EIS Communiqué

Sharing Election Infrastructure News and Resources

July 11, 2018 Volume 1, Issue 12

Elections Today: Whole New Ballgame

Orange County, California's **Neal Kelley**[1] knows a thing or two about elections. Since May 2004, Kelley has overseen and managed elections operations in Orange County, the fifth largest voting jurisdiction in the country, and was appointed **Registrar of Voters** in April 2006. His years of experience, however, in no way suggests he views elections management as a continual repetition of the past.

"**This is a whole new ballgame for us today**," said Kelley, in an interview with the EIS Communiqué, after a thankfully uneventful and smooth June 5 primary election. "In 2015, we knew about cyber issues, but we weren't talking about them like we are today."

Orange County not only talks cybersecurity --- it ***does*** cybersecurity --- a lot of it, starting with preparedness.

In April, Orange County published the 2018 Election Security Playbook (Security Playbook), a 27-page easy-to-read guide to anticipating, mitigating, and responding to cybersecurity threats, with a healthy dose of physical security measures to undertake for voter and vote integrity safety (see following story for more information).

[1] Neal Kelley is an appointed member and immediate past chair of the U.S. Election Assistance Commission (EAC) Board of Advisors, a member of the EAC Voting Systems Standards Board and the National Institute of Standards and Technology Voting Technical Guidelines Development Committee. He is also a member of the Election Infrastructure Subsector Government Coordinating Council.

Development of the Security Playbook began in January and was a collaborative effort among and between Kelley's internal teams, county information technology experts, the Sherriff's Office, and the OC Intelligence Assessment Center, a Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI) fusion center partnership.

Kelley considers the investment of time and effort well worth it. "We really wanted to get the playbook right and to produce a meaningful product for the public and for ourselves – that's why it took four to five months to produce," Kelley said. His office produced another more detailed cybersecurity guide for internal use only.

Message for Orange County, CA Voters: "We Take It Seriously"

The time and effort expended on the Security Playbook is just one measure of the diligence and determination of the Registrar of Voters office to get and keep things right for voters.

"I'd like to tell voters that we take the concept of election security very, very, seriously. We take the concept of election security to be as important as the tally of the vote. We have the processes in place to minimize threats and risks. For the last election (June 5th primary) we had our defenses up and double the security," he said

One indication of just how seriously OC takes election security is its reliance on the best practices and guidance in its Security Playbook. OC lives and breathes it, turning it into a way of doing business.

"We are religious ***and*** zealous in adhering to the playbook. It has morphed into our everyday operations," Kelley said, when asked how often the Security Playbook is practiced.

Ongoing training for staff is a must, and staff are confronted with OC-supplied phishing campaigns to maintain alertness.

The Security Playbook is a good example of the value that Kelley puts on collaboration and partnerships. Partnerships at all levels of government are integral to cybersecurity.

Cyber Partners: A Needed Force Multiplier

For the OC Registrar, essential partners are found at both the local and federal government levels.

"Local partners are super important –- from the Office of the District Attorney to the Sheriff's Department. The District Attorney's Office has expanded capabilities and is very responsive – they're onsite and in the field with us and can react to any issue regarding vote integrity. We've expanded our partnerships with the local Sheriff's office for increased physical protection for voters and votes," he said.

Significant federal partners for Orange County include the FBI for threat information and the National Institute of Standards and Technology, which has been a resource in advising on the use of its Cybersecurity Framework, which is discussed in the Security Playbook.

Another significant federal partner is the U.S. Election Assistance Commission (EAC). "The EAC is everywhere in the elections community," he noted.

"On the federal side, DHS has been super responsive and has provided tons of resources. DHS helped the MS-ISAC install an Albert sensor[2] two days before our [primary] election. I can't say enough about DHS," Kelley said.

"I cannot say enough about DHS. Since the beginning, DHS has been hopping over themselves to offer resources and assistance. Regional DHS folks [such as cybersecurity advisors] have been over the top responsive and are providing information for a statewide conference in July," Kelley said.

Asked if he had any complaints about DHS, Kelley demurred, saying he was not the best person to ask as "everything and everyone I've interacted with has gone very well."

If he had a complaint, it would be more of a concern. "My one complaint is how long can they keep the pace up? Do they have the bandwidth for all the available assessments," he asked.

Message for Election Community Colleagues: Use What DHS Offers

Kelley does have a concern about DHS services and products not used by the elections community.

"What bothers me is that with all DHS has to offer, not all [elections officials] are making use of what DHS offers. What I would say to other elections officials about working with DHS is, **'if you're not working with DHS now, you better be.' Take it seriously and take advantage of what DHS offers,**" Kelley said.

"Out of about 9,000 [elections communities], only about 500 have taken any DHS services. Without question, I would recommend DHS assessments --- we've taken them," he said, noting that OC finds the cyber hygiene assessment and subsequent reports very helpful. He encouraged elections colleagues not to get discouraged by any wait as the wait is worth it.

Future Cyber Needs: Funding, Collaboration, Partnerships

[2] An Albert sensor is an intrusion detection sensor placed on an organization's network which collects network data and sends it to the Multi-State Information Sharing and Analysis Center (MS-ISAC) for analysis under its fully managed network monitoring service. See MS-ISAC Services eBook

When asked what message(s) he had for partners, the response was immediate: "More funding! We continue to beg for more funds – the $380 million[3] [federal funding for election security] is fantastic, but this is an ongoing challenge for us all and funding is needed," he said.

Another message Kelley has for partners is to keep on keeping on.

"I'd like to say, 'please don't lose sight of how important this [election security] is. This is such a good start – I don't want us to lose momentum," he said.

Kelley also hopes for even closer collaboration with DHS in the future.

"I'd love to have DHS be part of our operational planning --- to include them in some way in our security planning. I'd like to go beyond the menu of services DHS offers and work with them including during the last 90 days before an election. There would still be a lot of value as various failure points can occur during that time," he said.

For Orange County, there are more than 90 days to its next election --- the 2018 mid-term election is November 6.

Orange County (CA) Issues Cyber-Centric Election Security Playbook

Demonstrating just how seriously it takes cybersecurity concerns in the wake of the 2016 elections, California's Orange County Registrar of Voters has published an election security guide, serving up a soup-to-nuts approach to cyber- and physical security that elections officials everywhere can adapt for use.

Released in April, the purpose of the 2018 Election Security Playbook (Security Playbook) is to serve as a handbook to prepare for, mitigate, and respond to both cyber- and physical security threats. The Playbook also serves as a cybersecurity primer basic enough for cyber neophytes yet substantive for network administrators --- defining terms such as "air-gapped systems" and providing examples of administrative, technical, and physical security controls, potential threats and exploits specific to elections and discussing mitigation strategies.

[3] The $380 million refers to the total amount of grant money available to improve the administration of elections for Federal office, including to enhance technology and make certain election security improvements for election security under the Help America Vote Act. For more information see https://www.eac.gov/2018-hava-election-security-funds.

While the Security Playbook offers insight and instruction, it notes more work is going on than is made public. “There are additional security measures in place that are not shared with the public to ensure that these additional mitigation efforts are not compromised.

One effort behind the scenes is the weekly cyber hygiene assessment reports Orange County’s Registrar of Voters office receives from the National Cybersecurity and Communications Integration Center in the DHS National Protection and Programs Directorate (NPPD). The report includes vulnerability scan results, new vulnerabilities detected and mitigated vulnerabilities on Interne- facing hosts. For more information on NPPD cyber hygiene assessments, visit Cyber Hygiene Assessments.

Election Security Web Page Up!

Remember –- DHS’s National Protection and Programs Directorate (NPPD) has created a webpage focused on elections infrastructure security-related issues now available on the DHS website. NPPD created the webpage to more effectively share elections infrastructure information and pertinent elections community documents. Content includes overviews on NPPD cyber services available at no cost to the state and local elections community and information on the electoral process, coordinating councils, and elections security. New information is added frequently. Visit: https://www.dhs.gov/topic/election-security .

EIS Background

DHS designated election infrastructure as critical infrastructure January 6, 2017. The designation created the Election Infrastructure Subsector under the Government Facilities sector, with DHS as its Sector Specific Agency (SSA). The designation set several actions in motion, such as the formation of coordinating councils, coordinated federal support, and the availability of services and tools for the Election Infrastructure Subsector. For more information on Communiqué topics, please contact the EISSA at EISSA@hq.dhs.gov.

Purpose

The EIS Communiqué series periodically informs subscribers of the numerous DHS services available to the EI community. DHS provides services on a no-cost, voluntary basis to state and local election officials.

EIS Communiqués highlight various services and tools, such as assessments, threat information-sharing programs, network protection, best practices, incident response, and developments at the federal level, along with related issues of interest to the EI community.

Thank you,

Election Infrastructure SSA

We want to hear from you! Send us your comments on how we may better serve you as well as questions, feedback, and ideas for future Communiqué topics at EISSA@hq.dhs.gov.

Subscriber Services

Click here to subscribe Click here to unsubscribe