King County Elections
PNWER– Cyber Security
July 23, 2018

Julie Wise
Director of King County Elections

- Elected 2015 to serve a 4 year term 2016-2019

- Prior to election, served as the Deputy Director

- Worked at King County Elections since 2000

- Washington State Certified Election Administrator

- Nationally Certified Election Registration Administrator

King County vote!

King County

- 1.3 million voters

- 191 jurisdictions

- Vote by Mail, 2009

- Largest county in the nation to vote entirely by mail

- 13th largest county in the country

The vision:
To be the leader in providing inclusive elections.
The mission:
We conduct fair, open and accurate elections.

King County
vote!

Safe and Secure

To fulfill our vision and mission we focus on:

- Physical security

- System security

We are working across King County departments and with national and state agencies to ensure our election systems are secure and safe across all platforms.

Election Systems: designated critical infrastructure

- January 2017 Secretary of Homeland Security designated election systems as critical infrastructure under existing Government Facilities Sector

- Established by the Patriot Act and given to "systems and assets, whether physical or virtual, so vital to the US that the incapacity or destruction of such systems and assets would have debilitating impact on security..."

Physical Security

22 security cameras monitored 24/7

Badge only access to ballot processing areas

6 webcams live stream when ballot processing begins

Designed specifically for elections; Consultant worked with casinos

Ballot storage and tabulation areas also require biometric and badge

Physical Security: Department of Homeland Security

- First Elections infrastructure review in the nation
  - U.S. Department of Homeland Security
  - November 30, 2017
- Focus:
  - Physical security of building
  - Security of materials

Physical Security: Department of Homeland Security

- Infrastructure Survey Tool (IST)
  - Applied to facilities, complexes, buffer areas and systems
  - Guides the national effort to manage risk to the Nation's critical infrastructure
- Protective Security Advisor (PSA)
  - Identify and document critical infrastructure
  - Evaluate and facilitate information sharing
- Significant Asset and Areas (SAAs)

# Physical Security: Department of Homeland Security

- Security Management Profile: Our office's security management program (both physical and cyber considerations) is exceptionally well-designed and implemented

- Electronic Security Systems: The placement of intrusion detection sensors perfectly complements other design features to ensure 100 percent coverage of critical locations on the second floor of the facility.

Physical Security: Department of Homeland Security

- Due to the confidential nature of the assessment, high-level summary of options for consideration based on potential vulnerabilities:
  - Use materials/messaging to provide direction for detecting and reporting suspicious activity using the "If you see something say something" public awareness campaign.
  - Coordinate security plan with local law enforcement and exercise it annually.
  - Review the business continuity plan and exercise it annually.
  - Minor improvements to parking lot area such as barriers to mitigate high-speed avenues of approach and improved lighting.

- King County Elections will be reviewing each of the options for consideration and putting together a plan to address the items that provide the desired enhancements in light of the facility's current security and resilience posture, anticipated growth or organizational changes, and budgetary outlook
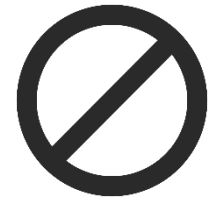
Cyber Security
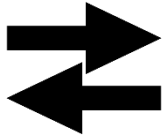
Database is completely separate from the tabulation system

Tabulation system is on an entirely closed network/air-gaped network

Separate systems for maximum security

To tamper with them, have to physically access space

Security layers: Secure access, dual authentication, 22 cameras and webcams

Cyber Security: State Auditor

- First Elections focused cyber security audit in Washington
  - Washington State Auditor
  - Began in late 2017
- Three phases:

  I. Application and network penetration testing

  II. Critical security controls assessments

  III. Critical security controls testing of processes

Cyber Security: State Auditor

- Progress:
  - Phases 1 and 2 complete, 3 completed July 31
  - Phase 1 report received
  - Final reports received in 2018 third quarter
- Results:
  - Work with KCIT to collaboratively review overall risk assessment and response to findings
    - *Begin in late July and continue through 2018*
  - Elections IT implemented remediation for findings, ensure hardware is regularly scanned
  - Anticipate Remediation Plan / Response completed by 12/31/18 with Work Plan for 2019

Additional measures

- Protection from hackers:

  - Tabulation system is closed network

  - Can only tamper through physical access

  - Physical access is secure

- Regular testing:

  - Per state law, do a logic and accuracy test before and during each election to ensure tabulating properly

  - This test is open to the public

Additional measures

- Security precautions:
  - Regularly work with KCIT
  - Regularly work with Secretary of State's Office to proactively address security threats
- Security assessments:
  - Dept. of Homeland Security analysis completed June 2018
  - SOS Office reviews every 5 years, includes security
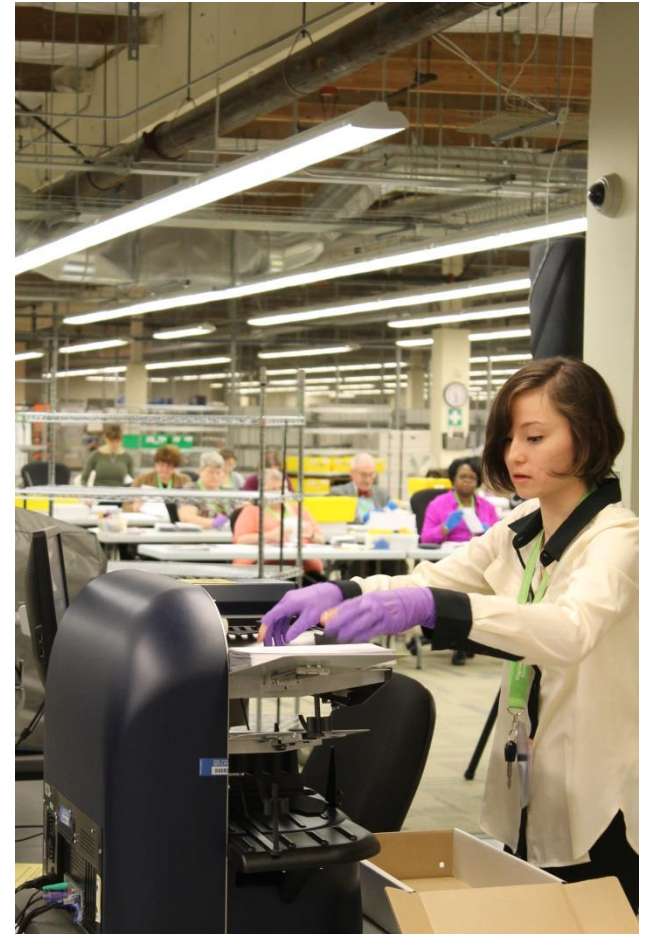
Thank you,

Julie Wise, King County Director of Elections
206.477.4140
Julie.Wise@kingcounty.gov

Follow us @KCElections

Follow our blog www.kcelections.com

Follow Julie Wise @KCE_Director