What are we Accountable For?
Security Standards and Resources for High Stakes Testing Programs
Agenda

★ 4 Helpful Resources
   ➤ Handbook on Test Security
   ➤ CCSSO TILSA Guidebook on Test Security
   ➤ ATP/CCSSO Operational Best Practices on Statewide Assessment
   ➤ International Test Commission Guidelines for the Security of Examinations, Tests and Other Assessments

★ Relevant examples/Highlights

★ Questions?
Focuses on how tests are delivered for:

- paper-and-pencil,
- technology-based, and
- classroom testing and writing assessment.

Each chapter addresses the prevalence of the problem and threats to security, prevention, and detection.

- Fremer, Ferrara, Security in Large-Scale, Paper and Pencil Testing
- Foster, Security Issues in Technology-Based Testing
- Woodruff, Security Issues in Classroom Testing
- Lane, Security Issues in Writing Assessment
Addresses issues essential to maintaining a secure testing program such as:

- planning and monitoring,
- physical security,
- the detection of group-based cheating,
- investigating misconduct, and
- communicating about security-related issues.
PART 2 AUTHORS

- Fitzgerald, Mulkey, Security Planning, Training, and Monitoring
- Scicchitano, Meade, Physical Security at Test Centers and The Testing Company
- Maynes, Educator Cheating and the Statistical Detection of Group-Based Test Security Threats
- Harris, Watkins Schoenig, Conducting Investigations of Misconduct
- Case, Donahue, Security-Related Communications
- Semko, Hunt, Legal Matters in Test Security
Insight into security issues within each of the Association of Test Publishers’ four divisions:

- certification/licensure,
- clinical,
- educational, and
- industrial/organizational testing

Part III’s conclusion revisits the issues addressed in the case studies and identifies common themes.
PART 3 AUTHORS

- *Carson*, Certification/Licensure Testing Case Studies
- *Williams, Rzepa, Sitarenios, Wheldon*, Clinical Testing Case Studies: Prevention, Detection, and Management of Falsified Test Development Data
- *Bartram, Burke*, Industrial/Organizational Testing Case Studies
- *Hatherill*, Commentary on Case Studies
- *Fremer, Wollack*, Conclusion: The Future of Test Security
For the Handbook in its Entirety

» Five Takeaways
» Five Predictions
1. What security vulnerabilities exist for all genres of testing?
2. The critical importance of security planning
3. Practical and proven strategies for preventing and detecting cheating
4. How security breaches have been dealt with in specific programs
5. What lessons have we learned from past instances of testing misbehavior?
In many high stakes testing programs:
1. Cheating detection statistical analyses will be performed routinely
2. Computer-based testing will increasingly become the norm
3. Technology developments will be critically important to test security
4. The internationalization of the program will increase
5. “Test Security Expert” will become a recognized and valued position
ADVICE FOR THE READER

- Review the Table of Contents
- “Skim read“ the chapters
- Earmark chapters and sections for staff to read or for you to return to
- Read sections as you deal with the issues addressed
LEADERS GUIDE: PREVENTING, DETECTING, AND FOLLOWING UP ON TESTING IRREGULARITIES

CENTER FOR CHIEF STATE SCHOOL OFFICERS

DESIGNED FOR STATE ASSESSMENT DIRECTORS
Ten Recommendations
- Prevention
- Detection
- Test Security Investigations
PREVENTION

A. Communicate Zero Tolerance
   1. Clear
   2. Consistent
   3. Frequently emphasized messages

B. Develop a Security Plan
   ➢ Comprehensive
   ➢ Up to date
C. Test Security Manager
   - Assignment (or)
   - Position

D. Test Security Audit
   - External
   - Formal test security standards
   - Security vulnerabilities
   - Recommendations for correcting
E. Use Multiple Data Forensics Methods
   1. Unusual Gains
   2. Similarity
   3. Erasures (Answer Changing)
   4. Person Fit Analyses
F. Introduce Data Forensics Very Carefully
   ➢ Think Through Planned Uses
   ➢ Prepare LEAs (and others) for Data Forensics Use
   ➢ Planful, Multi-step Public Information Program
G. Adhere to Legal and Regulatory Requirements

- Importance of “test user” agreement
- Clarify potential consequences of not following testing rules
- May want to seek changes to laws or regulations
H. Areas Needing Attention

- Level of evidence warranting an investigation
- Roles for state, district, and other staff
- Time lines
- Model investigations kit
I. Model Investigations Kit
   ➤ Clear definition of responsibilities
   ➤ Procedures for evaluating evidence
   ➤ Planning and conducting interviews
   ➤ Developing a report with recommendations
J. Focus Primarily on Improving Security in the Future

- Follow “Innocent Until Proven Guilty” approach, but be firm in your questioning
- Give most attention to the “Worst of the Worst”
- Consider other possible explanations for results
FOR MORE INFORMATION:

John Fremer
Caveon Consulting Services
Caveon LLC
215-805-3007(cell)
John.fremer@caveon.com
Important Test Security Resources

- International Test Commission Guidelines for the Security of Examinations, Tests and Other Assessments

- ATP/CCSSO Operational Best Practices for Statewide Large Scale Assessment Programs
Because…
ATP/CCSSO Operational Best Practices

✿ CCSSO = Council of Chief State School Officers

✿ June 2006

➢ ATP and CCSSO
➢ Identify and publish voluntary, non-regulatory best practices
➢ Collaboration of States and testing companies
➢ Goal: Strengthen statewide testing programs conducted under the No Child Left Behind Act (NCLB)
ATP/CCSSO Operational Best Practices

Published in Spring 2010:

🌟 Enhance the quality, accuracy, and timeliness of student test data derived from large scale assessments

🌟 Strengthen public confidence in the accuracy and quality of testing data and their uses
ATP/CCSSO Operational Best Practices

Broad, Comprehensive Treatment of Paper and Pencil Test Programs

- Program Management & Customer Service
- Item Development
- Item Banking
- Test Booklet Construction and Development
- Technical Defensibility
- Procurement

- Field Testing
- Test Administration
- Scoring
- Vendor management
- Materials Management
- Technical Support
- Data Management
- Switching Vendors
- Security
2013: Revised OBP for **CBT and Online Testing**

- Just published last week!

- May not be **precisely** applicable to “…(test programs) used on an international basis”

- Provides a **solid framework** from which others might seek to define a set of practices tailored to their testing programs

- ATP and the CCSSO encourage others to use this document
International Test Commission (ITC) Security Guidelines

International Test Commission Guidelines for the Security of Examinations, Tests and Other Assessments
History

- 2008--a test security “module” was requested by Research and Guidelines Committee

- 2010--A draft of the *International Test Commission Guidelines for the Security of Examinations, Tests and Other Assessments* submitted for review

- Significant revisions in 2011 and 2012

With increasing security problems, the guidelines are:

- intended to **share key elements of security best practices** to promote better security, and

- **defend the value of scores** produced through the assessment process
All high-stakes assessments, tests and exams

All stakeholders in the assessment process (publishers, users, students, test developers, etc.)

The entire assessment process from development to administration to results processing and scoring

Across all areas of testing (e.g., education, employment, certification/licensure government, clinical psychology, etc.)
The ITC Guidelines provide answers to these questions:

- **Threats.** What are the dangers?
- **Test Fraud.** How can we deal effectively with increasing security problems?
- **Terminology.** How can we best communicate about test security
ITC Guidelines: Structure

- Developing a Security Plan
- Implementing Security
- Responding to a Security Breach
Structure Part 1: Developing a Security Plan

- Understand your security vulnerabilities
- Understand the various cheating and piracy threats
- Determine where the greatest risk is for a particular testing program
- Create a formal plan to repair security vulnerabilities, detect and mitigate the threats, and deal promptly and effectively with breaches
- 22 guidelines and sub-guidelines
5. Security rules should be indicated clearly in the security plan and communicated to all interested parties. Consequences for violations of those rules should be clear.
Structure 2: Implementing Security

🌟 Manage security procedures during all aspects of assessment:

➢ Test Development
➢ Test Administration
➢ Collection and Storage of Materials and Test Results
➢ Reporting

🌟 69 guidelines and sub-guidelines
Example: Implementing Security Guideline “18.g” (of 69)

18.g. Proctors (invigilators) should not have an interest or stake in the test outcome. They should not be instructors or teachers for examinees nor familiar with the content covered by the exam.
Structure 3: Responding to a Breach

- Detecting a Breach
- Responding Quickly and Effectively
- 22 guidelines and sub-guidelines
4. Scores shown to be inaccurate and a result of test fraud should be immediately cancelled or invalidated.
A total of 113 guidelines

Following the guidelines (as appropriate) leads to:

- Fewer vulnerabilities
- Less risk from threats
- Fewer breaches
- Less damage from breaches
- More confidence in scores/decisions
Questions?
Thank You!

Dr. John Fremer
Caveon
John.fremer@caveon.com
@TestSecurityGuy

Steve Addicott
Caveon
Steve.addicott@caveon.com
@sdaddicott