

**Association of Test Publishers**  
**ATP Security Initiative**

**Security Plan Guidelines**

**DRAFT –**  
Version 1.2  
January 24, 2007

## ***Introduction***

This document was developed as a result of the work completed by the Security Planning Team of the ATP Security Initiative, which began in February 2006. The *Security Plan Guidelines* document is meant to provide assistance for testing organizations who wish to develop a Test Security Plan. The document is a series of questions for testing organizations to discuss and consider as they create a test security plan.

The first phase of this project was to provide a draft document. Contributors to the plan include members from the Security Planning subcommittee. A good deal of gratitude goes to the following individuals for their thoughtful contributions.

Security Plan – Christy Faria, Cisco Systems (write), John Fremer, Caveon Test Security (review)

Roles and Responsibilities – Christy Faria, Cisco Systems (write and review)

Budget and Funding – Tancy Stanbery, BCEN (write ) Doug Bastianelli, NAPB (review)

Legal agreements – Ashok Sarathy, GMAC (write and review)

Test Design – Cristina Goodwin, Strategic Solutions Consortium (write) Ashok Sarathy, GMAC (review)

Test Development – Cristina Goodwin, Strategic Solutions Consortium (write ) John Fremer, Caveon Test Security (review)

Test Publication – Jamie Mulkey, Caveon Test Security (write and review)

Test Administration – Roger Meade, Prometric (write) Ashok Sarathy, GMAC (review)

Test Scores and Results – Ashok Sarathy GMAC (write and review)

Physical Security – Doug Bastianelli, NAPB (write) Joan Knapp, Knapp & Associates (review)

Internet and Media monitoring – Jamie Mulkey, Caveon Test Security

Security Training and Awareness – John Fremer, Caveon Test Security (write) Christy Faria, Cisco Systems (review)

Information Security – Jamie Mulkey, Caveon Test Security

Security Incident Response Planning – Doug Bastianelli, NAPB (write) Ashok Sarathy, GMAC (review)

Special thanks is given to Caveon Test Security for providing the Test Security Plan framework which helped this work to commence.

The second phase of this project will be to hand off this document to a subsequent committee who will refine the draft, send it out for comment, and

communicate its availability to the testing community. Work for these activities is anticipated for the 2007 calendar year.

Comments and questions regarding this document should be made to the Division-Chair for the Certification Licensure Division, in care of Lauren Scheib, [LscheibATP@aol.com](mailto:LscheibATP@aol.com).

## Table of Contents

I.	Security Plan .....	5
II.	Roles and Responsibilities .....	6
III.	Budget and Financing .....	8
IV.	Legal Agreements .....	9
V.	Test and Item Design.....	11
VI.	Item and Test Development.....	12
VII.	Test Publication .....	13
VIII.	Test Administration.....	14
IX.	Test Scores and Test Results .....	15
X.	Physical Security .....	16
XI.	Information Systems .....	17
XII.	Internet and Media Monitoring.....	18
XIII.	Security Training .....	19
XIV.	Security Incident Response Planning.....	20

## I. Security Plan

- A. Does the certification program have a comprehensive security plan? Are actions defined for security breaches? Does a written, complete Security Plan exist?
  
- B. Is there management buy-in of the Security Plan?
- C. Has the Security Plan been made available to specified stakeholders?
  - 1) Have you defined the stakeholders and their access to specific sections of the plan?
  - 2) Are stakeholders identified by their organizational relationships instead of by their names?
- D. Does the Security Plan contain all necessary process components?
  - (a) Have security goals for the organization been defined?
  - (b) Has the organization decided how to measure test security success?
  - (c) Have supporting documents, such as proctor manuals, and employee, test taker, vendor, and contractor agreements, been revised to be in congruence with the Security Plan?
  - (d) Does the organization have a plan for monitoring performance of individuals and security efforts?
  - (e) How, to whom, and how often will the organization report progress on test security efforts?
  - (f) Is there a path for the flow and storage of confidential and secure test taker and exam information?
  - (g) Is there a defined and documented escalation path for taking action when a security incident occurs?
  - (h) Is there consolidated secure storage with restricted access for confidential and secure data files and documents?
  - (i) On what schedule will the Security Plan be reviewed and, as applicable, modified?
  - (j) Has your organization identified and defined the types of security breaches it might encounter?
  - (k) Has your organization identified and defined appropriate consequences for security breaches at all levels?
  
- E. Does your organization have in place statistical analyses for identifying candidate test taking aberrance and irregularities? Do you analyze test taker data for the following circumstances:
  - 1) Cheating;
  - 2) Piracy [stealing questions];
  - 3) Proxy testing and coaching;

- 4) Volatile retakes, and
  - 5) Changes in item performance?
- F. Does the Security plan contain all necessary documented policies and procedures?
- (a) Has your organization defined the roles and responsibilities for test security?
  - (b) Is there an annual budget and funding for both existing and potential security-related activities?
  - (c) Are legal precautions and agreements in place for test takers, Subject Matter Experts (SMEs), test delivery providers, contractors, suppliers, vendors, employees, and proctors?
  - (d) How has security been factored into the test and item design processes?
  - (e) What kind of security training program has been developed for those involved in developing and maintaining items and tests?
  - (f) What security precautions are in place for electronic and/or paper-based test publication?
  - (g) Do your test administration procedures include the security precautions test administrators should implement and provide them with a convenient method to report testing irregularities?
  - (h) How does your organization protect the confidentiality of test scores and results?
  - (i) How does your organization assure the security of data and information?
  - (j) Has your organization designed a process for Web and Media Monitoring?
  - (k) Is there a Security Awareness and Training program for all employees/SMEs/vendors/contractors?
  - (l) Does your organization have a documented Security Incident Response Plan?

## **II. Roles and Responsibilities**

- A. Are the security roles adequately described and the responsibilities covered?
- B. Has one person been given responsibility for the overall management of the security plan and the authority to apply and update these policies and procedures?
- C. Has security training been developed and delivered to all employees with test security responsibilities?

- D. Has responsibility been assigned for Web site research?
- 1) Are grey market Web sites monitored for IP content?
  - 2) Is there regular monitoring of online Auction Web sites [e.g. eBay, Amazon, Yahoo]?
  - 3) Is there a procedure and a budget in place to order and review suspect exam content, as needed?
  - 4) Is there a documented process for IP verification and escalations?
  - 5) Is there a process for tracking security violations?
- E. Has responsibility been assigned for enforcing security and infringement sanctions, as follows?
- 1) Is there a process to identify, track, and report test center activity?
    - (a) Are new security/enforcement initiative(s) formulated, as needed?
    - (b) Are the TDP test center and company policy and procedures reviewed and monitored for compliance with the TDP SOW requirements?
    - (c) Is there a process for initiating internal [e.g., Global Investigations] or TDP investigation(s) of suspect test center(s), when needed?
    - (d) Has test site misconduct been defined clearly in terms of both test takers and test administrators?
    - (e) Is there a formal liaison with legal counsel regarding program approvals and new policy inclusions?
  - 2) Has responsibility been assigned for identifying, tracking, and reporting candidate misconduct and for enforcing sanctions? Are there documented procedures in place to deal with:
    - (a) Credit Card Fraud;
    - (b) Using unauthorized notes, etc.;
    - (c) Using surveillance devices;
    - (d) Violating the retake policy, if applicable;
    - (e) Colluding with test site administrators;
    - (f) Identity fraud;
    - (g) Proxy testing;
    - (h) Score report, certification certificate fraud, and
    - (i) Testing under multiple test records?
  - 3) Are trademark and copyright protections [IP Policy Guidelines] in place?
  - 4) Has an exam copyright registration process [Certs, CCIE, Networking Academy] been implemented?

- 5) Is there a documented process for handling reports detecting aberrant test center or candidate behavior?
  - 6) Has responsibility been assigned for the security budget?
- F. Has responsibility been assigned for a security plan and coordination of the following security activities:
- 1) Creating new documents and regularly updating Security Enforcement program content
  - 2) Facilitating monthly Enforcement program manager meeting; tracking action items on agenda for completion
  - 3) Delegating responsibility to one individual in each functional group for security training and management
  - 4) Ensuring proper transfer of files among test vendor organizations
  - 5) Reviewing and approving TDP process and procedure for storage and transfer of exam content
  - 6) Identifying job descriptions that need to incorporate security-related responsibilities
  - 7) Assigning back-up responsibilities to oversee security to other personnel
  - 8) Ensuring that security policies are reflected in training materials and activities, and in job descriptions, job performance criteria, and other personnel guidelines
  - 9) Providing training so that all individuals understand their roles and responsibilities vis-à-vis security
  - 10) Providing all individuals with an up-to-date security manual (or with the portion that applies to them) that describes the security procedures for which they are responsible.

### **III. Budget and Financing**

- A. Is there a sufficient annual security budget and funding for the remediation of security breaches and for subsequent legal actions?
- B. Does the business plan for the new or upgraded certification include the need for security planning and its relative costs, including the
- 1) Development of security policies,
  - 2) Development of security manual, and
  - 3) Staffing/Workload analysis?
- C. Does your budget justification include the expected ROI from the:
- 1) Avoidance of unplanned item and test development;
  - 2) Results of Internet monitoring for test fraud and theft;
  - 3) Maintenance of program goodwill and reputation;

- 4) Cost and frequency of security incident response, and
  - 5) Confidence of stakeholders in the test results?
- D. Do your contracts with your test development and test delivery providers specify who will be fiscally responsible for various types of security breaches (before, during, and after exam development and delivery)?
- E. Does your legal budget include funding for assistance in identifying the responsibility for security breaches and in obtaining funding for remediation of security breaches?
- F. Does your operating budget include funding for responding to security breaches?
- G. Have you budgeted for the development of additional test form(s) in the event of a serious security breach?
- H. Does your budget consider the need for funds to keep pace with program growth and changes, as well as emerging security issues?
- I. Do your operating and capital budgets include financial projections for physical security needs, such as:
- 1) Safe(s), vaults, locked, limited-access storage,
  - 2) Separate lockable room for exam reviews,
  - 3) Controlled access to building, secure work areas, offices, and
  - 4) Equipment, such as additional computer(s), servers?

#### **IV. Legal Agreements**

- A. Have confidentiality and conflict of interest agreements with employees and contractors been executed properly?
- 1) Does your organization have a code of conduct that reflects its ethical and lawful business practices?
  - 2) Have employees and contractors agreed to this code of conduct with signature?
  - 3) How is compliance with this code of conduct tracked?
  - 4) Does your organization have a security awareness and education strategy to inform all employees/contractors of security issues no matter what their role?
  - 5) Does your organization have policies regarding access to extremely sensitive information (such as items, exams, and test taker data)?
  - 6) Have employees, contractors, and vendors who have access to sensitive information agreed to an Information Security Policy and signed a non-disclosure agreement?
  - 7) How is compliance to the Information Security Policy and non-disclosure agreement tracked?

- 8) Do your agreements with vendors and contractors include the provision to allow announced and/or unannounced security audits at their sites?
- 9) Does your organization provide appropriate training to personnel who have access to confidential data and the systems' infrastructure?
- 10) Does your organization have a set of policies and procedures about employee's and contractor's conduct to prevent cheating and the theft of questions, as well as to maintain confidentiality and security of information and safety of equipment at the test centers?
- 11) Do your employees and contractors agree with signature to these policies and procedures?
- 12) How do you track compliance to these procedures?
- 13) Are policies and procedures reviewed periodically? If updates are made to the policies, do employees and contractors have to re-certify to the new policies and procedures?
- 14) What controls are in place to ensure the return of equipment and removal of access rights when an employee or contractor severs ties with the organization?
- 15) If original agreements span a timeframe beyond the employee's or contractor's relationship with the organization, are those agreements tracked?

**B. Test Takers**

- 1) Does your organization have a code of conduct that reflects its ethical and lawful business practices for test takers?
- 2) Have test takers agreed to this code of conduct with signature?
- 3) How is compliance with this code of conduct tracked?
- 4) Does your organization have a security awareness and education strategy to inform all test takers of security issues no matter what their role?
- 5) Does your organization require test takers to report testing irregularities that they observe?

**C. Test Administrators/Proctors**

- 1) Do your agreements with test administrators and proctors prohibit their involvement in preparing or publishing test preparation materials, and delivering training or instruction in the exam?
- 2) Do the agreements require the test administrators to:
  - (a) Safeguard exam materials and information;
  - (b) Manage security compromise incidents as directed;
  - (c) Allow unannounced reviews of test security operations, and
  - (d) Provide regular reports on all test security operations?
- 3) Item Writers and Reviewers
- 4) Do item writers and reviewers sign a formal agreement requiring that they abide by the security provisions defined by your organization?

- 5) Does the agreement prohibit writers and reviewers from disclosing their role in item and test development, developing test preparation materials, and delivering training/instruction in the exam?
- 6) Does the agreement assign all proprietary rights and interests in exam materials and information to your organization and prohibit writers and reviewers from disclosing exam materials to any individual or organization?

## V. Test and Item Design

### A. Are certification tests and items protected by design?

- 1) Is it feasible to require randomization of items and answer options during exam delivery?
- 2) Are you able to create multiple forms of the exam and item clones that are similar in construct but dissimilar in inconsequential variables?
- 3) Can you clone each original exam form?
- 4) For paper and pencil exams, are you using printing strategies that scramble items within a form to mimic multiple forms?

### B. Selected-Response Items

- 1) Are selected-response items written with strategies for protecting content in mind?
- 2) Are novel materials being used to test higher-level concepts? Are you paraphrasing textbook language or the language used during instruction to avoid testing for simple recall?
- 3) Are you avoiding overly specific and overly general content?
- 4) Are you able to find a good blend of being specific enough to make the item meaningful yet complex enough to assess the construct of interest without introducing construct-irrelevant variance?
- 5) Is the item stem worded positively, avoiding negatives such as NOT or EXCEPT?
  - (a) If negatives are used, are they used sparingly and does the word always appear capitalized and in boldface?
- 6) Are less-memorable items being created by using longer item stems?
- 7) Are all the item distractors that are created for an item plausible ones?
- 8) Are you able to create multiple-response multiple-choice items? Items that require selecting all the options that apply will probably be more difficult to memorize than items with a single correct answer.
- 9) Are you able to incorporate brief scenarios or situations about which multiple questions can be asked? A scenario has the dual advantage

of providing a context or “situation” that the examinee must evaluate to answer one or more questions, while also providing much more information that pirates must memorize.

#### C. Computer-Based Selected-Response Items

- 1) Are computer-based selected-response items written with strategies for protecting content in mind?
- 2) Are drag-and-drop (or matching) items appropriate for your test?
- 3) Are sequencing items appropriate for your test? These items provide a jumbled list of tasks that the examinee must place in the sequence in which they must be completed in order to result in a correct outcome.
- 4) Are hotspot items appropriate for your test? These items may use images, diagrams, computer application interface components, or similar elements. The examinee must identify a feature or an area within the image, diagram, or interface by clicking on it.
- 5) Are you taking advantage of technology to develop new item types?
- 6) Are items and answer options randomized during exam delivery?

#### D. Performance Items

- 1) Are performance items written with strategies for protecting content in mind?
- 2) Are simulations appropriate for your test? : A simulation represents an actual environment, including tools or components that provide sensory feedback. Candidates demonstrate skills by manipulating the abstract representation of the environment, preferably using the same response modality as is required in the real world. To fulfill the definition of a simulation, the system must be able to respond to candidate input following multiple, not necessarily correct, actions. Typically, only targeted features of the environment are represented.
- 3) Are you able to test in a virtual environment? Candidates interact with a computer-based realistic virtual scenario, which could consist of anything from a feature about a piece of equipment to a complex system, in a manner that is representative of the real-world performance being evaluated. (Examples: software simulation that mimics a targeted feature set found in the actual software application; a personal computer-based representation of a nuclear reactor control panel.)
- 4) Are you able to conduct machine-scored or human scored live testing? Live testing uses a real-world environment and actual equipment to assess examinees’ ability to achieve an outcome.

## VI. Item and Test Development

- A. During item development and on-going maintenance, are the items and test results protected from unauthorized access?

- 1) Is item banking treated as a component of test security?
- 2) Is access to the item bank restricted and tracked?
- 3) Are changes to items recorded along with information about who made the change and when?
- 4) Does the item bank carry additional information regarding the use of the items (i.e., on which tests did the item appear, what is the exposure, item statistics, etc.)?
- 5) Does your organization have documented procedures for protecting the security of both soft and hard copies of items from development through disposal?
- 6) Do you prohibit including exam items in or attaching them to e-mail messages?
- 7) Do employees and contractor sign an acknowledgement indicating that exam development materials they have received have been returned and destroyed upon completion of a project?
- 8) Are multiple forms or pools of exams available to reduce over exposure?
- 9) Are there processes in place to detect the effect of exposure on both items and test forms?
- 10) Is there a plan in place to replace items and test forms when pre-determined exposure criteria are reached or when there is a security breach?
- 11) When beta testing items, are they seeded into operational forms?
- 12) When beta testing entire exam forms, are instructors, trainers, individuals associated with the creation and publication of exam preparation materials, and anyone previously banned from testing excluded from participation?

## **VII. Test Publication**

- A. How is test content protected during test publication and distribution?
  - 1) Is a secure process in place for transferring files to the TDP or test printer?
    - (a) Is a secure file transfer protocol used?
    - (b) Are the files sent encrypted?
  - 2) For test booklets, what measures are in place at the printer to assure the security of the test materials?
    - (a) Is the print vendor you are using licensed and bonded?
    - (b) Are booklets and test forms shipped using a bonded shipper?
    - (c) Are two individuals required to open the shipping container and count the appropriate number of exam booklets and forms received?
    - (d) Is the same procedure followed when the booklets and forms are shipped back?
- B. What remediation is planned for in the case of a security breach?

## VIII. Test Administration

### A. Security Procedures and Training

- 1) During test administration, are there adequate security procedures in place?
- 2) Do the test administration directions include sufficient information about security procedures, proctor responsibilities, and reporting mechanisms in the event of a problem on test day?
- 3) Do test site administrators and proctors receive training at least annually on security procedures?
- 4) Are the requirements for admission to the exam (e.g., identification documents, admission tickets) clearly described in the testing directions, the candidate information brochure, and ticket of admission?

### B. Before Testing

- 1) Are candidates without proper identification denied entry to the exam?
- 2) Are candidates required to sign-in before being admitted to testing?
- 3) Does the proctor match the signature on the candidate's identification to the sign-in signature?
- 4) Is there enough space for examinees to be seated well apart from one another or are there privacy panels between individual workspaces?
- 5) Are exam booklets and answer sheets stored in a locked cabinet, accessible only by authorized personnel, until the administration of the exam?
- 6) Are proctors instructed to remove or cover charts, posters, or other materials in the testing environment that might be sources for examination answers?

### C. During Testing

- 1) Are examinees continuously monitored throughout exam administration by trained proctors?
- 2) If a test administrator must leave the room, or is otherwise disengaged from directly monitoring examinees, is a proctor assigned immediately so that examinees are never left alone?
- 3) Are computer-based exams accessed only during the time of exam administration?
- 4) Is access to login information limited to the test administrator?
- 5) Have measures been instituted to control the possession and use of authorized and unauthorized materials by examinees?

- 6) Are bags/purses, books, papers, pagers, cell phones, calculators, and any electronic device that can be used to capture/record exam content prohibited from the testing room?
- 7) Is the proctor required to create a seating chart of all individuals being tested for that session and return it upon request?

D. After Testing

- 1) Do instructions for test administrators clearly describe what must be accounted for and returned after testing, and by when?
- 2) Are test administrators instructed to file detailed reports describing candidate misconduct such as candidate disruptions, observations of copying, discussing exam questions with other test takers, and use of unauthorized materials?
- 3) Are test administrators expected to report in detail:
  - (a) Missing, lost, or stolen exam materials; such as test booklets, answer sheets, and other confidential exam information?
  - (b) testing location disruptions, including but not limited to:
    - (i) lapses in monitoring/proctoring,
    - (ii) outside distracting noises
    - (iii) distracting activities or noise from candidates within the testing environment?

## IX. Test Scores and Test Results

- A. Are test scores and other results (i.e., candidate, site, proctor demographic information) protected during transmission between temporary and permanent storage sites, and while stored?
- B. Does your organization have an information security policy that describes a data classification matrix (restricted, confidential, public)? If so, how does your organization classify test scores and test results and other personally identifiable information?
  - 1) Has your organization mapped out the data flows surrounding sensitive information throughout every stage of the testing process (from registration to score reporting)?
  - 2) Does your organization have a secure network to protect such data flows?
  - 3) Do you have documentation of the logical layout of the network? Is an accurate inventory of the network and its components maintained? Has the location, responsibility, network connection, and exceptional behavior of every component of the network been accurately identified?

- 4) Have your network points been configured to resist denial of service attacks? Are the network components routinely checked to ensure that any known vulnerabilities have been eliminated?
- 5) Are temporary storage media kept in secure locations and accessible only to authorized personnel? Are temporary storage media disposed of securely when no longer required, using appropriate disposal facilities? When media is physically transported, what measures are in place to ensure the security of the information?
- 6) What physical and technology controls are in place to ensure the security of data throughout its transmission, storage, and retrieval?
- 7) How are the connection services (through which the data are transmitted) protected from unauthorized access?
- 8) How is access to sensitive data (such as test results and scores) controlled through user accounts and the management of such users? How are the integrity, confidentiality, and availability of such data preserved at all times?
- 9) Do users have unique and confidential account identifiers and passwords with which to access sensitive data (such as test results and scores)? What systems and rules are in place to enforce password complexity to protect the security of the data?
- 10) Which personnel in the organization have administrative access to production systems and applications? How is this privilege controlled?
- 11) What controls are in place to govern access between internal and external networks? Is zoning a feature that is ever considered while housing production systems? Do you have restricted zones to isolate primary application and database servers that store sensitive customer, test scores, and results data?
- 12) Does your organization have a policy about remote access and wireless access to secure and sensitive data?
- 13) Does your organization have a defined access control policy that clearly highlights logical access to information within data systems? Are data systems logically partitioned, configured, and locked down to prevent unauthorized access?

## **X. Physical Security**

- A. The physical location(s) where test items are developed and stored must be secure at all times. At each point in the process up through delivery of an examination, each test item should be able to be accounted for at any time.
- B. Depending on the sensitivity of the content, (e.g. a state licensure examination vs. a small practice exam with items removed from the examination item bank), you may want to evaluate the following:
  - 1) Onsite facilities

- (a) Is it possible to house your exam content in only one location?
- (b) Do you have a system for tracking visitors in your facilities?
- (c) Do you limit the number of staff that has access to secure test materials?
- (d) Do you have an additional secured room/area in your offices if you are unable to secure your facility completely (e.g. you share office space or are in a large multi-tenant building)?
- (e) Should you have additional monitoring (e.g. video) in the content storage area?
- (f) Can you verify which staff members handled test materials and when? Is there a check-out and check-in system used when accessing hard copy of secure materials?
- (g) Has one person been assigned primary responsibility for the secure storage area?
- (h) Can you identify exactly who currently is allowed access to your testing materials?
- (i) Is there a secure process for disposing of hard copy of items, tests, data files?

#### C. Offsite Content Creation/Review

- 1) Are there standard procedures and formats for securely transporting examination content off-site for item writing and reviews?
  - (a) Is material sent by a secure, verifiable, delivery service?
- 2) Does the offsite location (e.g., hotel, convention center) have secure storage that staff may use for the duration of the meeting/session?
- 3) Can a room/storage area be supplied to which only testing staff have the key/access?
- 4) Are item writers and reviewers trained on test security requirements prior to being given access to secure materials?
- 5) Are hard copies of item review materials numbered, signed for by the reviewer, and accounted for before reviewers are dismissed?
- 6) Is a staff member always in the room with secure materials?

## **XI. Information Systems**

- A. Is the program information (test scores, item answers, candidate information, etc.) secure from hackers and other unauthorized access?
  
- B. Does the organization support the seven principles of Access Control and Data Exchange?
  - 1) Data Classification
  - 2) User Access Management
  - 3) Privilege Management
  - 4) Password Management
  - 5) Intellectual Property Protection

- 6) Personal Data Privacy
  - 7) Data Flows
  - 8) Data Exchange
  - 9) Cryptographic Controls
- C. Is there limited access to test files to only those personnel who need to use them?
  - D. Are passwords changed on a routine basis?
  - E. When an individual leaves the organization, is there access to systems terminated?
  - F. Are systems that contain test and candidate data records routinely backed up?
    - 1) Nightly?
    - 2) Are systems backed up to tape which is taken offsite for archival?
    - 3) Are archives kept in a locked, fireproof location?
  - G. Is a business continuity plan in place?

## **XII. Internet and Media Monitoring**

- A. Does the program monitor the Internet and other media (such as test preparation materials) for disclosure of test content?
- B. Frequency and Type of Searches
  - 1) How often will searches be conducted?
  - 2) Who will conduct the searches?
  - 3) What kinds of sites (Web sites, discussion forums, braindump sites, auction sites, search engines, and other publicly accessible Internet venues where stolen exam content may be shared or sold) will be checked?
  - 4) What will you be searching for (print and computer-based “exam prep” materials such as books, guides, and practice exams)?
  - 5) Do you acquire and analyze print and computer-based “exam prep” materials such as books, guides, and practice exams immediately upon publication?
- C. Categorizing Sites
  - 1) Will sites be rated according to an estimate of the probable risk posed to the program (High, Medium, Low), based on the similarity of content to actual exam content?
  - 2) Will ownership, contact, publication, and distribution information (if available) for each identified source of actual or potential exam disclosure (“Source”), as well as IP address, hosting, and legal agent information be collected for Internet-based sources?
  - 3) Who will determine if content is being shared or sold commercially and for what price?

- 4) What kind of training will be provided to ensure that monitoring activities are comprehensive, thorough and produce actionable information?
- 5) Once identified, will each Source be saved or “cached” to preserve evidence for comparative analysis and other follow-up activities?

#### D. Resolution of Infringing Sites

##### 1) Notification of Sites/Level of Notice

- (a) Does your organization have a process for issuing cease and desist notices to individuals, organizations, Web sites, ISPs, and E-commerce engines that are publishing your secure exam material?
- (b) Does your organization send notices authorized by the Digital Millennium Copyright Act requesting that Internet hosting organizations, search engines, and auction operators remove or “takedown” offending Web site material?
- (c) Will your organization institute legal action to obtain damages or injunctions?

##### 2) Other resolutions

- (a) Will your organization implement sanctions for candidates who use those sites?
- (b) Will your organization publish information about the disclosure of secure materials and its response to that disclosure? If yes, then where will it be published, e.g., the organization’s Web site, in newsletters, or in industry publications?

### **XIII. Security Training**

- A. Has your organization developed appropriate training materials predicated on its security standards and the APA/NCME/AERA [Standards for Educational and Psychological Testing](#)?
- B. Does your organization provide test security training, including security responsibilities associated with each program regular staff position, to all personnel, contractors, and suppliers involved in exam development, exam publication, exam administration, and exam data management?
- C. How often are individuals in the organization trained/retrained on security procedures?
- D. When traveling with secure material, are employees, contractors, and others instructed not to check it in checked luggage but to either put it in carryon luggage or FedEx it to its destination?
- E. When working in public places such as airports or hotel lobbies, are employees, contractors, and others instructed not to divulge the nature of the secure material they are working on and not to work on secure material where unauthorized people might read it?

- F. Are security procedures revised and updated on a regular basis, and especially when there are changes in a testing program?
- G. Does your organization hold informal meetings or “brown bag” lunches to create and maintain an appreciation of the importance of security and to review the latest security incidents?
- H. Is your organization staying up-to-date on evolving technologies that can be used for cheating and incorporating into your security training procedures to curb their use?
- I. Will absorption of training be verified by assessment?

#### **xiv. Security Incident Response Planning**

A security incident is when test content is handled in any manner inconsistent with the procedures for secure development or delivery of examination content. It can include, but is not limited to, accidental removal of content from a secure area, failure of content transmission electronically, or candidate misconduct at a testing site.

- A. Questions that should be asked:
  - 1) What are the test delivery provider’s (where applicable) procedures for documenting security incidents?
  - 2) Is there a documented process and timeframe for collecting information after a reported security breach?
  - 3) Are there clear guidelines for taking any punitive actions, such as cancelling a test score?
  - 4) What is the extent of the security breach? Just how much content do you suspect has been compromised?
  - 5) If content wasn’t stolen/transmitted to unauthorized users, can you retrieve the content?
  - 6) What is the compromised item bank/individual items worth monetarily?
  - 7) Have statements from witnesses and test administrators been confirmed?
  - 8) Has additional evidence been collected that corroborates or refutes the allegation?
  - 9) Have you collected background information on the alleged perpetrator (residence, criminal and educational history (as appropriate and allowable by law)?
  - 10) Can the security or test administration irregularity be confirmed by statistical analysis?
  - 11) Have you analyzed the data for patterns of individual and organized test fraud and theft by the test administrator?
  - 12) Does your organization investigate suspected candidates, employees, contractors, and proctors with unannounced visits, “secret shopping,” email surveillance, and other monitoring activities, as appropriate and legal?

- 13) Are there any other stakeholders, such as a state board, that must be informed of, or concur with, your decision on the candidate or test administrator?
- 14) Can you still deliver a valid and reliable examination or must you stop testing? (For example, pretest items still in development might not be as big a problem as the compromise of calibrated questions.)
- 15) Are there mechanisms to flag the candidate should he/she try to register for the examination again?
- 16) Is a Prohibited Candidate Registry kept of those who are permanently or temporarily ineligible for testing?
- 17) Are there defined consequences for proctors/test administrators who are involved in security breaches, and do the proctors and test administrators know what they are?
- 18) Is there a separate review panel that evaluates the evidence and the investigative report and recommends further action?
- 19) Does your organization have a documented appeals process for candidates?