

# Threat Assessment and Contingency Planning for Election Administration

R. Michael Alvarez

Caltech/MIT VTP

July 9, 2006

# Current Environment Calls For Planning and Preparation

- Era of close elections (US, internationally).
- Heightened attention from public and press.
- Claims of threats reducing ability of election officials to do their work
- Rapid diffusion of allegations via blogs, email, etc.
- Election administration more complex, technologically sophisticated; but not necessarily more resource intensive.
- Bad things happen -- bottom line
- Threat: something that jeopardizes an election function so that it doesn't work as intended.

# Planning Is Imperative

- Planning for problems helps:
  - Prevent their occurrence
  - Mitigate their effects
  - Resolve their their implications
  - Insulate fallout
  - Builds confidence; voters, candidates, election officials

# Planning Helps Insure Security, But More!

- Threat assessment is seen by some as solely about security concerns.
- Security --- physical, electronic, procedural --- is indeed a piece of the assessment and planning puzzle.
- But it must be more than about only voting system security, more than the threat of “hackers”

# Example: Travis County, TX

- Travis County, Texas has developed a comprehensive assessment of threats to their voting process; their assessment and planning materials were honored by the Election Center last summer!
- Hurricane Rita story.
- Planning must cover more than just voting system security during election period!
  - Natural disaster
  - Unintentional human-caused disasters (power failures)
  - Scale: large and small problems
  - Problems before, during and well after election

# Other Examples

- State of Oregon requires annual security evaluations (not available to the public)
- California “requires” security evaluations (not available to the public)
- No doubt other states and local jurisdictions in the US have some undertaken some security planning, but few that we are aware of have undertaken a more comprehensive threat and contingency planning process

# How Can It Be Done?

- Scattered examples in the field of election administration should be studied for best practices (Utah study)
- NIST threat assessment process can provide some guidance
- Other methods: collect data on known threats (EAC study, Utah/Caltech study); collect perceptions data (Utah/Caltech; Electionline/VTP).
- Look to other models, for example, Secret Service (Borum et al. 1999); Newcastle Disease outbreak (Moynihan); Homeland Security? What can be learned from their processes, success AND FAILURES?

# A General Framework

- Identification of threat or contingency
- Estimate of likelihood (numerical or categorical) and impact
- Development of prevention and mitigation strategies
- Resource allocation based on evaluation of likelihood of occurrence and impact
  - Procedures, regulations and laws
  - Training
  - Physical and technological security

# Planning Must Be Contextual and Dynamic

- One-size will not fit all situations; planning must recognize the context
- Dynamic planning requires continual updating of estimated likelihood and impact, of prevention/mitigation strategies, and of changing context
- Not an abstraction