

DENNIS RICHARDSON  
SECRETARY OF STATE

LESLIE CUMMINGS, PhD  
DEPUTY SECRETARY OF STATE



STEPHEN N. TROUT  
DIRECTOR

255 CAPITOL STREET NE, SUITE 501  
SALEM, OREGON 97310-0722  
(503) 986-1518

## Oregon HAVA Grant Funding Utilization

The Federal grant will allow Oregon to implement Department of Homeland Security (DHS) recommendations for additional security and improvements for the 2018 and 2020 elections. The Secretary of State will use \$3,250,453 of these federal funds in this budget year in the following seven areas:

### 1. Essential Election Systems Availability \$2,393,637

The Secretary of State Elections Division provides the application used to support online voter registration, the Oregon Motor Voter (OMV) process, campaign finance reporting and transparency, ballot tracking, a ballot drop box locator tool, and candidate and voters' pamphlet statement filing. It is also how military and overseas voters access their electronic ballots, update their current location, and access the digital voters' pamphlet. Popularly known as ORESTAR (Oregon Elections System for Tracking and Reporting), these systems are operated and maintained in the Secretary of State data center. Improvements are needed to ensure continued operation in the event of attempted election interference, power outage, hardware failure, or other major disruption affecting the Capitol campus. This will require raising the elections systems to industry standards for survivability by adding a separate suite of elections-related computer servers and associated equipment in Salem (prior to 2018 general election), as well as a backup suite of equipment to be located in a secondary location (spring 2019).

### 2. Secured Access for State and Local Election Systems \$100,000

Oregon relies on county election offices to run many election functions. A security breach at any one county election office could compromise key election systems statewide. Cybersecurity can be enhanced through the implementation of multi-factor authentication.

Current election systems require a user name and password for access. Multi-factor authentication adds an extra step to enhance security and typically requires a user to present something they *know* (a username and password) and something they *have* (such as a one-time code received via text message or a physical device that provides a constantly changing code) in order to access an account. Only by having *both* of these things will the user confirm their identity and be able to gain access to the system.

Cybercriminals who obtain a user's password cannot access the system because they do not have the code needed for access. In the same way, a cybercriminal who steals the device with the changing code must also know the user's password for access. Multi-factor authentication is one of the strongest defenses against security breaches, and it is recognized as a best practice in elections.

Multi-factor authentication is needed because passwords are increasingly insecure. It would be implemented for county staff who access elections systems, as well as state elections and IT staff who also interact with the same systems.

### 3. Application Vulnerability Scanning \$50,000

The Secretary of State Security staff is currently using a web vulnerability scanning tool for Secretary of State software applications. However, the functionality of the tool is limited. Additional functionality, including web vulnerability scanning and software code analysis is needed. This would greatly enhance the identification and remediation of software vulnerabilities, both during software development and ongoing software application operations and maintenance. Such enhancements will mitigate cyber security exploits by malicious actors.

### 4. Increased IT Security Capacity \$272,132

Due to the increased workload and the need to address security deficiencies identified in the federal DHS Cyber Resiliency Review, two permanent IT Security positions are needed. These security professionals will implement, maintain, and monitor the security enhancements listed above, as well as the existing security protections for elections systems on an ongoing basis. They will also be responsible for cybersecurity incident response, cybersecurity training, and IT risk and vulnerability management.

### 5. Increased Voter Registry Efficiency \$78,684

Integrating Electronic Registration Information Center (ERIC) information automatically into OCVR, as is done currently with the National Change of Address information, will provide for a more accurate, secure and timely voter registration database by allowing information from ERIC to be electronically submitted to county election officials for their review and approval as compared with the current manual entry process. This will provide for more accurate records by removing data entry errors, allow for more rapid updates of information in the voter file, and reduce some costs of ballot mailings.

### 6. Statewide Ballot Tracking \$220,000

In order to provide voters with information on the status of their ballot and help to build trust and confidence in our election systems, the Elections Division will build a ballot tracking feature into OCVR so that voters can subscribe to updates of where their ballot is in the process from mailing outbound to received and accepted at the county elections office. This tool would be fully integrated with intelligent mail barcodes in order to see the ballot move through the entire process. This tool would be available for all

voters in the state. Voters can track their ballot on the Secretary of State's website, and/or their county election site. Voters can also subscribe to receive text message or email updates to track their ballot. There would also be a widget available on our website to allow voters to track their ballot without having to provide us phone numbers or emails for those with privacy concerns.

#### 7. Application Interface Projects (API) \$136,000

Create an API (application program interface) between the ORESTAR Campaign Finance database and Data.gov to increase transparency without risking failure to the application. This would provide public access to campaign finance reports and expand capacity and public visibility. Currently individuals wanting large amounts of campaign finance data have to scrape our website which is a security issue and has also caused the system to crash in the past. This has caused us to have to place limits on the amount of data that can be accessed. This API would allow us to provide all data in a more secure way and in a way that would not threaten our application. Through an API we would also be able to provide publicly releasable voter registration and ballot disposition data extract to Data.gov (restricted access).

The remaining \$2,112,528 will be allocated and spent during the 2019-21 biennium which begins July 1, 2019, and potentially the 2021-23 biennium. That spending must be approved by the legislature and we will be proposing a spending plan for the remainder of the funds later this year.