Denver Elections – Cybersecurity

Discussion with Elections Assistance Commission

October 4, 2017
Before Election Day

• Validation of PC configuration
  - Antivirus
  - Hardening (Group Policy Object – GPO, e.g., screen lock)
  - Patch level
• Penetration Test
• Network Hardware Configuration
• WiFi Scanning
• Training
• AUP Attestation – Acceptable Use Policy
• Software Change Freeze (before and after election)
Election Night Monitoring

- Denver Web Elections Operations Center (WebEOC)
- Denver Security Operations Center (SOC)
- Denver Emergency Operations Center (EOC) & Denver Police Department (DPD)
- Denver Threat & Vulnerability Monitoring
- Jefferson County
- Colorado Secretary of State
- Colorado Division of Homeland Security
- Colorado Office of Information Technology (OIT)
- Federal Bureau of Investigations (FBI)
- Federal Department of Homeland Security (DHS)
- Multi-State Information Sharing and Analysis Center (MS-ISAC)
- Indirect

DIAGRAM: Connecting all departments involved in election night monitoring.
Elections Network Segmentation

*SCORE: Statewide Colorado Registration and Election system

Michael’s Chart
Monitoring Technologies

- **HSIN Portal** - Homeland Security Information Network
  - Like a WebEx with Screen Sharing, but approved for govt use
- **SCORE**: Statewide Colorado Registration and Election system – statewide network performance monitoring
- **SolarWinds & OP5** – Network node status (Denver)
- **QRadar** - Security Event & Information Management (SEIM) – log monitoring (Denver)
- **WebEOC** - Web Elections Operations Center – Voter Service Center monitoring (Denver)
- **ELK** - Elasticsearch, Logstash, and Kibana
- **Geofeedia** – location based analytics platform – didn’t work out
Monitoring Technologies – continued

- Bridge line
- Listserv
- List of names and cell numbers
- SMS Text Messaging
- Face to Face Status
Homeland Security HSIN Portal

HSIN – Homeland Security Information Network
Election Day

Denver Mayor
Michael Hancock