Session A-1: State Critical Elements: Test Operations and Maintenance
Panelists: *Heather Peltier, John Olson, June Zack*
Moderator: *Mario Nunez, U.S. Department of Education, Office of State Support*

This panel discussion focused on various aspects of evidence needed for test administration, test and data security, and training and maintenance of a state assessment. Panelists who have served as recent peer reviewers offered observations on the types of evidence that demonstrate a state's adherence to the critical elements. This session addressed critical elements 2.3, 2.5, 2.6, and 4.7.

Mr. Mario Nunez opened the session and introduced the panelists.

Critical Element 2.3: Test Administration (page 40)

Ms. Heather Peltier said reviewers are looking for clear guidance from states on security, testing irregularities, special circumstances (e.g., cheating), and special situations (e.g., homebound students). Before, during, and after testing, checklists can be useful for coordinators and administrators. Guidance is needed on the testing environment (e.g., what can be displayed on the walls) and for selections made for computer-based testing. The state needs to provide evidence that guidance was provided in all these areas.

Evidence of training should be apparent in the submission. All individuals responsible for test administration must receive appropriate training, and variances in training must be explained. It is not sufficient to say the state offered training without providing evidence. Tennessee tracks non-participation. One challenge in Tennessee has been turnover for district testing coordinators. Also, the importance of providing seating charts and computer ID numbers to track which student was tested on which computer should be acknowledged in training forms. The state wants to deliver training material that people can use "out of the box," without adjustments for particular groups. Communication is key, whether through in-person training, monthly webinars, websites, listservs, text message alerts, or an open call-in line.

Technology-specific issues include computer-based testing, which usually requires a longer window. The preparation must be certified, with documentation of hands-on platform training. A weakness often seen is a lack of dates. True contingency plans are needed, not just standardized guidelines. It is useful to have an easily accessible troubleshooting guide. Documentation should be thorough, clear, concise, and easy to access. Although government requirements may appear to be "more hoops to jump through," in fact, peer review has been very beneficial to the state.

Critical Element 2.5: Test Security (page 43)

Mr. John Olson said test security is a relatively new requirement, and evidence of security provided by the states has been mixed. The Council of Chief State School Officers (CCSSO) Technical Issues in Large-Scale Assessment (TILSA) staff can be helpful. The best example of evidence is a comprehensive test security handbook that integrates everything relevant to security. There are four elements: prevention, detection, remediation, and follow-up. Summaries of reports indicating what takes place in the state's departments and schools are part of security, as is evidence of monitoring and minimization of irregularities. Test administrators' and test coordinators' manuals must have information on security that focuses on state-required procedures before, during, and after test administration. Prevention of the illicit use of technology and devices must be documented.

Training materials are important, and the state should have specific training sessions on security. Evidence is needed on who was trained and the secure use of test accommodations. This requires extensive communication with LEAs on the part of the state.

For detection, the state implements analytical, formal procedures for web monitoring. We look for score gains and timing—how long it takes students to respond to questions.

Procedures for reporting irregularities must be stated in a response plan, along with procedures for remediation of incidents. Documentation is needed for strategies and guidelines, while respecting students' privacy. Procedures and policies apply to all assessment components. It should be noted whether testing took place with paper and pencil or a computer. The use of computers has introduced new concerns.

"Bad evidence" would be haphazard materials that miss details or omit entire aspects of test security. Look at the Guide and try to address each point. If you can't, indicate that you are working on it and present your plans for meeting requirements. Note that the key procedures were followed.

Critical Element 2.6: Systems for Protecting Data Integrity and Privacy (page 45)

Ms. June Zack said concerns have changed with the advent of computer-assisted assessment. The same points are valid, but they present in different ways. We must devise systems for protecting data integrity and student privacy. The site where the test was delivered is an element: Is the computer secure? Can students access other programs while they are testing? Is email open? The vendor can help; in some systems, when the test is on, the computer locks out access to anything else. Test administrators need to document the prevention measures used. Think about contingencies: What if the electricity goes off during the test? Will data be lost? Will the students have to retake the entire test? These are questions to ask the vendor. You must know what to do and communicate it to the field. What if a student gets sick during testing? On a computer, you may be able to pause the test, automatically saving the work without losing the data. You have to know what the vendor is supplying and how it works. Document the process and communicate it to all test administrators. All of this information should be in the peer review submission.

Here are some other areas to address and document: How are data stored? Are there firewalls? Are the data encrypted? If the data are encrypted, who has the key? Are student identification data maintained separately, or kept with the test scores? Are there other things in the server that might be used and corrupted? It's important to know how your data are stored, document it, and ensure that your data are encrypted and secure. For example, cell phone photos of questions have appeared on the Internet. Document protection measure in your peer review submission.

Communicate your decision-making processes, and document that this information has been shared and understood. Training at the vendor site is needed annually to ensure awareness of new developments.

Work with your vendor to examine all parts of your system and to document risks and procedures. Is transmission over the web possible? Is transmission secure? Is it safe? If data items are on the web, it's best that they remain on the testing site for the least amount of time possible to minimize the risk of hackers gaining access to students' private information.

Critical Element 4.7: Technical Analysis and Ongoing Maintenance (page 58)

Mr. Olson said the state and vendor must work together. The most important document related to testing is the technical report. Aspects to consider are as follows:

- Alignment;
- Validity studies;
- Scale "drift" (which is important if the same test has been used for years);
- Item exposure (e.g., via Facebook); and
- Subgroup performance.

The technical advisory committee (TAC) can provide advice on what you should be doing to maintain quality.

Mr. Nunez offered two tips:

1. Organize your materials by critical elements and be as detailed as possible. If you submit material that answers more than one question, be sure to specify which critical element(s) the material addresses.
2. Be sure to include correct page numbers.

Questions and Comments

- Mr. Rodman Heart, Oregon Department of Education, asked: What tools, resources, or checklists will be made available? These might be helpful resources. Ms. Peltier agreed that providing resources was a great idea. Mr. Nunez said ED posts specific outcomes for each state assessment peer review online at https://www2.ed.gov/admins/lead/account/nclbfinalassess/index.html. He will consult with Mr. Peasley and Ms. Spitz on the possibility of using the website for checklists as well.
- Mr. Brian Blake, Massachusetts Department of Education*,* asked: What is the minimum percentage for proficiency levels? What is needed to meet the requirement? Ms. Peltier said the Ethics Commission might have data suppression guidelines. Mr. Nunez said he would forward the question to Ms. Spitz.
- Ms. Katia Foret of Delaware asked*:* Does "trouble-shooting guide" mean the phone number of the help desk or suggestions for what to do in particular situations? Ms. Peltier responded that it would probably contain both.
- Mr. Jesse Markow asked: What are the best ways to prepare hybrid or consortium submissions? How do you present the information in the most helpful way? Mr. Nunez referred Mr. Markow to page 21 of the Guide. It spells out what is needed by critical element. Mr. Olson said none of the panelists had reviewed consortium admissions, but the same principles apply: The submission should be well organized, reviewed by the state, and understandable before it is submitted to peer reviewers. This is critical, whether the submission comes from a consortium, a state, or a hybrid. It is important to use the template, along with documentation and notes, because of the volume of pages submitted to peer reviewers. Ms. Zack added that evidence must be clearly labeled.
- Mr. Nunez invited participants to submit additional questions to him on index cards.