

Best Practices: Managing Voting Systems

Security, Storage and Preventive Maintenance

Larry Haake

Chesterfield County General Registrar / Director of Elections

Best Practices

1. Security

- a) Physical
- b) Process

2. Storage

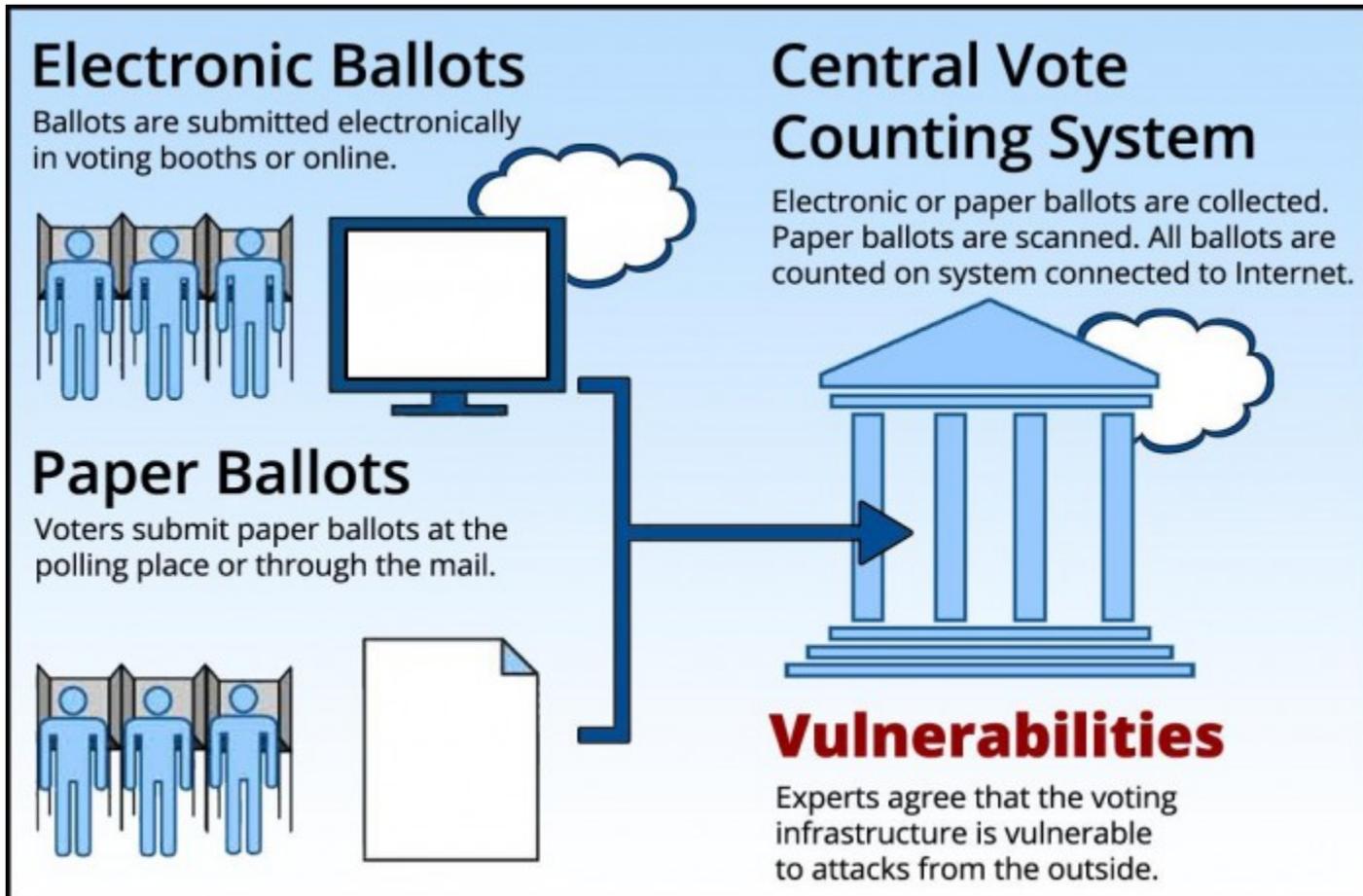
- a) Directly tied to physical security

3. Preventive Maintenance

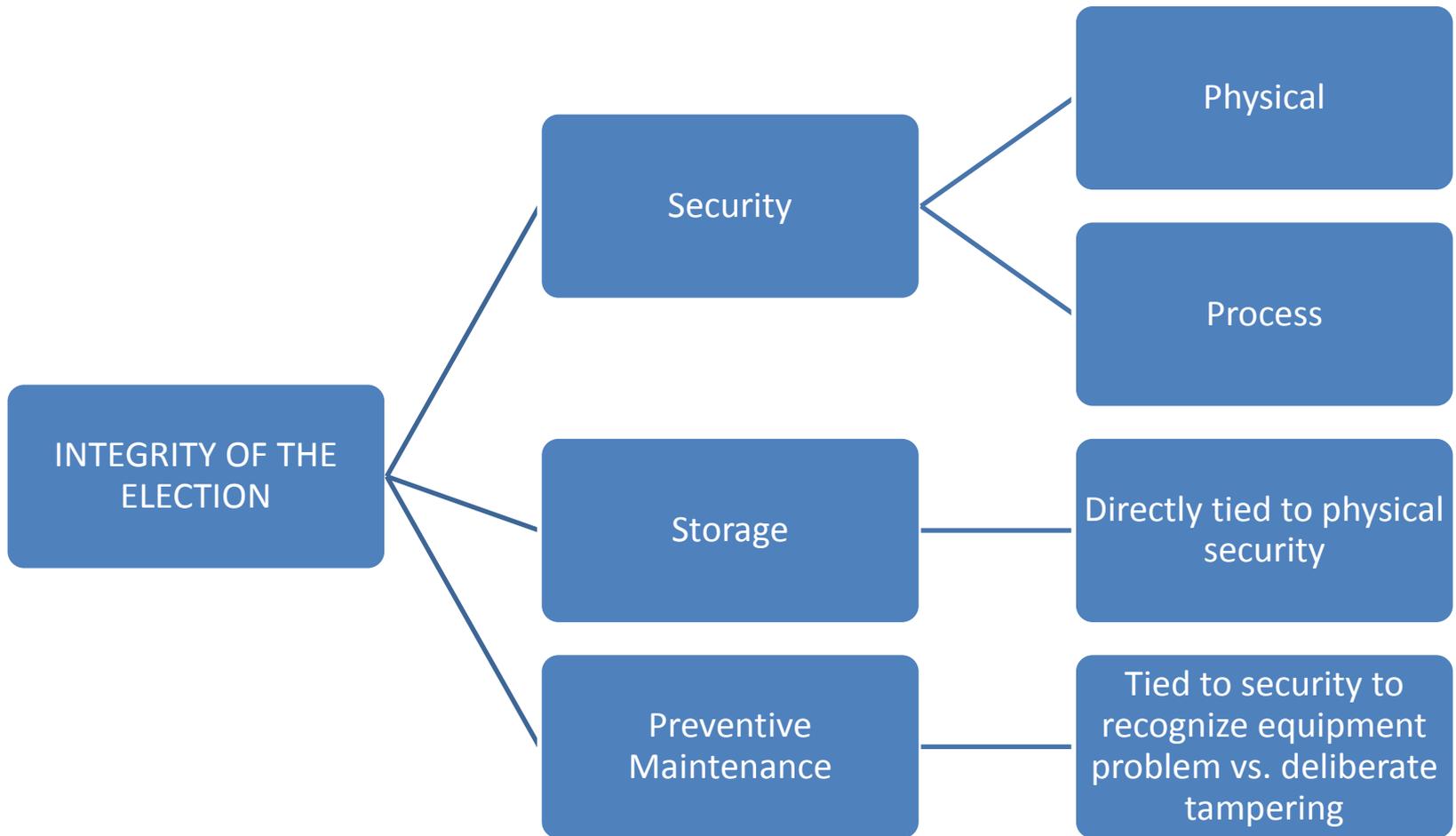
- a) Tied to security to recognize equipment problem vs. deliberate tampering

Perception

Foreigners Could Hack US Elections, Experts Say



Best Practices



Security Defined

1. Control

a) Access

b) Processes

i. Electronic – programming, data devices, etc.

ii. Logic & Accuracy (L&A) Tests

iii. Maintenance

2. Protection

a) Tampering – deliberate and inadvertent

3. Preserving the integrity of the election

a) Back-up machines, data devices, etc.

Legal Considerations

1. 24.2-625.1

a) Security Plan Required

b) 2007 – SB1226 Senator Janet Howell

2. 24.2-629

a) Vendor recommends procedures “for optimum security and functionality of the system”

Legal Considerations

3. 24.2-659

- a) Post-election Voting Machine (results) Security with Circuit Court Clerk
- b) Five Options for securing machines
 - i. A – Keys only
 - ii. B - Keys or data device
 - iii. C – Data device only
 - iv. D – Master data device
 - v. E – Data device when no votes on machine (2016)

Legal Considerations

1. When is a voting machine not a voting machine?
 - a) 24.2-659(H) – when there are no votes stored on the machine or its data device (7/1/2016)

Too Much Security?

1. For every security feature introduced, there must be a documented corresponding reaction to its breach.
 - a) Security Plan
 - b) Threat assessment

Threat Assessment

1. What could be consequences of a compromise of security/election integrity in a given scenario.
 - a) Machines stored
 - b) Machines in prep
 - c) Machines in transport to/from
2. How serious would that breach be?
 - a) Example: Broken lock on cage still has machine secured by its own locks
3. What action to be taken on a given compromise

Too Much Security?

1. For every security feature introduced, there must be a documented corresponding reaction to its breach.
 - a) Security Plan
 - b) Threat assessment
 - i. Don't "over-secure" and turn your job from elections to security director
 - c) Security levels
 - i. Security Level 1 – Security Level 3
– Medium, High, Highest

Recounts

1. Security is scrutinized during recounts
2. Tighten-up processes if a close election is expected
 - a) Maybe expect close elections more often than not
3. 2013 Chesterfield example

Physical/Process Security Stages

1. Security Tools

a) Locks built into the machine

i. Key tracking

b) Seals for data devices

i. Recording the seal number (L&A)

c) Transport carts (cages)

i. Secure with lock (more keys)

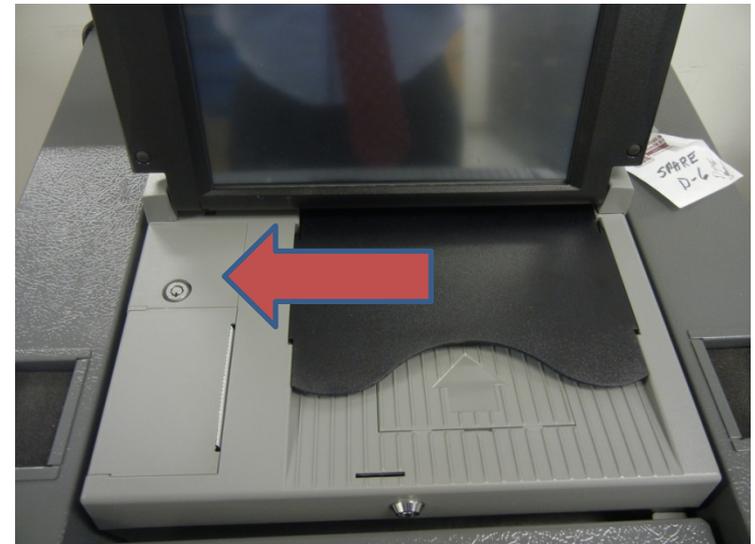
d) Room/building in which stored

i. Accessible by whom, when , for what

Physical/Process Security Stages

1. Locks built into the machine
 - a) Key tracking
 - b) Ensure the locks are locked
 - i. Greatest violators OOE

Physical/Process Security Stages



Physical/Process Security Stages

1. Locks built into the machine
 - a) Key tracking
 - b) Ensure the locks are locked
 - i. Greatest violators OOE
 - c) Lock tamper seals?
 - i. Maybe - depending on other levels of security
 - ii. Traditional lock seals easily damaged harmlessly
 - iii. Instruction to visually inspect lock/access points for evidence of tampering

Physical/Process Security Stages



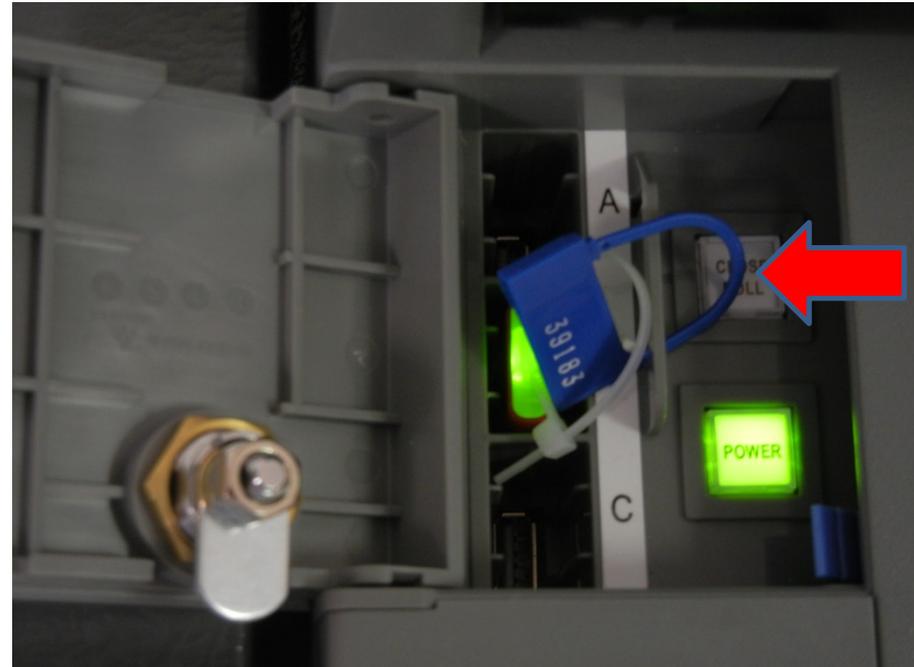
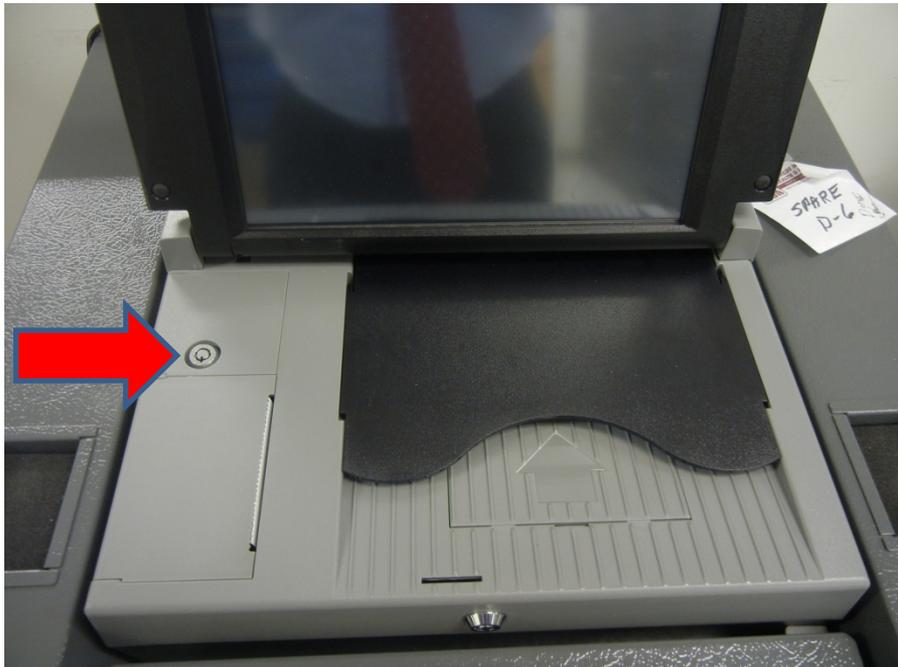
Physical/Process Security Stages



Physical/Process Security Stages

1. Seals for data devices

- a) Recording the seal number (L&A)
- b) Tamper seals – same as lock considerations



Physical/Process Security Stages

1. Transport carts (cages)
 - a) Secure with lock (more keys)
 - i. Keying level – Master/Individual
 - b) Stable device to withstand transport

Physical/Process Security Stages



Physical/Process Security Stages



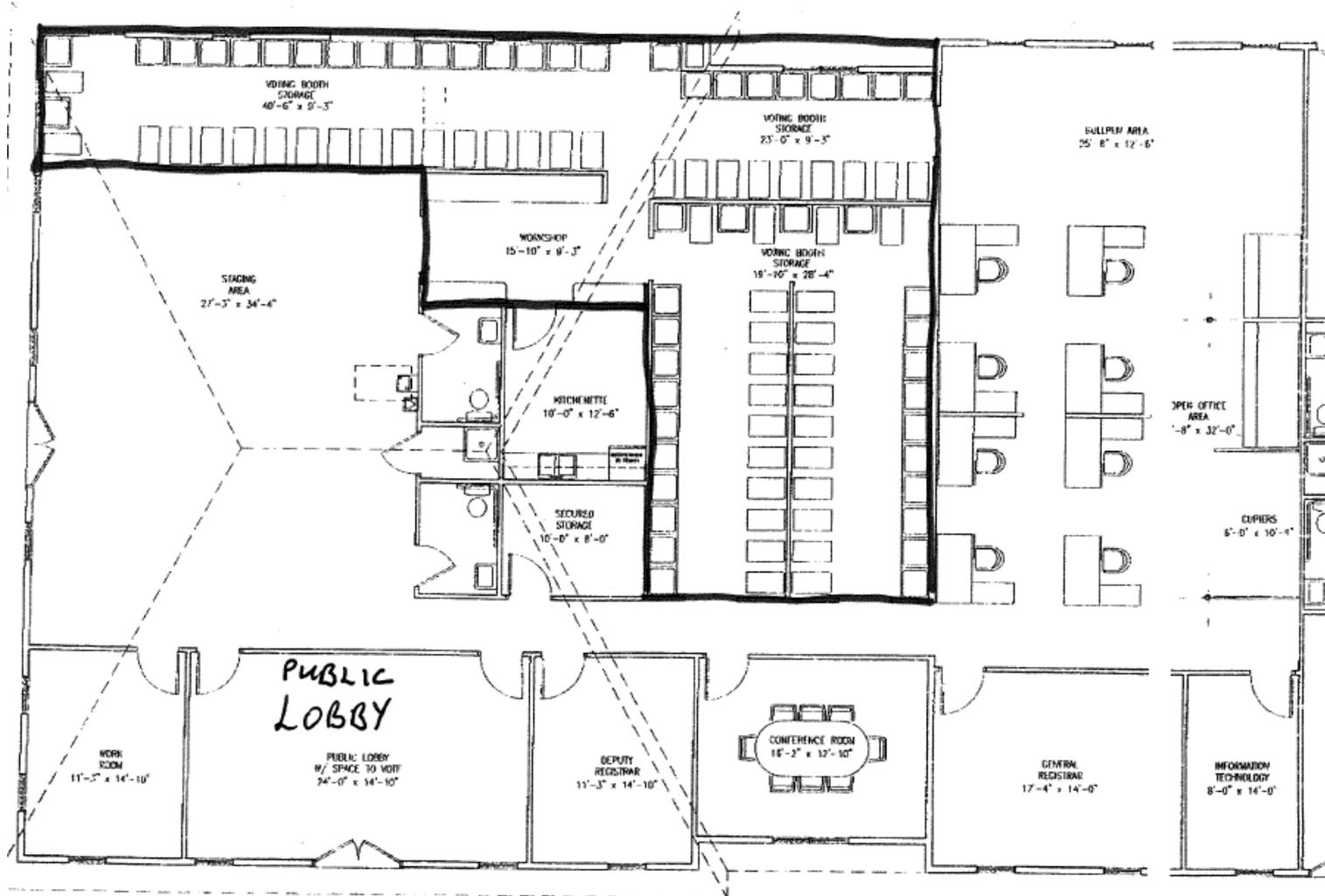
Physical/Process Security Stages

1. Transport carts (cages)
 - a) Secure with lock (more keys)
 - b) Stable device to withstand transport
 - c) Inspect before dispatch to and upon return from polling place
 - d) Instruction to OOE to inspect for tampering
 - e) Instruction that vote counter may not be staged until election morning – it remains locked in the cage

Physical/Process Security Stages

1. Room/building in which stored
 - a) Accessible by whom, when , for what
 - b) What level of security?
 - i. Medium (1) – free access by regular employees
 - ii. High (2) – access limited to needed personnel
 - iii. Highest (3) – access controlled by Director of Elections
 - Key control
 - Log control
 - Minimum level of employee access (2 people)
 - c) Burglar/fire alarms
 - d) Internal barriers, if needed

Physical/Process Security Stages



Physical/Process Security Stages



Physical/Process Security Levels

1. Routine storage – Security Level 1
 - a) Access by regular employees
2. Pre-election preparation and storage – Security Level 2
 - a) Access only to those needed
 - i. Staging coordinator, machine techs, etc.
3. During transportation to and from – Security Level 2
 - a) Know who is handling the transport
 - b) Document placement of equipment in building
 - c) Minimize exposure in non-secure polling place
4. During post-election period – Security Level 3
 - a) Minimal access – log controls
 - b) Key control
 - c) Maintain levels of physical security – cage lock, machine lock, seals, etc.

Preventive Maintenance

1. Ensures equipment operating properly, thus eliminating suspicion of tampering
2. Periodically
3. Vendor contracts vs. Break/Fix

Preventive Maintenance

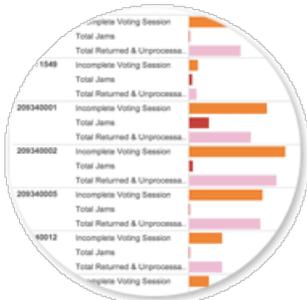


Preventive Maintenance

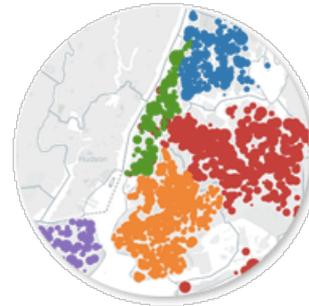
1. Ensures equipment operating properly, thus eliminating suspicion of tampering
2. Periodically, unless needed
3. Vendor contracts vs. Break/Fix
4. Pay attention during L&A
5. Document machine problems from election day
 - a) Voters will “mess” with things (so will OOE)
6. Vendor tools

Preventive Maintenance

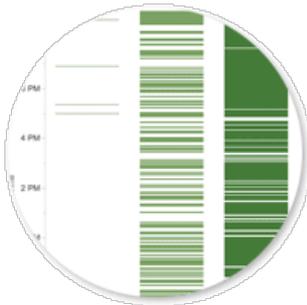
ES&S ElectionInsights



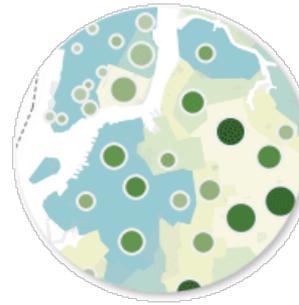
Voting Machine Data
We collect log files and error messages collected from each voting machine used in each polling location.



Regional Data
we gather geolocation information about each polling place in the region, in order to visualize this data on a map.



Polling Location Data
We gather the information about which machines are associated with each location, so that we can analyze the performance of a single location.



Publicly Available Data
We collect log files and error messages collected from each voting machine used in each polling location.

Preventive Maintenance

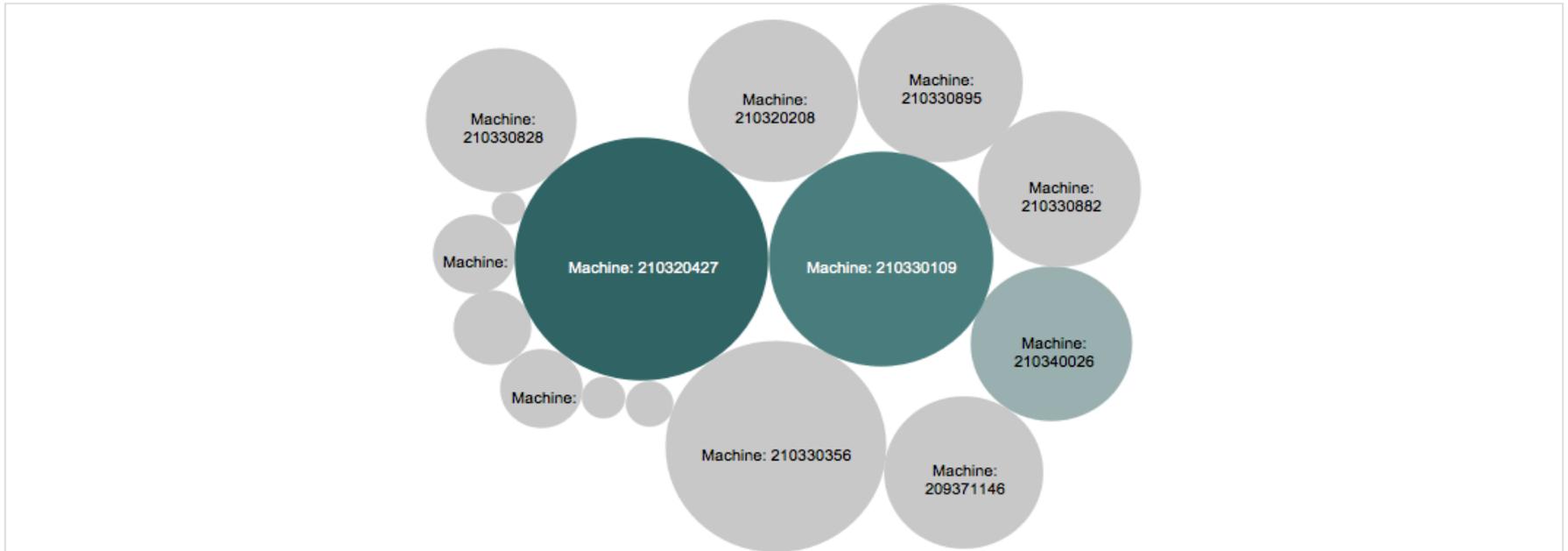
ES&S ElectionInsights

1. Poll opening and closing success
2. Voter volumes by time, location, and machine
3. Interrupted voting sessions by location, time, and source
4. Voter issues by location and time
5. Poll worker issues or errors by location and time
6. Equipment or ballot issues or errors by location and time
7. Equipment performance by machine, location, and time
8. Equipment aging by machine

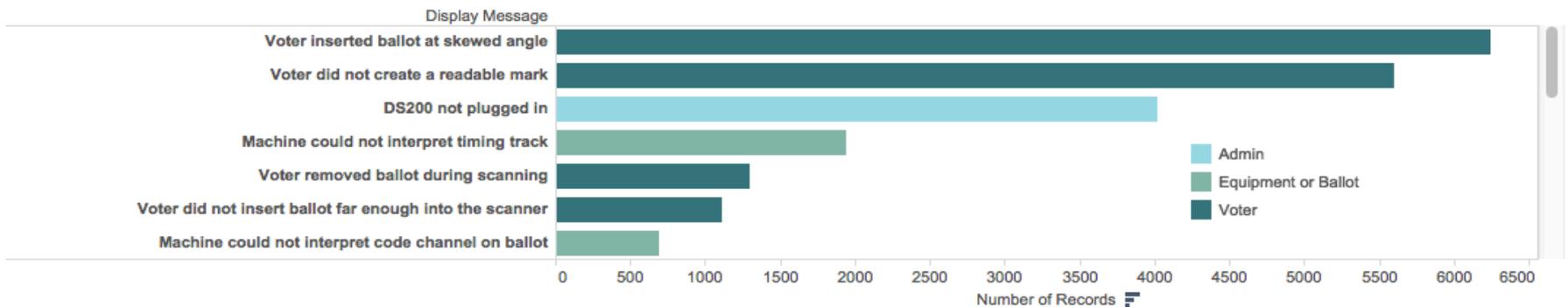
Preventive Maintenance

ES&S ElectionInsights

Top Equipment by # of Issues



Top Issues



Security & Maintenance

1. A mixture of art and science
2. We **HAVE** to consider these so that we can “say we did”
3. Done properly, it can get you out of a sticky situation
4. Done wrong or **NOT DONE**, you have no excuse
5. **REASONABLE** is the key