# A Threat Analysis on UOCAVA Voting Systems

## Overview

Lynne S. Rosenthal
lynne.rosenthal@nist.gov

NIST Voting Program
National Institute of Standards and Technology

EAC Standards Board Meeting
February 26-27, 2009

# Today's Topics

- EAC/NIST involvement in Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) -related voting
- Overview of NIST UOCAVA report
- Initial conclusions
- Next steps

# EAC/NIST Involvement in UOCAVA voting

- **Help America Vote Act** - EAC to study electronic transmission of ballots

- **National Defense Authorization Act FY2005** - EAC guidelines on electronic absentee voting

# EAC/NIST Involvement in UOCAVA voting

- NIST has expertise in computer and network security
  - Network and system threats and vulnerabilities
  - Sophisticated network-based attacks and defenses
  - Secure system and network management
- NIST provides technical support in the development of the voting guidelines
  - VVSG and associated tests
  - Technical research items
  - UOCAVA voting

# UOCAVA Report Overview - 1

- Threat Analysis for UOVAVA Voting Systems
  - Looks at using different transmission methods
    - Postal mail, telephone, fax, e-mail, web-based
  - Splits voting process into 3 stages
    - Voter registration/ballot request (e.g., FPCA)
    - Ballot delivery
    - Ballot return

# UOCAVA Report Overview - 2

- Threat analysis performed for each transmission option at each stage
  - Analysis based on NIST SP 800-30 *Risk Management Guide for Information Technology Systems*
- Identified mitigating security controls, where possible
  - Both technical and procedural controls
  - Security controls taken from NIST SP 800-53 *Recommended Security Controls for Federal Information Systems*

# Initial Conclusions - 1

**Registration and Ballot Request:**

- Main concern: handling/transmitting sensitive voter information
- Threats to electronic transmission can be mitigated through technical controls and procedures
- Threats to e-mail and web-based systems pose greater security challenges

# Initial Conclusions - 2

**Blank Ballot Delivery:**

- Main concerns: reliable delivery, integrity of ballots
- Threats to electronic transmission can be mitigated through technical controls and procedures
- Electronic ballot accounting more difficult than with physical ballots

# Initial Conclusions - 3

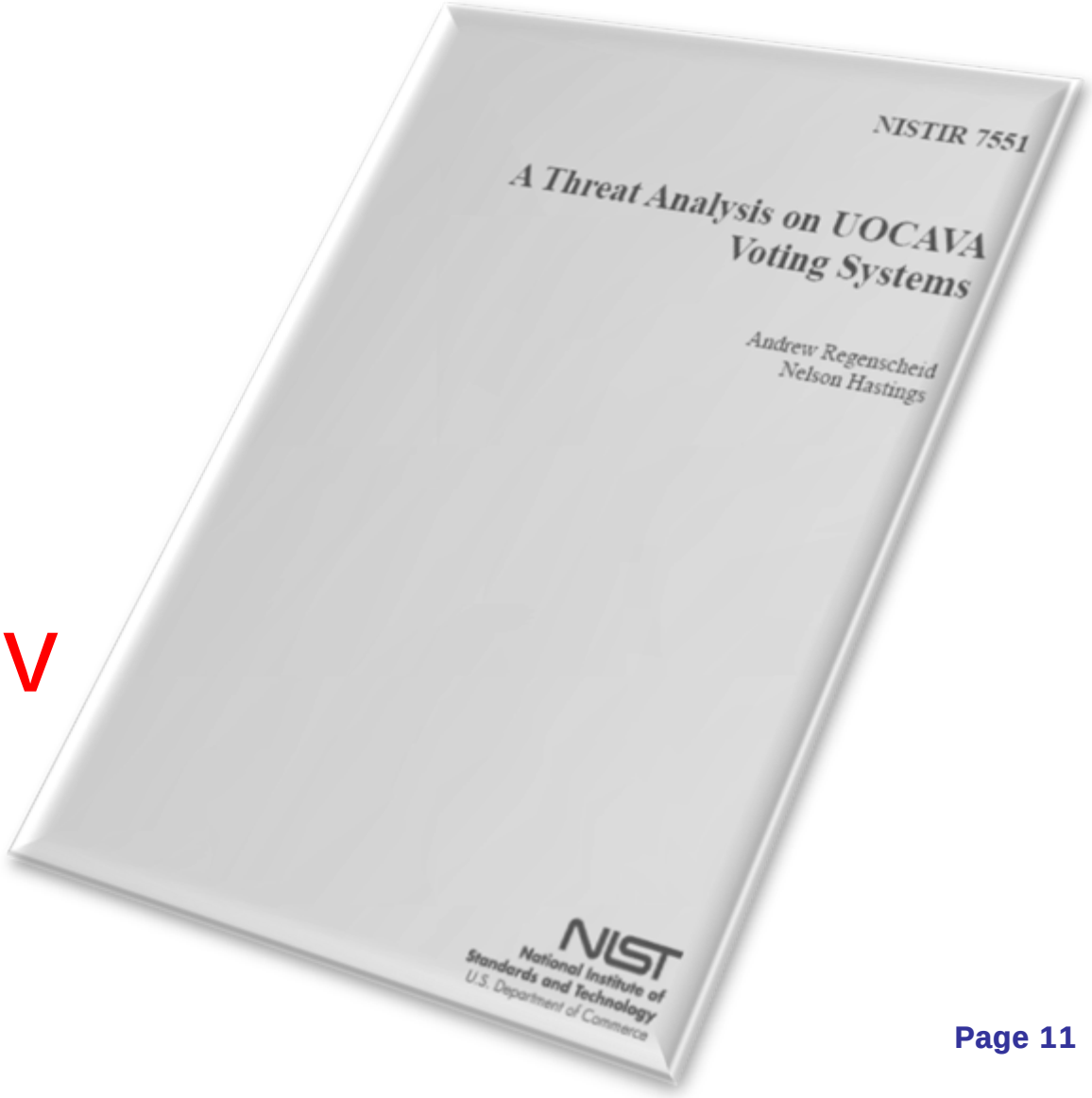
**Voted Ballot Return:**

- Main concerns: reliable delivery, privacy, integrity of voter selections
- Electronic methods pose significant challenges
- Fax presents fewest challenges, but limited privacy protection
- Threats to telephone, e-mail, and web voting more serious and challenging to overcome

# Next Steps

EAC/NIST will define the scope of the next phase:

- Develop guidelines for sending/receiving registration/request materials and blank ballots
- Develop high-level system goals and strategies for electronic ballot return




available at:

# vote.nist.gov

# Questions?

Lynne S. Rosenthal
National Institute of Standards and Technology
lynne.rosenthal@nist.gov