



# Introduction to Information Technology for Election Officials



Richmond, Virginia

June 30, 2016



# Instructors

**Merle S. King**

Center for Election Systems  
Kennesaw State University

**Brian J. Hancock**

Testing and Certification  
U.S. Election Assistance  
Commission

**Matt Masterson**

Commissioner  
U.S. Election Assistance  
Commission

# Course Topics

- Introduction to IT and Systems
- Benchmarking
- Election Technology
- Security
- Procuring IT
- The Future

### In modern elections, what are the Core Competencies of an Election Administrator?

- Auditor – must be able to create and implement audit programs to identify and correct errors to improve efficiency and effectiveness of operations
- Trainer – must be able to develop and implement training programs for poll workers and voters
- Information Technology Manager – managing large numbers of complex information systems, vendors and technical staff

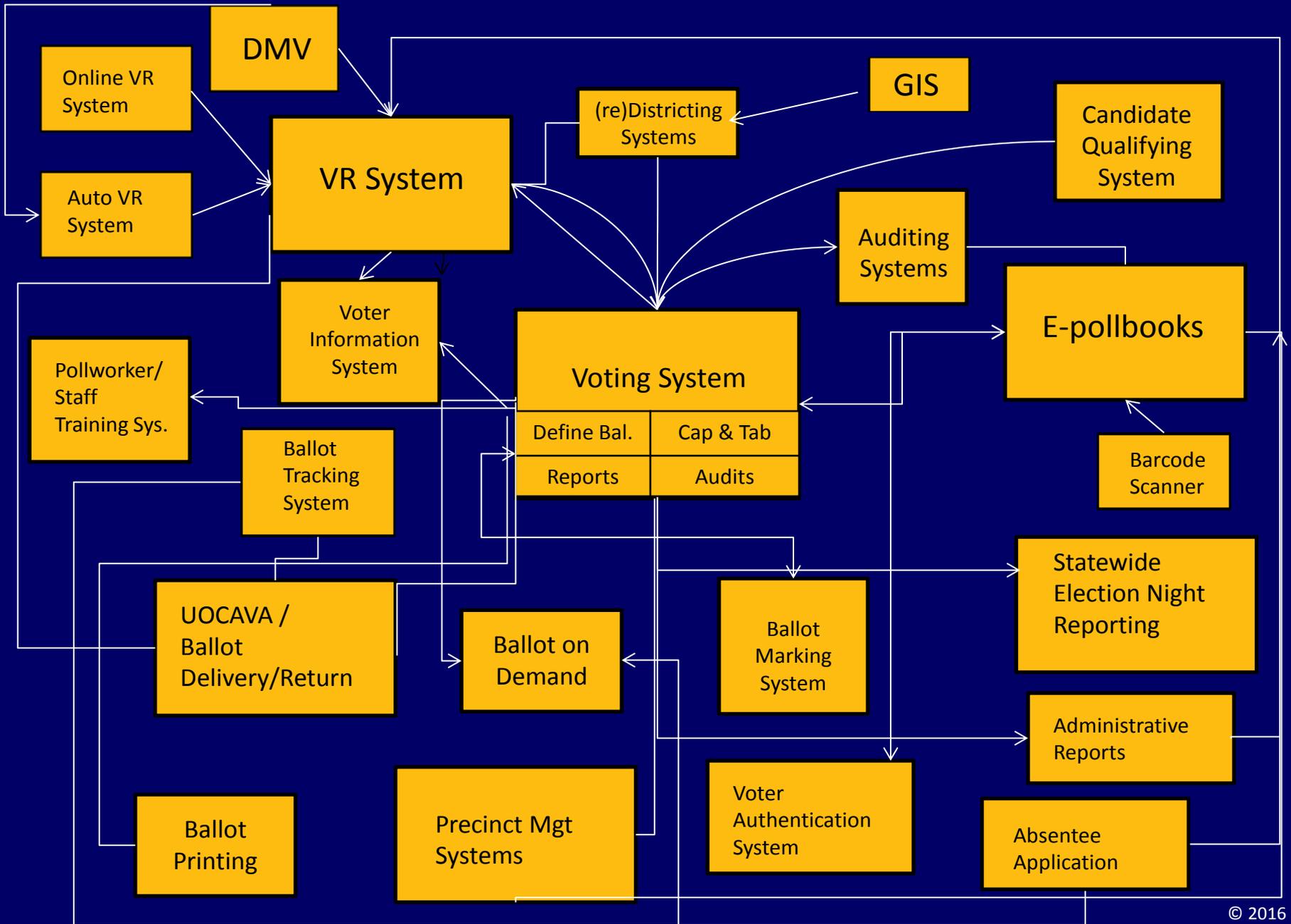
### Core Competencies (cont.)

- Lawyer – must know election law and how it is implemented within the jurisdiction
- HR Specialist – must know how to recruit, train, compensate and evaluate election workers
- Communication Officer – must know how to compose precise and persuasive communications across a spectrum of platforms
- Accountant – must know how to create operating budgets and make less, go further

## Introduction to Information Technology and Information Systems

- The typical county election official may be managing more technology than the county's IT department:
  - DREs
  - Scanners
  - EPBs
  - Servers
  - Desktops
  - Laptops
  - Tablets
  - Printers
  - Vendors
  - Phone systems
  - Copiers
  - Fax machines
  - Smart phones
  - GIS interfaces
  - VR system clients
  - Voter services
  - Software versions
  - Contracts
- Virtually every aspect of the election officials job is connected to IT.
- What part of an election officials job does not involve IT?

# Interaction of Voting and Election Systems





## Introduction to Information Technology and Information Systems

- Every profession, including EA, expects and requires a measure of professionalism from its members
- Professionalism includes attainment of certain competencies, certification of attainment, an expectation of ethical behavior, commitment to enhancing the profession and its body of knowledge, and...
- Demonstration of the **Attitudes, Knowledge and Skills**, required of the profession...

## **Attitudes**

- Flexibility – ability to accommodate change with little notice – adapt and overcome
- Resilience – not easily daunted by criticism or attacks
- Determination – see the task through to the end, in spite of resource and support issues
- Stick-to-it-iveness – never, ever, give up
- Willingness to listen and incorporate multiple points of view into decision making process
- Confidence and self-assurance
- Deliberate in decision making – decisions require follow through and have consequences

### **Attitudes (cont.)**

- Election administration is a profession, and as such, is subject to appropriate public expectations of performance, competencies, transparency and accountability
- Election administration requires the adherence to ethical behavior that enhances the credibility and transparency of election outcomes
- Elections offices are results driven organizations
- Voters are “customers” and are entitled to customer service expectations
- **Election officials are IT managers and all that entails**

### **Knowledge (IT)**

- Sufficient knowledge of IT and supporting processes to make informed decisions
- Knowledge of fundamental IT terminology
- Knowledge of how IT supports Election Administration
- Knowledge of dependencies on IT within the scope of the elections office
- Knowledge of election technologies, both within and external to the election jurisdiction

### **Skills (IT)**

- Able to recruit, select, and supervise staff with IT skills
- Able to evaluate IT alternatives and justify selection
- Able to evaluate risks and mitigation strategies associated with IT
- Able to integrate IT planning into overall election planning
- Able to communicate effectively with IT vendors and participate in decision making processes

### **Skills (IT) (cont.)**

- Able to review IT RFPs and contracts, ask meaningful questions and make informed decisions
- Able to evaluate IT audit plans and understand the significance of IT audit reports
- Able to use and/or direct the use of IT within the scope of the elections office
- Able to communicate the role of IT within the elections office to county IT staff, supervisory boards, and the media

## Concepts

- **Systems** are ubiquitous
- A system is a collection of unified components that transform inputs into outputs
- Systems may consist of subsystems
- Systems have controls that monitor the inputs and (especially) outputs to determine correctness of operation
- Consider the following systems:
  - Voter registration
  - Voting
  - Election night reporting
- How is a voting system, different from a voting machine?

# Benchmarking

“It is a capital mistake to theorize before one has data.”

- Sir Arthur Conan Doyle

# A means of improving performance by:

- Measuring what you are doing
- Comparing results with
  - Other jurisdictions,
  - Professional standards, and/or
  - Yourself over time
- Using the information to improve performance

# And demonstrating performance to:

- Budget authorities
- Political parties
- Advocates
- Policy makers
  - State CEOs
  - Legislators
  - Congress

# Demonstrating what?

- Effectiveness, we are doing the right things
- Efficiency, we are doing things right (for the least expenditure of resources)
- Impact of changes in policies, procedures, resources, etc.

# Effectiveness

- Contra Costa County, CA, was concerned with the rejection rate for absentee ballots
- Measured absentee ballot rejections
- Analyzed causes
- Put flyer explaining causes on colored paper in instructions June 98
- Refined flyer afterwards

# Efficiency

- States implementing online VR compared the cost of online voter registration with paper registration and found an average savings of \$.80- \$1.50 per registration.
- Calculated savings in one large county were:
  - \$206,779 in 2006
  - \$370,323 in 2008
- Ohio savings of over \$3 million.

# Impact

- Sacramento County faced a cut of 46% in its 2009-2010 general fund budget.
- With detailed financial records county was able to project budget impacts such as:
  - Cut of about 50% in number of polls
  - Elimination of bi-lingual election material resulting in non-compliance with VRA
  - Not mailing sample ballot pamphlets to each voter
- Proposed cuts were from 46% to 7%.

# How can it help with budgets?

- Improve efficiency, learn how to do the same thing with less money
- Demonstrate efficiency, show budget authorities that you are already being economical
- Demonstrate impact, show budget authorities the results of cuts
  - Must have credible documentation over time.

# Election Technology

"Any sufficiently advanced technology is indistinguishable from magic."

- Arthur C. Clarke

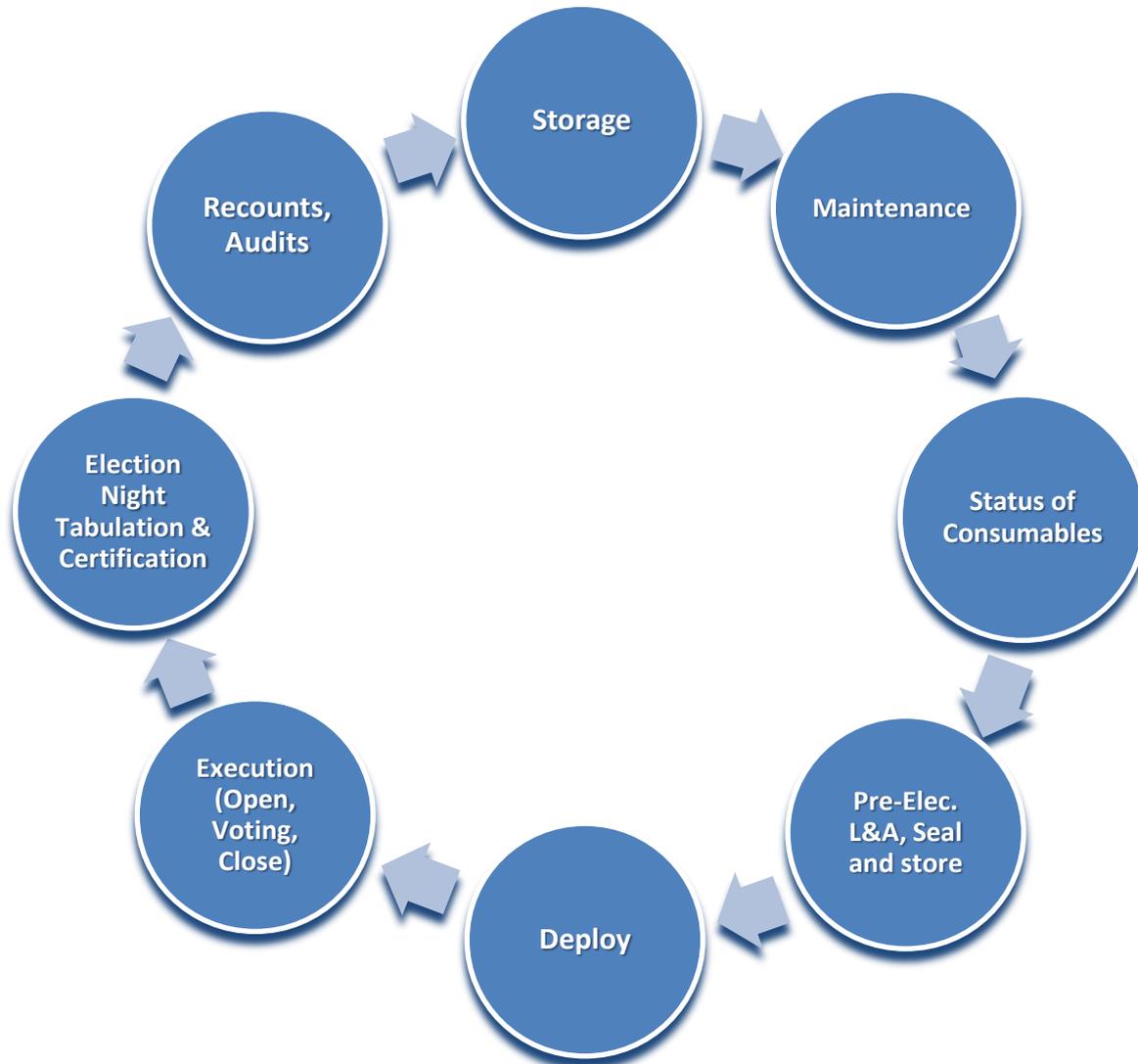
# Voting System

- Different systems present different IT challenges
- Understanding your system is crucial to your success
- Voting system is one of several systems prepared concurrently for the election

# What is a Voting System?

- Total combination of equipment and components used for:
  - Ballot Definition
  - Vote Cast & Capture
  - Vote Tabulation
  - Reporting & Displaying Results
  - Maintain and Produce Audit Trail Information

# Voting System Election Life Cycle



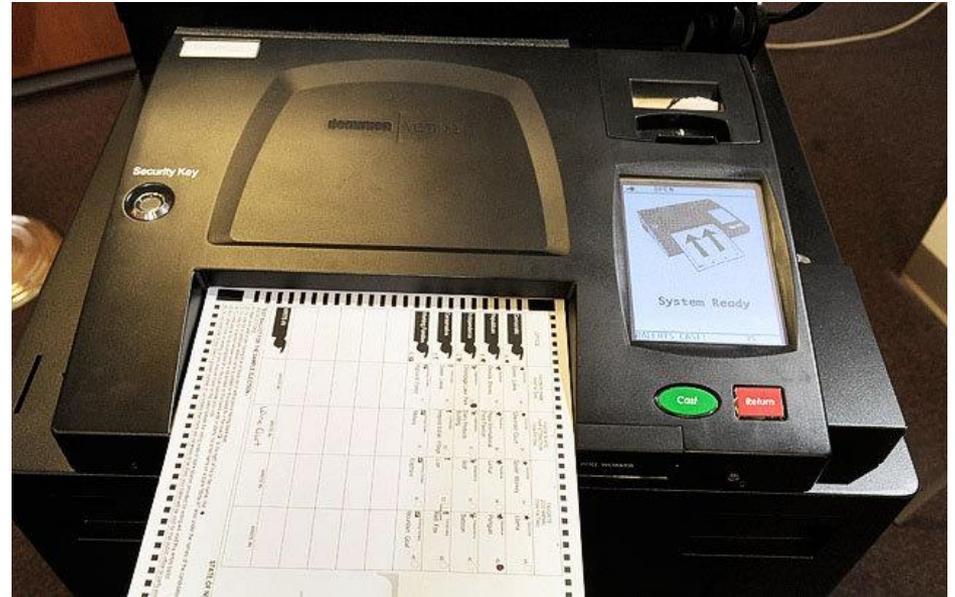
# Voting System Election Life Cycle (cont.)

- IT management concerns
  - Maintenance of custody
  - Logs
  - Documenting anomalies and capturing error messages
  - Documenting failures and maintenance issues
  - Monitoring environmental factors that can impact deployment
    - Turnout
    - Polling location changes

# Direct Recording Electronic (DRE)



# Precinct Count Optical Scan



# Central Count Optical Scanner



# Ballot Marking Devices



# Assistive Technologies (AT)



# Voting System Testing

- Certification Testing
- Acceptance Testing
- L&A Testing
- Validation Testing
- Volume/Load Testing
- Forensic Testing
- Post-Election Audits

# Certification Testing

- Purpose to establish baseline functionality, accessibility, and security of systems
- 2 main certification venues:
  - EAC Testing and Certification Program
  - State Certification
- Is there a place for local certification testing?  
If not, what role can locals play?

# EAC Testing & Certification

- Test voting systems to the Voluntary Voting System Guidelines (VVSG)
- Conformity Assessment
- Certify a certain system in a very specific configuration
- Provide state and locals with systems that have a certain level of performance (HAVA level)
- Quality Monitoring Program

# What EAC does not currently certify

- Voter Registration Databases
- Ballot on Demand Systems
- Pollworker Usability and Accessibility
- Electronic Pollbooks
- Blank Ballot Delivery Systems
- Online Ballot Marking Systems
- Election Night Reporting Systems
- ..... But we can assist in testing.

# State Certification Testing

- States take a variety of approaches to certification
- Ideally states are certifying systems to meet state/local specific needs. Various models:
  - Florida Certification
  - Virginia Certification
  - Nebraska Certification

# Acceptance Testing

- Test conducted to determine if the requirements of a contract are met
- Conducted prior to formally accepting a product as part of a contract
- Goal is to make sure **each** unit delivered works as intended and is identical to certified system
- Should be conducted after purchase and after maintenance/repair
- Who is responsible for conducting the AT?

# L&A Testing

## **Defined:**

The systematic pre-election testing of *every* ballot style and *every* component of a voting system

## **Purpose:**

To demonstrate that the ballot is accurate and that votes cast will be properly tabulated. Also, gives all parties including election official confidence that system will work on election day.

# L&A Testing

- Testing accessibility components
- Alternative language components
- Operational readiness of all components, including connectivity
- What does a successful L&A test affirm?
- Last, best chance to identify and correct anomalies in both ballot and systems

# Root Cause Analysis

- System of analyzing a problem to identify not only how a problem occurred, but **why** it occurred.
  - Root causes are specific underlying causes
  - Root causes are fixable
  - Root causes can be identified
  - Root causes have effective mitigations to prevent the problem from reoccurring.
- Example:
  - Red button, green button....

# Post-election Audits

The audit of election results, conducted after the polls have closed and before certification, by performing manual counts of paper ballots and voter-verifiable paper records in randomly selected units (e.g. precincts) and comparing them to the corresponding electronic or manual tallies, for the purpose of verifying the election result with a high level of confidence.

# Post-election Audits

- Some states mandate audits; some don't
- Audits are a great opportunity to evaluate all of your processes not just equipment
  - Pre-election process
  - Ballot design & printing
  - Election programming
  - Accessibility
  - Absentee processing

# Procuring IT

“You need to understand what you are buying, and why, how it will affect your business, and what the potential risks are. That detailed understanding may be beyond the scope of a procurement department.”

– Owen Williams

# IT Procurement

- Plan ahead
  - Write a sketch RFP even if you don't have to have one
  - Create a use case of what you want the technology to do
- LA County Example
- You can manage the vendors or they can manage you.... Pick.
- Use legal counsel to help and finalize the contract
- Build testing into the process
- Encourage competition

# Security

“An ounce of prevention is worth a pound of cure.”

-Ben Franklin

# Information Security

Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

# Physical Security

The component of information security that results from all physical measures necessary to safeguard a site or equipment, and thereby the data, from unauthorized access, use, or modification. This also includes protections from electrical and environmental (fire, smoke, temperature, etc) damage or destruction.

# Computer Security

The component of information security that results from providing logical protections to safeguard networks and data, including mechanisms such as encryption, integrity, and availability mechanisms.

# Risk Management

The process of identifying, evaluating, accepting, and controlling threats that could exercise vulnerabilities in a system.

# The Continuum

**Security**



Low

High

**Risk**



High

Low

# Authentication

The process of determining if an entity is who or what they are claiming to be and has access to the requested resource.

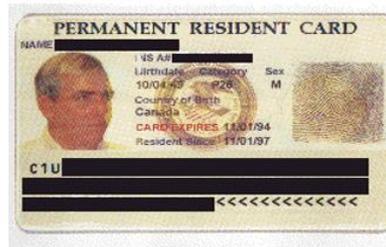
# Authentication Examples



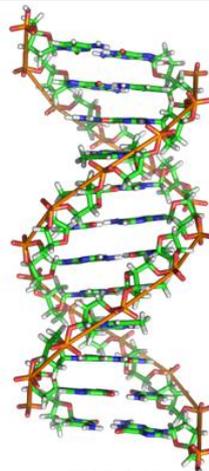
Token

Green Card

Password



Fingerprint



DNA

10011101101  
01010100000  
01011101010

Digital  
Signature

# Multifactor Authentication

- Multifactor Authentication involves using more than just one method of authenticating an entity
- Two-Factor authentication is regarded as strongly authentication
- The more factors, the better

# P@\$\$w0rDs!

- Main method computer driven authentication in use today:
  - ATM
  - Gas Station
  - Facebook
  - Voicemail-box

# Combinations



10 choices/character  
9,999  
Combinations

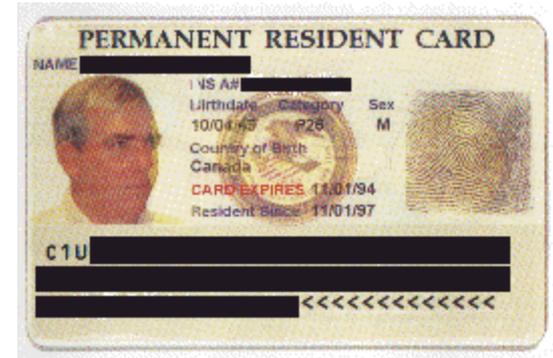
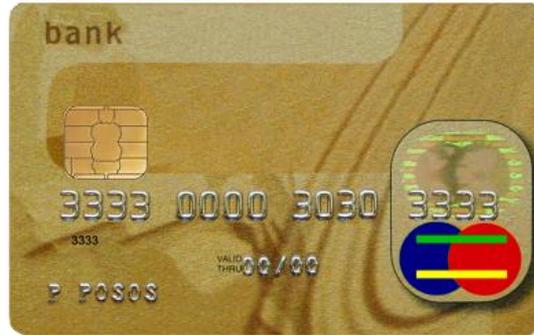


256 choices/character  
4,294,967,296  
Combinations

# Recommendations

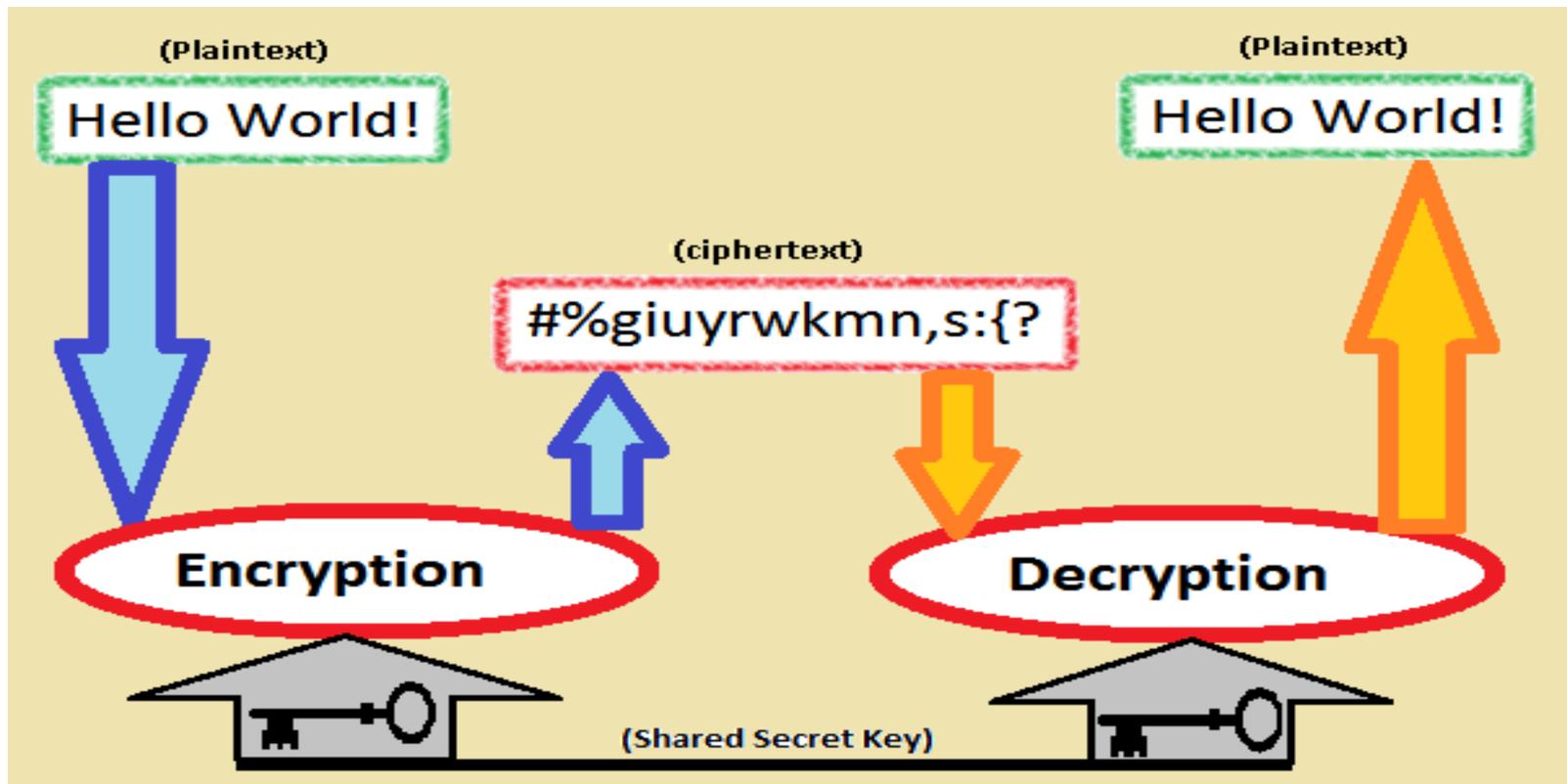
- Do not use default passwords
- Use different passwords for different accounts
- Use different passwords for different people
- Use different passwords for different elections
- No names or dictionary words
  - Example: JaneElection4
- Randomness
- At least 8 characters
- Consider a password manager for office desktops

# Tokens



# Cryptography 101

The practice and study of techniques for secure communication in the presence of third parties



# Cryptography 101

- What you need to know:
  - Nothing to be intimidated about
  - The hard stuff is handled by the equipment
  - Need to know how to manage access and sharing of the keys (see passwords)
  - Rapidly increasing usage in voting and election systems
  - Ask your vendor what is and is not encrypted in your system and what that means

# Access Control Topics

- Equipment
- Election Central
- Polling Place
- Personnel

# Controls

- Preventative Control – These keep a security breach from happening. Very expensive and designers must accurately anticipate a breach.
- Detective Control – Detects that a breach has occurred
- Corrective Control – Restores system correctness after disruption

# Equipment

Tamper Resistance	Tamper Detection
Delaying physical access to an entity	Providing evidence that an entity has been accessed

Needs to be kept both physically and logically secure at all times. This includes when not under direct human supervision.

# Locks & Keys

- Typically only Tamper Resistance is provided.
- Often can be bypassed without providing tamper detection.
- With 1000 identical keys in a jurisdiction for weak locks, locks and keys should not be assumed to provide a high degree of tamper resistance.

# Locks & Keys



# Seals

- Only provide evidence of tamper detection.
- More effective the more fragile.
- False alarms are typical
- Checking the seal number is key. Without checking, the seal is useless.
- Strong link in the Chain of Custody.
- If a seal is broken – Investigate!

# Seals Examples



# Storage

- Be aware of your environment;
  - Humidity, salt, fire, heat, sand, dust, cold, snow, ice, water, flooding (sprinkler systems!)
- Store equipment sealed with a documented chain of custody.
- Store units in a supervised area, CCTV can help
  - Have enough available space to record before you need to change storage mediums

# Disposal

- Think before you throw away.
- One LEO's trash is another's treasure
- Attempt to return unwanted units to the manufacturer.
- *Be careful* - COTS PC equipment can contain sensitive information.
- Destruction is always safer (PCs, HDDs, Memory Cards).
- Know your county's IT disposal policies

# Disposal

- DREs have archival memory that will contain cast ballot information from past elections. Flash the memory before disposing
- Software is not transferrable. When you sell a piece of used election equipment, you must remove the software (application and OS) before selling
- Do not buy used equipment and assume the software license comes with it!

# Polling Place Security

- Be aware access to polling place (entrances and exits)
- Have the ability to view the entire polling place at one time (360 degree view)
- Electronic Devices
- Perception



120 No cell phones

# Election Central Security

- Be aware of access to Election Central locations (entrances and exits)
- Temporary personnel
- Authorized personnel only- Very Complicated
  - Badges, lanyards, tags prominently displayed
  - If you're unsure of who a person is; ask.
- CCTV, cameras can help monitor the election office

# Personnel

- Separation of Duties
- Role rotation
- Least privilege
- Background checks

# Use of Wireless

- Think before you use
- Can provide an unauthorized entrance to election network
- Secure with a strong password
- WPA2 if you must (***Wi-Fi Protected Access 2***)
  - encrypt by providing your router not with an encryption key, but rather with a plain-English passphrase between 8 and 63 characters long. Using a technology called [TKIP](#) (for *Temporal Key Integrity Protocol*), that passphrase, along with the network SSID, is used to generate unique encryption keys for each wireless client. Those encryption keys are constantly changed.

# Portable Computing

- Often contain sensitive information
- Often used in unsafe environments
- Often stolen
- Phones and laptops are computers
- Backup and recovery

# The Future

**“My interest is in the future because I am going to spend the rest of my life there”**

**- Charles Kettering**

# What's Next?

- Precinct-less Voting
- Component Based Systems
- Virtualization (operating systems)
- Hardware Independence
- Enhanced Accessibility Mitigation
- Hybrid Systems – DRE & OpScan combined
- Internet Voting
- The only thing certain about the future...

**Change!**

# Questions?

Brian J. Hancock – [bhancock@eac.gov](mailto:bhancock@eac.gov)

Merle S. King – [mking@kennesaw.edu](mailto:mking@kennesaw.edu)

Matt Masterson – [mmasterson@eac.gov](mailto:mmasterson@eac.gov)

Thank You!