PA Department of State Security Strategy

• Replacement of paperless voting systems.
  • 100% of our allotted election security grant funding is committed to this.

• Voter registration database is delivered through a secure private network managed by the Commonwealth.

• We benefit from an enterprise-wide, multi-layered security strategy:
  ✓ Barriers and monitoring at the perimeter.
  ✓ Customized barriers and monitoring inside the perimeter.
  ✓ Strategic encryption of data in transit and data at rest.
  ✓ Event logging of data in use.
  ✓ Daily backups.
  ✓ Well-defined incident management and communications plans.
Security Posture Evolution

• Threats were not transitory prior to 2016.
• Persistent threats have resulted in a continuously-evolving security posture.
• Attitudes about election security among stakeholders have changed:
  • Increased focus on information sharing and communication.
    o Election Security Stakeholders Workgroup brings together state and county election directors and IT directors.
    o The Governor’s Interagency Election Preparedness and Security Workgroup.
  • Greater sensitivity to public perception and loss of confidence.
  • Enhanced cybersecurity and physical security awareness among election staff.
  • Greater willingness to engage third parties to assess vulnerabilities.
  • Practicing the universal remedy for getting and staying in shape – MORE EXERCISE.
What We Can Do Today

• Facilitating additional training opportunities for every person involved in the business process.
• Make sure password management principles and policies are consistent throughout the election ecosystem.
• Improved data analytics.
• Leverage federal and state partnerships to assist counties
  • Phishing campaigns.
  • Tabletop exercises.
  • Risk and vulnerability assessments.
The Future State

• Replacement of current voter registration database with a new system that has security best practices baked into the application(s).

• Systematic enforcement of uniform baseline security awareness training for all users at all levels.

• Role-based security training as a prerequisite for any level of privileged access.

• Closer monitoring of user accounts:
  • Continuously monitoring users’ access and activity.
  • Stricter thresholds and controls for privileged users.
  • Empowering managers to audit their users’ activity.