic.org/policy/accessibility/vpat. Complete each ACR in accordance with the instructions provided in the VPAT template. Each ACR must address the applicable Section 508 requirements referenced in the Work Statement. Each ACR shall state exactly how the JCT meets the applicable standards in the remarks/explanations column, or through additional narrative. All "Not Applicable" (N/A) responses must be explained in the remarks/explanations column or through additional narrative. Address each standard individually and with specificity, and clarify whether conformance is achieved throughout the entire JCT Item (for example - user functionality, administrator functionality, and reporting), or only in limited areas of the JCT Item.

Democracy Live Response:

Appendix 1 includes the Section 508, WCAG Conformance report and Appendix 2, the University of Washington Center on Technology and Disabilities report. The Center on Technology and Disabilities tested OmniBallot for WCAG and Section 508 compliance summary states:

University of Washington Center on Technology and Disabilities Executive Summary on OmniBallot
Overall, the site is very accessible in its current form. Keyboard access was effective in all web pages tested. Screen reader access was also strong. Screen reader navigation was mostly consistent and easy to understand. When marking ballots the state of the checkboxes was announced before and after making a selection. One recommendation is made below to improve usability.

Due to the fact that WCAG 2.0 AA Success Criteria are more explicit than the current 508 Standards, focus was directed to identifying compliance with WCAG 2.0 AA Success Criteria. https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/background/comparison-table-of-wcag2-to-existing-508-standards

Unless mentioned specifically below, WCAG 2.0 and Section 508 compliance was found to be met.

Refer to Appendix 1 – OmniBallot PAT WCAG 2.0aa Conformance Report
Refer to Appendix 2 - University of Washington Accessibility Test Report

4.1.2.8.3 Provide a description of the evaluation methods used to support Section 508 conformance claims. The Agency reserves the right, prior to making an award decision, to perform testing on some or all of the Vendor's proposed JCT items to validateSection 508 conformance claims made in the ACR.

Democracy Live Response:

Democracy Live has continuous evaluations of OmniBallot by voters with disabilities to ensure the system meets Section and WCAG 2.0aa (and 2.1aa requirements where applicable). The system has been tested by the Center for Technology and Disabilities, the State of California, the State of Michigan and the State of North Carolina for accessibility. The Conformance report and PAT are found in Appendix 1.

Refer to Appendix 1 – OmniBallot PAT WCAG 2.0aa Conformance Report
Refer to Appendix 2 - University of Washington Accessibility Test Report

4.1.2.8.4 Describe your approach to incorporating universal design principles toensure JCT products or services are designed to support disabled users.

Democracy Live Response:

The Democracy Live approach to accessible development and design is founded in our experience working in direct collaboration with members of the disability community over the last 12 years. The first accessible absentee technology ever deployed in the U.S. began with our lead developer (and current CTO) developing side-by-side in the home of a key member of the American Council of the Blind. Ever since that in-home development session in 2008, each version of our accessible remote balloting technology has been developed in cooperation and collaboration with actual voters with disabilities.

With over 80% of accessible remote balloting market in the U.S., OmniBallot has been deployed in thousands of elections. Democracy Live has had the benefit of receiving constant "real world" feedback from voters using the system. This accessibility feedback loop of listening and learning from real voters on their actual use of the system has enabled OmniBallot to become the most deployed accessible absentee technology in the U.S.

4.1.2.8.5 Describe plans for features that do not fully conform to the Section 508 Standards.

Democracy Live Response:

All features of OmniBallot fully conform and are compliant with Section 508.

4.1.2.8.6 Describe "typical" user scenarios and tasks, including individuals with disabilities, to ensure fair and accurate accessibility testing of the JCT product or service being offered.

Democracy Live Response:

Democracy Live has engaged more than twenty consultants with disabilities to engage, test and conduct education. The Democracy Live accessible balloting portal has been available to millions of voters, deployed in 24 states over the last decade. Thousands of voters have used and tested the OmniBallot Portal across all types of voters, including voters with disabilities. Democracy Live provides a test link to disability groups for voters who can test the system and give feedback and suggestions to the OmniBallot development team.

In the last 30 days (as of 11/15/2021) Democracy Live presented to over 100 voters with disabilities across multiple statewide disability conferences (including West Virginia) to listen, learn and demonstrate our accessible remote balloting.

Use case scenario #1:
A voter who has mobility challenges due to severe Parkinson's is able to use their home computer with their own assistive technology to access the OmniBallot portal via a link. Using their personal assistive input technology, the voter is able to access, mark, review and submit their ballot independently and privately.

Use case scenario #2:
A voter who is blind is able to use their home computer with their screen reader technology to access the OmniBallot portal via a link. Using their screen reader the voter is able to access, mark, review and submit their ballot independently and privately.

Democracy Live is confident that any voter with disabilities who can access Facebook, Amazon (or any Web site) can access OmniBallot. Voters using any combination of screen readers, browsers, operating systems and devices, will be able to access, mark and return their ballot independently and privately using OmniBallot. There are over 90 combinations of browsers, operating system and screen readers that voters typically use. OmniBallot works with every combination.

4.1.2.9 Prior to acceptance, the Agency reserves the right to perform testing on required JCT items to validate the Vendor's Section 508 conformance claims. If the Agency determines that Section 508 conformance claims provided by the Vendor represent a higher level of conformance than what is actually provided to the agency, the government shall, at its option, require the Vendor to remediate the item to align with the Vendor's original Section 508 conformance claims prior to acceptance.

Democracy Live Response:

Democracy Live agrees to this requirement.

4.1.3 Cyber Security Systems and Controls

4.1.3.1 Cybersecurity systems and controls are essential to distinguish, counteract, or decrease
security risks. These measures are required to manage threats targeting computer systems and networks. These measures must be adaptive and robust. To determine whether your cyber security systems and controls meet our desired standards:

Democracy Live Response

Democracy Live partners with Amazon AWS, the largest secure cloud provider in the U.S. AWS has been approved by the Department of Defense, Central Intelligence Agency, FBI and Department of Homeland Security. Amazon and Democracy Live team together to offer state and local governments the most deployed, secure hosting platform in the U.S. Remote electronic balloting requires a highly secure, stable and scalable cloud environment. AWS is the most proven cloud solution in the U.S. In over 4,000 deployments over the last decade, the Democracy Live remote balloting system has never been compromised.

Democracy Live has implemented controls for Controlled Unclassified Information (CUI) exceeding NIST 800-171 by electing the NIST 800-53 CSF Medium Impact controls to comply with more stringent FISMA standards. Democracy Live implements and maintains system security controls to protect any and all sensitive data from unauthorized access and use. Least privileged access is practiced with all system services and data along with monitoring and execution on our established Incident Response plan. (Refer to Appendix 3 – Incident Response Plan)

4.1.3.1.1 Please complete Attachment B - OWASP Application Level Security Verification Levels I -3. For all listed requirements please provide 2 pieces of supporting documentation. For any requirements that are lacking supportingdocumentation, please add to Attachment F - POA&M Tracker.

4.1.3.1.2 Please complete Attachment C - OWASP Mobile Application Level Security Verification if applicable. For all listed requirements please provide 2 pieces ofsupporting documentation. For any requirements that are lacking supporting documentation, please add to Attachment F - POA&M Tracker. If not applicable, please put N/A by all requirements.

4.1.3.1.3 Please complete Attachment D - Security Requirements for Databases. For all listed requirements please provide 2 pieces of supporting documentation. For any requirements that are lacking supporting documentation, please add to Attachment F - POA&M Tracker.

4.1.3.1.4 Please complete Attachment E - Select Controls from NIST SP 800-171. For all listed requirements please provide 2 pieces of supporting documentation. For any requirements that are lacking supporting documentation, please add toAttachment F - POA&M Tracker.

Democracy Live Response:

Democracy Live has completed and been approved (State of Michigan) for compliance to meet the NIST Cybersecurity Framework SP 800-53. Each of the above listed attachments (Attachment B - OWASP Application Level Security, Attachment C - OWASP Mobile Application Level Security Verification, Attachment D - Security Requirements for Databases and Attachment E - Select Controls from NIST SP 800-171) are included, where relevant to OmniBallot, as part of our NIST SP 800-53 compliance. (Refer to Appendix 4 and 5)

Refer to Appendix 4 - System Security Plan
Refer to Appendix 5 - OmniBallot Security White Paper | Michael Hamilton, Policy Adviser to Washington State, as the Chief Information Security Officer for the City of Seattle, Vice-Chair of the DHS State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC), and formerly in the private sector as the Managing Consultant for VeriSign Global Security.

State of Michigan Cybersecurity Compliance Officer: Gena Hyde HydeG@michigan.gov
1-888-767-6424

OmniBallot's cloud platform is compliant with the industry highest security, privacy and accessibility certification standards, including but not limited to:

- ISO/IEC 27001 Security Management Controls Standard
- ISO/IEC 27018 Personal Data Protection Standard
- FedRAMP Government Data Standards
- NIST 800-53 Security Control Standards

Democracy Live's comprehensive approach to security is based on a foundation of NIST, federal and state government recommended principles, policies, and processes that allow us to quickly adapt to evolving threats. This continuous approach includes identifying assets and risks, mitigating vulnerabilities, measuring effectiveness, and implementing improvements to the process. The OmniBallot web application itself is compliant with the NIST FIPS 200: Security Requirements for Federal Information and Information Systems standard.

4.2. Qualifications and Experience: Vendor should provide information and documentation regardingits qualifications and experience in providing services or solving problems similar in size, scope and complexity to those requested in this RFP. Information and documentation should include, but are not limited to, proposed staffing plans, descriptions of past projects completed (descriptions shouldinclude the location of the project, project manager name and contact information, type of project, and what the project goals and objectives where and how they were met.), references for prior projects including the value and period of performance of past projects, and any other information that Vendor deems relevant to the items identified as desirable or mandatory below.

Democracy Live Response:

As noted in our below response in Section 4.2.2.1, Democracy Live has deployed our accessible remote balloting portal in 24 States, covering over 2,000 jurisdictions. The electronic ballot return option was deployed Statewide in North Carolina, South Carolina, New Jersey, Delaware, a coalition of MA counties led by Boston), Utah County, Pierce County, WA and King County, WA and West Virginia.

A few examples are:

State of Michigan – OmniBallot Balloting Portal (1-way ballot delivery). Value: $1.5m over 5 years
Shelly Belton

Elections Operations Manager|Michigan Department of State – Bureau of Elections
Cell: 517-281-5085|BeltonS@Michigan.gov

State of North Carolina – OmniBallot Balloting Portal (2-way ballot delivery/return) Value: $420,000 over 1 year. Includes accessible ballot request portal.
Karen Bell, Director of Elections.
(919) 814-0700, karen.bell@ncsbe.gov

State of Pennsylvania - OmniBallot Balloting Portal (1-way Ballot delivery) $530,000 over 1 year. Includes accessible ballot request portal.
Sindhu Ramachandran,
717-216-9877
sramachand@pa.gov

State of South Carolina: OmniBallot Balloting Portal (2-way Ballot delivery/return): $178,000
Howard (Howie) Knapp
(803) 734-9059
hknapp@elections.sc.gov

State of Colorado: OmniBallot Balloting Portal (1-way Ballot Delivery): $194,000
State of Colorado – Trever Timmons
Chief Information Officer | Department of State
303.860.6946 (direct)
303.894.2200 (office)

Personnel Qualifications:

Led by our CEO, Bryan Finney Democracy Live has the largest and most experienced support and operations team dedicated to remote accessible balloting in the elections industry. Bryan has over 20 years in Elections technology and is a founding member of the DHS-sponsored SCC Executive Committee. Bryan has spoken in front of the Congress and the United Nations on issues of voting security and accessibility.

The Democracy Live Operations and Support Team is lead by Felicia Erlich.

Felicia Erlich, Esq. – Implementation/Project Manager
Democracy Live Director of Business Affairs/ Corporate Counsel and Head of Operations
Felicia Erlich
felicia@democracylive.com

Felicia has a Juris doctorate from California Western School of Law. Over her last 5 years with Democracy Live, Felicia has led the team to successfully deploy OmniBallot in over 1,200 elections across 21 states. Felicia is an active member of the Department of Homeland Security sponsored Elections Sector Emergency Response Task Force.

Island Pinnick – Developer Lead

Democracy Live Chief Technology Officer and Lead Architect of the OmniBallot Balloting Portal
Island Pinnick
island@democracylive.com

Democracy Live's Chief Technology Officer and lead developer of OmniBallot, Island has over a decade of experience in the elections industry. Island was awarded the Bill & Mary Gates Scholar of the Year at the University of Washington and a graduate in nano-technology engineering, Island developed the first and most widely deployed remote electronic balloting technology in the U.S.

Mark Pace – Chief Security Officer
Mark's cybersecurity experience began with Microsoft's ACE Team as part of Microsoft's Trustworthy Computing (TwC) Initiative. As a security lead at Microsoft, Mark performed threat analysis, security audits, and consulted on development best practices and security postures. In addition to Microsoft, Mark has provided security and consulting services to various firms including Qwest Communications and Fluke. Mark began his career with the team at Xerox Webster Research. Mark joined MSNBC as a founding member of the special projects launch team working projects for the Atlanta Olympics and Clinton/Dole Presidential race results.

Michael Hamilton, MS – Security Analyst
Michael has served as a Cybersecurity Policy Advisor for Washington State, Vice-Chair of the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC), Chief Information Security Officer for the City of Seattle, and Managing Consultant for VeriSign Global Security Consulting.

Nick Toomey – Technical Support and Data Coordinator
Democracy Live's Technical Accounts Manager, has experience supporting the implementations of over 1,500 electronic balloting implementations, across 20 states in the United States.

James Johnston – Network and Development Coordinator
Former U.S. Military, with a degree in computer programming and security from the University of Washington, James has deep level experience in secure development for voting and elections technologies.

4.2.1. Qualification and Experience Information: Vendor should describe in its proposal howit meets the desirable qualification and experience requirements listed below.

4.2.1.1. Vendor's tool has been reviewed by at least one (1) independent, nationally recognized organization supporting the Disability Community for its user acceptance and Section 508 conformity for voters living with disabilities. Copiesof any reports or public statements by the organization(s) should be provided tothe Agency for Confidential review.

Democracy Live Response:

OmniBallot is the most deployed accessible remote balloting technology in the United States. Pioneering the first accessible absentee deployment in 2009, Democracy Live has implemented secure, accessible remote balloting in more elections and jurisdictions than all other providers combined. As the industry leader in accessible absentee balloting, OmniBallot has had more testing in live elections than any other technology in this category.

OmniBallot has been tested by the University of Washington Center for Technology and Disabilities. (See Appendix 2 – University of Washington Accessibility Test Report) and testing by dozens of members of leading disability groups, such as the American Council of the Blind, National Federation of the Blind, Center for Independent Living and other organizations. Below are a few quotes regarding our accessible technology:

1) *The work of Democracy Live demonstrates that compliance with international standards on accessibility is readily achievable in the elections and voting space. Voters around the world have the right to equal access to participating in the democratic process and Democracy Live has gone a long way to producing technologies that helps achieve that goal.*
Janet Lord
Harvard Law School Project on Disability

2) *Democracy Live's system is a marvelous example of a universal design. It provides a valuable resource on voter information for all citizens, including those with disabilities who often lack access to this critical information about candidates and issues.*
Deborah Cook
University of Washington Center for Technology and Disability Studies

3) *As a voter and advocate who is blind, I believe that the voting experience should be accessible to all, including those with disabilities. The voting tool should be easy to use, while ensuring that voters are able to cast their vote in a secure, private and and independent fashion. After testing products developed by Democracy Live, I have determined that their products exceed my expectations, thereby providing equal access to voter information prior to and during the voting session, as directed by the United States Department of Justice and disability rights laws.*
Kenneth Semien, Sr.
President, American Council of the Blind of Texas

This is wonderful! It's clear and easy to follow, using various screen reader options works well, all information is provided, and even the write-in option is accessible, not always true with the machines. Great job! This is going to open up so many opportunities. It's also laying the groundwork for other kinds of things.
Vicky Prahin
Executive Director, American Council of the Blind of Ohio

4.2.2. Mandatory Qualification/Experience Requirements - The following mandatory qualification/experience requirements must be met by the Vendor as a part of its submitted proposal. Vendor should describe how it meets the mandatory requirements and include any areaswhere it exceeds the mandatory requirements. Failure to comply with mandatory requirements will lead to disqualification, but areas where the mandatory requirements are exceeded will be included in technical scores where appropriate. The mandatory qualifications/experiencerequirements are listed below.

4.2.2.1. Implemented tool in at least two (2) previous federal elections. A list of all previous federal elections, including the jurisdiction, shall be provided to theAgency.

Democracy Live Response:

Since 2010, the Democracy Live remote balloting portal has been deployed in six federal elections - 2010, 2012, 2014, 2016, 2018, 2020. This does not include nearly 1,000 off-year elections where OmniBallot has been deployed. In over 2,000 elections since 2009, Democracy Live has a 99% on-time Go Live rate.

After competitive bids, Democracy Live was selected and funded by the U.S. Department of Defense and the U.S. State Department. Additionally, the U.S. Department of Health and Human Services approved accessibility funding for jurisdictions to deploy Democracy Live accessible balloting technologies.

Democracy Live has been approved and selected in jurisdictions in the following states. With the exception of Alabama and the listed jurisdictions in Massachusetts, each customer has been deployed in at least one federal elections cycle (Primary and General): **(Bold indicates electronic ballot return.)**

- Michigan (Statewide)
- Pennsylvania (Statewide)
- **North Carolina** (Statewide)
- **New Jersey** (Statewide)
- Florida
- **Massachusetts (Boston, Cambridge, Watertown,)**
- **South Carolina** (Statewide)
- Washington D.C.
- **West Virginia** (Statewide)
- New York City
- Rhode Island (Statewide)
- **West Virginia** (Statewide)*
- Vermont (Statewide)
- Ohio (Majority of voters)
- Colorado (Statewide)
- **Delaware** (Statewide)
- Minnesota (Statewide)

- Texas
- California (Majority of counties)
- Washington State (Statewide)

*Recently selected/yet to be deployed

- North Carolina – Karen Bell
- South Carolina – Howard Knapp
- Colorado – **Caleb Thornton,** Legal, Policy, and Rulemaking Manager- Elections 303.894.2200 x 6386 caleb.thornton@coloradosos.gov

4.2.2.2.Vendor's applicable network and systems or tool have been assessed for security vulnerabilities by at least two (2) independent, federally recognized, certified, of industry specific equivalent technology or cybersecurity auditors. Copies of all assessments or equivalent reports shall be provided to the Agency.

Democracy Live Response:

OmniBallot from Democracy Live has been reviewed by:

- U.S. Department of Homeland Security – 2020 Full Penetration Testing
- Cybersecurity and Infrastructure & Security Agency (CISA) – 2020 Security & Vulnerability Test + Idaho National Labs – Code Review
- Over 100 Cybersecurity Researchers –2020 "White hat" Penetration and threat assessment (Synack Cybersecurity)
- Soteria Cybersecurity (2021) – Detailed cybersecurity review
- Amazon Web Services (AWS) – Security Architecture Review
- OmniBallot is the only remote electronic balloting technology to be officially certified in every State that requires certification (for one-way ballot transmission)
- National Cybersecurity Center (NCC) – Post election audits
- Shift State Cybersecurity (Former FBI cybersecurity)
- The OmniBallot "one-way" ballot delivery option is the only remote accessible balloting technology to be certified for use by every that requires certification. (CA, OH & FL)

Beginning in January, 2022 Synack, a leading Cybersecurity firm, will have cybersecurity researchers conducting constant 24/7/365 penetration and threat testing on the OmniBallot portal.

From Synack:
"Synack, the leading cybersecurity crowdsourcing research firm in the U.S., conducted a thorough review of the Democracy Live OmniBallot remote balloting system. After extensive testing and research none of over 100 cybersecurity researchers were able to compromise the OmniBallot system. Given the testing of OmniBallot concluded in 2020, Democracy Live and Synack have teamed up once again to ensure 24/7 365 cybersecurity assessment and penetration testing to ensure OmniBallot has the most comprehensive and constant cybersecurity and penetration testing in the elections space."

SECTION 5: VENDOR PROPOSAL

5.1. Economy of Preparation: Proposals should be prepared simply and economically providing a concise description of the items requested in Section 4. Emphasis should be placed on completeness and clarity of the content.

5.2. Incurring Cost: Neither the State nor any of its employees or officers shall be held liable forany expenses incurred by any Vendor responding to this RFP, including but not limited to preparation, delivery, or travel.

5.3. Proposal Format: Vendors should provide responses in the format listed below:

5.3.1. **Two-Part Submission:** Vendors must submit proposals in two distinct parts separate fromeach other: technical and cost. Technical proposals must not contain any cost information relating to the project. Cost proposal must contain all cost information and must be sealed in a separate envelope from the technical proposal to facilitate a secondary cost proposal opening.

5.3.2. **Title Page:** State the RFP subject, number, Vendor's name, business address, telephone number, fax number, name of contact person, e-mail address, and Vendor signature anddate. A title page shall be used for both the technical and cost proposals and will not be included in the page count.

5.3.3. **Table of Contents:** Clearly identify the material by section and page number for both the technical and cost volume. The table of contents will not be included in the page count.**Response Reference:** Vendor's response should clearly reference how the informationprovided applies to the RFP request. For example, listing the RFP number and restating the RFP request as a header in the proposal would be considered a clear reference.

Proposal Submission: All proposals (both technical and cost) must be submitted to the Purchasing Division **prior** to the date and time listed in Section 2, Instructions to VendorsSubmitting Bids as the bid opening date and time.

SECTION 6: EVALUATION AND AWARD

6.1. Evaluation Process: Proposals will be evaluated in two parts by a committee of three (3) or more individuals. The first evaluation will be of the technical proposal and the second is an evaluation ofthe cost proposal. The Vendor who demonstrates that it meets all of the mandatory specifications required and represents best overall value, shall be awarded the contract.

6.2. Evaluation Criteria: Proposals will be evaluated based on criteria set forth in the solicitation and information contained in the proposals submitted in response to the solicitation. The technical evaluation will be based upon the point allocations designated below for a total of 70 of the I 00 points. Cost represents 30 of the 100 total points

Evaluation Point Allocation:

Project Goals and Proposed Approach (§ 4.1.1.) **(15) Points Possible**

The extent to which the vendor demonstrates a convincing approach to achieving the goals andobjectives described in this RFP.

Mandatory Qualifications and Experience (§ 4.1.2.) **(30) Points Possible**

The extent of the vendor's qualifications and experience indicate the likelihood of success in carrying out the services described in this RFP.

Cyber Security and Controls (§ 4.1.3.) **(25) Points Possible**

Cybersecurity systems and controls are essential to distinguish, prevent, counteract, or decrease security risks. These measures are requiredfor threat-management of potentially targeted computer systems and networks. These measures should be adaptive and robust. Vendor should complete the various attachments listed in this Section and provide the information requested so that the State can evaluate the quality of the vendor's Cyber Security Systems and Controls. The items contained in this section are not mandatory requirements, but will be evaluated and included in the vendor's technical score.

Total Technical Score	70 Points Possible
Total Cost Score	30 Points Possible
Total Proposal Score	**100 Points Possible**

6.3. Technical Bid Opening: At the technical bid opening, the Purchasing Division will open and announce the technical proposals received prior to the bid opening deadline. Once opened, the technical proposals will be provided to the Agency evaluation committee for technical evaluation.

6.4. Technical Evaluation: The Agency evaluation committee will review the technical proposals, assign points where appropriate, and make a final written recommendation to the Purchasing Division.

6.5. Proposal Disqualification:

6.5.1. **Minimum Acceptable Score ("MAS"):** Vendors must score a minimum of70% (49 points) of the total technical points possible in order to move past the technical evaluation and have their cost proposal evaluated. All vendor proposals not attaining the MAS will be disqualified.

6.5.2. **Failure to Meet Mandatory Requirement:** Vendors must meet or exceed all mandatory requirements in order to move past the technical evaluation and have their cost proposals evaluated. Proposals failing to meet one or more mandatory requirements of the RFP will bedisqualified.

6.6. Cost Bid Opening: The Purchasing Division will schedule a date and time to publicly open and announce cost proposals after technical evaluation has been completed and the Purchasing Division has approved the technical recommendation of the evaluation committee. All cost bids received will be opened. Cost bids for disqualified proposals will be opened for record keeping purposes only andwill not be evaluated or considered. Once opened, the cost proposals will be provided to the Agencyevaluation committee for cost evaluation.

The Purchasing Division reserves the right to disqualify a proposal based upon deficiencies in thetechnical proposal even after the cost evaluation.

6.7. Cost Evaluation: The Agency evaluation committee will review the cost proposals, assign points in accordance with the cost evaluation formula contained herein and make a final recommendation to the Purchasing Division.

Cost Evaluation Formula: Each cost proposal will have points assigned using the following formula for all Vendors not disqualified during the technical evaluation. The lowest cost of all proposals is divided by the cost of the proposal being evaluated to generate a cost score percentage.That percentage is then multiplied by the points attributable to the cost proposal to determine the number of points allocated to the cost proposal being evaluated.

Step 1: Lowest Cost of All Proposals / Cost of Proposal Being Evaluated = Cost Score Percentage

Step 2: Cost Score Percentage X Points Allocated to Cost Proposal= **Total Cost Score**

<u>Example:</u>

Proposal I Cost is
$1,000,000Proposal 2
Cost is $I, I00,000
Points Allocated to Cost Proposal is 30

Proposal 1: Step 1 - $1,000,000 / $1,000,000 = Cost Score Percentage of I (100%)Step 2 - I X 30 = Total Cost Score of 30

Proposal 2: Step 1-$1,000,000 / $1,100,000 = Cost Score Percentage of0.909091 (90.9091%)Step 2- 0.909091 X 30 = Total Cost Score of 27.27273

6.8. Availability of Information: Proposal submissions become public and are available for reviewimmediately after opening pursuant to West Virginia Code §SA-3-1 l(h). All other information associated with the RFP, including but not limited to, technical scores and reasons for disqualification, will not be available until after the contract has been awarded pursuant to West Virginia Code of State Rules §148-1-6.3.d.

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand therequirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

Democracy Live, Inc.
(Company)

Bryan Finney, President

Contact Phone: (206) 465-5636
Date: 11-18-2021

REQUEST FOR PROPOSAL

West Virginia Secretary of State
CRFP SOS2200000001
Election E-Ballot Delivery Technology

Attachment A: Addendum Number 1 and Acknowledgement

Attachment B -OW ASP Application Level Security Verification Levels 1-3

Attachment C - OWASP Mobile Application Level Security Verification if applicable

Attachment D - Security Requirements for Databases

Attachment E - Select Controls from NIST SP 800-171

Attachment F - POA&M Tracker (Democracy Live, N/A)

1 Purchasing Affidavit

Attachment A

Addendum Number 1 and Acknowledgement

SOLICITATION NUMBER: CRFP SOS2200000001
Addendum Number: 1

The purpose of this addendum is to modify the solicitation identified as ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category:

[✓] Modify bid opening date and time

[ ] Modify specifications of product or service being sought

[✓] Attachment of vendor questions and responses

[ ] Attachment of pre-bid sign-in sheet

[ ] Correction of error

[ ] Other

Description of Modification to Solicitation:

Addendum No. 1 is issued for the following reasons:

1) To publish a copy of vendor's questions with the answers/responses.

2) To extend the technical opening date to Monday November 22, 2021 @ 1:30 to allow vendors more time to prepare and submit bids

--no other changes--

Additional Documentation: Documentation related to this Addendum (if any) has been included herewith as Attachment A and is specifically incorporated herein by reference.

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.

2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

Revised 6/8/2012

Attachment A - Addendum Number 1 and Acknowledgement

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFP SOS22*1

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[X] Addendum No. 1

[ ] Addendum No. 2

[ ] Addendum No. 3

[ ] Addendum No. 4

[ ] Addendum No. 5

[ ] Addendum No. 6

[ ] Addendum No. 7

[ ] Addendum No. 8

[ ] Addendum No. 9

[ ] Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Democracy Live, Inc.
Company

Authorized Signature

11-18-21
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.
Revised 6/8/2012

Attachment B

OWASP Application Level Security Verification Levels 1-3

Attachment B OWASP Application Level Security Verification Levels 1 - 3

Open Web Application Security Project – Application Security Verification Standard 4.0.2 Level 1

Democracy Live Response: As part of our NIST SP 800-53 Compliance (as required and approved by the State of Michigan), Democracy Live complies with the below NIST SP 800-71, controls where applicable to OmniBallot.

Password Security Requirements

- Verify that user set passwords are at least 8 characters in length (after multiple spaces are combined).
- Verify that passwords 64 characters or longer are permitted but may be no longer than 128 characters.
- Verify that password truncation is not performed. However, consecutive multiple spaces may be replaced by a single space.
- Verify that any printable Unicode character, including language neutral characters such as spaces and Emojis are permitted in passwords.
- Verify users can change their password.
- Verify that password change functionality requires the user's current and new password.
- Verify that passwords submitted during account registration, login, and password change are checked against a set of breached passwords either locally (such as the top 1,000 or 10,000 most common passwords which match the system's password policy) or using an external API. If using an API a zero knowledge proof or other mechanism should be used to ensure that the plain text password is not sent or used in verifying the breach status of the password. If the password is breached, the application must require the user to set a new non-breached password.
- Verify that a password strength meter is provided to help users set a stronger password.
- Verify that there are no password composition rules limiting the type of characters permitted. There should be no requirement for upper or lower case or numbers or special characters.
- Verify that there are no periodic credential rotation or password history requirements.
- Verify that "paste" functionality, browser password helpers, and external password managers are permitted.
- Verify that the user can choose to either temporarily view the entire masked password, or temporarily view the last typed character of the password on platforms that do not have this as built-in functionality.

General Authenticator Requirements

- Verify that anti-automation controls are effective at mitigating breached credential testing, brute force, and account lockout attacks. Such controls include blocking the most common breached passwords, soft lockouts, rate limiting, CAPTCHA, ever increasing delays between attempts, IP address restrictions, or risk-based restrictions such as location, first login on a device, recent attempts to unlock the account, or similar. Verify that no more than 100 failed attempts per hour is possible on a single account.

- Verify that the use of weak authenticators (such as SMS and email) is limited to secondary verification and transaction approval and not as a replacement for more secure authentication methods. Verify that stronger methods are offered before weak methods, users are aware of the risks, or that proper measures are in place to limit the risks of account compromise.

- Verify that secure notifications are sent to users after updates to authentication details, such as credential resets, email or address changes, logging in from unknown or risky locations. The use of push notifications - rather than SMS or email - is preferred, but in the absence of push notifications, SMS or email is acceptable as long as no sensitive information is disclosed in the notification.

Authenticator Lifecycle Requirements

- Verify system generated initial passwords or activation codes SHOULD be securely randomly generated, SHOULD be at least 6 characters long, and MAY contain letters and numbers, and expire after a short period of time. These initial secrets must not be permitted to become the long term password.

Credential Recovery Requirements

- Verify that a system generated initial activation or recovery secret is not sent in clear text to the user.

- Verify password hints or knowledge-based authentication (so-called "secret questions") are not present.

- Verify password credential recovery does not reveal the current password in any way.

- Verify shared or default accounts are not present (e.g. "root", "admin", or "sa").

- Verify that if an authentication factor is changed or replaced, that the user is notified of this event.

- Verify forgotten password, and other recovery paths use a secure recovery mechanism, such as time-based OTP (TOTP) or other soft token, mobile push, or another offline recovery mechanism. (C6)

Out of Band Verifier Requirements

- Verify that clear text out of band (NIST "restricted") authenticators, such as SMS or PSTN, are not offered by default, and stronger alternatives such as push notifications are offered first.

- Verify that the out of band verifier expires out of band authentication requests, codes, or tokens after 10 minutes.

- Verify that the out of band verifier authentication requests, codes, or tokens are only usable once, and only for the original authentication request.

- Verify that the out of band authenticator and verifier communicates over a secure independent channel.

Single or Multi-factor One Time Verifier Requirements

- Verify that time-based OTPs have a defined lifetime before expiring.

Fundamental Session Management Requirements

- Verify the application never reveals session tokens in URL parameters.

Session Binding Requirements

- Verify the application generates a new session token on user authentication.

- Verify that session tokens possess at least 64 bits of entropy.

- Verify the application only stores session tokens in the browser using secure methods such as appropriately secured cookies (see section 3.4) or HTML 5 session storage.

Session Logout and Timeout Requirements

- Verify that logout and expiration invalidate the session token, such that the back button or a downstream relying party does not resume an authenticated session, including across relying parties.

Cookie-based Session Management

- Verify that cookie-based session tokens have the 'Secure' attribute set.

- Verify that cookie-based session tokens have the 'HttpOnly' attribute set.

- Verify that cookie-based session tokens utilize the 'SameSite' attribute to limit exposure to cross-site request forgery attacks.

- Verify that cookie-based session tokens use "__Host-" prefix (see references) to provide session cookie confidentiality.

- Verify that if the application is published under a domain name with other applications that set or use session cookies that might override or disclose the session cookies, set the path attribute in cookie-based session tokens using the most precise path possible.

General Access Control Design

- Verify that the application enforces access control rules on a trusted service layer, especially if client-side access control is present and could be bypassed.

- Verify that all user and data attributes and policy information used by access controls cannot be manipulated by end users unless specifically authorized.

- Verify that the principle of least privilege exists - users should only be able to access functions, data files, URLs, controllers, services, and other resources, for which they possess specific authorization. This implies protection against spoofing and elevation of privilege.

- Verify that the principle of deny by default exists whereby new users/roles start with minimal or no permissions and users/roles do not receive access to new features until access is explicitly assigned.

- Verify that access controls fail securely including when an exception occurs.

Operation Level Access Control

- Verify that sensitive data and APIs are protected against Insecure Direct Object Reference (IDOR) attacks targeting creation, reading, updating and deletion of records, such as creating or updating someone else's record, viewing everyone's records, or deleting all records.

- Verify that the application or framework enforces a strong anti-CSRF mechanism to protect authenticated functionality, and effective anti-automation or anti-CSRF protects unauthenticated functionality.

Other Access Control Considerations

- Verify administrative interfaces use appropriate multi-factor authentication to prevent unauthorized use.

- Verify that directory browsing is disabled unless deliberately desired. Additionally, applications should not allow discovery or disclosure of file or directory metadata, such as Thumbs.db, .DS_Store, .git or .svn folders.

Input Validation Requirements

- Verify that the application has defenses against HTTP parameter pollution attacks, particularly if the application framework makes no distinction about the source of request parameters (GET, POST, cookies, headers, or environment variables).

- Verify that frameworks protect against mass parameter assignment attacks, or that the application has countermeasures to protect against unsafe parameter assignment, such as marking fields private or similar.

- Verify that all input (HTML form fields, REST requests, URL parameters, HTTP headers, cookies, batch files, RSS feeds, etc) is validated using positive validation (allow lists).

- Verify that structured data is strongly typed and validated against a defined schema including allowed characters, length and pattern (e.g. credit card numbers or telephone, or validating that two related fields are reasonable, such as checking that suburb and zip/postcode match).

- Verify that URL redirects and forwards only allow destinations which appear on an allow list, or show a warning when redirecting to potentially untrusted content.

Sanitization and Sandboxing Requirements

- Verify that all untrusted HTML input from WYSIWYG editors or similar is properly sanitized with an HTML sanitizer library or framework feature.

- Verify that unstructured data is sanitized to enforce safety measures such as allowed characters and length.

- Verify that the application sanitizes user input before passing to mail systems to protect against SMTP or IMAP injection.

- Verify that the application avoids the use of eval() or other dynamic code execution features. Where there is no alternative, any user input being included must be sanitized or sandboxed before being executed.

- Verify that the application protects against template injection attacks by ensuring that any user input being included is sanitized or sandboxed.

- Verify that the application protects against SSRF attacks, by validating or sanitizing untrusted data or HTTP file metadata, such as filenames and URL input fields, and uses allow lists of protocols, domains, paths and ports.

- Verify that the application sanitizes, disables, or sandboxes user-supplied Scalable Vector Graphics (SVG) scriptable content, especially as they relate to XSS resulting from inline scripts, and foreignObject.

- Verify that the application sanitizes, disables, or sandboxes user-supplied scriptable or expression template language content, such as Markdown, CSS or XSL stylesheets, BBCode, or similar.

Output Encoding and Injection Prevention Requirements

- Verify that output encoding is relevant for the interpreter and context required. For example, use encoders specifically for HTML values, HTML attributes, JavaScript, URL parameters, HTTP headers, SMTP, and others as the context requires, especially from untrusted inputs (e.g. names with Unicode or apostrophes, such as ねこ or O'Hara).

- Verify that output encoding preserves the user's chosen character set and locale, such that any Unicode character point is valid and safely handled.

- Verify that context-aware, preferably automated - or at worst, manual - output escaping protects against reflected, stored, and DOM based XSS.

- Verify that data selection or database queries (e.g. SQL, HQL, ORM, NoSQL) use parameterized queries, ORMs, entity frameworks, or are otherwise protected from database injection attacks.

- Verify that where parameterized or safer mechanisms are not present, context-specific output encoding is used to protect against injection attacks, such as the use of SQL escaping to protect against SQL injection.

- Verify that the application protects against JavaScript or JSON injection attacks, including for eval attacks, remote JavaScript includes, Content Security Policy (CSP) bypasses, DOM XSS, and JavaScript expression evaluation.

- Verify that the application protects against LDAP injection vulnerabilities, or that specific security controls to prevent LDAP injection have been implemented.

- Verify that the application protects against OS command injection and that operating system calls use parameterized OS queries or use contextual command line output encoding.

- Verify that the application protects against Local File Inclusion (LFI) or Remote File Inclusion (RFI) attacks.

- Verify that the application protects against XPath injection or XML injection attacks.

Deserialization Prevention Requirements

- Verify that serialized objects use integrity checks or are encrypted to prevent hostile object creation or data tampering.

- Verify that the application correctly restricts XML parsers to only use the most restrictive configuration possible and to ensure that unsafe features such as resolving external entities are disabled to prevent XML eXternal Entity (XXE) attacks.

- Verify that deserialization of untrusted data is avoided or is protected in both custom code and third-party libraries (such as JSON, XML and YAML parsers).

- Verify that when parsing JSON in browsers or JavaScript-based backends, JSON.parse is used to parse the JSON document. Do not use eval() to parse JSON.

Algorithms

- Verify that all cryptographic modules fail securely, and errors are handled in a way that does not enable Padding Oracle attacks.

Log Content Requirements

- Verify that the application does not log credentials or payment details. Session tokens should only be stored in logs in an irreversible, hashed form.

- Verify that the application does not log other sensitive data as defined under local privacy laws or relevant security policy.

Error Handling

- Verify that a generic message is shown when an unexpected or security sensitive error occurs, potentially with a unique ID which support personnel can use to investigate.

Client-side Data Protection

- Verify the application sets sufficient anti-caching headers so that sensitive data is not cached in modern browsers.

- Verify that data stored in browser storage (such as HTML5 local storage, session storage, IndexedDB, or cookies) does not contain sensitive data or PII.

- Verify that authenticated data is cleared from client storage, such as the browser DOM, after the client or session is terminated.

Sensitive Private Data

- Verify that sensitive data is sent to the server in the HTTP message body or headers, and that query string parameters from any HTTP verb do not contain sensitive data.

- Verify that users have a method to remove or export their data on demand.

- Verify that users are provided clear language regarding collection and use of supplied personal information and that users have provided opt-in consent for the use of that data before it is used in any way.

- Verify that all sensitive data created and processed by the application has been identified, and ensure that a policy is in place on how to deal with sensitive data.

Deployed Application Integrity Controls

- Verify that if the application has a client or server auto-update feature, updates should be obtained over secure channels and digitally signed. The update code must validate the digital signature of the update before installing or executing the update.

- Verify that the application employs integrity protections, such as code signing or sub-resource integrity. The application must not load or execute code from untrusted sources, such as loading includes, modules, plugins, code, or libraries from untrusted sources or the Internet.

- Verify that the application has protection from sub-domain takeovers if the application relies upon DNS entries or DNS sub-domains, such as expired domain names, out of date DNS pointers or CNAMEs, expired projects at public source code repos, or transient cloud APIs, serverless functions, or storage buckets (autogen-bucket-id.cloud.example.com) or similar. Protections can include ensuring that DNS names used by applications are regularly checked for expiry or change.

Business Logic Security Requirements

- Verify the application will only process business logic flows for the same user in sequential step order and without skipping steps.

- Verify the application will only process business logic flows with all steps being processed in realistic human time, i.e. transactions are not submitted too quickly.

- Verify the application has appropriate limits for specific business actions or transactions which are correctly enforced on a per user basis.

- Verify the application has sufficient anti-automation controls to detect and protect against data exfiltration, excessive business logic requests, excessive file uploads or denial of service attacks.

- Verify the application has business logic limits or validation to protect against likely business risks or threats, identified using threat modelling or similar methodologies.

File Upload Requirements

- Verify that the application will not accept large files that could fill up storage or cause a denial of service.

File Execution Requirements

- Verify that user-submitted filename metadata is not used directly by system or framework filesystems and that a URL API is used to protect against path traversal.

- Verify that user-submitted filename metadata is validated or ignored to prevent the disclosure, creation, updating or removal of local files (LFI).

- Verify that user-submitted filename metadata is validated or ignored to prevent the disclosure or execution of remote files via Remote File Inclusion (RFI) or Server-side Request Forgery (SSRF) attacks.

- Verify that the application protects against Reflective File Download (RFD) by validating or ignoring user-submitted filenames in a JSON, JSONP, or URL parameter, the response Content-Type header should be set to text/plain, and the Content-Disposition header should have a fixed filename.

- Verify that untrusted file metadata is not used directly with system API or libraries, to protect against OS command injection.

File Storage Requirements

- Verify that files obtained from untrusted sources are stored outside the web root, with limited permissions, preferably with strong validation.

- Verify that files obtained from untrusted sources are scanned by antivirus scanners to prevent upload of known malicious content.

File Download Requirements

- Verify that the web tier is configured to serve only files with specific file extensions to prevent unintentional information and source code leakage. For example, backup files (e.g. .bak), temporary working files (e.g. .swp), compressed files (.zip, .tar.gz, etc) and other extensions commonly used by editors should be blocked unless required.

- Verify that direct requests to uploaded files will never be executed as HTML/JavaScript content.

SSRF Protection Requirements

- Verify that the web or application server is configured with an allow of resources or systems to which the server can send requests or load data/files from.

Generic Web Service Security Verification Requirements

- Verify that all application components use the same encodings and parsers to avoid parsing attacks that exploit different URI or file parsing behavior that could be used in SSRF and RFI attacks.

- Verify that access to administration and management functions is limited to authorized administrators.

- Verify API URLs do not expose sensitive information, such as the API key, session tokens etc.

RESTful Web Service Verification Requirements

- Verify that enabled RESTful HTTP methods are a valid choice for the user or action, such as preventing normal users using DELETE or PUT on protected API or resources.

- Verify that JSON schema validation is in place and verified before accepting input.

- Verify that RESTful web services that utilize cookies are protected from Cross-Site Request Forgery via the use of at least one or more of the following: double submit cookie pattern, CSRF nonces, or ORIGIN request header checks.

SOAP Web Service Verification Requirements

- Verify that XSD schema validation takes place to ensure a properly formed XML document, followed by validation of each input field before any processing of that data takes place.

Dependency

- Verify that all components are up to date, preferably using a dependency checker during build or compile time.

- Verify that all unneeded features, documentation, samples, configurations are removed, such as sample applications, platform documentation, and default or example users.

- Verify that if application assets, such as JavaScript libraries, CSS stylesheets or web fonts, are hosted externally on a Content Delivery Network (CDN) or external provider, Subresource Integrity (SRI) is used to validate the integrity of the asset.

Unintended Security Disclosure Requirements

- Verify that web or application server and framework error messages are configured to deliver user actionable, customized responses to eliminate any unintended security disclosures.

- Verify that web or application server and application framework debug modes are disabled in production to eliminate debug features, developer consoles, and unintended security disclosures.

- Verify that the HTTP headers or any part of the HTTP response do not expose detailed version information of system components.

HTTP Security Headers Requirements

- Verify that every HTTP response contains a Content-Type header. text/*,/ +xml and application/xml content types should also specify a safe character set (e.g., UTF-8, ISO 8859-1).

- Verify that all API responses contain Content-Disposition: attachment; filename="api.json" header (or other appropriate filename for the content type).

- Verify that a Content Security Policy (CSP) response header is in place that helps mitigate impact for XSS attacks like HTML, DOM, JSON, and JavaScript injection vulnerabilities.

- Verify that all responses contain X-Content-Type-Options: nosniff header.

- Verify that a Strict-Transport-Security header is included on all responses and for all subdomains, such as Strict-Transport-Security: max-age=15724800; includeSubdomains.

- Verify that a suitable "Referrer-Policy" header is included, such as "no-referrer" or "same-origin".

- Verify that the content of a web application cannot be embedded in a third-party site by default and that embedding of the exact resources is only allowed where necessary by using suitable Content-Security-Policy: frame-ancestors and X-Frame-Options response headers.

Validate HTTP Request Header Requirements

- Verify that the application server only accepts the HTTP methods in use by the application/API, including pre-flight OPTIONS, and logs/alerts or any requests that are not valid for the application context.

- Verify that the supplied Origin header is not used for authentication or access control decisions, as the Origin header can easily be changed by an attacker.

- Verify that the Cross-Origin Resource Sharing (CORS) Access-Control-Allow-Origin header uses a strict allow list of trusted domains and subdomains to match against and does not support the "null" origin.

Select Controls from Open Web Application Security Project – Application Security Verification Standard 4.0.2 Level 2

Secure Software Development Lifecycle

- Verify the use of a secure software development lifecycle that addresses security in all stages of development.

- Verify documentation and justification of all the application's trust boundaries, components, and significant data flows.

- Verify implementation of centralized, simple (economy of design), vetted, secure, and reusable security controls to avoid duplicate, missing, ineffective, or insecure controls.

- Verify availability of a secure coding checklist, security requirements, guideline, or policy to all developers and testers.

Authentication Architectural Requirements

- Verify that communications between application components, including APIs, middleware and data layers, are authenticated. Components should have the least necessary privileges needed.

- Verify that the application uses a single vetted authentication mechanism that is known to be secure, can be extended to include strong authentication, and has sufficient logging and monitoring to detect account abuse or breaches.

- Verify that all authentication pathways and identity management APIs implement consistent authentication security control strength, such that there are no weaker alternatives per the risk of the application.

Access Control Architectural Requirements

- Verify enforcement of the principle of least privilege in functions, data files, URLs, controllers, services, and other resources. This implies protection against spoofing and elevation of privilege.

- Verify the application uses a single and well-vetted access control mechanism for accessing protected data and resources. All requests must pass through this single mechanism to avoid copy and paste or insecure alternative paths.

- Verify that attribute or feature-based access control is used whereby the code checks the user's authorization for a feature/data item rather than just their role. Permissions should still be allocated using roles.

Input and Output Architectural Requirements

- Verify that input and output requirements clearly define how to handle and process data based on type, content, and applicable laws, regulations, and other policy compliance.

- Verify that serialization is not used when communicating with untrusted clients. If this is not possible, ensure that adequate integrity controls (and possibly encryption if sensitive data is sent) are enforced to prevent deserialization attacks including object injection.

Cryptographic Architectural Requirements

- Verify that there is an explicit policy for management of cryptographic keys and that a cryptographic key lifecycle follows a key management standard such as NIST SP 800-57.

- Verify that consumers of cryptographic services protect key material and other secrets by using key vaults or API based alternatives.

- Verify that all keys and passwords are replaceable and are part of a well-defined process to re-encrypt sensitive data.

- Verify that the architecture treats client-side secrets—such as symmetric keys, passwords, or API tokens—as insecure and never uses them to protect or access sensitive data.

Errors, Logging and Auditing Architectural Requirements

- Verify that a common logging format and approach is used across the system.

- Verify that logs are securely transmitted to a preferably remote system for analysis, detection, alerting, and escalation.

Data Protection and Privacy Architectural Requirements

- Verify that all sensitive data is identified and classified into protection levels.

- Verify that all protection levels have an associated set of protection requirements, such as encryption requirements, integrity requirements, retention, privacy and other confidentiality requirements, and that these are applied in the architecture.

Communications Architectural Requirements

- Verify the application encrypts communications between components, particularly when these components are in different containers, systems, sites, or cloud providers.

- Verify that application components verify the authenticity of each side in a communication link to prevent person-in-the-middle attacks. For example, application components should validate TLS certificates and chains.

Malicious Software Architectural Requirements

- Verify that a source code control system is in use, with procedures to ensure that check-ins are accompanied by issues or change tickets. The source code control system should have access control and identifiable users to allow traceability of any changes.

Secure File Upload Architectural Requirements

- Verify that user-uploaded files are stored outside of the web root.

- Verify that user-uploaded files - if required to be displayed or downloaded from the application - are served by either octet stream downloads, or from an unrelated domain, such as a cloud file storage bucket. Implement a suitable Content Security Policy (CSP) to reduce the risk from XSS vectors or other attacks from the uploaded file.

Configuration Architectural Requirements

- Verify the segregation of components of differing trust levels through well-defined security controls, firewall rules, API gateways, reverse proxies, cloud-based security groups, or similar mechanisms.

- Verify that the build pipeline warns of out-of-date or insecure components and takes appropriate actions.

- Verify that the build pipeline contains a build step to automatically build and verify the secure deployment of the application, particularly if the application infrastructure is software defined, such as cloud environment build scripts.

- Verify that application deployments adequately sandbox, containerize and/or isolate at the network level to delay and deter attackers from attacking other applications, especially when they are performing sensitive or dangerous actions such as deserialization.

- Verify the application does not use unsupported, insecure, or deprecated client-side technologies such as NSAPI plugins, Flash, Shockwave, ActiveX, Silverlight, NACL, or client-side Java applets.

Credential Storage Requirements

- Verify that passwords are stored in a form that is resistant to offline attacks. Passwords SHALL be salted and hashed using an approved one-way key derivation or password hashing function. Key derivation and password hashing functions take a password, a salt, and a cost factor as inputs when generating a password hash.

- Verify that the salt is at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes. For each credential, a unique salt value and the resulting hash SHALL be stored.

- Verify that if PBKDF2 is used, the iteration count SHOULD be as large as verification server performance will allow, typically at least 100,000 iterations.

Credential Recovery Requirements

- Verify that if OTP or multi-factor authentication factors are lost, that evidence of identity proofing is performed at the same level as during enrollment.

Look-up Secret Verifier Requirements

- Verify that lookup secrets can be used only once.

- Verify that lookup secrets have sufficient randomness (112 bits of entropy), or if less than 112 bits of entropy, salted with a unique and random 32-bit salt and hashed with an approved one-way hash.

- Verify that lookup secrets are resistant to offline attacks, such as predictable values.

Out of Band Verifier Requirements

- Verify that the out of band verifier retains only a hashed version of the authentication code.

- Verify that the initial authentication code is generated by a secure random number generator, containing at least 20 bits of entropy (typically a six digital random number is sufficient).

Single or Multi Factor One Time Verifier Requirements

- Verify that symmetric keys used to verify submitted OTPs are highly protected, such as by using a hardware security module or secure operating system based key storage.

- Verify that approved cryptographic algorithms are used in the generation, seeding, and verification of OTPs.

- Verify that time-based OTP can be used only once within the validity period.

- Verify that if a time-based multi factor OTP token is re-used during the validity period, it is logged and rejected with secure notifications being sent to the holder of the device.

Cryptographic Software and Devices Verifier Requirements

- Verify that cryptographic keys used in verification are stored securely and protected against disclosure, such as using a Trusted Platform Module (TPM) or Hardware Security Module (HSM), or an OS service that can use this secure storage.

- Verify that the challenge nonce is at least 64 bits in length, and statistically unique or unique over the lifetime of the cryptographic device.

- Verify that approved cryptographic algorithms are used in the generation, seeding, and verification.

Service Authentication Requirements

- Verify that if passwords are required for service authentication, the service account used is not a default credential. (e.g. root/root or admin/admin are default in some services during installation.

- Verify that passwords are stored with sufficient protection to prevent offline recovery attacks, including local system access.

Session Binding Requirements

- Verify that session token are generated using approved cryptographic algorithms.

Session Logout and Timeout Requirements

- Verify that the application gives the option to terminate all other active sessions after a successful password change (including change via password reset/recovery), and that this is effective across the application, federated login (if present), and any relying parties.

- Verify that users are able to view and (having re-entered login credentials) log out of any or all currently active sessions and devices.

Token Based Session Management

- Verify the application uses session tokens rather than static API secrets and keys, except with legacy implementations.

- Verify that stateless session tokens use digital signatures, encryption, and other countermeasures to protect against tampering, enveloping, replay, null cipher, and key substitution attacks.

Other Access Control Considerations

- Verify the application has additional authorization (such as step up or adaptive authentication) for lower value systems, and / or segregation of duties for high value applications to enforce anti-fraud controls as per the risk of application and past fraud.

Data Classification

- Verify that regulated private data is stored encrypted while at rest, such as Personally Identifiable Information (PII), sensitive personal information, or data assessed likely to be subject to EU's GDPR.

Algorithms

- Verify that industry proven or government approved cryptographic algorithms, modes, and libraries are used, instead of custom coded cryptography.
- Verify that encryption initialization vector, cipher configuration, and block modes are configured securely using the latest advice.
- Verify that random number, encryption or hashing algorithms, key lengths, rounds, ciphers or modes, can be reconfigured, upgraded, or swapped at any time, to protect against cryptographic breaks.
- Verify that known insecure block modes (i.e. ECB, etc.), padding modes (i.e. PKCS#1 v1.5, etc.), ciphers with small block sizes (i.e. Triple-DES, Blowfish, etc.), and weak hashing algorithms (i.e. MD5, SHA1, etc.) are not used unless required for backwards compatibility.
- Verify that nonces, initialization vectors, and other single use numbers must not be used more than once with a given encryption key. The method of generation must be appropriate for the algorithm being used.

Random Values

- Verify that all random numbers, random file names, random GUIDs, and random strings are generated using the cryptographic module's approved cryptographically secure random number generator when these random values are intended to be not guessable by an attacker.
- Verify that random GUIDs are created using the GUID v4 algorithm, and a Cryptographically-secure Pseudo-random Number Generator (CSPRNG). GUIDs created using other pseudo-random number generators may be predictable.

Secret Management

- Verify that a secrets management solution such as a key vault is used to securely create, store, control access to and destroy secrets.
- Verify that key material is not exposed to the application but instead uses an isolated security module like a vault for cryptographic operations.

Log Content Requirements

- Verify that the application logs security relevant events including successful and failed authentication events, access control failures, deserialization failures and input validation failures.

- Verify that each log event includes necessary information that would allow for a detailed investigation of the timeline when an event happens.

Log Processing Requirements

- Verify that all authentication decisions are logged, without storing sensitive session tokens or passwords. This should include requests with relevant metadata needed for security investigations.

- Verify that all access control decisions can be logged and all failed decisions are logged. This should include requests with relevant metadata needed for security investigations.

Log Protection Requirements

- Verify that the application appropriately encodes user-supplied data to prevent log injection.

- Verify that all events are protected from injection when viewed in log viewing software.

- Verify that security logs are protected from unauthorized access and modification.

- Verify that time sources are synchronized to the correct time and time zone. Strongly consider logging only in UTC if systems are global to assist with post-incident forensic analysis.

Error Handling

- Verify that a "last resort" error handler is defined which will catch all unhandled exceptions.

General Data Protection

- Verify the application protects sensitive data from being cached in server components such as load balancers and application caches.

- Verify that all cached or temporary copies of sensitive data stored on the server are protected from unauthorized access or purged/invalidated after the authorized user accesses the sensitive data.

- Verify the application minimizes the number of parameters in a request, such as hidden fields, Ajax variables, cookies and header values.

- Verify the application can detect and alert on abnormal numbers of requests, such as by IP, user, total per hour or day, or whatever makes sense for the application.

Sensitive Private Data

- Verify accessing sensitive data is audited (without logging the sensitive data itself), if the data is collected under relevant data protection directives or where logging of access is required.

- Verify that sensitive information contained in memory is overwritten as soon as it is no longer required to mitigate memory dumping attacks, using zeroes or random data.

- Verify that sensitive or private information that is required to be encrypted, is encrypted using approved algorithms that provide both confidentiality and integrity.

- Verify that sensitive personal information is subject to data retention classification, such that old or out of date data is deleted automatically, on a schedule, or as the situation requires.

Client Communications Security Requirements

- Verify that secured TLS is used for all client connectivity, and does not fall back to insecure or unencrypted protocols.

- Verify using online or up to date TLS testing tools that only strong algorithms, ciphers, and protocols are enabled, with the strongest algorithms and ciphers set as preferred.

- Verify that old versions of SSL and TLS protocols, algorithms, ciphers, and configuration are disabled, such as SSLv2, SSLv3, or TLS 1.0 and TLS 1.1. The latest version of TLS should be the preferred cipher suite.

Server Communications Security Requirements

- Verify that connections to and from the server use trusted TLS certificates. Where internally generated or self-signed certificates are used, the server must be configured to only trust specific internal CAs and specific self-signed certificates. All others should be rejected.

- Verify that encrypted communications such as TLS is used for all inbound and outbound connections, including for management ports, monitoring, authentication, API, or web service calls, database, cloud, serverless, mainframe, external, and partner connections. The server must not fall back to insecure or unencrypted protocols.

- Verify that all encrypted connections to external systems that involve sensitive information or functions are authenticated.

- Verify that proper certification revocation, such as Online Certificate Status Protocol (OCSP) Stapling, is enabled and configured.

Malicious Code Search

- Verify that the application source code and third party libraries do not contain unauthorized phone home or data collection capabilities. Where such functionality exists, obtain the user's permission for it to operate before collecting any data.

- Verify that the application does not ask for unnecessary or excessive permissions to privacy related features or sensors, such as contacts, cameras, microphones, or location.

Business Logic Security Requirements

- Verify the application has configurable alerting when automated attacks or unusual activity is detected.

File Integrity Requirements

- Verify that files obtained from untrusted sources are validated to be of expected type based on the file's content.

File Execution Requirements

- Verify that the application does not include and execute functionality from untrusted sources, such as unverified content distribution networks, JavaScript libraries, node npm libraries, or server-side DLLs.

RESTful Web Service Verification Requirements

- Verify that the message headers and payload are trustworthy and not modified in transit. Requiring strong encryption for transport (TLS only) may be sufficient in many cases as it provides both confidentiality and integrity protection. Per-message digital signatures can provide additional assurance on top of the transport protections for high-security applications but bring with them additional complexity and risks to weigh against the benefits.

SOAP Web Service Verification Requirements

- Verify that the message payload is signed using WS-Security to ensure reliable transport between client and service.

GraphQL and other Web Service Data Layer Security Requirements

- Verify that query allow list or a combination of depth limiting and amount limiting is used to prevent GraphQL or data layer expression Denial of Service (DoS) as a result of expensive, nested queries. For more advanced scenarios, query cost analysis should be used.

Build

- Verify that the application build and deployment processes are performed in a secure and repeatable way, such as CI / CD automation, automated configuration management, and automated deployment scripts.

- Verify that compiler flags are configured to enable all available buffer overflow protections and warnings, including stack randomization, data execution prevention, and to break the build if an unsafe pointer, memory, format string, integer, or string operations are found.

- Verify that server configuration is hardened as per the recommendations of the application server and frameworks in use.

- Verify that the application, configuration, and all dependencies can be re-deployed using automated deployment scripts, built from a documented and tested runbook in a reasonable time, or restored from backups in a timely fashion.

Dependency

- Verify that third party components come from pre-defined, trusted and continually maintained repositories.

- Verify that the attack surface is reduced by sandboxing or encapsulating third party libraries to expose only the required behaviour into the application.

Validate HTTP Request Header Requirements

- Verify that HTTP headers added by a trusted proxy or SSO devices, such as a bearer token, are authenticated by the application.

Select Controls from Open Web Application Security Project – Application Security Verification Standard 4.0.2 Level 3

General Authenticator Requirements

- Verify impersonation resistance against phishing, such as the use of multi-factor authentication, cryptographic devices with intent (such as connected keys with a push to authenticate), or at higher AAL levels, client-side certificates.

- Verify that where a Credential Service Provider (CSP) and the application verifying authentication are separated, mutually authenticated TLS is in place between the two endpoints.

Session Logout and Timeout Requirements

- If authenticators permit users to remain logged in, verify that re-authentication occurs periodically with 2FA both when actively used after 12 hours or after an idle period of 15 minutes.

Algorithms

- Verify that encrypted data is authenticated via signatures, authenticated cipher modes, or HMAC to ensure that ciphertext is not altered by an unauthorized party.

General Data Protection

- Verify that regular backups of important data are performed and that test restoration of data is performed.

- Verify that backups are stored securely to prevent data from being stolen or corrupted.

Code Integrity Controls

- Verify that a code analysis tool is in use that can detect potentially malicious code, such as time functions, unsafe file operations and network connections.

Malicious Code Search

- Verify that the application source code and third party libraries do not contain back doors, such as hard-coded or additional undocumented accounts or keys, code obfuscation, undocumented binary blobs, rootkits, or anti-debugging, insecure debugging features, or otherwise out of date, insecure, or hidden functionality that could be used maliciously if discovered.

- Verify that the application source code and third party libraries does not contain time bombs by searching for date and time related functions.
- Verify that the application source code and third party libraries does not contain malicious code, such as salami attacks, logic bypasses, or logic bombs.
- Verify that the application source code and third party libraries do not contain Easter eggs or any other potentially unwanted functionality.

Attachment C

OWASP Mobile Application Level Security Verification

Attachment C OWASP Mobile Application Level Security Verification if applicable

Open Web Application Security Project – Mobile Application Security Verification Standard 1.2 Level 3

Democracy Live Response: Democracy Live has implemented controls for Controlled Unclassified Information (CUI) exceeding NIST 800-171 by electing the NIST 800-53 CSF Medium Impact controls to comply with the more stringent 800-53 standards. As part of our NIST SP 800-53 Compliance (as required and approved by the State of Michigan), Democracy Live complies with the below NIST SP 800-71 controls, where applicable to OmniBallot.

Architecture, design and threat modeling

- All app components are identified and known to be needed.
- Security controls are never enforced only on the client side, but on the respective remote endpoints.
- A high-level architecture for the mobile app and all connected remote services has been defined and security has been addressed in that architecture.
- Data considered sensitive in the context of the mobile app is clearly identified.
- The app should comply with privacy laws and regulations.

Data Storage and Privacy

- System credential storage facilities need to be used to store sensitive data, such as PII, user credentials or cryptographic keys.
- No sensitive data should be stored outside of the app container or system credential storage facilities.
- No sensitive data is written to application logs.
- No sensitive data is shared with third parties unless it is a necessary part of the architecture.
- The keyboard cache is disabled on text inputs that process sensitive data.
- No sensitive data is exposed via IPC mechanisms.
- No sensitive data, such as passwords or pins, is exposed through the user interface.

Cryptography

- The app does not rely on symmetric cryptography with hardcoded keys as a sole method of encryption.
- The app uses proven implementations of cryptographic primitives.
- The app uses cryptographic primitives that are appropriate for the particular use-case, configured with parameters that adhere to industry best practices.
- The app does not use cryptographic protocols or algorithms that are widely considered depreciated for security purposes.
- The app doesn't re-use the same cryptographic key for multiple purposes.
- All random values are generated using a sufficiently secure random number generator.

Authentication and Session Management

- If the app provides users with access to a remote service, some form of authentication such as username/password authentication is performed at the remote endpoint.
- If stateful session management is used, the remote endpoint uses randomly generated session identifiers to authenticate client requests without sending the user's credentials.
- If stateless token-based authentication is used, the server provides a token that has been signed using a secure algorithm.
- The remote endpoint terminates the existing session when the user logs out.
- A password policy exists and is enforced at the remote endpoint.
- The remote endpoint implements an mechanism to protect against the submission of credentials an excessive number of times.
- Sessions are invalidated at the remote endpoint after a predefined period of inactivity and access tokens expire.

Network Communication

- Data is encrypted on the network using TLS. The secure channel is used consistently throughout the app.
- The TLS settings are in line with current best practices, or as close as possible if the mobile operating system does not support the recommended standards.
- The app verifies the X.509 certificate of the remote endpoint when the secure channel is established. Only certificates signed by a valid CA are accepted.

Platform Interaction

- The app only requests the minimum set of permissions necessary.
- All inputs from external sources and the user are validated and, if necessary, sanitized. This includes data received via the UI, IPC mechanisms such as intents, custom URLs, and network sources.
- The app does not export sensitive functionality via custom URL schemes, unless these mechanisms are properly protected.
- The app does not export sensitive functionality through IPC facilities, unless these mechanisms are properly protected.
- JavaScript is disabled in WebViews unless explicitly required.
- WebViews are configured to allow only the minimum set of protocol handlers required (ideally, only https is supported). Potentially dangerous handlers, such as file, tel and app-id, are disabled.
- If native methods of the app are exposed to a WebView, verify that the WebView only renders JavaScript contained within the app package.
- Object deserialization, if any, is implemented using safe serialization APIs.

Code Quality and Build Settings

- The app is signed and provisioned with valid certificate, of which the private key is property protected.
- The app has been built in release mode, with settings appropriate for a release build (e.g. non-debuggable).
- Debugging symbols have been removed from native binaries.
- Debugging code and developer assistance code (e.g. test code, backdoors, hidden settings) have been removed. The app does not log verbose errors or debugging messages.
- All third party components used by the mobile app, such as libraries and frameworks, are identified, and checked for known vulnerabilities.
- The app catches and handles possible exceptions.
- Error handling logic in security controls denies access by default.
- In unmanaged code, memory is allocated, freed and used securely.
- Free security features offered by the toolchain, such as byte-code minification, stack protection, PIE support and automatic reference counting, are activated.

Select Controls from Open Web Application Security Project – Mobile Application Security Verification Standard 1.2 Level 2

Architecture, design and threat modeling

- All app components are defined in terms of the business functions and/or security functions they provide.
- A threat model for the mobile app and the associated remote services has been produced that identifies potential threats and countermeasures.
- All security controls have a centralized implementation.
- There is an explicit policy for how cryptographic keys (if any) are managed, and the lifecycle of cryptographic keys is enforced. Ideally, follow a key management standard such as NIST SP 800-57.
- A mechanism for enforcing updates of the mobile app exists.

- Security is addressed within all parts of the software development lifecycle.
- A responsible disclosure policy is in place and effectively applied.

Data Storage and Privacy

- No sensitive data is included in backups generated by the mobile operating system.
- The app removes sensitive data from views when backgrounded.
- The app does not hold sensitive data in memory longer than necessary, and memory is cleared explicitly after use.
- The app educates the user about the types of personally identifiable information processed, as well as security best practices the user should follow in using the app.
- No sensitive data should be stored locally on the mobile device. Instead data should be retrieved from a remote endpoint.

Authentication and Session Management

- A second factor of authentication exists at the remote endpoint and the 2FA requirement is consistently enforced.

Network Communication

- The app either uses its own certificate store, or pins the endpoint certificate or public key, and subsequently does not establish connections with endpoints that offer a different certificate or key, even if signed by a trusted CA.
- The app doesn't rely on a single insecure communication channel (email or SMS) for critical operations, such as enrollments and account recovery.
- The app only depends on up-to-date connectivity and security libraries.

Platform Interaction

- The app protects itself against screen overlay attacks. (Android only)
- A WebView's cache, storage, and loaded resources (JavaScript, etc.) should be cleared before the WebView is destroyed.
- Verify that the app prevents usage of custom third-party keyboards whenever sensitive data is entered.

Select Controls from Open Web Application Security Project – Mobile Application Security Verification Standard 1.2

Impede Dynamic Analysis and Tampering

- The app detects, and responds to, the presence of a rooted or jailbroken device either by alerting the user or terminating the app.
- The app prevents debugging and/or detects, and responds to, a debugger being attached. All available debugging protocols must be covered.
- Obfuscation is applied to programmatic defenses, which in turn impede de-obfuscation via dynamic analysis.

Impede Comprehension

- All executable files and libraries belonging to the app are either encrypted on the file level and/or important code and data segments inside the executables are encrypted or packed. Trivial static analysis does not reveal important code or data.

Impede Eavesdropping

- As a defense in depth, next to having solid hardening of the communicating parties, application level payload encryption can be applied to further impede eavesdropping.

Attachment D

Security Requirements for Databases

Attachment D Security Requirements for Database

Democracy Live Response: Democracy Live has implemented controls for Controlled Unclassified Information (CUI) exceeding NIST 800-171 by electing the NIST 800-53 CSF Medium Impact controls to comply with the more stringent standards. Democracy Live implements and maintains system security controls to protect any and all sensitive data from unauthorized access and use. Least privilege access is practiced with all system services and data along with monitoring and incident response plans.

As part of our NIST SP 800-53 Compliance (as required and approved by the State of Michigan), Democracy Live complies with the below NIST SP 800-171 controls, where applicable to OmniBallot.

Security Controls from Department of Defense – Security Requirements Guide for Databases (Moderate Controls)

The DBMS must limit the number of concurrent sessions to an organization-defined number per user for all accounts and/or account types.

The DBMS must protect against a user falsely repudiating having performed organization-defined actions.

The DBMS must be able to generate audit records when privileges/permissions are retrieved.

The DBMS must be able to generate audit records when unsuccessful attempts to retrieve privileges/permissions occur.

The DBMS must initiate session auditing upon startup.

The DBMS must produce audit records containing sufficient information to establish what type of events occurred.

The DBMS must produce audit records containing time stamps to establish when the events occurred.

The DBMS must produce audit records containing sufficient information to establish where the events occurred.

The DBMS must produce audit records containing sufficient information to establish the sources (origins) of the events.

The DBMS must produce audit records containing sufficient information to establish the outcome (success or failure) of the events.

The DBMS must produce audit records containing sufficient information to establish the identity of any user/subject or process associated with the event.

The DBMS must include additional, more detailed, organization-defined information in the audit records for audit events identified by type, location, or subject.

The DBMS must by default shut down upon audit failure, to include the unavailability of space for more audit log records; or must be configurable to shut down upon audit failure.

The DBMS must be configurable to overwrite audit log records, oldest first (First-In-First-Out - FIFO), in the event of unavailability of space for more audit log records.

The DBMS must use system clocks to generate time stamps for use in audit records and application data.

The audit information produced by the DBMS must be protected from unauthorized read access.

The audit information produced by the DBMS must be protected from unauthorized modification.

The audit information produced by the DBMS must be protected from unauthorized deletion.

The DBMS must protect its audit features from unauthorized access.

The DBMS must protect its audit configuration from unauthorized modification.

The DBMS must protect its audit features from unauthorized removal.

The DBMS must limit privileges to change software modules, to include stored procedures, functions and triggers, and links to software external to the DBMS.

The DBMS software installation account must be restricted to authorized users.

Database software, including DBMS configuration files, must be stored in dedicated directories, or DASD pools, separate from the host OS and other applications.

Database objects (including but not limited to tables, indexes, storage, stored procedures, functions, triggers, links to software external to the DBMS, etc.) must be owned by database/DBMS principals authorized for ownership.

The role(s)/group(s) used to modify database structure (including but not necessarily limited to tables, indexes, storage, etc.) and logic modules (stored procedures, functions, triggers, links to software external to the DBMS, etc.) must be restricted to authorized users.

Default demonstration and sample databases, database objects, and applications must be removed.

Unused database components, DBMS software, and database objects must be removed.

Unused database components that are integrated in the DBMS and cannot be uninstalled must be disabled.

Access to external executables must be disabled or restricted.

The DBMS must uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).

If passwords are used for authentication, the DBMS must store only hashed, salted representations of passwords.

If passwords are used for authentication, the DBMS must transmit only encrypted representations of passwords.

The DBMS must obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

The DBMS must use NIST FIPS 140-2 validated cryptographic modules for cryptographic operations.

The DBMS must separate user functionality (including user interface services) from database management functionality.

The DBMS must invalidate session identifiers upon user logout or other session termination.

The DBMS must recognize only system-generated session identifiers.

The DBMS must maintain the authenticity of communications sessions by guarding against man-in-the-middle attacks that guess at Session ID values.

The DBMS must fail to a secure state if system initialization fails, shutdown fails, or aborts fail.

In the event of a system failure, the DBMS must preserve any information necessary to determine cause of failure and any information necessary to return to operations with least disruption to mission processes.

The DBMS must protect the confidentiality and integrity of all information at rest.

The DBMS must isolate security functions from non-security functions.

Attachment E

Select Controls From NIST SP 800-171

Attachment E Select Controls from NIST SP 800-171

Democracy Live Response: Democracy Live has implemented controls for Controlled Unclassified Information (CUI) exceeding NIST 800-171 by electing the NIST 800-53 CSF Medium Impact controls to comply with the more stringent standards. Democracy Live implements and maintains system security controls to protect any and all sensitive data from unauthorized access and use. Least privilege access is practiced with all system services and data along with monitoring and incident response plans.

As part of our NIST SP 800-53 Compliance (as required and approved by the State of Michigan), Democracy Live complies with the below NIST SP 800-71 controls, where applicable to OmniBallot.

Select Controls from NIST SP 800-171

- Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
- Limit system access to the types of transactions and functions that authorized users are permitted to execute.
- Monitor and control remote access sessions.
- Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
- Authorize wireless access prior to allowing such connections.
- Protect wireless access using authentication and encryption.
- Control connection of mobile devices.
- Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.
- Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.
- Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.
- Correlate audit record review, analysis, and reporting processes for investigation and response toindications of inappropriate, suspicious, or unusual activity.
- Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
- Establish and enforce security configuration settings for information technology products employed inorganizational systems.
- Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.
- Employ the principle of least functionality by configuring organizational systems to provide onlyessential capabilities.
- Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.
- Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all,permit-by-exception (whitelisting) policy to allow the execution of authorized software.
- Identify system users, processes acting on behalf of users, and devices.
- Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.

- Use multifactor authentication (MFA) for local and network access to privileged accounts and fornetwork access to non-privileged accounts.
- Store and transmit only cryptographically-protected passwords.
- Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.
- Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.
- Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.
- Require multifactor authentication to establish nonlocal maintenance sessions via external networkconnections and terminate such connections when nonlocal maintenance is complete.
- Control the use of removable media on system components.
- Ensure that organizational systems containing sensitive data are protected during and after personnel actions such as terminations and transfers.
- Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.
- Protect and monitor the physical facility and support infrastructure for organizational systems.
- Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems are identified.
- Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.
- Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.
- Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of the information systems.
- Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.
- Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
- Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).
- Protect the authenticity of communications sessions.
- Identify, report, and correct system flaws in a timely manner.
- Provide protection from malicious code at designated locations within organizational systems.
- Monitor system security alerts and advisories and take action in response.
- Update malicious code protection mechanisms when new releases are available.
- Monitor organizational systems including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
- Employ the principle of least privilege, including for specific security functions and privileged accounts.
- Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

- Perform maintenance on organizational systems.
- Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.
- Prohibit the use of portable storage devices when such devices have no identifiable owner.
- Screen individuals prior to authorizing access to organizational systems containing sensitive data.
- Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of sensitive data.
- Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.
- Implement cryptographic mechanisms to prevent unauthorized disclosure of sensitive data duringtransmission unless otherwise protected by alternative physical safeguards.
- Employ FIPS-validated cryptography when used to protect the confidentiality of sensitive data.
- Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.
- Identify unauthorized use of the organizational systems.
- Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
- Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.
- Limit unsuccessful logon attempts.
- Use session lock with pattern-hiding displays to prevent access and viewing of data after a period ofinactivity.
- Terminate (automatically) a user session after a defined condition.
- Route remote access via managed access control points.
- Verify and control/limit connections to and use of external systems.
- Limit use of portable storage devices on external systems.
- Provide security awareness training on recognizing and reporting potential indicators of insider threat.
- Review and update logged events.
- Alert in the event of an audit logging process failure.
- Protect audit information and audit logging tools from unauthorized access, modification, and deletion.
- Limit management of audit logging functionality to a subset of privileged users.
- Analyze the security impact of changes prior to implementation.
- Control and monitor user-installed software.
- Enforce a minimum password complexity and change of characters when new passwords are created.
- Allow temporary password use for system logons with an immediate change to a permanent password.
- Obscure feedback of authentication information.
- Test the organizational incident response capability.

- Supervise the maintenance activities of maintenance personnel without required access authorization.
- Protect the confidentiality of backup sensitive data at storage locations.
- Escort visitors and monitor visitor activity.
- Remediate vulnerabilities in accordance with risk assessments.
- Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.
- Establish and manage cryptographic keys for cryptography employed in organizational systems.
- Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation.

STATE OF WEST VIRGINIA
Purchasing Division

PURCHASING AFFIDAVIT

CONSTRUCTION CONTRACTS: Under W. Va. Code § 5-22-1(i), the contracting public entity shall not award a construction contract to any bidder that is known to be in default on any monetary obligation owed to the state or a political subdivision of the state, including, but not limited to, obligations related to payroll taxes, property taxes, sales and use taxes, fire service fees, or other fines or fees.

ALL CONTRACTS: Under W. Va. Code §5A-3-10a, no contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and: (1) the debt owed is an amount greater than one thousand dollars in the aggregate; or (2) the debtor is in employer default.

EXCEPTION: The prohibition listed above does not apply where a vendor has contested any tax administered pursuant to chapter eleven of the W. Va. Code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

DEFINITIONS:

"Debt" means any assessment. premium. penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium. penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.

"Employer default" means having an outstanding balance or liability to the old fund or to the uninsured employers' fund or being in policy default, as defined in W. Va. Code § 23-2c-2, failure to maintain mandatory workers' compensation coverage, or failure to fully meet Its obligations as a workers' compensation self-insured employer. An employer is not in employer default if it has entered into a repayment agreement with the Insurance Commissioner and remains in compliance with the obligations under the repayment agreement.

"Related party" means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceed five percent of the total contract amount.

AFFIRMATION: By signing this form, the vendor's authorized signer affirms and acknowledges under penalty of law for false swearing (W. *Va.* Code §61-5-3) that: (1) for construction contracts, the vendor Is not In default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, that neither vendor nor any related party owe a debt as defined above and that neither vendor nor any related party are in employer default as defined above, unless the debt or employer default Is permitted under the exception above.

WITNESS THE FOLLOWING SIGNATURE:

Vendor's Name: Democracy Live, Inc.

Authorized Signature: ______________________ Date: 11/18/2021

State of Washington

County of King, to-wit:

Taken, subscribed, and sworn to before me this 18 day of November, 2021.

My Commission expires November 20, 2024.

A MICHELLE BRUCCHIERI
Notary Public
State of Washington
Commission # 20120598
My Comm. Expires Nov 20, 2024

NOTARY PUBLIC A. Michelle Brucchieri

Purchasing Affidavit (Revised 01/19/2018)

Appendix 1

OmniBallot PAT WCAG 2.0aa Conformance Report

Appendix 1: PAT WCAG 2.0aa Conformance

Guideline	Pass	Technique
Principle 1 – Perceivable	**AAA**	
Guideline 1.1 – Text Alternatives		
1.1.1 Non-text Content – Level A	Yes	Limited use of graphic content. Text alternatives provided for graphics and icons when necessary.
Guideline 1.2 – Time-based Media	**n/a**	
1.2.1 Audio-only and Video-only (Prerecorded) – Level A	n/a	OmniBallot does not pre-record audio or video.
1.2.2 Captions (Prerecorded) – Level A	n/a	OmniBallot does not pre-record audio or video.
1.2.3 Audio Description or Media Alternative (Prerecorded) – Level A	n/a	OmniBallot does not pre-record audio or video.
1.2.4 Captions (Live) – Level AA	n/a	OmniBallot does not pre-record audio or video.
1.2.5 Audio Description (Prerecorded) – Level AA	n/a	OmniBallot does not pre-record audio or video.
1.2.6 Sign Language (Prerecorded) – Level AAA	n/a	OmniBallot does not pre-record audio or video.
1.2.7 Extended Audio Description (Prerecorded) – Level AAA	n/a	OmniBallot does not pre-record audio or video.
1.2.8 Media Alternative (Prerecorded) – Level AAA	n/a	OmniBallot does not pre-record audio or video.
1.2.9 Audio-only (Live) – Level AAA	n/a	OmniBallot does deploy live audio or video.
Guideline 1.3 – Adaptable	**Yes**	
1.3.1 Info and Relationships – Level A	Yes	Use of landmarks, roles, labels, headings, semantic markup, and structured HTML. Use of CSS to control visual display
1.3.2 Meaningful Sequence – Level A	Yes	Content ordered from top to bottom. DOM order matches visual order.
1.3.3 Sensory Characteristics – Level A	Yes	Warning icons are accompanied by warning text.
Guideline 1.4 – Distinguishable	**Yes**	
1.4.1 Use of Color – Level A	Yes	Warning text is accompanied by a graphic icon, bold typeface, and the word warning. CSS is used to change visual representation of items with focus.
1.4.2 Audio Control – Level A	n/a	There is no audio playback in OmniBallot.
1.4.3 Contrast (Minimum) – Level AA	Yes	All text and background text meet a 4.5:1 contrast ratio. Warning text is also bold and 16pt for readability.
1.4.4 Resize text – Level AA	Yes	Text can be resized to 200% using the + and – keys
1.4.5 Images of Text – Level AA	n/a	There are no images of text in OmniBallot.
1.4.6 Contrast (Enhanced) – Level AAA	Yes	All regular text is a 7:1 contrast. All large text is at least a 4.5:1 contrast.
1.4.7 Low or No Background Audio – Level AAA	Yes	No background audio used.
1.4.8 Visual Presentation – Level AAA	Yes	Headers specify text and background colors in CSS. Borders are used to separate content. Main text does not use text or background color attributes.
1.4.9 Images of Text (No Exception) – Level AAA	Yes	No images of text are used.
Principle 2 – Operable		
Guideline 2.1 – Keyboard Accessible	**Yes**	
2.1.1 Keyboard – Level A	Yes	All elements and functionality are accessible via keyboard using tab and arrow keys.
2.1.2 No Keyboard Trap – Level A	Yes	No elements trap keyboard focus.
2.1.3 Keyboard (No Exception) – Level AAA	Yes	All elements and functionality are accessible via keyboard using tab and arrow keys.
Guideline 2.2 – Enough Time	**Yes**	
2.2.1 Timing Adjustable – Level A	Yes	No time limits are imposed on users.
2.2.2 Pause, Stop, Hide – Level A	Yes	No moving, blinking, scrolling, or auto updating information.
2.2.3 No Timing – Level AAA	Yes	No time limits are imposed on users.
2.2.4 Interruptions – Level AAA	Yes	No interruptions are presented to users.
2.2.5 Re-authenticating – Level AAA	Yes	Users do not have expiring sessions.
Guideline 2.3 – Seizures	**Yes**	
2.3.1 Three Flashes or Below Threshold – Level A	Yes	No flashing
2.3.2 Three Flashes – Level AAA	Yes	No flashing
Guideline 2.4 – Navigable	**Yes**	
2.4.1 Bypass Blocks – Level A	Yes	Using headings, landmarks, and semantic HTML. Also do not use repeated blocks.
2.4.2 Page Titled – Level A	Yes	All pages have an H1 title tag.
2.4.3 Focus Order – Level A	Yes	Yes, all items are focusable using tab or arrow keys.

2.4.4 Link Purpose (In Context) – Level A	Yes	All links use text that describes what the link does.
2.4.5 Multiple Ways – Level AA	Yes	The application is a step by step process with forward and backward navigation.
2.4.6 Headings and Labels – Level AA	Yes	Structured headings are used on every page. All input elements are properly labeled.
2.4.7 Focus Visible – Level AA	Yes	A clear focus indicator highlights the focus of all active elements.
2.4.8 Location – Level AAA	Yes	Page steps are clearly identified using x of y format.
2.4.9 Link Purpose (Link Only) – Level AAA	Yes	All links use text that describes what the link does.
2.4.10 Section Headings – Level AAA	Yes	All page content is separated by hierarchal use of headings.
Principle 3 – Understandable		
Guideline 3.1 – Readable	**Yes**	
3.1.1 Language of Page – Level A	Yes	Lang attribute is applied to html element
3.1.2 Language of Parts – Level AA	Yes	Full page content is translated including ballot content.
3.1.3 Unusual Words – Level AAA	Yes	Simple, common language is used throughout the application.
3.1.4 Abbreviations – Level AAA	Yes	No abbreviations are used.
3.1.5 Reading Level – Level AAA	Yes	Simple, common language is used throughout the application.
3.1.6 Pronunciation – Level AAA	Yes	Simple, common language is used throughout the application.
Guideline 3.2 – Predictable	**Yes**	
3.2.1 On Focus – Level A	Yes	Focus is shown, but does not change context or content.
3.2.2 On Input – Level A	Yes	Changing any input value does not change focus or context.
3.2.3 Consistent Navigation – Level AA	Yes	Navigation is the same on every page, in the same place, using a navigation role.
3.2.4 Consistent Identification – Level AA	Yes	Labelling and styling are consistent through the application.
3.2.5 Change on Request – Level AAA	Yes	Automatic updates or changes in context are not made.
Guideline 3.3 – Input Assistance	**Yes**	
3.3.1 Error Identification – Level A	Yes	Errors are clearly identified using an icon and are presented in descriptive text.
3.3.2 Labels or Instructions – Level A	Yes	Ballot instructions are provided before ballot marking.
3.3.3 Error Suggestion – Level AA	Yes	Overvote errors describe why the error occurred, and how to resolve the error.
3.3.4 Error Prevention (Legal, Financial, Data) – Level AA	n/a	OmniBallot provides review screens for all data entered. Change links are provided in the review interface to provide quick and easy edits.
3.3.5 Help – Level AAA	Yes	Each page includes instructions for the voter.
3.3.6 Error Prevention (All) – Level AAA	Yes	Users are presented with a review page. They can change any selection before printing.
Principle 4 – Robust		
Guideline 4.1 – Compatible	**Yes**	
4.1.1 Parsing – Level A	Yes	Application has valid HTML including unique IDs and hierarchal structure.
4.1.2 Name, Role, Value – Level A	Yes	All elements use semantic markup, or define aria-label, aria-labelledby, and role attributes.

This document is confidential.

Appendix 2

University of Washington Accessibility Test Report

Appendix 2 - University of Washington Accessibility Test Report

UWCTDS

Center for Technology and Disability Studies

(206) 685-4181-V
(206) 616-1396 TTY • (206) 543-4779 Fax

university of washington

Box 357920 Seattle, WA 98195-7920

Evaluation Date: 5/6/2019

Web Accessibility Testing and Report hours: 4 hours @ $125/hr

Website Evaluated: https://sites.omniballot.us/UW/app/home

Testing Technology and Evaluative Tools Used

The website was tested on Windows 10 using JAWS 2018 and Chrome browser. While this is a typical assistive technology configuration, it should be noted that not all operating systems, screen readers, or browsers are the same. Results may vary somewhat between platforms and circumstances, as with any internet technology.

The following content and tools were used to test for WCAG 2.0AA and Section 508 compliance:

- Web Content Accessibility Guidelines: http://www.w3.org/rlVWCAG20/
- WAVE Browser Extensions (For Chrome and Firefox): http://wave.webaim.org/extension/
- WebAIM color checker: http://wave.webaim.org/extension/
- WebAIM Web Accessibility Checklist (WCAG 2.0 Guidelines): webaim.org/standards/wcag/checklist/
- Markup Validation Service: http://validator.w3.org/
- US Dept of Health & Human Services: HTML 508 Compliance Checklist: https://www.hhs.gov/web/section-508/making-files-accessible/checklist/html/index.html
- ICT refresh: https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule/single-file-version#E205-content

Executive Summary

Overall, the site is very accessible in its current form. Keyboard access was effective in all web pages tested. Screen reader access was also strong. Screen reader navigation was mostly consistent and easy to understand. When marking ballots the state of the checkboxes was announced before and after making a selection. One recommendation is made below to improve usability.

Due to the fact that WCAG 2.0 AA Success Criteria are more explicit than the current 508 Standards, focus was directed to identifying compliance with WCAG 2.0 AA Success Criteria. https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/background/comparison-table-of-wcag2-to-existing-508-standards
Unless mentioned specifically below, WCAG 2.0 and Section 508 compliance was found to be met.

General Evaluation and Commentary

1.3.2 Meaningful Sequence

When reading the Sierra County Elections Department PDF with Jaws, the reading order does not align with the visual order in which information is presented. The line "I declare that:" is read before "Voter's Declaration/Oath of Voter". Taking a look in Adobe Acrobat Pro, the reading order is incorrect for these two lines although the document is tagged in the correct order. Correcting the reading order and then running the auto tag utility fixes this issue.

1.4.3 Contrast

There are several different color combinations on this website that did not meet Level AA Criterion for contrast. In order to comply with WCAG 2.0 AA criterion one of the following conditions must be met:

- Text and images of text have a contrast ratio of at least 4.5:1.
- Large text - at least 18 point (typically 24px) or 14 point (typically 18.66px) and bold - has a contrast ratio of at least 3:1.

On most of the pages the buttons have a background color of #007fb6 with white text color #eeeeee which has a contrast ratio of 3.84:1. The font size was found to be typically 16px which is equivalent to 12 pt font.

The links such as "Skip to Bottom" in the County Voter Information Guide or "How to Vote" under Additional Info are in #007fb6 with a white background #eeeeee, contrast ratio 3.84:1 which do not provide adequate contrast for the 16px font. On mouse hover the links are even lighter # 00a3e5, contrast ratio of 2.46:1.

Recommendation is to change the background color to increase the contrast ratio to 4.5:1 or increase the font size to 18 point (typically 24px) or 14 point (typically 18.66px) and bold.

2.4.1 Bypass Blocks

The "Skip to Bottom" links in the Reference Ballot do not function.

2.4.2 Page Titled

Web pages are not titled <title></title>

2.4.6 Headings and Labels

Inconsistent use of Headings in the Additional Info- How to Vote page. There are two "How to Vote" level 2 headings. Also one instance of the heading "How to Vote" is in all caps whereas the other is not. Towards the bottom of the page "Spanish Language Assistance" is heading level 1 which is inconsistent with the Heading structure above.

2.4.7 Focus Visible

On the Print Your Choices page of the Ballot Marking Application, the "Print Selection" button does not change to yellow on hover or on focus with keyboard navigation. The blue focus rectangle does not provide enough contrast to the blue button background color.

3.2.4 Consistent Identification

The “Continue” buttons at the bottom of the Welcome Voters page are recognized as links by Jaws whereas the “Continue” buttons on other pages are recognized as buttons. Recommendation to change the links to buttons on the Welcome page to improve consistency.

3.3.2 Labels or Instructions

In the Ballot Marking Instructions page the instructions state to “click on the following link” however there are no links following. “Go Back” and “Continue to Ballot” are both buttons. Also in the tab order and using Jaws, the next object the user comes to is the “Go Back” button. Recommendation to provide more specific instructions for improved understanding of next steps.

4.1.1 Parsing

The W3 Validator tool was used for these findings: http://validator.w3.org/
On all the pages, the below error was identified. This is also mentioned under section 2.4.2.

Error: Element `title` must not be empty.

From line 5, column 10; to line 5, column 17

```
↩ <title></title>↩ <ba
```

On the live ballot application page the following errors were identified. Despite these errors, the page was completely accessible using Jaws indicating that the page has appropriate tag structure.

Error: Forbidden code point U+0085.

At line 89, column 7902

```
="["+a+"]",s="…",c=RegExp("^"
```

Error: Forbidden code point U+007f.

At line 724, column 6200

```
e","\t":"Tab","□":"Delete",""
```

Error: Forbidden code point U+001b.

At line 724, column 6213

```
,"□":"Delete","":"Escape",Del
```

Error: Forbidden code point U+0090.

At line 724, column 6462

```
O:"/","`":"0","□":"NumLock"};j
```

Error: Forbidden code point U+0085.

At line 773, column 8977

```
="["+a+"]",c="…",u=RegExp("^"
```

Usability

Hidden headings are used for Language and Main Menu to provide information and quick navigation access to screen reader users. For consistency, consider adding a similar heading to the list of links for Instructions, Candidate Statements, Measures, etc.

Appendix 3

Incident Response Plan

DEMOCRACY LIVE

Prepared By: Information Security Office
Last Updated: June 26, 2020
Last Updated By: Mark Pace

Cybersecurity Incident Response Plan

Appendix 3 - Incident Response Plan

PURPOSE

Democracy Live is the largest provider of cloud and tablet-based voting technologies in the United States. The OmniBallot suite of services, a universal accessible balloting platform for state and local governments, stores Voter Registration information as well as state and local Ballot Style information. Democracy Live manages and maintains technical infrastructure required to host and maintain this information. Additionally, Democracy Live partners with Amazon AWS, and utilizes vendors of digital services and products to manage and maintain this data and infrastructure.

This Cyber Security Incident Response Plan outlines the procedures the Democracy Live Information Security Office (ISO) implements to detect and respond to unauthorized access or disclosure of private information from OmniBallot systems hosted on AWS infrastructure. More specifically, this plan defines the roles and responsibilities of various Democracy Live ISO staff with respect to the identification, isolation and remediation of data security breaches, outlines the timing, direction and general content of communications among affected stakeholders, and defines the different documents that will be required during various steps of the incident response.

Democracy Live also implements best-practices designed to proactively reduce the risk of unauthorized access or disclosure, such as training staff with respect to legal compliance requirements, following appropriate physical security and environmental controls for technical infrastructure, deploying digital security measures such as firewalls, malware detection, and numerous other industry standard and advanced detection systems.

In the event of a cyber security incident, ISO staff have been trained to expeditiously deal with the incident. ISO staff are trained on a bi-annual basis to recognize anomalies in the systems they regularly utilize, and to report any such anomalies as soon as possible to the Incident Response Manager so the Incident Response Team can be mobilized. Throughout the year the Incident Response Manager and members of the Incident Response Team are kept up to date on the latest security threats and trained in modern techniques of incident remediation.

The availability and protection of the information resources managed by the systems we maintain is of paramount importance to us and our customers and will always be a core value of our organization.

DEFINITIONS

Event

An event is an exception to the normal operation of IT infrastructure, systems, or services. Not all events become incidents.

Cyber Security Incident

A Cyber Security Incident is any event that, as assessed by ISO staff, threatens the confidentiality, integrity or availability of the information resources we support or utilize internally, especially sensitive information whose theft or loss may be harmful to individuals, our customers, our partners, or our organization.

Incidents may be established by review of a variety of sources including, but not limited to ISO monitoring systems, reports from Democracy Live staff or outside organizations and service degradations or outages. Discovered incidents will be declared and documented in ISO's incident documentation system.

Complete IT service outages may also be caused by security-related incidents, but service outage procedures will be detailed in Business Continuity and/or Disaster Recovery procedures.

Incidents will be categorized according to potential for restricted data exposure or criticality of resource using a High-Medium-Low designation. The initial severity rating may be adjusted during plan execution.

Detected vulnerabilities will not be classified as incidents. The ISO employs tools to scan the OmniBallot system environment and depending on severity of found vulnerabilities may warn affected users, disconnect affected machines, or apply other mitigations. In the absence of indications of sensitive data exposure, vulnerabilities will be communicated and the ISO will pursue available technology remedies to reduce that risk.

Personally Identifiable Information (PII)

For the purpose of meeting security breach notification requirements, PII is defined as a person's first name or first initial and last name in combination with one or more of the following data elements:

- Social security number
- State-issued driver's license number
- State-issued identification card number
- Financial account number in combination with a security code, access code or password that would permit access to the account
- Medical and/or health insurance information

ROLES AND RESPONSIBILITIES

The Incident Response Process incorporates the Information Security Roles and Responsibilities definitions and extends or adds the following Roles.

Incident Response Team (IRT)

The IRT consists of experts across different fields in the organization whose mandate is to navigate the organization through a Cyber Security Incident from initial investigation, to mitigation, to post incident review and analysis. Members include the Incident Response Manager, technical hardware and networking experts, front-end engineering experts, communications experts and legal experts.

Incident Response Manager (IRM)

The IRM is responsible for overseeing all aspects of the Cyber Security Incident, especially the IRT. The main focus of the IRM is to ensure proper implementation of the procedures outlined within the Cyber Security Incident Response Plan, to maintain appropriate Incident Logs throughout the incident, and to act as the key liaison between IRT experts and the organization's Senior Management team. Concluding a Cyber Security Incident, the IRM will conduct a review of the incident and produce two deliverables an Incident Summary Report and a Process Improvement Plan.

Cyber Security Incident Log

The Cyber Security Incident Log will be used to capture critical information about a Cyber Security Incident and the ISO response to that incident. The log should be maintained while the incident is in progress.

Incident Summary Report (ISR)

The ISR is a deliverable document prepared by the IRM at the conclusion of a Cyber Security Incident. The ISR will provide a detailed summary of the incident including how and why it occurred, the estimated data loss, affected parties, and all impacted services. Finally, the ISR will examine the procedures of the Cyber Security Incident Response Plan, including how the IRT followed the procedures and whether updates to the IRP are required. The template for the ISR may be seen in Appendix A.

Process Improvement Plan (PIP)

The PIP is a deliverable document prepared by the IRM concluding a Cyber Security Incident and will provide recommendations for preventing or minimizing the impact of future Cyber Security Incidents based upon "lessons learned" from the recently-completed incident report. This plan should be kept confidential for security purposes. The template for the PIP may be viewed in Appendix B.

INCIDENT RESPONSE TEAM

TECHNICAL CONTACTS:

INCIDENT RESPONSE:

MANAGER LEGAL COUNSEL:

In addition to those individuals listed above, additional experts may be included on the IRT, depending upon the nature and scope of the incident. In particular, a software support expert from the team that supports the software in question will likely be necessary. These additional members will be chosen by the IRM.

Name	Email	Work Phone	Mobile Phone

COMMUNICATIONS SPECIALIST

Name	Email	Work Phone	Mobile Phone

INCIDENT MANAGEMENT PRINCIPLES

Confidentiality

Investigation

During a Cyber Security Incident investigation, the IRM or members of the IRT will gather information from multiple computer systems and/or conduct interviews with key personnel based on the scope of the incident in question. All information gathered or discovered during a Cyber Security Incident will be strictly confidential throughout the investigative process. All members of the Cyber Security Incident Response Team are trained in information security and data privacy best practices and follow the policies outlined in the Democracy Live Security Policies document. At the conclusion of the investigative process, the IRM will brief Senior Management on the relevant details of the incident and the results of the investigation (see Briefing of Senior Management in the Response Phase on page 9). During this phase, no confidential information will be shared unless it is strictly relevant to the investigation and/or the incident itself.

Affected Stakeholders

In the event the incident involves the unauthorized access or disclosure of confidential voter registration information, Democracy Live will communicate any information relevant to the incident as well as any additional requested information to which they have a right (e.g. specific registration records, balloting records, etc.). Democracy Live does reserve the right to withhold certain information at the discretion of the IRM if that information may jeopardize current or future investigations, or pose a security risk to Democracy Live or other entities.

In the event the incident is limited only to OmniBallot systems not containing sensitive or confidential information, it will be the discretion of Democracy Live Management and the IRM whether or not to share information related to the incident with outside stakeholders.

Report Management

All reports generated throughout an investigation in addition to any evidence gathered will be stored and managed by the IRM. Any digital records will be securely stored on the Democracy Live network in a location only accessible by the IRM and approved Senior Management. In the event past records of incidents require review, a written request must be submitted to the IRM that includes the requestor, the information requested and the purpose of the request. The IRM will review the request and retains the discretion to approve or deny any request. Incident summary information will always be made available by the IRM.

COMMUNICATION GUIDELINES

- Communication with customers, will be disseminated via Senior Management.
- Initial communication to affected stakeholders should occur as expeditiously as possible upon the identification of the incident. In some cases, this may include an initial communication (letter, email, phone call) that simply states that Democracy Live is aware of the issue and is addressing it, with the promise of a follow up. Scenarios for the release of Personally Identifiable Information (PII) are as follows:
  - Should the unauthorized release of Voter Registration data occur, Democracy Live shall notify the customers affected by the release in the most expedient way possible. Democracy Live will require this notification to occur within 2 hours after the breach is discovered.
- Updated communications will come from Management or the Incident Response Manager. As staff receive requests from customers for information, they should pass those requests along to the Incident Response Manager.
- Democracy Live staff should be clearly informed and be familiar with the Democracy Live Security Policy which informs what information is public and what is internal/confidential.
- Communication with news media will be initiated by Senior Management.
- Incoming news media calls and requests for information will be directed through Senior Management. A communication response plan (talking points, interview refusal statement, etc.) will be formulated as needed, with information coming from Senior Management and the ISO.

Training

The continuous improvement of incident handling processes implies that those processes are periodically reviewed, tested and translated into recommendations for enhancements. Democracy Live staff inside and outside of the ISO will be periodically trained on procedures for reporting and handling incidents to ensure that there is a consistent and appropriate response to incidents, and that post-incident findings are incorporated into procedural enhancements.

CYBER SECURITY INCIDENT PHASES

Identify

Overview

All Democracy Live staff have a responsibility to remain vigilant and protect the data stored within the systems we support. Any event that threatens the confidentiality, integrity or availability of the information resources we support or utilize internally should immediately be reported to a supervisor or the IRM if a supervisor is unavailable. Supervisors should immediately bring the incident to the attention of the IRM.

Incident Types

Types of cyber incidents that may threaten the organization are:

- Unauthorized attempts to gain access to a computer, system or the data within
- Service disruption, including Denial of Service (DoS) attack

- Unauthorized access to critical infrastructures such as servers, routers, firewalls, etc.
- Virus or worm infection, spyware, or other types of malware
- Non-compliance with security or privacy protocols
- Data theft, corruption or unauthorized distribution

Incident Symptoms

Signs a computer may have been compromised include:

- Abnormal response time or non-responsiveness
- Unexplained lockouts, content or activity
- Locally hosted websites won't open or display inappropriate content or unauthorized changes
- Unexpected programs running
- Lack of disk space or memory
- Increased frequency of system crashes
- Settings changes
- Data appears missing or changed
- Unusual behavior or activity by Democracy Live staff, contractors, partners or other actors

ASSESS

Overview

Once anomalous activity has been detected or reported, it is incumbent upon the IRM to determine the level of intervention required. Other members of the IRT may be required to provide input during this phase to assist with determining if an actual security threat exists. If it is determined there is an active security threat or evidence of an earlier intrusion, the IRM will alert the entire IRT immediately so the situation may be dealt with as expeditiously as possible.

Considerations

- What are the symptoms?
- What may be the cause?
- What systems have been / are being / will be impacted?
- How wide spread is it?
- Which stakeholders are affected?

Documentation

Regardless of whether it is determined there is a security threat, the IRM will accurately document the scenario in a Cyber Security Incident Log. All Cyber Security Incident Logs will be stored in a single location so incident information may be reviewed in the future. This report should contain information such as:

- Who reported the incident?
- Characteristics of the activity
- Date and time the potential incident detected
- Nature of the incident (Unauthorized access, DDoS, Malicious Code, No Incident Occurred, etc.)
- Potential scope of impact
- Whether the IRT is required to perform incident remediation?

RESPOND

Briefing of Senior Management

Upon determining that a significant incident or breach has occurred, Senior Management should be notified immediately. As additional information is uncovered throughout the investigation, Senior Management should be briefed by the IRM so appropriate decisions, such as allocating additional staff, hiring outside consultants and involving law enforcement can be made. Additionally, based on the incident, it will be incumbent on Senior Management to determine the appropriate stakeholders to notify of the incident and the appropriate medium to do so. Senior Management should take into consideration the nature of the information or systems involved, the scope of the parties affected, timeliness, potential law enforcement interests, applicable laws and the communication requirements of all parties involved.

Initial Response

This first step in any cyber incident response is to determine the root cause and origin of the incident and isolate the issue. This may involve measures up to and including immediately disconnecting particular workstations, services or network devices from the network to prevent additional loss. While this is occurring, it is necessary to examine firewall and system logs, as well as possibly perform vulnerability scans, to ensure the incident has not spread to other areas in order to define the entire scope of the incident. Throughout this process, it will be critical to preserve all possible evidence and document all measures taken in detail. Thorough review and reporting on the incident will be required once the threat has been removed, the vulnerabilities have been removed and the systems have been restored.

Remediation and Recovery

Once the cause has been determined and appropriately isolated, the IRT will need to remediate the vulnerabilities leading to the incident. This may involve some or all of the following:

- Install patches and updates on systems
- Infections cleaned and removed
- Re-image or re-install operating systems of infected machines
- Change appropriate passwords
- Conduct a vulnerability scan of any compromised machines before reconnecting them to the network
- Restore system backups where possible
- Document all recovery procedures performed and submit them to the IRM
- Closely monitor the systems once reconnected to the network

REPORT

Overview

Once the threat has been mitigated and normal operation is restored, the IRM will compile all available information used in the investigation to produce an accurate and in-depth summary of the incident in an Incident Summary Report (ISR). An example copy of the ISR is located in Appendix A. Throughout the incident, the IRT will have kept Incident Logs that contain detailed records wherever possible, and these shall serve as the basis of the report. Interviews will also be conducted with appropriate members of the

IRT to obtain any additional information that may be available to augment the logs and records kept throughout the process.

Report Contents

The Incident Summary Report (ISR) will include all pertinent information to the incident, but at minimum:

- Dates and times of milestones throughout the process (e.g. incident detection, verification, notifications, remediation steps, completion, etc.)
- List of symptoms or events leading to discovery of the incident
- Scope of impact
- Mitigation and preventative measures
- Restoration logs
- Stakeholder communications (including copies of memos, emails, etc. where possible)

Timeframe

The ISR should be prepared as expeditiously as possible following the incident so future preventative measures may be taken as quickly as possible. Information to prepare the ISR and interviews with the IRT should be conducted immediately to ensure the greatest possible accuracy of information.

REVIEW

Post-Incident Review Meeting

At the conclusion of the incident, the IRM and select members from the IRT will meet with Senior Management to discuss the event in detail, review response procedures and construct a Process Improvement Plan (PIP) if necessary, to prevent a reoccurrence of that or similar incidents. The compiled Incident Report constructed by the IRM will serve as a guide for the meeting.

The meeting should be a full debrief of the incident and will present findings to be discussed. The IRM will share the full scope of the breach (as comprehensively as possible), causes of the breach, how it was discovered, potential vulnerabilities that still exist, communication gaps, technical and procedural recommendations, and the overall effectiveness of the response plan.

As a whole, the group will review the information presented and will determine any weakness in the process and determine all the appropriate actions moving forward to modify the plan, address any vulnerabilities and what communication is required to various stakeholders.

Process Improvement Plan

The IRM will draft a Process Improvement Plan (PIP) based on the results of this meeting. The plan should discuss any applicable items necessary to, prevent future incidents to the extent practicable, including cost, resources, and time frame requirements where possible. The PIP will also include a review strategy to ensure all recommendations made in the PIP are met in a timely fashion and functioning appropriately. Areas of focus may include, but are not limited to:

- New services required
- Patch or upgrade plans
- Training plans (Technical, end users, etc.)

- Policy or procedural change recommendations
- Recommendations for changes to the Incident Response Plan

Additionally, the PIP will be kept strictly confidential for security purposes. Any communication required to clients or to the public must be drafted separately and include only information required to prevent future incidents.

APPENDIX A

INCIDENT SUMMARY REPORT

Incident	Summary
Origination Date / Time (GMT)	
Detected Date / Time (GMT)	
Communication Date	
Communicated To (External)	
Reported To (Internal)	
Responding IRT Member	
Scope: System(s) Affected	
Symptoms	
Type and Scope	
Corrective Actions	
Mitigation Processes and Internal Communication	
Communications Log (Attach drafts for written communications, synopsis for verbal communication)	

APPENDIX B

PROCESS IMPROVEMENT PLAN

Improvement	Summary
Areas of Success	
Areas in Need of Improvement	
Recommended Improvements to Avoid Future Incidents	
Recommended Improvements to the Cyber Security Incident Response Plan	
Resources Required	
Timeframe	
Cost	

APPENDIX C:

INCIDENT LOG

Incident Log	
Title of Incident	
Date Opened	
Description	
Action / Remediation (Date/ Time)	
Action / Remediation	
Performed By	
Resources Required	
Timeframe	
Cost	

APPENDIX D

SAMPLE CUSTOMER LETTER

DATE

This letter is to inform you of an incident that occurred within the OmniBallot system. This incident resulted in voter registration data being compromised by an outside entity. Our Incident Response Team acted quickly to assess and mitigate the situation. At this time, we are able to share the following details:

[insert a brief description of the breach or unauthorized release, the dates of the incident and the date of discovery; a description of the types of personally identifiable information affected; an estimate of the number of records affected; a brief description of Democracy Live's investigation or plan to investigate]

Please know that Democracy Live is committed to protecting and securing Voter Registration data. Our team has extensive training in data security and privacy, and our systems have many controls in place to protect your records. Our team is working with a group of experts to review the incident and implement appropriate measures to protect against this type of incident from occurring in the future. Please contact your Democracy Live representative with any questions you may have regarding this incident and our response.

Sincerely,

APPENDIX E

SAMPLE STAFF MEMO

DATE

Dear Staff,

This letter is to inform you of an incident that occurred on DATE within Democracy Live's OmniBallot system. This incident resulted in [voter registration, corporate data or, other sensitive data] being compromised by an outside entity. Our response team acted quickly to assess and mitigate the situation.

ISO wants to ensure that you have key details of the incident so you are well-informed when speaking with customers and colleagues. Please note that Democracy Live Senior Management is handling communication with the affected parties. Should you receive any related inquiries, please direct them to the Information Security Office (ISO).

At this time, we are able to share the following details:

[insert a brief description of the breach or unauthorized release, the dates of the incident and the date of discovery; a description of the types of personally identifiable information affected; an estimate of the number of records affected; a brief description of the educational agency's investigation or plan to investigate]

As more details become available, we will be disseminated as appropriate. Please contact the ISO should you have any questions or immediate concerns regarding this incident.

Sincerely,

Appendix 4

System Security Plan

v2.7.211109

DEMOCRACY LIVE

System Security Plan

Democracy Live Internal: Registered and Restricted

1. SYSTEM IDENTIFICATION

1.1. System Name/Title

OmniBallot Suite

1.1.1. System Categorization:

Moderate Impact for Confidentiality

1.2. Responsible Organization:

Name:	Democracy Live, Inc.
Address:	
Phone:	

1.2.1. **Information Owner** (Point of contact responsible for providing and/or receiving VR Data):

Name:	
Title:	
Office Address:	
Work Phone:	
E-Mail Address:	

1.2.2. **System Owner** (assignment of security responsibility):

Name:	
Title:	
Work Phone:	
e-Mail Address:	

1.2.3. System Security Officer:

Name:	
Title:	
Office Address:	
Work Phone:	
E-Mail Address:	

1.3. OmniBallot Suite

OmniBallot Suite is a Software as a Service (SaaS) cloud-based multi-tenant suite of applications which provide services to Voters and Elections Officials. The services available to Voters include Absentee Ballot Requests, Absentee Ballot Delivery, Client-side Ballot Marking, and Electronic Ballot Return. OmniBallot features an Administrative application that is made available to Democracy Live Customers to enable them to manage the various Voter-facing Ballot services. Customers may request any or all of the Voter-facing service applications based on their needs and their constituents. The Administrative Application includes features to manage all the Voter-facing applications.

2. SYSTEM ENVIRONMENT

2.1. Application Architecture

The application architecture adheres to standard three logical tier industry best-practices segregating the presentation client, a static Single Page Application (SPA), from the services API for data delivery, and the data persistence layer for storage. The system architecture segregates each customer into a tenant account using an account id to identify the specific data storage location. Data for each tenant is persisted in separate databases and S3 Buckets for storage of each tenant's data. Customer tenant data is never co-mingled in any persistent store.

2.1.1. High-Level Application Architecture

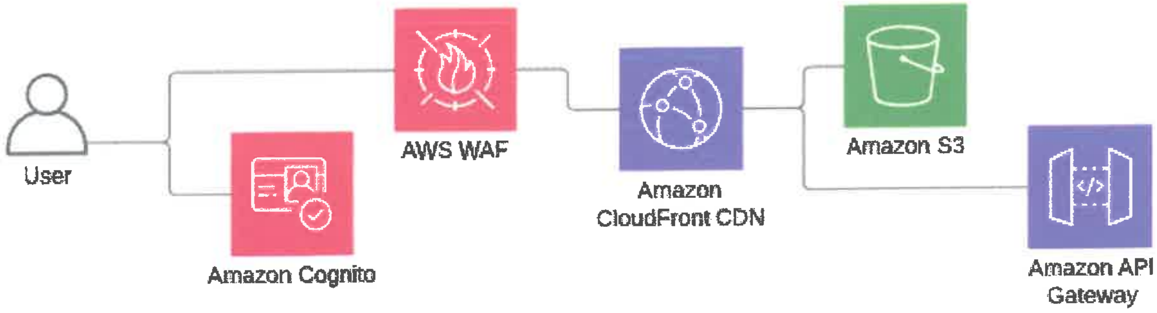
OmniBallot design is based on the JAM-Stack design pattern JavaScript, API's, and Markup. Implementing a JAM-Stack architecture brings many benefits including better performance, higher security, lower cost of scaling, a better developer experience, and a better segregation between logical layers. This logical architecture allows for cleaner separation of concerns and much higher cohesion and lower coupling.

This architecture allows for Static resources – web pages to be stored on S3 buckets and can be delivered via CDN to the client browser eliminating the need for a resource-intensive web-server to render the web page. This design also allows for only a single call as the web page is a Single Page Application (SPA) eliminating round-trips for additional web pages. Separation of concerns is maintained and resources are scoped to their specific logical role.

2.1.1.1. *Logical Tiers*

Web site hosting is on S3 and all traffic is routed through CloudFront CDN which implements a Web Application Firewall (WAF) to inspect and re-route traffic. All unencrypted traffic to port 80 is routed to port 443 which utilizes TLS1.2 encryption for all traffic to the rest of the system.

A high-level diagram follows depicting the high-level architecture of the logical tiers. The diagram includes Authentication via AWS Cognito which implements JSON Web Tokens (JWT) for session authentication and authorization based on claims in the JWT:



2.1.2. High-Level Network Topology

The system network topology consists of AWS infrastructure services. From a high-level, the services used provide high availability and numerous security controls. OmniBallot utilizes all the available security services available from AWS and will routinely review the security posture of the network to ensure a hardened environment. Democracy Live DevOps/IT personnel are required to keep abreast of the latest developments in AWS services and will assess any new services to determine if they provide an additional benefit to the overall system.

2.1.2.1. *Domain Name System: Route 53*

The AWS Route 53 service is used to provide domain name resolution and to route traffic using various CNAME, A record and additional alias records. Route 53 is responsible for relaying domain traffic to CloudFront.

2.1.2.2. *Content Delivery Network: CloudFront*

CloudFront is content delivery network (CDN) offered by AWS. CDN's provide a globally-distributed network of proxy servers which cache content and provide low-latency delivery of content. CloudFront is configured with a Web Application Firewall (WAF).

2.1.2.3. *Web Application Firewall (WAF)*

WAF is implemented as a security layer to protect resources against common web exploits that may affect availability, compromise security, or consume excessive resources. The AWS WAF is configured to monitor and control traffic that is routed either to S3 Buckets or API Gateway. Security rules are implemented to block common attack patterns, such as SQL injection or cross-site scripting.

2.1.2.4. *S3 Storage Buckets*

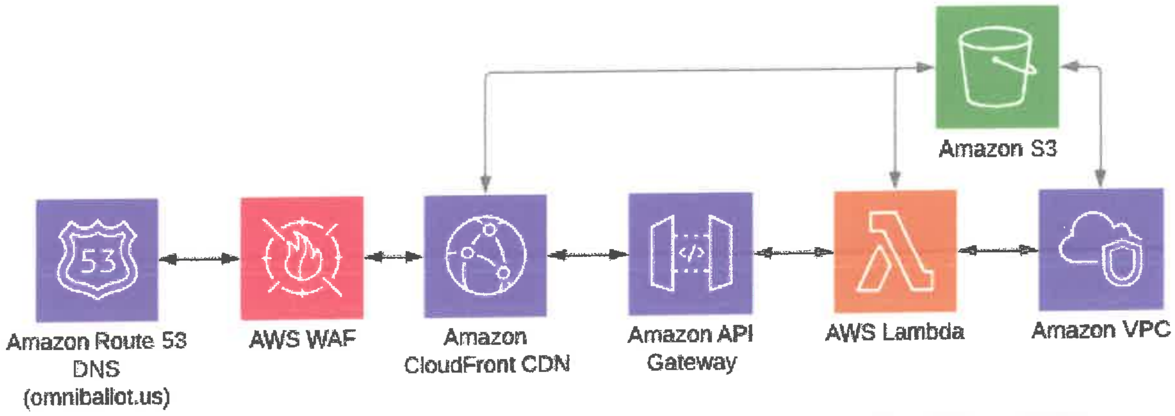
AWS S3 provides a fully managed service to manage files and provide high availability by replicating data across multiple servers within AWS data centers. S3 provides strong read-after-write consistency for PUTs and DELETEs of objects in the Amazon S3 bucket in all AWS Regions. This applies to both writes to new objects as well as PUTs that overwrite existing objects and DELETEs. In addition, read operations on Amazon S3 Select, Amazon S3 Access Control Lists, Amazon S3 Object Tags, and object metadata (e.g., HEAD object) are strongly consistent. S3 provides 11-9's of availability (99.999999999%).

2.1.2.5. *API Gateway*

AWS API Gateway provides a fully managed service to maintain, monitor, and secure the OmniBallot APIs. API Gateway provides access to the Business Logic APIs hosted on AWS Lambda Functions and via VPC Link to FarGate services running in a private subnet of a Virtual Private Cloud. The API Gateway is used to configure CORS support and to provide custom Authorizers to specific end-points.

2.1.2.6. *Lambda Functions (Serverless)*

AWS Lambda Functions are an AWS service that provide an independent unit of deployment which support the a microservice architecture. Lambda functions serve as a proxy to the VPC hosting FarGate elastic container services and provide an additional layer of security by which input and output data can be sanitized. The Lambda functions also provide an additional layer of security to validate API keys as well as User Authorization to access restricted APIs.



2.1.3. Virtual Private Cloud (VPC)

The AWS Virtual Private Cloud (VPC) is provisioned to provide a secure and logically isolated network within the AWS Cloud infrastructure that supports launching additional AWS resources in a virtual network that has been specifically defined for the OmniBallot services. The VPC provides complete control over the OmniBallot virtual networking environment. The VPC is configured with our own IP address range, set of subnets, routing tables, and network gateways. The VPC is configured to support a public facing subnet for ingress and egress traffic into the configured private subnets. VPC are configured to support redundant Availability Zones (AZ) across Regions.

2.1.3.1. Internet Gateway

The Internet Gateway (IGW) is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the Internet.
The IGW serves two purposes: to provide a target in the VPC route tables for internet-routable traffic, and to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses.

2.1.3.2. Network Address Translation (Private Egress Only)

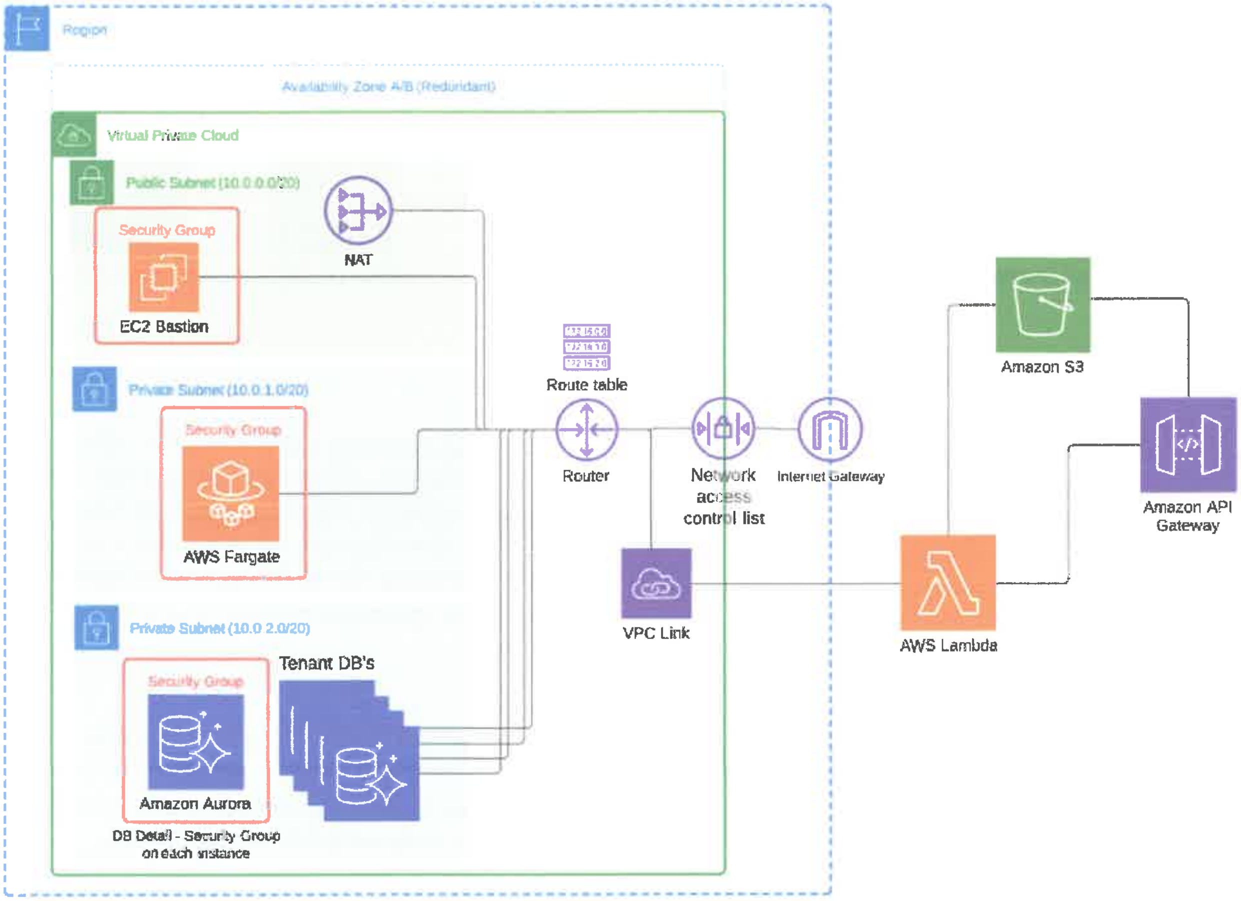
AWS Network Address Translation (NAT) instance is hosted in the public subnet in the VPC to enable application servers and database instances in the private subnet to initiate outbound IPv4 traffic to the internet or other AWS services, but prevent the instances from receiving inbound traffic initiated by anyone on the Internet.

2.1.3.3. Network Access Control Lists

AWS Network Access Control Lists (NACL) function as an additional layer of traffic security for the VPC. The NACL is configured as a stateless firewall for controlling network traffic in and out of the subnets in the VPC. The NACLs are configured with rules similar to the security groups in order to add an additional layer of security to the VPC.

2.1.3.4. Security Groups

AWS Security Groups (SG) act as a virtual firewall for our compute instances to control inbound and outbound traffic. Instances launched in a VPC, are assigned a security group. SG's are designed to act at the instance level, not the subnet level so each instance in a subnet in your VPC is assigned a different set of security groups based on access level. Since SG's are granular and stateful, separate rules are configured to control inbound and outbound traffic specific to the service instance. Granular SG rules are configured more specifically to the port and protocols necessary for that service instance.



3. REQUIREMENTS

(Note: The source of the requirements is NIST Special Publication 800-53 Rev. 4 Moderate Impact Controls)

This document provides a description of how all of security requirements are being implemented or planned to be implemented for the OmniBallot Suite System. The major sections follow the control families defined in NIST SP 800-53 Rev. 4. The description for each security requirement contains:

1. a security requirement control and number;
2. how the security requirement is being implemented or planned to be implemented; and
3. any scoping guidance that has been applied (e.g., compensating mitigations(s) in place due to implementation constraints in lieu of the stated requirement). If the requirement is not applicable to the system, rationale is provided.

3.1. [AC] Access Control

3.1.1. [AC-02] Account Management

Democracy Live employs automated mechanisms to support the management of information system accounts.

- a) Democracy Live identifies and selects the following system accounts to support organizational missions/business functions:
  - a) OmniBallot Users
  - b) OmniBallot User Manager
- b) Democracy Live assigns a tenant account manager to manage user accounts for that tenant.
- c) OmniBallot does not support "groups" and only assigns specified tenant account managers to the User Manager role.
- d) Democracy Live specifies users and role membership for each tenant of OmniBallot. User Manager role authorization is on a tenant basis. User account authorization is provided on a tenant basis and managed by the assigned User Manager role.
- e) Each tenant is responsible for creating authorized users and assigning the appropriate personnel for the User Manager role.
- f) Democracy Live creates, enables, modified, and deletes system accounts based on tenant requirements for managing User Manager accounts.
  - a) Creation of accounts is by request only from an authorized tenant representative. The user may, if the option is selected, be required to provide a secondary method of authentication (MFA).
  - b) Enabling system accounts is part of the creation/provisioning process. Users will be required to login to actively enable the account. Inactive accounts will be disabled after 60 days of inactivity.
  - c) Modifications to user accounts are managed by the User Manager role.
  - d) Deletion of accounts is managed by the User Manager. Democracy Live will also remove any User Manager role accounts when the tenant contract has ended.
- h) Notification is the responsibility of the tenant to handle their user accounts. The User Manager is responsible for handing provisioning and de-provisioning of accounts in use by the tenant.
- i) Democracy Live authorizes access to OmniBallot based on valid requests from the tenant for either User Manager role accounts or User accounts. Democracy Live shall receive requests from designated tenant personnel to provide valid access authorization and intended system usage.

3.1.2. [AC-02 (1)] Automated System Account Management

Democracy Live employs automated mechanisms to support the management of OmniBallot accounts.

Status: Implemented

OmniBallot supports automated system account management which includes using automated mechanisms to create, enable, modify, disable, and remove accounts; notify account managers when an account is created, enabled, modified, disabled, or removed; monitor system account usage; and report atypical system account usage. OmniBallot mechanisms include internal system functions and email notifications.

3.1.3. [AC-02 (2)] Removal of Temporary / Emergency Accounts

OmniBallot automatically disables temporary and emergency accounts after 15 days of inactivity. OmniBallot automatically removes disabled accounts 10 days after being marked as disabled. OmniBallot does not support "Emergency" accounts.

Status: Implemented

OmniBallot will automatically disable or remove any accounts after 60 days of inactivity. OmniBallot does not have the ability to create temporary or emergency accounts.

3.1.4. [AC-02 (3)] Disable Inactive Accounts

OmniBallot automatically disables User accounts after 60 days of inactivity and User Manager accounts after 365 days.

Status: Implemented

OmniBallot will automatically disable or remove any accounts after 60 days of inactivity.

3.1.5. [AC-02 (4)] Automated Audit Actions

OmniBallot automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies both organization personnel and tenant account managers.

Status: Implemented

OmniBallot tracks all changes to user accounts and sends a notification email regarding activity on user accounts. Notification email is sent to organization personnel and tenant account managers on a daily basis.

3.1.6. [AC-03] Access Enforcement

OmniBallot enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Status: Implemented

OmniBallot restricts transactions for the specific account and authorized users in the User or User Administration role. OmniBallot only allows transactions on the specific tenant data for the authorized user account.

3.1.7. [AC-04] Information Flow Enforcement

OmniBallot enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on principle of least privilege policy.

Status: **Implemented**

OmniBallot restricts the access to PII using the Least Privilege principal as defined in the Democracy Live Security Policy. All data meeting the moderate or PII classification is handled by personnel who have been briefed and fully understand the nature of the data. Only those with authorization to handle data have access to PII. Further all PII sensitive fields within a record are hashed prior to storage either by the customer or the automated data ingestion service. Voter PII is never transmitted to the client and is not persisted in the system "in the clear".

3.1.8. [AC-05] Separation of Duties

Democracy Live

a. Separates Operations, Development, DevOps, and System Administrators roles;
b. Documents separation of duties of individuals; and
c. Defines information system access authorizations to support separation of duties.

Status: **Implemented**

Democracy Live segregates roles within the various departments. Operations does not have access to the System Network and Developers do not have access to specific data within the system unless specifically authorized for the purpose of managing system data.

a. Democracy Live segregates data based on duty and role at Democracy Live
b. Democracy Live defines the following personnel roles:
    a. Sales
    b. Operations
    c. Development
    d. DevOps Administrators
    e. System Administrators
c. System access follows the DL policy principle of Least Privilege and supports separation of duties as defined in (b) above.

OmniBallot further defines three roles:

a. User
b. User Manager
c. System Administrator (same as personnel role)

3.1.9. [AC-06] Least Privilege

Democracy Live employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Status: **Implemented**

Democracy Live practices the principal of least privilege across the entire organization. All personnel in all departments are required to read and sign off on the Democracy Live Security

Policy and the policy is reviewed semi-annually. All new hires are required to read and sign-off on the Security Policy.

3.1.10. [AC-06 (1)] Authorize Access to Security Functions

Democracy Live explicitly authorizes access to the system infrastructure (AWS) services by assigning specific personnel to specific groups with access to services only necessary to fulfill the specific duties assigned to their role.

Status: Implemented

Democracy Live practices the principal of least privilege across the entire organization. All personnel in all departments are required to read and sign off on the Democracy Live Security Policy. The Security Policy is reviewed and revised, if necessary, semi-annually. All new hires are required to read and sign-off on the Security Policy. Security functions include establishing system and application accounts, assigning audit events, security groups, application firewall, and file storage provisioning and permissions.

Only assigned roles are able to carry out functions within that role. The following roles are assigned security functions:

a. OmniBallot Operations. Specific personnel are assigned administrative roles with Operations to handle provisioning and de-provisioning tenant User and User Manager accounts.
b. Development. Specific personnel are assigned administrative roles to manage system maintenance, application log auditing, and deployment tasks.
c. DevOps. Specific personnel are assigned administrative roles to manage system and service deployment and configuration tasks. DevOps is also responsible for reviewing and assigning security keys and permissions to system storage and compute services.

3.1.11. [AC-06 (2)] Non-Privilege Access for Non-Security Functions

Democracy Live requires that users of OmniBallot accounts, or roles, with access to security functions or security-relevant information, use non-privileged accounts or roles, when accessing non-security functions.

Status: Implemented

Democracy Live requires users of OmniBallot accounts, or roles, with access to any security-related feature of the system or application to use a different specific non-privileged account or role, when accessing any non-security related features or functions.

3.1.12. [AC-06 (5)] Privileged Accounts

Democracy Live restricts privileged accounts on the system to authorized Administrators of the system.

Status: Implemented

Democracy Live authorizes network access to Operations personnel only for specifically defined and compelling operational needs on a temporary basis as approved by the CTO.
Democracy Live only grants authorized network access to Developer and DevOps roles with the need to administer or configure services within the system network.

All system infrastructure services are accessible through a connection to AWS services by authorized personnel only. Developers and DevOps are the only two roles with potential access to system services. The concept of Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device).

3.1.13. [AC-06 (9)] Auditing Use of Privileged Functions

OmniBallot audits the execution of privileged functions.

Status: Implemented

OmniBallot services are supported by AWS infrastructure and all services are monitored by CloudTrail for creation, modification, and access. All actions performed on system infrastructure are subject to logging and available in immutable audit logs.

3.1.14. [AC-06 (10)] Prohibit Non-Privileged Users from Executing Privileged Functions

OmniBallot prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Status: Implemented

OmniBallot services are only accessible by authorized personnel and non-privileged users cannot execute any privileged services or functions. Any attempt to access or modify services are monitored by CloudTrail for creation, modification, and access. All actions performed on system infrastructure are subject to logging and available in immutable audit logs to facilitate non-repudiation.

3.1.15. [AC-07] Unsuccessful Login Attempts

Democracy Live

a. Enforces a limit of consecutive invalid logon attempts by a user during a defined time period; and
b. Automatically delays next logon prompt according to a defined delay algorithm when the maximum number of unsuccessful attempts is exceeded.

Status: Implemented

AWS Cognito is used for Authentication and provides protections against brute-force attacks, but does not provide a configuration by which to set a specific lockout. Cognito will use a built-in algorithm to detect brute-force attacks.

AWS Cognito does implement a lockout policy by default, but the policy is not public to customers due to security reasons.

Cognito User Pools implements a throttling and back-off mechanism where supplied passwords for a given user name is found to be incorrect. In particular, Cognito itself does not disable an account automatically where N attempts takes place against a user.

After a series of consecutive failed login attempts, Cognito throws an error – "NotAuthorizedException: Password attempts exceeded" for a certain lockout period.

Cognito uses a complex rule internally to determine the number of failed attempts and the duration of lockout in between the failed attempts. If an attempt to login happens again, the lockout time is exponentially increased. However, once a successful login is made after that lockout period has expired, the counter is reset. The maximum lockout time is a few minutes (this is internal to the AWS Cognito service and subject to change). These policy settings are not visible/modifiable via AWS console or AWS APIs/CLI commands, nor are they customizable on the account level.

3.1.16. [AC-08] System Use Notification

OmniBallot:

a. Displays to users a system use notification "block-out" banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that
   1. Users are accessing a U.S. Government information system
   2. Information system usage may be monitored, recorded, and subject to audit;
   3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
   4. Use of the information system indicates consent to monitoring and recording;

b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and

c. For publicly accessible systems:
   1. Displays system use information regarding privacy and terms of use policy;
   2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
   3. Includes a description of the authorized uses of the system.

Status:	Implemented

The OmniBallot Administration application displays a block-out screen similar to a paywall after a user logs into the system.
The block-out screen is an option a customer my choose to enable based on their requirements.

The block-out screen is displayed over the entire UI after login and requires a user to explicitly click the "Accept" button to acknowledge they accept the presented information regarding access to the system. The block-out screen may contain the following information:

1. Users are accessing a U.S. Government information system;
2. OmniBallot usage may be monitored, recorded, and subject to audit;

3. Unauthorized use of OmniBallot is prohibited and subject to criminal and civil penalties; and

4. Use of OmniBallot indicates consent to monitoring and recording;
   b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and
   c. For publicly accessible systems the block-out screen is not implemented but the site contains links to the privacy and terms of use policies for access to the public-facing OmniBallot application.

3.1.17. [AC-11] Session Lock

OmniBallot:

a. Prevents further access to the system by initiating a system lock after 20 minutes of inactivity on the application.
b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

Status: Implemented

OmniBallot implements a session locking display feature to prevent viewing of data or use after a period of 20 minutes of user inactivity in the application. The Session Lock feature refreshes the screen and navigates to display the login screen to prompt the user to login using their credentials.

3.1.18. [AC-12] Session Termination

OmniBallot automatically terminates a user session after 20 minutes of inactivity.

Status: Implemented

OmniBallot implements the same session termination after 20 minutes of inactivity. This feature is the same as AC-11.

3.1.19. [AC-14] Permitted Actions without Identification or Authorization (Anonymous).

OmniBallot:

a. Identifies [Assignment: organization-defined user actions] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and
b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

Status: Implemented

All access to the OmniBallot system requires authentication for access to the Administration applications. Voters must also authenticate to use any of the voter-facing applications. Authentication is also required for all system or infrastructure access. Anonymous access is not an option with any Democracy Live system or application.

3.1.20. [AC-17] Remote Access

Monitor and control remote access sessions.

a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
b. Authorizes remote access to the information system prior to allowing such connections.

Status: Implemented

OmniBallot is a web-based application accessible over the Internet and requires authentication and authorization to access any of the web-based applications. OmniBallot applications may be configured to also require multi-factor authentication (MFA) to gain access to the system.

Democracy Live also leverages AWS infrastructure for system services and requires MFA and authorization to access any of the AWS services in use.

3.1.21. [AC-17 (1)] Automated Monitoring / Control

OmniBallot monitors and controls remote access methods.

Status: Implemented

OmniBallot implements AWS Cognito for application authentication and authorization. Cognito maintains a log of all activity including failed login attempts. Audit logs are available for reporting through CloudTrail logs.

3.1.22. [AC-17 (2)] Protection of Confidentiality / Integrity Using Encryption

OmniBallot employs cryptographic mechanisms to protect the confidentiality of remote access sessions.

Status: Implemented

OmniBallot implements AWS CloudFront, S3, and API Gateway to encrypt HTTP traffic using SSL/TLS 1.1 between the client and AWS services. All traffic to port 80 or HTTP is redirected to port 443 using HTTPS.

3.1.23. [AC-17 (3)] Managed Access Control Points

OmniBallot routes remote access through managed access control points.

Status: Implemented

OmniBallot implements CloudFront with a Web Application Firewall (WAF) to monitor and route traffic to various services. OmniBallot also utilizes security groups within the system Virtual Private Cloud (VPC) to further restrict port and originating IP access.

3.1.24. [AC-17 (4)] Privileged Commands / Access

Democracy Live

c. Authorizes the execution of privileged commands and access to security-relevant information via remote access only for Developers or DevOps; and
d. Documents the rationale for such access in the security plan for the information system.

Status: Implemented

Democracy Live implements role-based access control (RBAC) to systems and services. All access to CloudTrail services or database access requires the use of a specific authorized role to execute any commands. Access to any security related information within the applications require MFA and authorization with a permitted role to gain access to any privileged service commands.

3.1.25. [AC-18] Wireless Access

Democracy Live

a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and
b. Authorizes wireless access to the information system prior to allowing such connections.

Status: Implemented

Democracy Live requires personnel to only access the system via wireless in a known network setting. Wireless usage from any public location is not allowed.

All traffic between OmniBallot services and client utilize an encrypted (HTTPS) connection using TLS1.1.

3.1.26. [AC-18 (1)] Wireless Access | Authentication and Encryption

OmniBallot protects wireless access to the system using authentication of users and encryption.

Status: Implemented

OmniBallot protects wireless access to the system using AWS Cognito for user authentication and utilize an encrypted (HTTPS) channel using TLS1.2.

3.1.27. [AC-19] Access Control for Mobile Devices

Democracy Live

a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and
b. Authorizes wireless access to the information system prior to allowing such connections

Status: Implemented

Democracy Live does not allow mobile devices to be connected to any information system. Mobile devices may connect to web-based applications through the internet and use the application through the user interface provided. Mobile devices cannot be used to transmit, handle, or manage any data outside the usage of the OmniBallot web application.

Democracy Live implements AWS Cognito for authentication and authorization. HTTPS / TLS1.1 is also implemented to protect the confidentiality and integrity of information transmitted between the OmniBallot web applications and the mobile device.

3.1.28. [AC-19 (5)] Full Device | Container-Based Encryption

Democracy Live employs full-device encryption to protect the confidentiality and integrity of information on any mobile laptop device.

Status: Implemented

Democracy Live requires any mobile laptop device maintain full disk encryption to protect any information contained on the laptop device.

3.1.29. [AC-20] Use of External Information Systems

Democracy Live establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

a. Access the information system from external information systems; and
b. Process, store, or transmit organization-controlled information using external information systems.

Status: Implemented

Democracy Live establishes terms and conditions through the service contract with the customer. Customers are required to coordinate access to systems with Democracy Live DevOps team to establish access to any OmniBallot services. Democracy Live DevOps team coordinates the provisioning of user and role access for customers to transmit and store information in the OmniBallot system. Access to OmniBallot systems will only be to either AWS S3 Buckets or specific API end-points made available by DevOps.

3.1.30. [AC-20 (1)] Limits on Authorized Use

Democracy Live permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:

a. Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or
b. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

Status: Implemented

Democracy Live limits authorized access to OmniBallot systems to customers based on the requirements to integrate with external information systems. Democracy Live verifies the implementation of the security controls through security audits of AWS Config which monitors and identifies any accounts with misconfigured access permissions. Democracy Live's DevOps team works closely with the customer team to verify integration points and usage of the integration point.

3.1.31. [AC-20 (2)] Portable Storage Devices

Democracy Live prohibits the use of organization-controlled portable storage devices by authorized individuals on external information systems.

Status: Implemented

Democracy Live security policy prohibits the use of organization-controlled portable storage devices by any authorized individual on external information systems.

3.1.32. [AC-21] Information Sharing

Democracy Live

a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for Personally Identifiable Information (PII) or other potentially sensitive Voter information.
b. Employs a Security Policy regarding Personally Identifiable Information (PII) to assist users in making information sharing/collaboration decisions.

Status: Implemented

Democracy Live Security Policy defines PII and sensitive information and the handling of such information by Democracy Live personnel and the sharing of that information with the customer. Democracy Live does not, typically, handle PII or sensitive information in the clear and will emphasize to the customer this information should be hashed prior to sharing with Democracy Live. In the advent of PII being shared in the clear, Democracy Live will handle the information according the Security Policy regarding handling PII or sensitive information.

3.1.33. [AC-22] Publicly Accessible Content

Democracy Live

a. Designates individuals authorized to post information onto a publicly accessible information system;
b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and
d. Reviews the content on the publicly accessible information system for nonpublic information semi-annually and removes such information, if discovered.

Status:	Implemented

Democracy Live designates content editors who are authorized to post information on the Democracy Live website. The Democracy Live website does not contain any customer information or data relating to the contractual engagement. Content posted to the website is reviewed by the content editor and management staff prior to posting. Website content is reviewed both on a semi-annual basis and prior to and post publishing any new content to the website.

3.2. [AT] Awareness and Training

3.2.1. [AT-01] Security Awareness Policies & Procedures

Democracy Live

a. Develops, documents, and disseminates to all Democracy Live personnel that manage or handle Democracy Live information assets:
    1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Reviews and updates the current:
    1. Security awareness and training policy semi-annually; and
    2. Security awareness and training procedures semi-annually.

Status:	Implemented

Democracy Live Security Policy ensures that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems

All Democracy Live personnel are aware of the Security Policy and Procedures. All new hires will be required to sign-off on reading the Security Policy and all employees must re-verify their familiarity with Policies and Procedures during the semi-annual Security Review.

Democracy Live personnel are required to complete a security awareness training based on their role and responsibility. Security awareness training is completed on a semi-annual basis.

3.2.2. [AT-02] Awareness and Training

Democracy Live provides basic security awareness training to information system users (including managers, senior executives, and contractors):

a. As part of initial training for new users;
b. When required by information system changes; and
c. Semi-annually thereafter.

Status: Implemented

All Democracy Live personnel are informed and trained on security specific issues as they relate to their role in the organization. System Administrators, Developers, and DevOps are further required to participate in Security Reviews and more in-depth training.

3.2.3. [AT-02 (1)] Practical Exercises

Democracy Live includes practical exercises in security awareness training that simulate actual cyber-attacks and Democracy Live engages external pen-testing exercises on a semi-annual basis.

Status: Implemented

All Democracy Live personnel are trained on security specific issues as they relate to their role in the organization. System Administrators, Developers, and DevOps are further required to participate in Security Reviews and more in-depth training and participate in pen-testing exercises as well as keeping abreast of new and emerging cybersecurity threats and vulnerabilities.

3.2.4. [AT-02 (2)] Insider Threat

Democracy Live includes security awareness training on recognizing and reporting potential indicators of insider threat.

Status: Implemented

All Democracy Live personnel will be provided insider threat security awareness training and will be required to comply with Security Policies and Procedures which stipulates any suspicious activity is to be reported to management.

3.2.5. [AT-03] Role-Based Security Training

Democracy Live provides basic security awareness training to information system users (including managers, senior executives, and contractors):

a. Before authorizing access to the information system or performing assigned duties;
b. When required by information system changes; and
c. Semi-annually thereafter.

Status: Implemented

Democracy Live requires all personnel, when on-boarding, receive a copy of the Democracy Live Security Policy and are required to read and sign an attestation they have read and understand all policies and procedures described in the Security Policy. All personnel are required to also review the Security Policy and sign an attestation on a semi-annual basis.

All Democracy Live personnel are informed and trained on security specific issues as they relate to their role in the organization. System Administrators, Developers, and DevOps are further required to participate in Security Reviews and more in-depth training.

3.3. [AU] Audit and Accountability

3.3.1. [AU-01] Policy and Procedures

Democracy Live

a. Develops, documents, and disseminates to authorized personnel or roles:
   1. Business process-level or System-level audit and accountability policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;
b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
c. Reviews and updates the current audit and accountability:
   1. Policy semi-annually and following system configuration updates; and
   2. Procedures semi-annually and following system configuration updates.

Status: Implemented

Democracy Live maintains a Security Policy which outlines an accountability policy for all personnel and addresses responsibilities, and accountability controls within the organization.

3.3.2. [AU-02] Event Logging

Democracy Live

a. Identify the types of events that the system is capable of logging in support of the audit function: event types that the system is capable of logging;
b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
c. Specify the following event types for logging within the system along with the frequency of (or situation requiring) logging for each identified event type;
d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and
e. Review and update the event types selected for logging semi-annually.

Status: Implemented

OmniBallot systems utilizes CloudTrail and custom database audit tables defined per tenant to record all system activity. System audit logs are available for ninety (90) days and may be preserved for a longer duration if requested by the customer.

Democracy Live will determine that OmniBallot is capable of auditing the following events: user name, IP address, access timestamp, system action taken, any additional function specific info, warnings, and errors;

a. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;

b. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and

c. Determines that the following events are to be audited within the information system: user name, IP address, access timestamp, system action taken, any additional function specific info, warnings, and errors (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event.

3.3.3. [AU-03] Content of Audit Records

Democracy Live

a. What type of event occurred;
b. When the event occurred;
c. Where the event occurred;
d. Source of the event;
e. Outcome of the event; and
f. Identity of any individuals, subjects, or objects/entities associated with the event.

Status: Implemented

AWS CloudTrail logs ensure that actions taken by individual users of the system are tracked and uniquely traced to those users providing non-repudiation. CloudTrail logs the type of event that occurred, when the event occurred, where (which system) in which the event occurred, event outcome, and identity of the source associated with the event.

3.3.4. [AU-03 (1)] Additional Audit Information

OmniBallot application generates audit records containing the following additional information.

Status: Implemented

AWS CloudTrail generates system audit logs stored in S3 buckets. OmniBallot additionally generates application-level logs which documents actions invoked in the application. The event information logged includes audit Id, Account Id, Election Id, Entity Id, Action taken, Timestamp, user email, HTTP Method, Service REST URL, IP address, Trace ID, Detail of changes made.

3.3.5. [AU-04] Audit Storage Capacity

Allocate audit log storage capacity to accommodate audit log retention requirements.

Status: Implemented

CloudTrail Audit logs are stored in S3 buckets and no storage capacity limit is defined or enforced. Audit logs are retained for one year.

3.3.6. [AU-05] Response to Audit Logging Processing Failures

CloudTrail Audit logging and Democracy Live

a. Alerts authorized personnel or roles within one hour in the event of an audit logging process failure; and
b. Takes the following additional actions.

Status: Implemented

Audit logs are maintained by CloudTrail and stored in read-only S3 bucket containers. CloudTrail is a managed service provided by AWS with an SLA of 99.9% uptime. S3 bucket containers are durable storage containers with a guaranteed uptime of “Eleven Nines” 99.999999999%.

3.3.7. [AU-06] Audit Record Review, Analysis, and Reporting

Democracy Live

a. Reviews and analyzes system audit records semi-annually and post-elections for customers for indications of unusual activity and the potential impact of the inappropriate or unusual activity;
b. Report findings to authorized personnel or customers; and
c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

Status: Implemented

Democracy Live audits logs semi-annually and post-elections per customer to ensure no unusual activity was present during the election period before and after. A report is generated from the logs showing all actions taken on the system and reports any unusual activity.

3.3.8. [AU-06 (1)] Automated Process Integration

Democracy Live Integrates audit record review, analysis, and reporting processes using automated mechanisms.

Status: Implemented

Democracy Live implements AWS CloudWatch as well as custom filters to monitor and analyze audit logs to provide alerts and reporting.

3.3.9. [AU-06 (3)] Correlate Audit Record Repositories

Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

Status: Implemented

Democracy Live implements AWS CloudTrail, CloudWatch, and custom audit logs across different S3 buckets and repositories to provide system-wide situational awareness encompassing system services, network monitoring, and application monitoring.

3.3.10. [AU-07] Audit Record Reduction and Report Generation

Provide and implement an audit record reduction and report generation capability that:

a. Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and
b. Does not alter the original content or time ordering of audit records.

Status: Implemented

AWS Athena provides report generation capability on demand as well as on-demand analysis and discovery. Athena does not allow altering of original audit log content.

3.3.11. [AU-07 (1)] Automatic Processing

Provide and implement the capability to process, sort, and search audit records for events of interest based on fields within audit records.

Status: Implemented

AWS Athena provides report generation capability and the ability to sort and search audit records for events of interest. Search capability is based on SQL and all fields captured in the event logs are available for query.

3.3.12. [AU-08] Time Stamps

Audit logging services

a. Uses internal system clocks to generate time stamps for audit records; and
b. Record time stamps for audit records that meet a granularity of time measurement to the millisecond, uses Coordinated Universal Time, has a fixed local time offset from Coordinated Universal Time, and/or that include the local time offset as part of the time stamp.

Status: Implemented

All CloudTrail, CloudWatch, and OmniBallot audit logs include timestamps. Timestamps are either in UTC or offset by time zone (GMT-7).

3.3.13. [AU-09] Protection of Audit Information

Democracy Live

a. Protects audit information and audit logging tools from unauthorized access, modification, and deletion; and

b. Alerts authorized personnel or roles upon detection of unauthorized access, modification, or deletion of audit information.

Status: Implemented

All CloudTrail and CloudWatch audit records are encrypted by default in S3. Only system root is allowed to access S3 with delete access and a CloudWatch alarm is configured for any logins under system root. This is a privileged account and is only to be used for system-wide access under special circumstances.

3.3.14. [AU-09 (4)] Access by Subset of Privileged Users

Democracy Live authorizes access to management of audit logging functionality to only authorized privileged users or roles.

Status: Implemented

Only system root is allowed to access S3 with delete access to CloudTrail audit logs. A CloudWatch alarm is configured for any logins under system root which sends an email to the Administrator group. System root is a privileged account and is only to be used for system-wide access under special circumstances. No other users have access to CloudTrail audit logs beyond read-only.

3.3.15. [AU-11] Audit Record Retention

Democracy Live retains audit records for time period consistent with records retention policy to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

Status: Implemented

CloudTrail audit logs are retained for a period of two years per compliance policy and to provide forensic analysis of any security events in the future.

3.3.16. [AU-12] Audit Record Generation

Democracy Live

a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on system components and services;

b. Allow authorized personnel or roles to select the event types that are to be logged by specific components of the system; and
c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.

Status: Implemented

CloudTrail, CloudWatch, and a custom application generate audit records for various event types across the system. System level audit records are generated by CloudTrail, service level audit records are generated by CloudWatch, and application-level audit records are generated by a custom service designed to capture application activity. All audit event types can be queried and selected based on field value criteria.

3.4. [CA] Security Assessment

3.4.1. [CA-01] Security Assessment and Authorization

Democracy Live

a. Develops, documents, and disseminates to all relevant personnel:
   1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and
b. Reviews and updates the current:
   1. Security assessment and authorization policy semi-annually; and
   2. Security assessment and authorization procedures semi-annually.

Status: Implemented

The Democracy Live Security Review is performed on a semi-annual basis to address the purpose, scope, roles, and responsibilities of the security program in place to ensure the Democracy Live risk management strategy is effective and reflects the current threat environment.

3.4.2. [CA-02] Security Assessments

Democracy Live

a. Develops a security assessment plan that describes the scope of the assessment including:
   1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and
b. Assesses the security controls in the information system and its environment of operation at least semi-annually to determine the extent to which the controls are implemented correctly, operating

as intended, and producing the desired outcome with respect to meeting established security requirements;

c. Produces a security assessment report that documents the results of the assessment; and

d. Provides the results of the security control assessment to management.

Status: Implemented

Democracy Live conducts a security assessment which includes system inventory, security training for personnel, and a review of authorization policy and roles on a semi-annual basis. The security review deliverable is an assessment report including system services inventory, personnel security training, and Security Policy reviews.

Independent assessor will be brought in to conduct assessments of the network architecture. AWS Well Architected Review by AWS personnel will assess and review the system architecture and provide feedback on best practices and system configuration.

3.4.3. [CA-02 (1)] Independent Assessors

Democracy Live employs third-party of independent assessors or assessment teams with autonomy to conduct security control assessments.

Status: Implemented

Independent assessors are engaged routinely to conduct code audits, network scanning, and penetration testing. Democracy Live also engages AWS to perform a Well Architected Review by AWS personnel will assess and review the system architecture and provide feedback on AWS best practices and system configuration for performance and security.

3.4.4. [CA-03] System Interconnections

Democracy Live

a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;

b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and

c. Reviews and updates Interconnection Security Agreements either semi-annually or upon customer contract termination or renewal.

Status: Not Applicable

OmniBallot does not maintain dedicated connections between information systems.

3.4.5. [CA-05] Plan of Action & Milestones

Democracy Live

a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and

b. Updates existing plan of action and milestones semi-annually based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Status: Implemented

Democracy Live Incident Response plan and Security Reviews document any remedial actions taken in response to a security incident or discovered through Security Reviews. The Incident Response plan documents the plan of action to report and document any actions taken to correct any weaknesses or deficiencies leading to a security incident. Any security weaknesses or deficiencies discovered during the Security review are documented and remediation scheduled for implementation based on assessed impact severity.

3.4.6. [CA-06] Security Authorization

Democracy Live

a. Assigns a senior-level executive or manager as the authorizing official for the information system;

b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and

c. Updates the security authorization semi-annually.

Status: Implemented

The CTO or CSO as the senior level manager is assigned as the authorizing official (AO) and will grant Authorization to Operate (ATO) for OmniBallot. The AO is responsible for reviewing the Security Review report and documentation and will provide the AOT when satisfied all controls are in place.

3.4.7. [CA-07] Continuous Monitoring

Democracy Live

a. Establishment of metrics to be monitored;

b. Establishment of frequencies for monitoring and frequencies for assessments supporting such monitoring;

c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;

d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;

e. Correlation and analysis of security-related information generated by assessments and monitoring;

f. Response actions to address results of the analysis of security-related information; and

g. Reporting the security status of organization and the information system to management on a semi-annual basis unless there is a security event.

Status: Implemented

Democracy Live continuously monitors the OmniBallot system across a number of metrics. These metrics include monitoring of the network traffic via flow logs on the Virtual Private Cloud (VPC), CloudWatch metrics and alarming configured to notify the Developers, and DevOps of any application error threshold exceptions as well as any anomalous traffic or data.

Democracy Live also utilizes AWS Config, Inspector, and Guard Duty to monitor AWS services for configuration changes, and security issues.

3.4.8. [CA-07 (1)] Independent Assessment

Democracy Live employs assessors or assessment teams with independence to monitor the security controls in the information system on an ongoing basis.

Status: Implemented

Democracy Live works with independent assessors to routinely conduct code audits, network scanning, and penetration testing. Democracy Live also engages with AWS consulting to perform Well Architected Reviews to assess any system architecture changes and provide feedback on AWS best practices and system configuration for performance and security.

Additionally, Democracy Live security team, and DevOps monitors notification emails from other agencies EISSA, MS-ISAC, ICS-CERT, and US-CERT regarding recent threat information with regards to type of threat events and relevance to the system and the organization.

3.4.9. [CA-07 (4)] Independent Assessment

Democracy Live ensures risk monitoring is an integral part of the continuous monitoring strategy that includes the following:

a. Effectiveness monitoring;
b. Compliance monitoring; and
c. Change monitoring.

Status: Implemented

Democracy Live utilizes AWS CloudTrail, CloudWatch, and custom log monitors in addition to automated compliance monitors to comply with a continuous monitoring policy.

3.4.10. [CA-09] Internal System Connections

Democracy Live

d. Authorizes internal connections of information system components or classes of components to the information system; and
e. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

Status: Implemented

Democracy Live authorizes internal connections to services based on API connections from various services. For example, AWS API Gateway connects to a Lambda Service which may or may not connect to a Fargate cluster. These connections between our internal services (Lambda and Fargate) are authorized through the use of service roles which permit or restrict the level of access to the internal API (Fargate) and/or any persistence layer (database/file server) by role based on requests to the API and authorization tokens presented to the API.

3.5. [CM] Configuration Management

3.5.1. [CM-01] Configuration Management Policies & Procedures

Democracy Live

a. Develops, documents, and disseminates to all relevant and authorized personnel or roles:
   1. Business process-level and/or System-level configuration management policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;

b. Designate an Executive Manager to manage the development, documentation, and dissemination of the configuration management policy and procedures; and
   1. When required due to architectural changes are required; and

c. Review and update the current configuration management:
   1. Policy semi-annually and following system architecture redesign; and
   2. Procedures semi-annually and following system design or system architecture changes.

Status: Implemented

Democracy Live Configuration Management Policy documents and Configuration management policies used to manage risks from system changes impacting baseline configuration settings, system configuration and security. System configuration is managed using the AWS CloudFormation templates and the Cloud Development Kit (CDK) which provides Infrastructure as a Service (IaaS) and Infrastructure as Code (IaC). All systems are configured using IaC and are managed in version control.

3.5.2. [CM-02] Baseline Configuration

Democracy Live

a. Develops, documents, and maintains under configuration control, a current baseline configuration of the system; and

b. Review and update the baseline configuration of the system:
   1. Semi-annually;
   2. When required due to system changes; and
   3. When system components are installed or upgraded.

Status: Implemented

Democracy Live maintains a system configuration baseline using AWS IaC to allow consistent deployment of systems. AWS IaC is an automated system to allow configuration of the network topology and services implemented. Version control is used to maintain and track version changes in addition to tracking within AWS CloudFormation which provides logging, versioning, and roll-back capabilities.

3.5.3. [CM-02 (2)] Automation Support for Accuracy and Currency

Democracy Live maintains the currency, completeness, accuracy, and availability of the baseline configuration of the system using automated mechanisms.

Status: Implemented

Democracy Live utilizes AWS IaC to automate the maintenance of the baseline configuration of all systems used by OmniBallot. Democracy Live maintains a system configuration baseline using AWS IaC to allow consistent deployment of systems.

3.5.4. [CM-02 (3)] Retention of Previous Configurations

Democracy Live retains all previous versions of baseline configurations of the system to support rollback.

Status: Implemented

Democracy Live retains all previous versions of the baseline configuration for all system configurations. System baseline configurations are stored in a version control system and utilizes AWS IaC to automate the deployment of the baseline configuration used by OmniBallot.

3.5.5. [CM-02 (7)] Configure Systems and Components for High-Risk Areas

Democracy Live

a. Issues systems with configurations to individuals traveling to locations that the organization deems to be of significant risk; and
b. Apply the following controls to the systems or components when the individuals return from travel.

Status: Implemented

Democracy Live does not specifically store or disseminate any high-value data. Systems at-risk, such as laptops issued to personnel are required by the Democracy Live Security Policy to maintain anti-virus software in addition to encrypted hard-drives and secure passwords.

3.5.6. [CM-03] Configuration Change Control

Democracy Live

a. Determines and documents the types of changes to the system that are configuration-controlled;
b. Reviews proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;
c. Documents configuration change decisions associated with the system;
d. Implements approved configuration-controlled changes to the system;
e. Retains records of configuration-controlled changes to the system for one year;
f. Monitors and reviews activities associated with configuration-controlled changes to the system; and
g. Coordinates and provides oversight for configuration change control activities through configuration change control audits that reviews system changes semi-annually or on major system design or architectural updates.

Status: Planned to be Implemented

The full change control process including proposal, justification, implementation, testing, review, and disposition of system changes has yet to be documented. The current process does include support for code commits and merge control on a branch that is peer reviewed before being deployed to the current operational system.

3.5.7. [CM-03 (2)] Testing, Validating, and Documentation of Changes

Democracy Live tests, validates, and documents changes to the system before finalizing the implementation of the changes.

Status: Implemented

A Continuous Integration and Deployment (CI/CD) automation mechanism has been implemented to support testing and validation of system changes. System changes are documented in code as IaC which provides a consistent and repeatable process by which system configuration changes are deployed.

3.5.8. [CM-03 (4)] Security and Privacy Representatives

Democracy Live requires security and privacy representatives to be members of DevOps or development teams and authorized to perform system configuration changes.

Status: Implemented

Security and privacy representatives are members of DevOps or development teams and are the only authorized personnel to perform system configuration changes.

3.5.9. [CM-04] Impact Analysis

Democracy Live analyzes changes to the system to determine potential security and privacy impacts prior to change implementation.

3.5.10. [CM-04 (2)] Verification of Controls

After system changes, Democracy Live verifies that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.

Status: Implemented

System changes are deployed via CI/CD processes which implements unit and integration testing to verify security and privacy controls have been implemented per reviewed requirements and verified to operate as intended.

3.5.11. [CM-05] Access Restrictions for Change

Democracy Live defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the system.

Status: Implemented

AWS Console access is restricted to only authorized personnel and follows the Security Policy of least privilege. All changes to the system can only be made either through console access or API access which all adhere to the Policy of Least Privilege. Access to system configuration is restricted to DevOps and specific developer personnel.

3.5.12. [CM-06] Configuration Settings

Democracy Live

a. Establishes and documents configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using secure configurations;
b. Implements the configuration settings;
c. Identifies, documents, and approves any deviations from established configuration settings for system components based on operational requirements; and
d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Status: Implemented

Access to the system component library is restricted to the DevOps and development teams. Access to the code repository requires MFA access and any changes to system components or configuration are required to be committed and merged with the current production branch in the code repository.

3.5.13. [CM-07] Least Functionality

Democracy Live

a. Configures the system to provide only mission essential capabilities; and
b. Prohibits or restricts the use of the following functions, ports, protocols, software, and/or services:

Status: Implemented

OmniBallot is configured to only use essential services required for the system to operate. Based on the system topology, certain ports, protocols, and services are restricted based on security best-practices and level of access required. The system architecture and design follow industry best practices in segregating application architecture into an n-Tiered system. All database access, for instance, is configured with a Security Group to restrict traffic to a specific port, protocol, and application middleware server IP. All other access is denied.

3.5.14. [CM-07 (1)] Periodic Review

Democracy Live

a. Reviews the system semi-annually to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and
b. Disable or remove functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure.

Status: Implemented

A semi-annual security review and audit is conducted to identify any security issues with the system configuration. This review is part of the configuration change security review. All unnecessary functions, ports, protocols, software, and/or services are either removed or disabled.

3.5.15. [CM-07 (2)] Prevent Program Execution

Prevent program execution in accordance with defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

Status: Implemented

OmniBallot does not allow for arbitrary program execution and access to any service to arbitrarily deploy or execute code is restricted by both policy and procedure. OmniBallot restricts access to only Authorized users and Administrators who are able to deploy code into production.

3.5.16. [CM-07 (5)] Authorized Software – Allow by Exception

Democracy Live

a. Identifies software programs authorized to execute on the system;
b. Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and

c. Reviews and updates the list of authorized software programs semi-annually or prior to implementation.

Status: Implemented

Democracy Live and OmniBallot do not rely on any additional application code executing outside the context of the application. OmniBallot does not implement any non-vetted application code and does not use or rely on any third-party software applications to operate OmniBallot.

3.5.17. [CM-07(5)] Least Functionality | Authorized Software / Whitelisting

Require and enforce oversight of all software packages or programs that are authorized to execute on the system.

Status: Implemented

Democracy Live does not rely on additional application code executing outside the context of the application.

3.5.18. [CM-08] System Component Inventory | Updates / Installs

Democracy Live

a. Develops and documents an inventory of system components that:
   1. Accurately reflects the system;
   2. Includes all components within the system;
   3. Does not include duplicate accounting of components or components assigned to any other system;
   4. Is at the level of granularity deemed necessary for tracking and reporting; and
   5. Includes the following information to achieve system component accountability: necessary to achieve effective system component accountability; and

b. Review and update the system component inventory semi-annually.

Status: Implemented

Inventory of components is maintained as part of the Infrastructure as Code (IaC) and system components are described in the code that is deployed. The full inventory of code and modules are available in source control and DevOps and development follow the principle of Don't Repeat Yourself (DRY) to only develop one instance or implementation of a component for easy use/re-use.

3.5.19. [CM-08 (1)] Information System Component Inventory | Updates / Installs

Maintain inventory of components integral to installations and system updates.

Status: Implemented

Inventory of components will be maintained as part of the IaaC system components which are described in the code that is deployed.

3.5.20. [CM-08 (1)] Updates During Installation and Removal

Update the inventory of system components as part of component installations, removals, and system updates.

Status: Implemented

The full inventory of system components is available through source control and is maintained as part of normal development and deployment of the system. All components are regularly reviewed as part of the on-going development and maintenance process.

3.5.21. [CM-08 (3)] Automated Unauthorized Component Detection

Democracy Live

a. Detects the presence of unauthorized hardware, software, and firmware components within the system using automated mechanisms running on a weekly basis; and
b. Takes the following actions when unauthorized components are detected: notification of authorized personnel of any unauthorized hardware, or software.

Status: Implemented

Third party tools are implemented to provide scanning of containers and the network for malicious or unauthorized access to systems.

3.5.22. [CM-09] Configuration Management Plan

Democracy Live develops, documents, and implements a configuration management plan for the system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;
b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
c. Defines the configuration items for the system and places the configuration items under configuration management;
d. Is reviewed and approved by authorized personnel or roles; and
e. Protects the configuration management plan from unauthorized disclosure and modification.

Status: Implemented

The Democracy Live Configuration Management plan defines processes and procedures consistent with industry best practices and establishes a process for the software development lifecycle (SDLC) for managing system development and deployment.

3.5.23. [CM-10] Software Usage Restrictions

Democracy Live

a. Uses software and associated documentation in accordance with contract agreements and copyright laws;

b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Status: Implemented

All software implemented within OmniBallot is open-sourced and MIT-licensed software allowing free use and verification of the source code. Any code used within the system is reviewed for licensing restrictions before being integrated into the system.

3.5.24. [CM-11] User-Installed Software

Democracy Live

a. Establishes policies governing the installation of software by users;
b. Enforces software installation policies through the following methods: code review and configuration review; and
c. Monitor policy compliance semi-annually.

Status: Implemented

All software implemented within OmniBallot is vetted prior to use by the DevOps, and development teams. Democracy Live Security Policy requires all software installed by users on their local machines to be authorized by Democracy Live Security Operations (SECOPS).

3.5.25. [CM-12] Information Location

Democracy Live

a. Identifies and documents the location of sensitive information and the specific system components on which the information is processed and stored;
b. Identifies and documents the users who have access to the system and system components where the information is processed and stored; and
c. Documents changes to the location (i.e., system or system components) where the information is processed and stored.

Status: Implemented

OmniBallot leverages AWS Macie which is a fully managed automated security and privacy service using Machine Learning and pattern matching to discover and protect sensitive information (PII) stored in AWS S3 Buckets. Democracy Live also protects any sensitive or private data by pre-encrypting any PII prior to storage.

3.5.26. [CM-12 (1)] Automated Tools to Support Information Location

Democracy Live uses automated tools to identify sensitive information (PII) used by system components to ensure controls are in place to protect organizational information and individual privacy.

Status: Implemented

Democracy Live protects sensitive or private data by pre-encrypting any PII prior to storage so PII is never transmitted or stored in the clear while under management by OmniBallot or Democracy Live.

3.6. [CP] Contingency Planning

3.6.1. [CP-01] Contingency Planning Policy and Procedures

Democracy Live

a. Develops, documents, and disseminates to all operational personnel:
   1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and

b. Reviews and updates the current:
   1. Contingency planning policy semi-annually; and
   2. Contingency planning procedures semi-annually.

Status: Implemented

Democracy Live disseminates to all operations personnel a copy of the Democracy Live Disaster Recovery Plan which describes contingencies in the advent of an emergency and addresses the purpose, scope, roles, and responsibilities of Democracy Live personnel. The Disaster Recovery Plan as well as the Democracy Live Incident Response plan covers contingencies for all systems and operational or security failures.

3.6.2. [CP-02] Contingency Planning

Democracy Live

a. Develops a contingency plan for the information system that:
   1. Identifies essential missions and business functions and associated contingency requirements;
   2. Provides recovery objectives, restoration priorities, and metrics;
   3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
   4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
   5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
   6. Is reviewed and approved by Executive Management;

b. Distributes copies of the contingency plan to key system management contingency personnel within System Administration, Development, and DevOps;

c. Coordinates contingency planning activities with incident handling activities;

d. Reviews the contingency plan for the information system semi-annually;
e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
f. Communicates contingency plan changes key system management contingency personnel within System Administration, Development, and DevOps; and
g. Protects the contingency plan from unauthorized disclosure and modification.

Status: Implemented

Democracy Live has documented contingency plans in a Democracy Live Disaster Recovery plan document. The Disaster Recovery plan identifies business functions and contingency requirements along with recovery objectives, priorities, and metrics. The Disaster recovery plan describes the roles and responsibilities of team members and their functions.

3.6.3. [CP-02 (1)] Coordinate with Related Plans

Democracy Live coordinates contingency plan development with organizational elements responsible for related plans.

Status: Implemented

Democracy Live coordinates contingency plans in accordance with the shared responsibility model with AWS. Democracy Live is responsible for application and data availability and recovery while AWS is responsible for system and service infrastructure. Democracy Live coordinates contingency plans with development and DevOps teams to ensure clear communication and roles and responsibilities of each team. AWS is required to notify system administrators and DevOps of any operational issues with system infrastructure.

3.6.4. [CP-02 (3)] Resume Essential Missions / Business Functions

Democracy Live plans for the resumption of essential missions and business functions within one (1) hour of contingency plan activation.

Status: Implemented

Barring any major disaster which would incapacitate an entire geographic region (major earthquake affecting the entire West Coast of the U.S.), Democracy Live Disaster Recovery plans can resume normal operations of essential missions or business functions within one (1) hour of the incident. Implementing Infrastructure as Code (IaC) facilitates rapid recovery and deployment of all services from a code repository containing the latest snapshot of the production environment. Utilizing AWS infrastructure and IaC, full network topology and service infrastructure can be recreated within an hour of catastrophic failure.

3.6.5. [CP-02 (8)] Identify Critical Assets

Democracy Live identifies critical information system assets supporting essential missions and business functions.

Status: Implemented

Democracy Live has identified and inventoried all critical information system assets that support essential missions and business functions. All identified assets are cataloged in an inventory list and exist as part of the IaC code-base.

3.6.6. [CP-03] Contingency Training

Democracy Live provides contingency training to information system users consistent with assigned roles and responsibilities:

a. Within one (1) month of assuming a contingency role or responsibility;
b. When required by information system changes; and
c. Semi-annually thereafter.

Status: Implemented

Simulated events will be part of the disaster recovery plans, procedures, and tests. Table Top Exercises (TTX) will be used along with other simulated events to test Disaster Recovery plans and procedures on a semi-annual basis or if a major system architecture change is implemented.

3.6.7. [CP-04] Contingency Plan Testing

Democracy Live:

a. Tests the contingency plan for the information system semi-annually using the test scenarios defined in the Disaster Recovery Plan to determine the effectiveness of the plan and the organizational readiness to execute the plan;
b. Reviews the contingency plan test results; and
c. Initiates corrective actions, if needed.

Status: Implemented

Disaster recovery tests are included in the Disaster Recovery plans and test scenarios outlined in the plan are executed and reviewed on a semi-annual basis or if a major system architecture change is implemented affecting services used.

3.6.8. [CP-04 (1)] Coordinate with Related Plans

Democracy Live coordinates contingency plan testing with organizational elements responsible for related plans.

Status: Implemented

Democracy Live will coordinate with any outside customers contingency plans and testing as applicable to the integration and reliance on Democracy Live or customer infrastructure. Plans will include contacts in outside agencies and / or technical procedures which need to be implemented.

3.6.9. [CP-06] Alternate Storage Site

Democracy Live:

a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and
b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

Status: Implemented

OmniBallot implements AWS Aurora Serverless Clusters for the tenant database. Aurora cluster Recovery Time Objective (RTO) is within one (1) hour and Recovery Point Objective (RPO) is within five (5) hours. Depending on the client and the size of the database, these times may be less than the stated RPO/RTO.

Any additional data storage is implemented in AWS S3 which has a stated durability of "Eleven Nines" (99.999999999%) protecting against any site-level failures, errors, or threats. S3 also designed to have 99.99% availability.

3.6.10. [CP-06 (1)] Separation from Primary Site

Democracy Live identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

Status: Implemented

OmniBallot leverages AWS S3 and Aurora Serverless services for data persistence. Both services operate in a multi-redundant environment across multiple availability zones. S3 is a global service which spans multiple geographic regions as well. Aurora serverless maintains multiple cluster instances with near instantaneous fail-over in addition to read-replicas over multiple availability zones.

Database back-up snapshots are stored in S3 buckets and are available for database restoration with the RPO/RTO stated previously.

3.6.11. [CP-06 (3)] Separation from Primary Site

Democracy Live identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Status: Implemented

As stated previously OmniBallot leverages AWS S3 and Aurora Serverless services for data persistence.

AWS manages the services infrastructure and provides multi-redundant services across either geographic zones or availability zones (data-centers). This system topology mitigates or nearly eliminates any potential area-wide disruption or disaster.

3.6.12. [CP-07] Alternate Processing Site

Democracy Live:

a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of OmniBallot services for essential missions/business functions within the Disaster Recovery Plan RTO/RPO when the primary processing capabilities are unavailable;
b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and
c. Ensures that the alternate processing site provides information security safeguards equivalent to those of the primary site.

Status: Implemented

Democracy Live implements IaC to consistently and efficiently deploy infrastructure services and applications. AWS IaC provides the ability to codify the system services infrastructure topology and configuration in code thus effectively eliminating operator error in configuring or deploying services.

In addition to IaC, AWS provides system redundancy across either geographic zones (states) and availability zones (data-centers) which provide, in combination with IaC, the infrastructure to satisfy alternate processing site requirements.

3.6.13. [CP-07 (1)] Separation from Primary Site

Democracy Live identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

Status: Implemented

Democracy Live leverages AWS infrastructure in a shared responsibility model. AWS is responsible for physical system infrastructure and security of those systems. CloudFront (CDN), Web Application Firewalls (WAF), Security Groups (Firewalls), and Virtual Private Clouds (VPC) provide the hosted infrastructure in a multi-redundant environment. The application architecture of OmniBallot utilizes serverless services which are ephemeral in nature. These services are created and destroyed during deployments and updates to the system. Any threat that may breach the system would be eliminated during the next refresh during a system update or system timeout in the case of AWS Lambdas.

3.6.14. [CP-07 (2)] Accessibility

Democracy Live identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Status: Implemented

Democracy Live implements CloudWatch Alarms which notifies relevant personnel in the advent of an issue or outage experienced on the OmniBallot application. The Democracy Live Disaster Recovery plan outlines process and procedures in the event of a disruption.

3.6.15. [CP-07 (3)] Priority of Service

Democracy Live develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).

Status:	Implemented

The Democracy Live Disaster Recovery plan outlines process and procedures in the event of a disruption. With IaC, any disruption in services due to outage can be re-deployed in the same state as the last known production deployment.

3.6.16. [CP-08] Telecommunication Services

Democracy Live establishes alternate telecommunications services including necessary agreements to permit the resumption of system operations for essential missions and business functions within one (1) hour when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Status:	Implemented

Democracy Live utilizes AWS infrastructure which maintains multi-redundant and private backbone services. High-speed backbone and multi-redundant telecommunication providers nearly guarantee no disruptions in networking communications on the network.

3.6.17. [CP-08 (1)] Priority of Service Provisions

Democracy Live:

a. Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and

b. Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

Status: Implemented

Democracy Live utilizes AWS infrastructure which maintains multi-redundant and private backbone services. High-speed backbone and multi-redundant telecommunication providers nearly guarantee no disruptions in networking communications on the network.

3.6.18. [CP-08 (2)] Single Point of Failure

Democracy Live obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

Status: Implemented

Democracy Live utilizes AWS infrastructure which maintains multi-redundant and private backbone services. High-speed backbone and multi-redundant telecommunication providers nearly guarantee no disruptions in networking communications on the network.

3.6.19. [CP-09] Information System Backup

Democracy Live:

c. Conducts backups of user-level information contained in the information system as described in the Disaster Recovery Plan.

d. Conducts backups of system-level information contained in the information system as described in the Disaster Recovery Plan;

e. Conducts backups of information system documentation including security-related documentation as described in the Disaster Recovery Plan; and

f. Protects the confidentiality, integrity, and availability of backup information at storage locations.

Status: Implemented

Democracy Live conducts back-ups of all data contained in the database as described in the Disaster Recovery Plan. All data is protected by encryption at rest both in S3 and the databases. All storage location data confidentiality and integrity are maintained using encryption keys and audit logs. Keys rotated on a semi-annual basis unless a security issue requires a key refresh. Audit logs are reviewed either on a customer requirement basis or on a quarterly basis unless a security issue requires inspection.

3.6.20. [CP-09(1)] Information System Backup | Testing Reliability / Integrity

Democracy Live tests backup information semi-annually to verify media reliability and information integrity.

Status: Implemented

Democracy Live tests backup process and procedure and the Disaster Recovery Plan to verify reliability and information integrity on a semi-annual basis.

3.6.21. [CP-10] Information System Recovery and Reconstitution

Democracy Live provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

Status: Implemented

Democracy Live implements IaC to provide full system recovery and reconstitution in the advent of a disruption, compromise, or failure. IaC provides a reliable repeatable deployment of system services based on the latest production commit in version control.

3.6.22. [CP-10 (2)] Transaction Recovery

OmniBallot implements transaction recovery for systems that are transaction-based.

Status: Implemented

OmniBallot utilizes AWS Aurora Serverless services to provide MySQL database services. Aurora serverless utilizes a proprietary log shipping protocol and network attached storage which provides transaction recovery and redundancy.

3.7. [IA] Identification and Authentication

3.7.1. [IA-01] Identification and Authentication Policy and Procedures

Democracy Live:

a. Develops, documents, and disseminates to System Administrators, Developers, and DevOps personnel:
   1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and

b. Reviews and updates the current:
   1. Identification and authentication policy semi-annually; and
   2. Identification and authentication procedures semi-annually.

Status: Implemented

Democracy Live maintains a Security Policy document which contains the policies and procedures impacting identification and authentication.

The Security Policy maintains all access to the OmniBallot system services (AWS) by any personnel will require MFA.

Access to OmniBallot Administration application by Users, or User Administrators may opt-in to use MFA at their discretion. Cognito supports SMS MFA for OmniBallot.

3.7.2. [IA-02] Identification and Authentication (Organizational Users)

OmniBallot uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Status: Implemented

All access to OmniBallot by any user in any role will require authentication. Users and User Administrators are also tenant based and are provisioned on a tenant basis.

3.7.3. [IA-02 (1)] Network Access to Privileged Accounts

The information system implements multifactor authentication for network access to privileged accounts.

Status: Implemented

See IA-1

3.7.4. [IA-02 (2)] Network Access to Non-Privileged Accounts

The information system implements multifactor authentication for network access to non-privileged accounts.

Status: Implemented

See IA-1

3.7.5. [IA-02 (3)] Local Access to Non-Privileged Accounts

The information system implements multifactor authentication for local access to privileged accounts.

Status: Implemented

OmniBallot does not allow access directly to AWS services as local access. All access to AWS services is restricted to Democracy Live personnel and maintained on a least privilege basis. All local access to AWS by authorized personnel must use MFA.

3.7.6. [IA-02 (8)] Network Access to Privileged Account – Replay Resistant

The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.

Status: Implemented

Authentication is secured by AWS Cognito and always requires login credentials using an encrypted channel and using cryptographically secure authentication and authorization tokens (JWT) for all users of OmniBallot. OmniBallot users may also be required to use MFA if the customer has requested this feature.

AWS Service access requires the same level of security along with a requirement of MFA.

3.7.7. [IA-02 (11)] Remote Access – Separate Device

The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets the Time-based One Time Password Authentication policy.

Status: Implemented

OmniBallot implements multifactor authentication (MFA) using SMS as implemented by AWS Cognito for access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets the strength of mechanism requirements (SMS for Cognito). This feature is available to customers upon request.

3.7.8. [IA-02 (12)] Acceptance of PIV Credentials

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.

Status: Not Applicable

OmniBallot does not use PIV credentials.

3.7.9. [IA-03] Identification and Authentication

The information system uniquely identifies and authenticates specific types of devices before establishing a local; remote; or network connection.

Status: Not Applicable

OmniBallot is a web-based application that does not implement any further out-of-band local, remote, or network authentication.

3.7.10. [IA-04] Identifier Management

Democracy Live:

a. Receiving authorization from authorized personnel to assign an individual, group, role, or device identifier;
b. Selecting an identifier that identifies an individual, group, role, or device;
c. Assigning the identifier to the intended individual, group, role, or device;
d. Preventing reuse of identifiers for a defined time period; and
e. Disabling the identifier after 90 days of inactivity.

Status: Implemented

OmniBallot does not implement any mechanisms to authorize or assign device identifiers.
User or Role identifiers are established through the use of tokens (JWT) which identifies authenticated and authorized users of the system.

3.7.11. [IA-05] Identifier Management

Democracy Live manages information system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
b. Establishing initial authenticator content for authenticators defined by the organization;
c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
e. Changing default content of authenticators prior to information system installation;
f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
g. Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type];
h. Protecting authenticator content from unauthorized disclosure and modification;
i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
j. Changing authenticators for group/role accounts when membership to those accounts change.

Status: Implemented

Democracy Live and OmniBallot support the use of external MFA authenticators. Democracy Live does not supply or disseminate any device or authenticator to Democracy Live personnel or customers.

OmniBallot leverages Cognito for authentication. Cognito requires users to create a password when first logging in after their account has been provisioned. Democracy Live does not generate or provide authenticators to any customers or users of the system.

3.7.12. [IA-05 (1)] Password-Based Authentication

OmniBallot, for password-based authentication:

a. Enforces minimum password complexity of case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type;
b. Enforces at least the following number of changed characters when new passwords are created;
c. Stores and transmits only cryptographically-protected passwords;
d. Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum];
e. Prohibits password reuse for at least 24 generations; and
f. Allows the use of a temporary password for system logons with an immediate change to a permanent password.

Status: Implemented

OmniBallot implements AWS Cognito for authentication. The configuration can enforce a minimum number of characters, a mix of upper and lower-case, special characters, and numbers.
Cognito Stores and transmits only cryptographically-protected passwords.
Cognito can enforce password expirations of unused accounts. The default setting is 7 days and can be configured up to 90 days.
Cognito does not prohibit password reuse.
OmniBallot does not currently support assigning temporary passwords for system logins.

3.7.13. [IA-05 (2)] PKI-Based Authentication

OmniBallot, for PKI-based authentication:

a. Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;
b. Enforces authorized access to the corresponding private key;
c. Maps the authenticated identity to the account of the individual or group; and
d. Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

Status: Not Applicable

OmniBallot does not implement any PKI authentication schemes.

3.7.14. [IA-05 (3)] In-Person or Trusted Third-Party Registration

Democracy Live requires that the registration process to receive specific authenticators be conducted in person before a registration authority with authorization by authorized personnel.

Status: Not Applicable

OmniBallot does not support third-party or in-person registration.

3.7.15. [IA-05 (11)] Hardware Token-Based Authentication

The information system, for hardware token-based authentication, employs mechanisms that satisfy token quality requirements.

Status: Not Applicable

OmniBallot does not currently support hardware token authentication.

3.7.16. [IA-06] Authenticator Feedback

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Status: Implemented

OmniBallot obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. User credentials are never delivered to the client and authentication is performed by Cognito using both encrypted channel and password encryption.

3.7.17. [IA-07] Cryptographic Module

The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

Status: Not Applicable

OmniBallot does not implement any additional cryptographic modules.

3.7.18. [IA-08] Identification and Authentication (Non-Organizational Users)

The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

Status: Implemented

OmniBallot creates unique accounts for non-organizational users in coordination with the customer. Non-organizational accounts are uniquely identified and also follow the Democracy Live Security Plan policy of least privilege.

3.7.19. [IA-08 (1)] Acceptance of PIV Credentials from Other Agencies

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.

Status: Not Applicable

OmniBallot does not accept or use PIV credentials in the system.

3.7.20. [IA-08 (2)] Acceptance of Third-Party Credentials

The information system accepts only FICAM-approved third-party credentials.

Status: Not Applicable

OmniBallot does not accept or use FICAM third-party credentials in the system.

3.7.21. [IA-08 (3)] Use of FICAM-Approved Products

Democracy Live employs only FICAM-approved information system components in OmniBallot to accept third-party credentials.

Status: Not Applicable

OmniBallot does not accept or use FICAM products in the system.

3.7.22. [IA-08 (4)] Use of FICAM-Issued Profiles

The information system conforms to FICAM-issued profiles.

Status: Not Applicable

OmniBallot does not accept or use FICAM profiles in the system.

3.8. [IR] Incident Response

3.8.1. [IR-01] Incident Response Policy and Procedures

Democracy Live

a. Develops, documents, and disseminates to relevant operational personnel:
    1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and

b. Reviews and updates the current:
    1. Incident response policy semi-annually; and
    2. Incident response procedures semi-annually or if significant deficiencies are discovered.

Status: Implemented

The Democracy Live Incident Response Plan documents the response policy addressing, scope, roles, responsibilities and coordination of organizational entities in response to an incident.

The Incident response policies and procedures are reviewed and updated semi-annually unless a significant deficiency or any incident response policy or procedures are found to be insufficient.

3.8.2. [IR-02] Incident Response Training

Democracy Live

a. Within 10 days of assuming an incident response role or responsibility;

b. When required by information system changes; and

c. Semi-annually thereafter.

Status: Implemented

Democracy Live provides incident response training to OmniBallot personnel consistent with their assigned roles and responsibilities within 10 days of assuming an incident response role or responsibility or when required by major system architecture or service changes and/or semi-annually thereafter as part of the semi-annual Security Review.

3.8.3. [IR-03] Incident Response Testing

Democracy Live tests the incident response capability for the information system semi-annually using [Assignment: organization-defined tests] to determine the incident response effectiveness and documents the results.

Status: Implemented

Democracy Live tests the incident response capability to determine the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies through the use of checklists and tabletop exercise (TTX) conducted on a semi-annual basis during the semi-annual Security Review.

3.8.4. [IR-03 (2)] Coordination with Related Plans

Democracy Live coordinates incident response testing with organizational elements responsible for related plans.

Status: Implemented

Democracy Live coordinates incident response testing with related organizational plans during the semi-annual Security Review which includes Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans as documented in the Disaster Recovery Plan and Security Policy documents.

3.8.5. [IR-04] Incident Handling

Democracy Live

a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;

b. Coordinates incident handling activities with contingency planning activities; and
c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.

Status: Implemented

Democracy Live implements an incident handling capability for security incidents that include preparation, detection, and analysis using AWS services to provide reports and notifications to initiate containment, eradication, and recovery plans and processes. Incident handling activities are coordinated with contingency planning activities as documented in the Disaster Recovery and Incident Response plans. Any lessons learned or deficiencies discovered are further incorporated into incident response procedures and training.

3.8.6. [IR-04 (1)] Automated Incident Handling Processes

Democracy Live employs automated mechanisms to support the incident handling process.

Status: Implemented

Democracy Live utilizes AWS Security Hub, Guard Duty, and Config services to automate incident reporting and notification.

3.8.7. [IR-05] Incident Monitoring

Democracy Live tracks and documents information system security incidents.

Status: Implemented

Democracy Live automates incident monitoring by utilizing AWS Guard Duty, Config, and Security Hub services to create automated tracking and analysis of security incidents. CloudWatch alarming is implemented to send notifications to relevant authorized personnel when pre-determined thresholds are exceeded.

Incident alerting via email will be available to all incident response personnel for operational awareness and to create a notification audit trail via email.

3.8.8. [IR-06] Incident Response

Democracy Live

a. Requires personnel to report suspected security incidents to the organizational incident response capability within a defined time period; and
b. Reports security incident information to appropriate authorized personnel.

Status: Implemented

Democracy Live requires personnel to report any suspicious or suspected security incidents to authorized personnel to activate the Incident Response team to investigate the incident. Democracy

Live personnel are required to report any suspected activity immediately upon becoming aware of such activity as documented in the Security Policy and Incident Response documents.

3.8.9. [IR-06 (1)] Automated Reporting

Democracy Live employs automated mechanisms to assist in the reporting of security incidents.

Status: Implemented

Democracy Live automates incident reporting by utilizing AWS Guard Duty, Config, and Security Hub services to generate notifications and reporting of security incidents. CloudWatch alarming is implemented to send notifications to relevant authorized personnel when pre-determined thresholds are exceeded.

3.8.10. [IR-07] Incident Response Assistance

Democracy Live provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

Status: Implemented

Democracy Live assigns an incident response support resource to assist organizational personnel with advice and assistance for the handling and reporting of security incidents. Democracy Live personnel are made aware of the resources available during on-boarding and as documented in the Security Policy.

3.8.11. [IR-07 (1)] Automation Support for Availability of Information / Support

Democracy Live employs automated mechanisms to increase the availability of incident response-related information and support.

Status: Implemented

Democracy Live employs automated mechanisms to increase the availability of incident response-related information and support using AWS services such as Guard Duty, Config, and Security Hub to provide automated scanning and notification to authorized Democracy Live personnel.

3.8.12. [IR-08] Incident Response Plan

Democracy Live

a. Develops an incident response plan that:
    1. Provides the organization with a roadmap for implementing its incident response capability;
    2. Describes the structure and organization of the incident response capability;
    3. Provides a high-level approach for how the incident response capability fits into the overall organization;

   4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
   5. Defines reportable incidents;
   6. Provides metrics for measuring the incident response capability within the organization;
   7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
   8. Is reviewed and approved by [Assignment: organization-defined personnel or roles];

b. Distributes copies of the incident response plan to authorized incident response personnel;
c. Reviews the incident response plan semi-annually;
d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
e. Communicates incident response plan changes to incident response personnel; and
f. Protects the incident response plan from unauthorized disclosure and modification.

Status: Implemented

Democracy Live maintains a comprehensive Incident Response Plan addressing incident response capability and the coordination and sharing of information with external organizations, including, for example, external service providers and organizations involved in the supply chain for organizational information systems.

3.9. [MA] Maintenance

3.9.1. [MA-01] Maintenance Policies and Procedures

Democracy Live

a. Develops, documents, and disseminates to authorized personnel:
   1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and

b. Reviews and updates the current:
   1. System maintenance policy semi-annually; and
   2. System maintenance procedures semi-annually.

Status: Implemented

Democracy Live Development and DevOps team performs system maintenance as part of the on-going Software Development Lifecycle (SDLC). The policies and procedures follow the Democracy Live Security Policies and procedures take into account both the Security Policies as well as Continuous Integration and Deployment (CI/CD) along with IaC deployments.

3.9.2. [MA-02] Controlled Maintenance

Democracy Live

a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;

c. Requires that personnel explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;

d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;

e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and

f. Includes [Assignment: organization-defined maintenance-related information] in organizational maintenance records.

Status: Implemented

Democracy Live hosts the OmniBallot application on AWS infrastructure and participates in the AWS Shared Responsibility Model which relies on AWS to maintain all hardware and physical environments. Democracy Live is responsible for all OmniBallot services and security regarding these services. Additional information regarding maintenance can be found in the Democracy Live Security Policy document.

3.9.3. [MA-03] Maintenance Tools

Democracy Live approves, controls, and monitors information system maintenance tools.

Status: Implemented

Democracy Live does not utilize any hardware tools that interface with the AWS infrastructure. All tools used by Democracy Live used to maintain OmniBallot are either services provided by AWS or systems that have been vetted and approved by Democracy Live Developers, or DevOps prior to use.

3.9.4. [MA-03 (1)] Inspect Tools

Democracy Live inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

Status: Implemented

All maintenance tools used shall be subject to inspection if used on any electronic system within Democracy Live offices or facilities. No unidentified media or tools are to be used on or with any system in the organization. All client machines in use by Democracy Live personnel are required by the Democracy Live Security Policy to be running anti-virus software and personnel have been prohibited to use any unknown media devices on client machines.

3.9.5. [MA-03 (2)] Inspect Media

Democracy Live checks media containing diagnostic and test programs for malicious code before the media are used in the information system.

Status: Implemented

All media used in systems shall be subjected to a virus scan. No unidentified media is to be used on or with any system in the organization. All client machines in use by Democracy Live personnel are required by the Democracy Live Security Policy to be running an anti-virus software and personnel are prohibited to use any unknown media devices on client machines.

3.9.6. [MA-04] Non-Local Maintenance

Democracy Live

a. Approves and monitors nonlocal maintenance and diagnostic activities;
b. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;
c. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;
d. Maintains records for nonlocal maintenance and diagnostic activities; and
e. Terminates session and network connections when nonlocal maintenance is completed.

Status: Implemented

All maintenance tools used shall be subject to inspection if used on any electronic system within Democracy Live offices or facilities. No unidentified media or tools are to be used on or with any system in the organization. All maintenance or diagnostic tool requirements are subject to the Democracy Live Security Policy.

3.9.7. [MA-05] Maintenance Personnel

Democracy Live

a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;
b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and
c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

Status: Implemented

Democracy Live does not permit third-party maintenance personnel access the OmniBallot system. All maintenance is performed by Democracy Live authorized personnel and are subject to the Democracy Live Security Policy.

3.9.8. [MA-06] Timely Maintenance

Democracy Live obtains maintenance support and/or spare parts for system components within a reasonable amount of time based on level and type of failure.

Status: Implemented

Democracy Live does not maintain any hardware for the operation of OmniBallot services. AWS is responsible for all hardware and physical infrastructure systems.

3.10. [MP] Media Protection

3.10.1. [MP-01] Media Protection Policy and Procedures

Democracy Live

d. D Develops, documents, and disseminates to all Democracy Live personnel:
   1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and

e. Reviews and updates the current:
   1. Media protection policy semi-annual; and
   2. Media protection procedures semi-annual.

Status: Implemented

The Democracy Live Security Policy documents a policy regarding the proper use of non-digital and digital media assets.

3.10.2. [MP-02] Media Access

Democracy Live restricts access to digital and/or non-digital media to authorized personnel.

Status: Implemented

The Democracy Live Security Policy documents policy regarding proper storage and access of non-digital and digital media assets.

3.10.3. [MP-03] Media Marking

Democracy Live

a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and

b. Exempts system media from marking as long as the media remain within a securely controlled area accessible only by authorized personnel.

Status: Implemented

The Democracy Live Security Policy documents policy regarding proper marking and access of sensitive non-digital and digital media assets.

3.10.4. [MP-04] Media Storage

Democracy Live

a. Physically controls and securely stores digital and/or non-digital media within a securely controlled area; and
b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Status: Implemented

The Democracy Live Security Policy documents policy regarding proper media storage and access of sensitive non-digital and digital media assets.

3.10.5. [MP-05] Media Protection

Democracy Live

a. Protects and controls system media during transport outside of controlled areas using security safeguards;
b. Maintains accountability for information system media during transport outside of controlled areas;
c. Documents activities associated with the transport of information system media; and
d. Restricts the activities associated with the transport of information system media to authorized personnel.

Status: Implemented

The Democracy Live Security Policy documents policy regarding proper media protection and transport of sensitive non-digital and digital media assets.

3.10.6. [MP-06] Media Sanitization

Democracy Live

a. Sanitizes system media prior to disposal, release out of organizational control, or release for reuse using approved sanitization techniques and procedures in accordance with applicable federal and organizational standards and policies; and
b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Status: Implemented

The Democracy Live Security Policy documents policy regarding proper media sanitization of sensitive non-digital and digital media assets. Refer to Democracy Live Security Policy for proper sanitization of digital media assets.

3.10.7. [MP-07] Media Protection

Democracy Live

a. Restrict the use of removable media on local machines; and
b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.

Status: Implemented

The Democracy Live Security Policy documents policy regarding proper media sanitization of sensitive non-digital and digital media assets. Refer to Democracy Live Security Policy for proper sanitization of digital media assets.

The Democracy Live Security Policy prohibits the use of portable storage devices for which the owner is not known. Refer to Democracy Live Security Policy for proper device usage

---

3.11. [PE] Physical and Environmental Protection Policy and Procedures

3.11.1. [PE-01] Physical and Environmental Policy and Protection

Democracy Live

a. Develops, documents, and disseminates to authorized personnel:
   1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and
b. Reviews and updates the current:
   1. Physical and environmental protection policy semi-annually; and
   2. Physical and environmental protection procedures semi-annually.

Status: Not Applicable

Democracy Live utilizes AWS hosted infrastructure to support the OmniBallot application service. AWS implements a shared responsibility model in which AWS is responsible for all physical and environmental protections at AWS hosted facilities. Democracy Live is responsible for all software implemented on the hosted services provided by AWS

3.11.2. [PE-02] Physical Access Authorizations

Democracy Live

a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the OmniBallot system resides;
b. Issues authorization credentials for facility access;
c. Reviews the access list detailing authorized facility access by individuals semi-annually; and
d. Removes individuals from the facility access list when access is no longer required.

Status: Not Applicable

Democracy Live utilizes AWS hosted infrastructure to support the OmniBallot application service. AWS implements a shared responsibility model in which AWS is responsible for all physical and environmental protections at AWS hosted facilities. Democracy Live is responsible for all software implemented on the hosted services provided by AWS

3.11.3. [PE-03] Physical Access Control

Democracy Live

a. Enforces physical access authorizations at [Assignment: organization-defined entry/exit points to the facility where the information system resides] by;
b. Maintains physical access audit logs for all entry/exit points;
c. Provides security safeguards to control access to areas within the facility officially designated as publicly accessible;
d. Escorts visitors and monitors visitor activity or circumstances requiring visitor escorts and monitoring;
e. Secures keys, combinations, and other physical access devices;
f. Inventories physical access devices semi-annually; and
g. Changes combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Status: Not Applicable

Democracy Live utilizes AWS hosted infrastructure to support the OmniBallot application service. AWS implements a shared responsibility model in which AWS is responsible for all physical and environmental protections at AWS hosted facilities. Democracy Live is responsible for all software implemented on the hosted services provided by AWS and does not have any physical access to the hosted datacenters.

3.11.4. [PE-04] Access Control for Transmission Medium

Democracy Live controls physical access to system distribution and transmission lines within organizational facilities using security safeguards.

Status: Not Applicable

Democracy Live utilizes AWS hosted infrastructure to support the OmniBallot application service. AWS implements a shared responsibility model in which AWS is responsible for all physical and environmental protections at AWS hosted facilities. Democracy Live is responsible for all software implemented on the hosted services provided by AWS and does not have any physical access to the hosted datacenter networks or telecommunication network.

3.11.5. [PE-05] Access Control for Output Devices

Democracy Live controls physical access to OmniBallot output devices to prevent unauthorized individuals from obtaining the output.

Status: Implemented

Democracy Live Security Policy prohibits personnel from sending data to output devices such as printers, copiers, scanners, or facsimile machines. Only authorized and approved personnel are allowed to send data to output devices in approved circumstances and with data that is not considered sensitive.

3.11.6. [PE-06] Monitoring Physical Access

Democracy Live

a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;
b. Reviews physical access logs per AWS frequency and upon occurrence of various events; and
c. Coordinates results of reviews and investigations with the organizational incident response capability.

Status: Not Applicable

Democracy Live utilizes AWS hosted infrastructure to support the OmniBallot application service. AWS implements a shared responsibility model in which AWS is responsible for all physical and environmental protections at AWS hosted facilities. Democracy Live does not have any visibility into this control.

3.11.7. [PE-06 (1)] Monitoring Physical Access

Democracy Live monitors physical intrusion alarms and surveillance equipment.

Status: Not Applicable

Democracy Live utilizes AWS hosted infrastructure to support the OmniBallot application service. AWS implements a shared responsibility model in which AWS is responsible for all physical and environmental protections at AWS hosted facilities. Democracy Live does not have any visibility into this control.

3.11.8. [PE-08] Visitor Access Records

Democracy Live

d. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;

e. Reviews physical access logs per AWS frequency and upon occurrence of various events; and

f. Coordinates results of reviews and investigations with the organizational incident response capability.

Status: Not Applicable

Democracy Live utilizes AWS hosted infrastructure to support the OmniBallot application service. AWS implements a shared responsibility model in which AWS is responsible for all physical and environmental protections at AWS hosted facilities. Democracy Live does not have any visibility into this control.

3.11.9. [PE-09] Power Equipment and Cabling

Democracy Live protects power equipment and power cabling for the information system from damage and destruction.

Status: Not Applicable

Democracy Live utilizes AWS hosted infrastructure to support the OmniBallot application service. AWS implements a shared responsibility model in which AWS is responsible for all physical and environmental protections at AWS hosted facilities. Democracy Live does not have any visibility into this control.

3.11.10. [PE-10] Emergency Power

Democracy Live provides a short-term uninterruptible power supply to facilitate orderly transition of the information system to long-term alternate power in the event of a primary power source loss.

Status: Not Applicable

Democracy Live utilizes AWS hosted infrastructure to support the OmniBallot application service. AWS implements a shared responsibility model in which AWS is responsible for all physical and environmental protections at AWS hosted facilities. Democracy Live does not have any visibility into this control.

3.11.11. [PE-11] Emergency Lighting

Democracy Live employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Status: Not Applicable

Democracy Live utilizes AWS hosted infrastructure to support the OmniBallot application service. AWS implements a shared responsibility model in which AWS is responsible for all physical and environmental protections at AWS hosted facilities. Democracy Live does not have any visibility into this control.

3.11.12. [PE-13] Fire Protection

Democracy Live employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

Status: Not Applicable

Democracy Live utilizes AWS hosted infrastructure to support the OmniBallot application service. AWS implements a shared responsibility model in which AWS is responsible for all physical and environmental protections at AWS hosted facilities. Democracy Live does not have any visibility into this control.

3.11.13. [PE-13 (3)] Automatic Fire Suppression

Democracy Live employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

Status: Not Applicable

Democracy Live utilizes AWS hosted infrastructure to support the OmniBallot application service. AWS implements a shared responsibility model in which AWS is responsible for all physical and environmental protections at AWS hosted facilities. Democracy Live does not have any visibility into this control.

3.11.14. [PE-14] Temperature and Humidity Controls

Democracy Live

a. Maintains temperature and humidity levels within the facility where the information system resides at acceptable levels; and
b. Monitors temperature and humidity levels on an acceptable frequency.

Status: Not Applicable

Democracy Live utilizes AWS hosted infrastructure to support the OmniBallot application service. AWS implements a shared responsibility model in which AWS is responsible for all physical and environmental protections at AWS hosted facilities. Democracy Live does not have any visibility into this control.

3.11.15. [PE-15] Water Damage Protection

Democracy Live protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Status: Not Applicable

Democracy Live utilizes AWS hosted infrastructure to support the OmniBallot application service. AWS implements a shared responsibility model in which AWS is responsible for all physical and environmental protections at AWS hosted facilities. Democracy Live does not have any visibility into this control.

3.11.16. [PE-16] Delivery and Removal

Democracy Live authorizes, monitors, and controls information system components entering and exiting the facility and maintains records of those items.

Status: Not Applicable

Democracy Live utilizes AWS hosted infrastructure to support the OmniBallot application service. AWS implements a shared responsibility model in which AWS is responsible for all physical and environmental protections at AWS hosted facilities. Democracy Live does not have any visibility into this control.

3.11.17. [PE-17] Alternate Work Site

Democracy Live

a. Employs security controls at alternate work sites;
b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and
c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

Status: Not Applicable

Democracy Live utilizes AWS hosted infrastructure to support the OmniBallot application service. AWS implements a shared responsibility model in which AWS is responsible for all physical and environmental protections at AWS hosted facilities. Democracy Live does not have any visibility into this control.

3.12. [PL] Security Planning Policy and Procedures

3.12.1. [PL-02] System Security Planning

Status: Implemented

Refer to Democracy Live System Architecture for infrastructure topology and system enterprise architecture.
Refer to Democracy Live Network Security Requirements for authorization boundaries, operational context, and security requirements of the system.

3.12.2. [PL-04] Rules of Behavior

Status: Implemented

Refer to Democracy Live Security Policy on behavior and handling of information. All personnel are required to read the Security Policy and sign-off. Security Policy personnel refresh/re-read acknowledgement occurs semi-annually.

3.12.3. [PL-08] Information Security Architecture

Requirements and approach taken with regards to protecting confidentiality, integrity, and availability of information.

Status: Implemented

Refer to Democracy Live System Architecture for infrastructure topology and system architecture security involving multi-tenant architecture and separation of accounts.

3.13. [PS] Personnel Security

3.13.1. [PS-01] Personnel Security Policy and Procedures

Status: Implemented

Refer to Democracy Live Security Policy for details on personnel security policies and procedures.

3.13.2. [PS-02] Personnel Risk Designation

Status: Implemented

Democracy Live information resources are assigned security levels based on the sensitivity of the information controlled by the resource. The security level governs the policy applied to the system. Personnel are also assigned security levels based on least privilege access policy based on role and responsibility in the organization. All personnel accessing the system are required to submit to a criminal background check.

3.13.3. [PS-03] Personnel Screening

Status: Implemented

All personnel accessing the system will be required to submit to a criminal background check and will be required to read and sign-off on accepting the guidance and stipulations in the Democracy Live Security Policy before start of work.

3.13.4. [PS-04] Personnel Termination

Status: Implemented

All terminated personnel will be required to turn in any corporate assets and will be subject to an exit interview. All credentials and access will be revoked upon termination.

3.13.5. [PS-05] Personnel Transfer

Status: Implemented

All transferred personnel will be required to undergo appropriate security training and re-read and sign the Democracy Live Security Policy as it more specifically pertains to their new role. All access to systems will be updated to reflect the new role at this time.

3.13.6. [PS-06] Access Agreements

Status: Implemented

All third-party providers will be required to read and sign off on appropriate security awareness policies and procedures. Third party providers will not have access to any sensitive information unless specifically requested and approved by Democracy Live Executive Management.

3.13.7. [PS-07] Third Party Providers

Status: Implemented

All third-party providers will be required to undergo appropriate security awareness training, read and sign the Democracy Live Security Policy as it more specifically pertains to their role. All access to systems will be updated to reflect the role after verifying training and signature.

3.13.8. [PS-08] Personnel Sanctions

Status: Implemented

Any individual that fails to comply with the Democracy Live Security Policies and Procedures will be subject to a formal sanction process. See the Democracy Live Security Policies for details on the formal sanction process.

3.14. [RA] Risk Assessment

3.14.1. [RA-01] Risk Assessment Policies and Procedures

Democracy Live

a. Develops, documents, and disseminates to all relevant personnel:
   1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and

b. Reviews and updates the current:
   1. Risk assessment policy semi-annually; and
   2. Risk assessment procedures semi-annually.

Status: Implemented

The Democracy Live Security Policy documents the risk assessment policies and procedures for securing systems and information and addresses purpose, scope, roles, and responsibilities for organization personnel.

3.14.2. [RA-02] Security Categorization

Democracy Live

g. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

h. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and

i. Ensures that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

Status: Implemented

The Democracy Live Security Policy documents security categorization and classification. The system classifies information under the same four (4) security levels outlined in the Security Policy.
Four security levels exist, from the lowest (Level One) to the highest (Level Four).

1. Level One – Resources are open to corporate clients or other third parties. This may include physical access as well as general system login, excluding administrative access. No sensitive information will reside on these systems. Level One resources must be treated with caution similar to that of public resources.
2. Level Two – Resources are only available to Democracy Live personnel. This may include physical as well as general system access, possibly including administrative access based on role and the principal of least privilege. Application-level access may be granted to outside users with authorization from Executive Management.
3. Level Three – Resources are physically accessible only by IT system personnel. Limited system access may be available to other staff members if the role requires and only by authorization from management. Application-level access will only be granted to outside users that are authenticated over a secure channel. Automated access to restricted to only encrypted and authenticated channels.
4. Level Four – Resources are physically and electronically accessible to IT personnel only. Highly sensitive information may reside on these resources, but encryption will be enabled for sensitive fields before storage. Additionally, all data will be encrypted at rest. No direct application-level access is allowed. Automated access will be restricted to a small set of well-defined encrypted, authenticated channels.

3.14.3. [RA-03] Risk Assessment

Democracy Live

a. Conduct a risk assessment, including:

   1. Identifying threats to and vulnerabilities in the system;

2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and
3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;

b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;

c. Document risk assessment results in [Selection: security and privacy plans; risk assessment report; [Assignment: organization-defined document]];

d. Review risk assessment results [Assignment: organization-defined frequency];

e. Disseminate risk assessment results to [Assignment: organization-defined personnel or roles]; and

f. Update the risk assessment [Assignment: organization-defined frequency] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

Status: Implemented

Democracy Live assesses risk based on impact from unauthorized access, use, disclosure, disruption, modification, or destruction of data. Risk assessment is documented in the Risk Assessment and Management Program document. The Risk Assessment and Management document is reviewed and updated semi-annually. Risk assessment results are disseminated to Executive Management, Operations, System Administrators, Developers, and DevOps.

3.14.4. [RA-03 (1)] Supply Chain Risk Assessment

Democracy Live

a. Assess supply chain risks associated with systems, system components, and system services; and;

b. Update the supply chain risk assessment semi-annually, when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.

Status: Implemented

Democracy Live assesses risk based on impact from unauthorized access, use, disclosure, disruption, modification, or destruction of data. Risk assessment is documented in the Risk Assessment and Management Program document. The Risk Assessment and Management document is reviewed and updated semi-annually. Risk assessment results are disseminated to Executive Management, Operations, System Administrators, Developers, and DevOps.

3.14.5. [RA-05] Vulnerability Scanning

Democracy Live

a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported;

b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

    1. Enumerating platforms, software flaws, and improper configurations;
    2. Formatting checklists and test procedures; and
    3. Measuring vulnerability impact;

c. Analyzes vulnerability scan reports and results from security control assessments;

d. Remediates legitimate vulnerabilities within defined response times in accordance with an organizational assessment of risk; and

e. Shares information obtained from the vulnerability scanning process and security control assessments with relevant authorized personnel to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Status: Implemented

Democracy Live utilizes AWS Security Hub, Config, Guard Duty, and CloudWatch along with additional tools to continuously monitor OmniBallot systems and services for improper configurations, software flaws resulting in errors or exceptions. Continuous scanning tools such as Security Hub or Config assesses risk based on impact from improper configurations. Security Hub in particular ranks system configuration security against Security Standards based on AWS Foundational Security Best Practices as well as CIS Foundations Benchmarks.

Any information obtained from the monitoring tools are disseminated to Administrators, Developers, and DevOps for remediation based on level of impact.

Legitimate vulnerabilities are evaluated based on impact and assigned a risk level which dictates the remediation timeframe with high impact vulnerabilities receiving the highest priority and shortest remediation timeframe. Vulnerability Management is documented in more detail in the Vulnerability Management Policy.

3.14.6. [RA-05 (2)] New Scan

Democracy Live updates the information system vulnerabilities on a continuous basis.

Status: Implemented

Democracy Live utilizes AWS services to continuously scan the system for vulnerabilities. Democracy Live DevOps personnel review scan reports on a weekly basis to verify all systems are secure and correctly configured.

3.14.7. [RA-05 (5)] Privileged Access

The information system implements privileged access authorization to system services for selected vulnerability scanning activities.

Status: Implemented

Democracy Live utilizes AWS services to provide vulnerability scanning activities. These services have specific authorized access to services to provide the reports necessary for remedial action.

3.14.8. [RA-05 (11)] Public Disclosure Program

Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

Status: Implemented

Democracy Live utilizes external vulnerability scanning by third-party providers and maintains an email address by which security issues may be reported.

3.14.9. [RA-07] Risk Response

Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.

Status: Implemented

Democracy Live responds to security vulnerability findings appropriate to the level of risk associated with the finding as outlined in the Security Policy.

3.14.10. [RA-09] Risk Response

Identify critical system components and functions by performing a criticality analysis for systems, system components, or system services at decision points in the system development life cycle.

Status: Implemented

Democracy Live reviews critical systems and system components during the planning stages of the SDLC. Further analysis is performed during system development and final peer review is completed prior to any system or system component being deployed into the production environment.

3.15. [SA] System and Services Acquisition

3.15.1. [SA-01] System & Services Acquisition Policies & Procedures

Democracy Live:

a. Develops, documents, and disseminates to all relevant personnel or roles:
   1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and

b. Reviews and updates the current:
   1. System and services acquisition policy semi-annually; and
   2. System and services acquisition procedures semi-annually.

Status: Implemented

Democracy Live develops, documents, and disseminates to System Administrators, Developers, and DevOps an acquisition policy that addresses scope, roles, and responsibilities with regards to services acquisition. These policies are outlined in the Democracy Live Security plan.

3.15.2. [SA-02] Allocation of Resources

Democracy Live:

a. Determines information security requirements for the information system or information system service in mission/business process planning;
b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and
c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

Status: Implemented

Democracy Live maintains security requirements documented in the Democracy Live Security Plan. Resources are allocated according to this plan and the relevant services are implemented to protect the OmniBallot application from various threats and threat vectors.

Democracy Live maintains discretion in allocating resources for operational and system security. Various tools and platforms are integrated to provide additional security measures.

3.15.3. [SA-03] System Development Lifecycle

Democracy Live:

a. Manages the information system using a defined system development life cycle (SDLC) that incorporates information security considerations;
b. Defines and documents information security roles and responsibilities throughout the system development life cycle;
c. Identifies individuals having information security roles and responsibilities; and
d. Integrates the organizational information security risk management process into system development life cycle activities.

Status: Implemented

Democracy Live manages the development of the OmniBallot application using a well-defined software development lifecycle (SDLC) that incorporates information security considerations. Democracy Live incorporates the use of JIRA as an agile task tracking application which provides the ability to tag development tasks as security related. All tasks require a separate feature branch for development and are subject to a pull-request and peer code review when complete. Security tagged tasks also require a security review of the code prior to committing to the main production branch.

3.15.4. [SA-04] Acquisition Process

Democracy Live includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

a. Security functional requirements;
b. Security strength requirements;
c. Security assurance requirements;
d. Security-related documentation requirements;
e. Requirements for protecting security-related documentation;
f. Description of the information system development environment and environment in which the system is intended to operate; and
g. Acceptance criteria.

Status: Implemented

Democracy Live implements AWS services for all application infrastructure. AWS services are SOC-2 Type 2 and FEDRamp compliant in the US-WEST region in which all OmniBallot services are implemented.

3.15.5. [SA-04 (1)] Functional Properties of Security Controls

Democracy Live requires developers of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.

Status: Implemented

Democracy Live does not outsource any of the development of OmniBallot application features or functions. Democracy Live follows a strict SDLC which initiates with a system requirement task in JIRA which is assessed for any security implications and tagged with a "security" label. All tasks tagged with a security label are subject to both a peer code review and a code security review prior to a pull request being accepted and merged with the main production branch. All security related code also contains developer comments describing the security control.

OmniBallot may incorporate open-source libraries as part of the application. All open-source libraries are subject to a security review and static code analysis.

3.15.6. [SA-04 (2)] Implementation Information for Security Controls

Democracy Live requires developers of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: security-relevant external system interfaces and source code.

Status: Implemented

The Democracy Live SDLC requires a security review of the OmniBallot system to review the design and implementation of the security controls to be employed for any feature or function that is developed for the OmniBallot application. When a task is entered into the project backlog in JIRA, the task is tagged with a security label which requires a review of the feature. This includes: security-relevant external system interfaces and source code.

3.15.7. [SA-04 (9)] Functions / Ports / Protocols / Services in Use

Democracy Live requires developers of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.

Status: Implemented

Democracy Live incorporates IaC using AWS services CloudFormation and the Cloud Development Kit (CDK) to specify the network services in use by OmniBallot. Any changes to the network topology though use of the CDK is subject to the same SDLC process and security vetting procedures as application code. All services are vetted for port and protocol usage. Security groups and Network Access Control Lists (NACL) are configured within the IaC definitions.

3.15.8. [SA-04 (10)] Use of Approved PIV Products

Democracy Live employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

Status: Not Applicable

No PIV products are in use in the system.

3.15.9. [SA-05] Information System Documentation

Democracy Live:

a. Obtains administrator documentation for the information system, system component, or information system service that describes:
   1. Secure configuration, installation, and operation of the system, component, or service;
   2. Effective use and maintenance of security functions/mechanisms; and
   3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;
b. Obtains user documentation for the information system, system component, or information system service that describes:
   1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
   2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
   3. User responsibilities in maintaining the security of the system, component, or service;

c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and takes [Assignment: organization-defined actions] in response;
d. Protects documentation as required, in accordance with the risk management strategy; and
e. Distributes documentation to System Administrators, Developers, and DevOps personnel.
f.

Status: Implemented

Democracy Live implements IaC which provides a level of self-documentation for all System Administrators, Developers, or DevOps personnel working on the system.

System documentation at a high level is included at the beginning of this document describing the high-level architecture and network topology in use for the OmniBallot application.

Additional system design and implementation documentation may include data flow diagrams, architecture, and topology diagrams depicting system configuration and usage.

3.15.10. [SA-08] Security Engineering Principles

Democracy Live applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

Status: Implemented

Democracy Live and OmniBallot applies information system security engineering principles in the specification, design, development, implementation, and modification of OmniBallot and supporting infrastructure.

Democracy Live leverages AWS and engineering principles to implement the 5-Pillars of a well architected framework which contribute to security and reliability as defined by AWS (https://aws.amazon.com/blogs/apn/the-5-pillars-of-the-aws-well-architected-framework/).

Operational Excellence: ability to support development and run workloads effectively, gain insight into their operation, and continuously improve supporting processes and procedures to delivery business value.

Security: ability to protect data, systems, and assets to take advantage of cloud technologies to improve your security. Additionally, OmniBallot is routinely peer reviewed and subject to third-party code reviews, network scans, and pen-testing exercises.

Reliability: ability of a workload to perform its intended function correctly and consistently when it's expected to. This includes the ability to operate and test the workload through its total lifecycle.

Performance and Efficiency: ability to use computing resources efficiently to meet system requirements, and to maintain that efficiency as demand changes and technologies evolve.

Cost Optimization: ability to run systems to deliver business value at the lowest price point.

3.15.11. [SA-9] External Information System Services

Democracy Live:

a. Requires that providers of external information system services comply with organizational information security requirements and employ security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
c. Employs processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.

Status: Implemented

Democracy Live requires external system providers to comply with the security controls around system access and data management. Democracy Live does not handle PII in the clear and requires external data providers to either hash sensitive fields prior to hand off or provide Democracy Live with the list of sensitive fields contained in the data so such fields are hashed prior to ingestion and storage by OmniBallot.

Democracy Live also requires specific provisioned roles and accounts for each customer accessing an OmniBallot service or API and will coordinate with the customer to provision those accounts.

Democracy Live monitors and audits usage of such accounts and will notify the customer in the event of a suspected breach of security or improper usage of the account.

3.15.12. [SA-9 (2)] Identification of Functions / Ports / Protocols / Services

Democracy Live requires providers of external system services to identify the functions, ports, protocols, and other services required for the use of such services.

Status: Implemented

Democracy Live does not interface with any third-party providers to share information except customers for whom Democracy Live has entered into a contractual agreement and all known integration points are identified and reviewed for security implications.

Democracy Live will identify the functions, ports, protocols, and other services required by customers for the use of OmniBallot services. An inventory of the specific API and S3 buckets access will be created and maintained along with the associated external systems connecting to such services.

3.15.13. [SA-10] Developer Configuration Management

Democracy Live requires developers of the OmniBallot system, system component, or information system service to:

a. Perform configuration management during system, component, or service design; development; implementation; and operation;
b. Document, manage, and control the integrity of changes to configuration items under configuration management;
c. Implement only organization-approved changes to the system, component, or service;
d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and
e. Track security flaws and flaw resolution within the system, component, or service and report findings to System Administrators, Developers, or DevOps.

Status: Implemented

Configuration management will be implemented as IaC using the AWS CDK during system design, development and implementation. System configuration management will be documented by the CDK and integrity will be maintained using this feature. All changes to configuration will be developed on a feature branch and subject to peer review and security review for potential security impacts of changes before merging with the master operational branch.

Security flaws will be tracked and flaw resolution within the system, component, or service and any finding will be reported to Security personnel.

3.15.14. [SA-11] Developer Security Testing and Evaluation

Democracy Live requires the developer of the information system, system component, or information system service to:

a. Create and implement a security assessment plan;
b. Perform unit; integration; system; regression testing/evaluation at a depth and code coverage percentage based on categorization of the specific code-base;
c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
d. Implement a verifiable flaw remediation process; and
e. Correct flaws identified during security testing/evaluation.

Status: Implemented

Democracy Live follows a “shift-left” testing methodology which also incorporates elements of security review and testing and includes the following:

Basic Feature Testing: testing each feature/function of the component for input/output correctness and reliability. This includes implementing input/output sanitization libraries for all data I/O.

Code Review: all new features are subject to peer-review during the commit/pull-request process of the SDLC. Additional security reviews are also required for features impacting security.

Static Code Analysis: static code analysis tools are used to detect any issues with the code quality prior to review and deployment.

Unit Testing: unit tests are written for components that are complex and are subject to complex data models or business rules. Unit testing is prescriptive and may not include 100% code coverage.

3.16. [SC] System and Communications Protection

3.16.1. [SC-01] System and Communications Protection Policy and Procedures

Democracy Live:

a. Develops, documents, and disseminates to authorized personnel:
   1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and

b. Reviews and updates the current:
   1. System and communications protection policy semi-annually; and
   2. System and communications protection procedures semi-annually.

Status: Implemented

Democracy Live maintains a system and communication policy and procedures with respect to the OmniBallot application internal system network and any workstations or user access to those systems in the Democracy Live Security Policy. Access to any system resources is either through the AWS Console, AWS SDK or AWS API. Access using any of these methods is restricted to authorized personnel only and further restricted to a least privilege policy as documented in the Democracy Live Security Policy.

3.16.2. [SC-02] Application Partitioning

OmniBallot separates user functionality (including user interface services) from information system management functionality.

Status: Implemented

OmniBallot separates user functionality (including user interface services) from Administration management functionality. Administrative functionality is contained in a separately segregated User Interface that requires authentication and authorization to access the application.

The OmniBallot Voter-Facing application suite is a separate application that is segregated by functionality, code-base, and system services.

The Administrative Management application is both physical and logical. The separation includes a separate web administrative interface that implements isolated authentication methods for Administrative Users from any other system resources. Segregation of system and user functionality includes isolating administrative interfaces on different domains and with additional access controls.

3.16.3. [SC-04] Information in Shared Resources

OmniBallot prevents unauthorized and unintended information transfer via shared system resources.

Status: Implemented

OmniBallot prevents unauthorized and unintended information transfer via shared system resources. OmniBallot prevent information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to the service pool via AWS managed services.

3.16.4. [SC-05] Denial of Service Protection

OmniBallot system protects against or limits the effects of the following types of denial-of-service attacks by employing Web Application Firewalls and monitoring systems.

Status: Implemented

AWS CloudFront and AWS provide real-time monitoring and protection against DoS and DDoS attacks. Democracy Live will work closely with AWS as a partner to closely monitor systems during high-profile usage.

3.16.5. [SC-07] Boundary Protection

Democracy Live:

a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;

b. Implements subnetworks for publicly accessible system components that are logically separated from internal organizational networks; and

c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Status: Implemented

Democracy Live utilizes AWS infrastructure and services. Democracy Live monitors communications at the external boundary (CloudFront) and at key internal boundaries within the system.

Public APIs as Lambda functions are implemented for publicly accessible system components that are physically separated from internal organizational networks; and will connect to external networks or information systems only through managed interfaces or connection to non-shared resources such as segregated S3 buckets arranged in accordance with organizational security policy and procedure.

3.16.6. [SC-07 (3)] Access Points

Democracy Live limits the number of external network connections to the information system.

Status: Implemented

Democracy Live utilizes AWS infrastructure and services. Democracy Live limits the access of external network connections to OmniBallot services. API access to specific private services or AWS S3 Buckets are limited to authorized customers by contractual agreement only and all access is authorized by customer specific account permissions.

3.16.7. [SC-07 (4)] External Telecommunication Services

Democracy Live:

a. Implements a managed interface for each external telecommunication service;
b. Establishes a traffic flow policy for each managed interface;
c. Protects the confidentiality and integrity of the information being transmitted across each interface;
d. Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and
e. Reviews exceptions to the traffic flow policy semi-annually and removes exceptions that are no longer supported by an explicit mission/business need.

Status: Implemented

OmniBallot utilizes various AWS services to host the application services offered by Democracy Live. Traffic flow policy is documented in the Security Policy and is part of the Security Review. All traffic across the managed network is encrypted using TLS1.1 (HTTPS) and traffic is restricted to the services available within VPC hosting the application. Any external traffic flow into the network is also required to be encrypted and requires both authentication and authorization of the account for access which is negotiated with each customer requesting access.

3.16.8. [SC-07 (5)] Boundary Protection | Deny by Default / Allow By Exception

The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).

Status: Implemented

OmniBallot utilizes AWS services including VPC. The VPC implements both NACL (Network ACLs) and Security Groups to provide boundary protection that is deny by default and allow by exception. Rules allow typical firewall traffic for a specific protocol and port as well as specific IP addresses. Only specific traffic is allowed such as HTTPS over port 443.

3.16.9. [SC-07 (7)] Prevent Split Tunneling for Remote Devices

OmniBallot, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

Status: Not Applicable

OmniBallot is a web-based application and the systems infrastructure does not allow connecting to the service infrastructure directly via VPN.

3.16.10. [SC-08] Transmission Confidentiality & Integrity

OmniBallot protects the confidentiality and integrity of transmitted information.

Status: Implemented

OmniBallot protects the confidentiality and integrity of transmitted data using end-to-end encrypted channels over port 443 using TLS1.1.

3.16.11. [SC-08 (1)] Cryptographic or Alternate Physical Protection

OmniBallot implements cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by alternative physical safeguards.

Status: Implemented

OmniBallot protects the confidentiality and integrity of transmitted data using end-to-end encrypted channels over port 443 using TLS1.1.

3.16.12. [SC-10] Network Disconnect

The information system terminates the network connection associated with a communications session at the end of the session or after a period of inactivity.

Status: Implemented

OmniBallot utilizes TLS1.1 (HTTPS) and a WebAPI which will terminate the network connection associated with a communications session at the end of the session or after twenty (20) minutes of inactivity.

3.16.13. [SC-12] Cryptographic Establishment & Management

The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with requirements for key generation, distribution, storage, access, and destruction.

Status: Implemented

OmniBallot utilizes strong cryptographic keys using the AWS key store to establish and manage cryptographic keys for required cryptography employed within OmniBallot in accordance with the Democracy Live Security Policy and Procedures.

3.16.14. [SC-13] Cryptographic Protection

The information system implements cryptographic uses and type of cryptography required for each use in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Status: Implemented

OmniBallot implements AWS KMS and AWS Param Store in accordance with the Democracy Live Security Policy.

3.16.15. [SC-15] Collaborative Computing Devices

Democracy Live:

a. Prohibits remote activation of collaborative computing devices with the following exceptions: where remote activation is to be allowed; and
b. Provides an explicit indication of use to users physically present at the devices.

Status: Not Applicable

OmniBallot is a web-based application and does not distinguish between devices.

3.16.16. [SC-17] Public Key Infrastructure Certificates

The organization issues public key certificates under a certificate policy or obtains public key certificates from an approved service provider.

Status: Implemented

Democracy Live obtains public key certificates from Let's Encrypt an approved service provider.

3.16.17. [SC-18] Mobile Code

Democracy Live:

a. Defines acceptable and unacceptable mobile code and mobile code technologies;
b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
c. Authorizes, monitors, and controls the use of mobile code within the information system.

Status: Not Applicable

OmniBallot is a SaaS web-based application available through a browser. No native mobile client code has been developed.

3.16.18. [SC-19] Voice Over Internet Protocol

Democracy Live:

a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and

b. Authorizes, monitors, and controls the use of VoIP within the information system.

Status: Not Applicable

OmniBallot does not implement or use VOIP in the application.

3.16.19. [SC-20] Secure Address Resolution (DNSSEC)

Democracy Live:

a. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and

b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

Status: Planned to be Implemented

Democracy Live implements DNSSEC for the OmniBallot domain (omniballot.us) to protect against hijacking Internet endpoints using man-in-the-middle attacks and DNS spoofing.

3.16.20. [SC-21] Secure Name / Address Resolution Service (Recursive or Caching Resolver)

OmniBallot requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Status: Implemented

OmniBallot utilizes AWS infrastructure which provides a secure address resolution cache resolver.

3.16.21. [SC-22] Architecture and Provisioning for Name / Address Resolution Service

The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

Status: Implemented

OmniBallot relies on AWS for address resolution services. AWS Route 53 provides DNS resolution for the omniballot.us domain and additional subdomains used by the system. AWS provides redundancy to eliminate single points of failure and provides multiple authoritative domain name servers configured for redundancy.

3.16.22. [SC-23] Session Authenticity

The information system protects the authenticity of communications sessions.

Status: Implemented

OmniBallot relies on AWS services to provide session authenticity and the following supporting systems. AWS Cognito provides Authentication through User Pools and a JWT session authorization token. The token is only issued to Authenticated users of the system. Additional session API JWT tokens is required to access any OmniBallot API. API Gateway Authorization service provides security and validation of the API JWT tokens.

3.16.23. [SC-28] Protection of Information at Rest

The information system protects the confidentiality and integrity of information at rest.

Status: Implemented

All data stored within the system is encrypted at rest. All keys will be stored in a secure location and access restricted to personnel on a least privilege policy. Additionally, all PII fields within the data are pre-hashed prior to storage and are not available in the clear.

3.16.24. [SC-39] Process Isolation

The information system maintains a separate execution domain for each executing process.

Status: Implemented

OmniBallot utilizes service provided by the AWS hosting infrastructure. Specific processes are isolated per the architecture and segregation of physical layers in accordance with the system topology. Each application container is segregated at a micro-services level thus maintaining separate execution domains and processes.

3.17. [SI] System and Information Integrity

3.17.1. [SI-01] System and Information Integrity Policy and Procedures

Democracy Live

a. Develops, documents, and disseminates to all relevant personnel:

1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and

b. Reviews and updates the current:
   1. System and information integrity policy semi-annually; and
   2. System and information integrity procedures semi-annually.

Status: Implemented

The Democracy Live Software Development Lifecycle (SDLC) incorporates Continuous Integration and Continuous Deployment CI/CD pipelines for deployment to the production environment for various aspects of the OmniBallot application. System integrity is also managed through both source code peer reviews for new system features and unit testing for some of the components of the system. Additional controls addressing system integrity include service and component versioning, static code analysis, and routine system monitoring for errors or exceptions.

3.17.2. [SI-02] Flaw Remediation

Democracy Live

a. Identifies, reports, and corrects information system flaws;
b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Installs security-relevant software and firmware updates within the defined time period based on severity of the flaw; and
d. Incorporates flaw remediation into the organizational configuration management process.

Status: Implemented

All system flaws will be identified and logged for remediation including potential vulnerabilities resulting from those flaws. Security flaws will be remediated immediately and take precedence over feature development. All security flaws discovered during security assessments will also be given high priority and patches for remediation will be developed, tested, and deployed to the system as quickly as possible.

3.17.3. [SI-02 (2)] Automated Flaw Remediation Status

Democracy Live employs automated mechanisms to continuously monitor systems to determine the state of services with regard to flaw remediation.

Status: Implemented

Democracy Live utilizes AWS CloudWatch for continuous monitoring of system status and to assist with remediation of system flaws when discovered or notified. OmniBallot service metrics are monitored by AWS CloudWatch and notifications are configured for various metrics to notify DevOps of issues when they occur or normal operating thresholds are exceeded.

3.17.4. [SI-03] Malicious Code Protection

Democracy Live

a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
c. Configures malicious code protection mechanisms to:
    1. Perform periodic scans of the information system on a semi-annual basis and real-time scans of files from external sources at endpoints, and network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy; and
    2. Quarantine and remove malicious code, and send alerts to administrators in response to malicious code detection; and
d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Status: Implemented

Malicious code protections are implemented at all system ingress and egress points to detect and eradicate any malicious code that may be introduced into the system. Malicious code protection mechanisms perform scans on all files that are saved or persisted to S3. Any suspected malicious code is quarantined and notification email is sent notifying DevOps and Security personnel of a potential threat.

System entry-points include CloudFront which will implement a Web Application Firewall (WAF) configured to block all incoming traffic except for port 443. All port 80 traffic will be routed to port 443 and secured using TLS1.1. API Gateway traffic will also be subject to the same WAF rules as CloudFront. All files that are uploaded to S3 buckets are subject to anti-virus and malware scans.

3.17.5. [SI-03 (1)] Central Management

Democracy Live centrally manages malicious code protection mechanisms.

Status: Implemented

Malicious code protections are managed centrally within an anti-virus scanning service which evaluates all files uploaded to S3.

3.17.6. [SI-03 (2)] Automatic Updates

OmniBallot automatically updates malicious code protection mechanisms.

Status: Implemented

OmniBallot utilizes a scanning server to monitor files uploaded to be saved to S3. Files are scanned for viruses or malware and are quarantined if a virus or malware is detected. Notification is sent to System Administrators / DevOps for further investigation.

3.17.7. [SI-04] Information System Monitoring

Democracy Live

a. Monitors the information system to detect:
   1. Attacks and indicators of potential attacks in accordance with monitoring objectives; and
   2. Unauthorized local, network, and remote connections;

b. Identifies unauthorized use of the information system through monitoring techniques and methods;

c. Deploys monitoring devices:
   1. Strategically within the information system to collect organization-determined essential information; and
   2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;

d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;

f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and

g. Provides system monitoring information to authorized System Administrators as needed or on a notification or reporting basis.

Status: Implemented

Democracy Live utilizes AWS services Web Application Firewall (WAF) and CloudWatch to monitor and detect attacks and potential threats to identify threat actors scanning the network, attempted injection attacks, network probing, unauthorized network connections, Denial of Service or Distributed Denial of Service (DoS | DDoS) attacks, and unauthorized access to systems. The monitoring systems provide notification alerts to DevOps and Security personnel if the level of threat is deemed to be credible and actionable.

Credible and actionable threats will be elevated to incident response and immediate action will be taken to analyze and neutralize the threat. Appropriate incident response plans and policies will be implemented in the advent of a credible threat.

3.17.8. [SI-04 (2)] Automated Tools for Real-Time Analysis

Democracy Live employs automated tools to support real-time analysis of events.

Status: Implemented

OmniBallot utilizes real-time monitoring and analysis to notify DevOps and Security personnel of active threats detected on the system.

3.17.9. [SI-04 (4)] Inbound and Outbound Communications

OmniBallot monitors inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions.

Status: Implemented

OmniBallot utilizes real-time monitoring of both inbound and outbound traffic analysis to notify DevOps and Security personnel of any unusual or unauthorized activity or conditions on the system.

3.17.10. [SI-04 (5)] System Generated Alerts

OmniBallot alerts authorized personnel when the following indications of compromise or potential compromise occur.

Status: Implemented

OmniBallot utilizes real-time monitoring to notify DevOps and Security personnel of any indications of compromise or potential compromise occurs on the system.

CloudWatch alarms are configured to notify personnel of unauthorized use of the system which include token re-use, accessing API end-points without a token, high number of requests or failed requests to an end-point.

3.17.11. [SI-05] Security Alerts, Advisories, and Directives

Democracy Live

a. Receives information system security alerts, advisories, and directives from external organizations on an ongoing basis;
b. Generates internal security alerts, advisories, and directives as deemed necessary;
c. Disseminates security alerts, advisories, and directives to: authorized personnel within the organization; and
d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

Status: Implemented

Democracy Live Security personnel receive updated security alerts, advisories, and directives from various internal and governmental sources including CISA, DHS, EISSA, MS-ISAC Advisory.

OmniBallot is hosted on AWS infrastructure and buffer overflow attacks are very difficult to be executed against the infrastructure. AWS is responsible for patching all system infrastructure that may be vulnerable including routers and firewalls.
OmniBallot does not implement any low-level code that has direct memory access.

3.18. [CO] Job Schedules SOS Accessible Absentee Voter

SOS Absentee Voter application customization for Michigan.

3.18.1. [CO-01] Job Schedules Appropriately Authorized

Are all job schedules appropriately authorized by IT personnel and/or end users?

Status: Implemented

Scheduled jobs executing on the OmniBallot application are appropriately authorized as the system account is used to execute all scheduled jobs on the system. The system does not allow any unattended execution of actions by any other role other than the system role. No active users are granted access or are assigned to the system role.

3.18.2. [CO-02] Job Schedules Authorized Access

Is access to the job scheduling tool restricted to those individuals requiring access based upon job responsibilities?

Status: Implemented

Access to the job scheduling tool is restricted to authorized personnel in IT. DevOps and developers are the only roles granted access to manage job scheduling and scheduling is managed within the same development lifecycle and process which requires code review and merging with the system production baseline.

3.18.3. [CO-03] Job Schedules Completed Appropriately

Are scheduled jobs completed on a timely basis to support end user requirements and are met/resolved in a timely manner?

Status: Implemented

Job schedules are required to run within the execution context of the Lambda serverless service. Lambda services are designed to run no longer than five minutes. All scheduled jobs are required to complete with the execution context of the hosting Lambda serverless function. Errors or failures are logged in CloudWatch and alarms are configured to notify personnel of any job failures.

3.18.4. [PD-CM1] Version Control

Is source code version control system utilized to ensure that changes between versions are tracked and that access is restricted to the source code?

Status: Implemented

Democracy Live implements version control for all system component code and infrastructure code deployed for OmniBallot. All code versions are tracked and monitored by DevOps and developers. All access to source code is restricted to authorized users with MFA only.

3.18.5. [PD-CM2] Version Control

Are development, testing and production environments segregated for changes to application programs?

Status: Implemented

Democracy Live maintains separate versioning environments to segregate changes for development, testing, and production. Segregated versioning environments allow for deployment of various versions across test and production environments allowing for segregation of test and production environments.

4. Appendix: Document History and Distribution

4.1. Document History

Version	Date	Author	Notes
2.2	2020-08-14	Mark Pace	Updated draft includes additional control families
2.3	2020-09-29	Mark Pace	Update additional control families
2.4	2020-11-05	Mark Pace	Update control status and edit families
2.5	2020-03-30	Mark Pace	Adds MI specific controls CO/PD-CM
2.6	2021-05-23	Mark Pace	Adds S3 description to topology
2.7	2021-11-09	Mark Pace	Update implementation descriptions and review security controls per updated system implementation.

Appendix 5

OmniBallot Security White Paper, Michael Hamilton

Security White Paper:
OMNIBALLOT Balloting Portal

DEMOCRACYLIVE
VOTER INFORMATION TECHNOLOGIES

Author

This review was conducted and this paper authored by Michael Hamilton, an information security practitioner with more than 30 years of experience, notably with roles in government as a Policy Adviser to Washington State, as the Chief Information Security Officer for the City of Seattle, Vice-Chair of the DHS State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC), and formerly in the private sector as the Managing Consultant for VeriSign Global Security.

Appendix 5 - OmniBallot Security White Paper

Executive Summary

This document summarizes the standards of practice met for information security for the OmniBallot electronic ballot return (EBR) product. In addition, it enumerates the series of security assessments, evaluations, and technical testing that has occurred over the preceding year.

As a product that facilitates EBR, OmniBallot has a special responsibility to maintain demonstrable security controls, both to reduce the likelihood of a security incident as well as minimize the impact if and when such an incident occurs. Both the frequency and types of assessments conducted exceed requirements for application testing. The OmniBallot product has undergone frequent testing by a number of independent third parties, including those affiliated with the US Government such as the Department of Homeland Security and Idaho National Laboratory (CISA). While applications are generally tested for security annually, the OmniBallot product has been assessed six times in the preceding 12 months.

Each of the assessments has identified mostly low- and some medium-severity issues, and OmniBallot staff have addressed each of the corrective actions. Note that none of the issues identified appear to be exploitable to modify the outcome of an election. OmniBallot is also compared to published standards of practice published by NIST for UOCAVA voting, and is aligned well with those standards. Additionally, the product has been approved as compliant with NIST 800-53 at the moderate level by the State of Michigan in an additional independent evaluation.

This paper also addresses objections brought up by a member of the academic community in a single research paper. It does not represent a full risk assessment of the OmniBallot product; this review is underway and being conducted by the Center for Information Assurance and Cybersecurity at the University of Washington. Publication of results is scheduled for early Q1 2022.

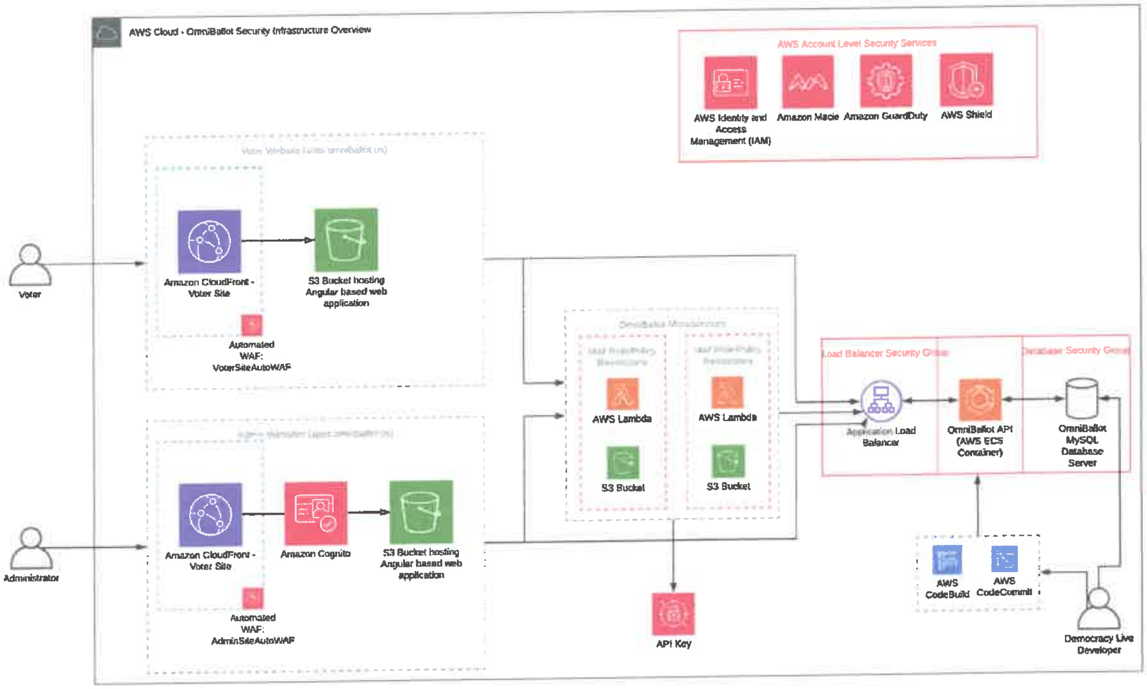
Introduction

OmniBallot is a system for electronic ballot return (EBR), using methods equivalent to the secure transmission documents performed every day. It is not an online voting system. The system is based on foundational principles of simplicity for the voting experience, yet resistant to tampering and fraud. OmniBallot is used today in 24 states and deployed in 2500 jurisdictions to facilitate secure balloting for the disabled and overseas military. The Democracy Live balloting portal has been used in over 2000 elections since 2008 without significant security incident and made available to over 10 million voters over the last decade. Voters in 96 countries have used the solution.

Architecture of the Product

The design principles employed in the architecture of the product are focused on simplicity and security. Simplicity, as few variables need to be controlled. For example, the voter is presented with the minimum amount of information needed to comply with the jurisdiction's requirements on voter identification; as few form fields as are necessary, and with multiple integrity checks between application tiers.

A high-level depiction of the application architecture is depicted below.


AWS Cloud - OmniBallot Security Infrastructure Overview
AWS Account Level Security Services
AWS Identity and Access Management (IAM)
Amazon Macie
Amazon GuardDuty
AWS Shield
Voter
Voter Website (sites.omniballot.us)
Amazon CloudFront - Voter Site
S3 Bucket hosting Angular based web application
Automated WAF: VoterSiteAutoWAF
Administrator
Amazon CloudFront - Voter Site
Amazon Cognito
S3 Bucket hosting Angular based web application
Automated WAF: AdminSiteAutoWAF
OmniBallot Microservices
IAM Role/Policy Restrictions
AWS Lambda
S3 Bucket
IAM Role/Policy Restrictions
AWS Lambda
S3 Bucket
API Key
Load Balancer Security Group
Application Load Balancer
OmniBallot API (AWS ECS Container)
Database Security Group
OmniBallot MySQL Database Server
AWS CodeBuild
AWS CodeCommit
Democracy Live Developer

Authenticated voters are assigned a JWT token used to validate subsequent requests to the system. Prior to submission, the voter's ballot is generated and stored as an immutable object in AWS S3 by using AWS Object Lock. A direct link to the file is then returned to the voter using a temporary signed URL. This allows the voter to view their ballot prior to submission providing assurance selections have been accurately received by the system. The voter accepts the ballot and corresponding documents and then submits their ballot package.

A notification email is triggered notifying elections officials of the voter submission. The submission can only be accessed by logging into the OmniBallot administrative portal using strong credentials and MFA. All interactions within the OmniBallot portal are logged to an audit table and are clearly presented along side the voter submission making all admin activity auditable and transparent to other administrative users. Access controls are in place which prevent a single administrator from accessing voter identifying information and the voter ballot ensuring voter privacy remains protected.

Administrators track the status of the ballot through a process of downloading, reviewing, approval, and completion. Ballots remain immutably stored in S3 for 90 days after the election. After which time they can optionally be removed from the system by an administrator.

Security Assessments of the Product

The security architecture and code base of the OmniBallot product has received multiple independent security assessments by the federal government (DHS/CISA), Idaho National Laboratory, and Synack, a private sector cybersecurity firm. An early review of the product (reference) performed reverse engineering of client-side communication and configuration and simulated the server-side as a "minimal compatible" analog. This paper serves as a response and rebuttal to the points brought up in that paper, as well as other objections which repeat a narrative that has not been informed by exposure to the product, its internals, security and integrity controls, or how a voter may independently verify a completed ballot under the control of the voting jurisdiction.

Corrective actions identified through these examinations – none severe – have been corrected and retesting is in progress. High-level descriptions of the testing are enumerated below.

Solteria Web Application Test

November, 2021

Solteria conducted a web application penetration test of the OmniBallot system. A total of four issues were detected, with 2 rated as low severity and 2 rated as informational. All corrective actions have been applied.

Synack Assessment

OCTOBER 2020 – FEBRUARY 2021

The Synack Crowdsourced Security Testing Platform provides the industry's most comprehensive, continuous penetration test with actionable results. Synack performed a comprehensive assessment with the following components:

Voter-Facing Components

This assessment reviewed the voter facing components of OmniBallot. Researchers reviewed the system for vulnerabilities relating to (but not limited to) voter privacy, ballot delivery and ballot submission. The assessment had the following phases:

- Reconnaissance and discovery
- Penetration testing
- Validation of findings
- Patch validation
- Performance

> *Notes: The assessment determined that a voter's information and ballot selections cannot be modified by a threat actor. One material finding was identified and immediately corrected.*

Administrative Applications

This assessment reviewed the administrative applications in OmniBallot, including a comprehensive vulnerability analysis. These applications are where elections officials manage election information and ballot submissions in the system. Researchers reviewed the system for vulnerabilities relating to (but not limited to) election data integrity, ballot data manipulation, and submitted ballot integrity.

A total of 6 vulnerabilities were identified, five have been addressed.

> *Notes: One vulnerability reported is that an election official or administrator could change the application configuration to remove these fields. This is by design, as each voting jurisdiction has unique requirements for voter identification.*

Server Infrastructure and Security

Phase 1 of this assessment reviewed the OmniBallot technical architecture in the context of security, and from the perspective of an external attacker attempting to gain access. Phase 2 reviewed the infrastructure from an internal perspective as if an attacker gained access to the infrastructure or as a hostile insider.

> *Notes: The only vulnerability identified was determined to be theoretical, and not subject to exploitation.*

ShiftState Security ScoreCard

October 2020

ShiftState conducted a vulnerability scan on the system and reviewed Democracy Live's publicly available information to determine what information might be used by a threat actor to elicit trust. This scan is more of a security hygiene review rather than a penetration test, however the information on public information was used to improve operational security.

CISA / INL Critical Product Evaluation

August 2020

The Department of Homeland Security Cyber Security and Infrastructure Security Agency (CISA), in cooperation with Idaho National Laboratory (INL) provided a *full product evaluation* including a code review, administrative application testing, and voter application testing. The scope of the testing included the application programming interface server, the administrative portal, the Amazon Web Services components, and the voter portal.

Improvements that were implemented after the testing included greater use of server-side input validation and configuration management. All findings have been addressed.

DHS Penetration Test

June 2020

DHS performed an external penetration test of OmniBallot. The test focused on both the administrative and voter facing applications in OmniBallot from the perspective of an external attacker. They were not given credentials to the system.

The examination included intelligence gathering, phishing to attempt password compromise, and an assault on the web-facing application. The assessment team further evaluated Democracy Live against the NIST Cyber Security Framework for additional administrative and technical controls.

A single cross-site scripting flaw was identified, quickly remediated and additional controls implemented to detect phishing attempts. No high-risk findings were identified, and the testing team commented favorably on the speed and efficacy of Democracy Live's process for remediation and re-testing.

RSM Penetration Test

January 2020

RSM performed an external penetration on OmniBallot including both the admin and voter applications. RSM was provided a test environment and detailed information about the system to aid their review and testing.

Alignment with UOCAVA platform best practices and recognized standards

Several papers written by the National Institute of Standards and Technology and the Office of the Director of National Intelligence were reviewed for alignment and applicability. Authoritative guidance included:

- Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters
- Information System Security Best Practices for UOCAVA Supporting Systems
- NIST Activities on UOCAVA Voting
- UOCAVA Electronic Ballot Transmission: Recommendations to Mitigate Security Risks

Recommended practices that are applicable to the development and operation of electronic ballot transmission include:

- Involving state and local election officials in the development of any research on issues and risk mitigations for electronic ballot return options
- forming a collaborative group of experts to conduct a comparative risk analysis of all ballot return methods, electronic and non-electronic; and
- reducing overall cyber risks to elections infrastructure by following the guidance in the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

The recommendations for electronic ballot transmission provide some detail as to security standards that apply to FAX machines used in voting – for example physical and network security, segmentation, etc. Absent from the discussion is the presence of vulnerabilities in the System Signaling 7 (SS7) system that is used globally to route phone calls. It is well known that these vulnerabilities are commonly exploited by nation-states to surveil communications. FAX systems should be deprecated in favor of other, more secure methods and this is discussed in a paper by Jonathan Katz at the University of Maryland.

The OmniBallot operational infrastructure was also aligned with the **NIST 800-53** standard, and was approved as compliant at the moderate level by the State of Michigan. NIST 800-53 is a superset of the controls that are embedded within the NIST Cyber Security Framework. Rather than outcomes to be met, these are specific and prescriptive controls that have been applied, assessed, and approved.

Additional Controls

Many of the controls are not technical but serve to create confidence with voters and election officials. These include:

Ballot Tracking – Ballots are monitored for signs of manipulation at key points and voters are presented with an assurance that the hashes for the submitted and received ballots are identical.

Voter ballot verification – Voters are able to review their completed ballots prior to counting. Note that ballots can be inspected by voters both to verify that the ballot is immutably stored under object locking, and an independent verification that is optionally operated by the voter's local election authority as an independent integrity check.

Integrity Assurance – using the Object Lock write once read many (WORM) facility in AWS, ballot manipulation is only possible under extraordinary conditions. Would require someone at AWS with admin credentials and a significant amount of effort to conduct at scale. Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents. Alarms are investigated and tracked by personnel.

Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited to 30 days by legal or contractual obligations.

Multi-factor authentication (MFA) – the Democracy Live architecture requires MFA for administrative access to the application, as well as to the Office 365 office applications. MFA is also required for customers to access ballots returned through Electronic Ballot Return.

Monthly vulnerability scanning - the application is routinely scanned by the Department of Homeland Security and results provided to Democracy Live.

Inheritance of AWS security controls – AWS uses a shared responsibility model and is demonstrably compliant with several regulatory standards such as FedRamp. There is no absolute location for stored information, object locking creates immutable records that are resistant to tampering.

Incident Response Plan

Democracy Live maintains a detailed incident response plan for aberrational events that may indicate a security issue. In the event of a cyber security incident, Information Security Office (ISO) staff have been trained to expeditiously deal with the incident. ISO staff are trained on a bi-annual basis to recognize anomalies in the systems they regularly utilize, and to report any such anomalies as soon as possible to the Incident Response Manager so the Incident Response Team can be mobilized.

Planned Additional Security Improvements

Anomalous event detection and response – Using Cloudwatch, Cloudtrail and Guard Duty logging and alerting facilities, Democracy Live will be provided with high-fidelity alerting on aberrational events.

These will be reviewed by analysts, who will initiate incident response if necessary. This enhancement to monitoring, detection and response is planned for Q4 2021.

API security monitoring – Democracy Live is evaluating services for continuous API monitoring, the results of which will also be provided to the monitoring team.

Annual auditing – Democracy Live has contracted an auditing firm to perform annual auditing of the security and availability controls of the application architecture and management framework. The result of this examination will be provided to qualified requesters under NDA as a SOC-2 type 2 report.

Continuous vulnerability monitoring – Contracting is underway to engage Synack for continuous human-based monitoring of the code base and public-facing exposure of the OmniBallot application, such that every change made to the application will be immediate exposed to testing prior to promotion to production status.

Blockchain as an integrity control – the hash for ballots would be stored on the chain and verifiable through an independent, objective third party providing the service.

Third-party validation of corrective actions – contracting with SLI (EAC-approved laboratory) for a review of all corrective actions identified through these multiple security examinations.

Academic Objection Handling

In mid-2020 a paper was published as part of an academic work by researchers at MIT and the University of Michigan. In this paper a number of objections were raised regarding the security of the OmniBallot product. Since the time of publication, the Democracy Live team has addressed these objections in order to work collaboratively with the academic community to generate a solution for disabled voters, deployed military, and emergency circumstances that would require a rapidly deployed system for online ballot delivery. In the table below we enumerate those objections along with the Democracy Live response.

Assertion or Finding	Democracy Live Response
OmniBallot is tool for conducting "online voting"	OmniBallot is simply a secure document transmission system.
No independent security testing	See above for the details of security testing that has been performed, and continuous scanning being conducted
No end-to-end verifiability	Addressed by allowing voters to validate the integrity and veracity of their own ballot
Ballots can be misdirected	No different than any other method; low risk. Voter may verify ballot submitted, was ballot received.
Data located in Amazon cloud	This is a security feature, not a vulnerability. Amazon's shared responsibility model is fully implemented.
The application collects PII	Data collected do not meet the definition of PII, unless required by the contracted jurisdiction

Predictable path names for statewide deployments	Not possible to abuse this to effect voter fraud; PIN or other credentialing is deployed to verify voter authenticity.
Unauthorized access to the voter's device by someone other than the voter	Addressed through signature matching and/or other forms of voter credentialing. No different than postal absentee ballots.
Client-side malware	Would require extensive resources and planning to conduct at scale; low risk. Voters can verify the ballot, by using any Web-connected device.
Hostile insider in the Democracy Live or service provider (AWS) infrastructure	Manipulation would be detected through monitoring for aberrational behavior, alerts are delivered in real-time, monitoring logs are immutable, and preventive administrative controls are robust.
Adversary with control over 3rd-party code	Routine code reviews for third-party components such as encryption libraries. Voters can confirm ballot submitted was ballot received.

Discussion

The primary use case of the OmniBallot application is for ballot delivery to voters with disabilities deployed military and overseas voters. Given that the Covid-19 pandemic and associated lockdowns occurred well in advance of the 2020 election, states had time to develop and adopt previously unused methods of voting, relying heavily on mail-in voting and distributed drop boxes. Had the pandemic occurred in August, there would have been insufficient time to make these changes. Similarly, given the increase in natural disasters or other unforeseen events, there may be a need to rapidly deploy a ballot transmission system that is not reliant on current facilities and procedures, which may not be available. For these reasons, the OmniBallot system should be considered as a viable fallback in times of emergency, or to ensure access to the balloting process to voters who would otherwise be unable to vote.

NIST publication NISTIR 7770 describes the security considerations for remote electronic UOCAVA voting, which concluded that Internet voting systems cannot be audited to provide the same confidence as audits of polling place systems, using an argument that malware on personal computers poses a serious threat. Note that OmniBallot is not responsible for vote counting, but simply electronic ballot return (EBR), which is much more analogous to DocuSign than a "online voting". Further, while malware on personal computers could indeed cause issues, the ability to perform a coordinated attack ***at scale*** to change the outcome of an election is unlikely if not impossible. Additionally, voters using the ballot verification tool can confirm their ballot was accurately received at the election's office. The paper also concludes that the lack of a public infrastructure for secure voter authentication is problematic, and while this condition continues to persist, empirical results from actual elections do not support the assertion that the use of jurisdictionally defined voter identification information is vulnerable to abuse, given the use of voter validation policies.

Author

This review was conducted and this paper authored by Michael Hamilton, an information security practitioner with more than 30 years of experience, notably with roles in government as a Policy Adviser to Washington State, as the Chief Information Security Officer for the City of Seattle, Vice-Chair of the DHS State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC), and formerly in the private sector as the Managing Consultant for VeriSign Global Security.

References

NISTIR 7682 - Information System Security Best Practices for UOCAVA Supporting Systems

https://www.govinfo.gov/content/pkg/GOVPUB-C13-de16c1db691d2e7bb917c16e1d316843/pdf/GOVPUB-C13-de16c1db691d2e7bb917c16e1d316843.pdf

NISTIR 7700 – Security Considerations for Remote Electronic UOCAVA Voting

https://www.nist.gov/system/files/documents/itl/vote/NISTIR-7700-feb2011.pdf

NISTIR 7711 – Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters

Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters (nist.gov)

A Threat Analysis on UOCAVA Voting Systems

https://www.nist.gov/system/files/documents/itl/vote/uocava-threatanalysis-final.pdf

UOCAVA Electronic Ballot Transmission: Recommendations to Mitigate Security Risks

uocava_ballot_return_technical_recommendations_3ULmxP6.pdf (turnout.rocks)

Electronic Ballot Return - Overview

http://www.cs.umd.edu/~jkatz/electronic-ballot-return.pdf

NIST Activities on UOCAVA Voting

NIST Activities on UOCAVA Voting | NIST

Electronic Ballot Return for Military and Overseas Voters: Considerations for Achieving Balance Between Security and Ballot Access

CSG_Electronic-Ballot-Return-for-Military-and-Overseas-Voters_Considerations-for-Achieving-Balance-Between-Security-and-Ballot-Access.pdf