U.S. Department of Transportation
Federal Motor Carrier Safety Administration

Physical Site Assessment

For National Registry Testing Organizations

Bunmi Ogunlade, CISSP, CISM, CAP
Information System Security Manager
Federal Motor Carrier Safety Administration (FMCSA)
June 11, 2012



Office of Research and Information Technology

CONTENT

1. National Registry Program Overview
2. Purpose of Physical Site Assessment
3. Who is a Medical Examiner?
4. Who are Testing Organizations?
5. Security Requirement for Testing Organization
6. Roles and Responsibilities
7. Standard of Assessment
8. Physical Site Assessment Process
9. Assessment Methodology
10. Assessment Report
11. References
12. Questions and Answers

National Registry Program Overview

Background

Mission and goals of Federal Motor Carrier Safety Administration (FMCSA) is to reduce crashes, injuries and fatalities involving commercial motor vehicles.

FMCSA developed National Registry program to improve highway safety and driver health by requiring that medical examiners be trained and certified so they can determine effectively whether a CMV driver's medical fitness for duty meets FMCSA's standards.

Purpose of Physical Site Assessment

Assessment of Testing Organizations

- **FMCSA needs assurance that its information (in digital or non-digital form) and that of the MEs who are being tested at the site are securely received, processed and maintained at the testing facility.**
- **For compliance with:**
  - Privacy Act of 1974, and
  - Federal Information Security Management Act (FISMA) of 2002

Who is a Medical Examiner?

Medical Examiners (ME)

Certified Medical Examiners are individuals that conduct physical examinations required for interstate commercial motor vehicle (CMV) drivers.

49 CFR 390.5, Medical Examiners must be licensed, certified, or registered in accordance with applicable State laws and regulations to perform physical examinations.

- **Prospective MEs must meet the following criteria to qualify**
  1. Participate in required training
  2. Conduct test at Certified Testing Organization
- **Once certified, MEs contact information will be publicly available to CMV drivers**

Who are Testing Organizations (TOs)?

Certification of Testing Organizations

Testing Organizations are companies that deliver FMCSA medical examiner certification test to Medical Examiners.

- **Prospective or viable Testing Organization must meet FMCSA Security and Privacy requirement.**
  - Physical site assessment will be carried out by FMCSA Designated Representatives
  - FMCSA Designated Representative/Assessor will schedule a physical site assessment with the Testing Organization once FMCSA has determined that the organization is a viable TO.
- **Once certified, testing organization contact information will be publicly available to MEs**

Security Requirement for Testing Organizations

Testing Organization must meet the following criteria:

(a) The testing organization has documented policies and procedures that:

(1) Use secure protocols to access, process, store, and transmit all test items, test forms, test data, and candidate information and ensure access by authorized personnel only.

(2) Ensure testing environments are reasonably comfortable and have minimal distractions.

(3) Prevent to the greatest extent practicable the opportunity for a test taker to attain a passing score by fraudulent means.

(4) Ensure that test center staff who interact with and proctor examinees or provide technical support have completed formal training, demonstrate competency, and are monitored periodically for quality assurance in testing procedures.

(5) Accommodate testing of individuals with disabilities or impairments to minimize the effect of the disabilities or impairments while maintaining the security of the test and data.

Security Requirement for Testing Organizations cont'd.

Testing Organization must meet the following criteria:

(b) Testing organizations that offer testing of examinees not at locations that are operated and staffed by the organizations but by means of remote, computer-based systems must, in addition to the requirements of paragraph (a) of this section, ensure that such systems:

(1) Provide a means to authenticate the identity of the person taking the test.

(2) Provide a means for the testing organization to monitor the activity of the person taking the test.

(3) Do not allow the person taking the test to reproduce or record the contents of the test by any means.

Roles and Responsibilities

FMCSA's Role

- **FMCSA will review, audit and monitor performance of medical examiners, testing organizations, and drivers.**

Designated Representative/Assessor

- **This group of people is task to conduct physical site assessment on 8 <u>VIABLE</u> Testing Organizations behalf of FMCSA.**

Standard of Assessment

Assessment Standard

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 3, "*Recommended Security Controls for Federal Information Systems and Organizations".*

Physical Site Assessment Process

Physical Site Assessment Process

- **FMCSA Designated Representative or Assessor will schedule site assessment with viable TO.**
- **FMCSA Designated Representative will make physical site assessment checklist available to TO prior to site visit.**
- **Assessment will take between 4 to 6 hours.**
- **Assessor will prepare an Site Assessment Report for approval.**

Assessment Methodology

1. Visual Inspection or Walkthrough

- **Assessor should be escorted through the site to include at minimum:**
  - Entrance and Exit Areas
  - Testing Areas
  - Areas where Test related material is collected, processed and/or stored
    - Cabinets
    - Working areas of personnel who handles this information (cubicles, and/or offices)
  - Emergency Exit Route
  - Fire Suppression Agents (e.g. water sprinklers, fire extinguishers, fire hoses/connection)
  - Fire Alarms
  - Heating, Ventilation, and Air Conditioning (HVAC)
  - Emergency Lights
  - Alternate Power Source (e.g. generator, uninterruptible power supply)
  - Monitoring devices (e.g. cameras, intrusion detection mechanisms)
  - Media Disposal/Sanitization Mechanisms (e.g. shredders or secure console bins)
    - Media includes for example CDs, DVDs, paper, etc.
    - Check if personally identifiable information (PII) is protected at rest

Assessment Methodology cont'd

2. Interviews

- **Assessor will need to at least interview the following persons or a designate:**
  - Receptionist/Person who is stationed in the entrance area
  - Human Resource Representative
  - Testing Coordinator
  - Facilities/Property Management Representative
  - IT Personnel responsible for maintenance activities on testing computers
  - Person responsible for real-time monitoring of cameras in testing area

Assessment Methodology

3. Documentation Review

- **Assessor would need to review documentation to include at minimum:**
  - Visitor Access Record
  - Key Log
  - Maintenance Log (of testing computers)
  - Certificate of Destruction (if 3rd party document shredding company used)
  - Sections of Tenant/Facilities Handbook or related document that outlines how the following is maintained:
    - Fire Suppression Agents, Building /Office Access, Office Security
  - Security Policy
  - Personnel Policy (or related document)
    - Personnel Screening (background checks)
    - Personnel Transfer and Termination
  - Privacy Policy (or related document)

Assessment Report

Assessment Report

- Assessor will prepare a Physical Site Assessment Report to FMCSA Security Office for review
- Assessor will notify TO any deficiency found during the assessment.
- FMCSA security office will review the report and recommend for approval or denial within 3 weeks.
- TO will develop a plan (POA&M) to mitigate all findings
- Assessor will revalidate the mitigation which may require another site visit if evidence of mitigation can not be produced .

References

- Public Law (Pub. L.)109-59, *The Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (SAFETEA-LU)*, August 2005
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*
- Pub. L. 93-579, *Privacy Act* of 1974
- Title III of the E-Government Act of 2002 (Pub. L. 107-347, 116 Stat. 2899, *Federal Information Security Management Act (FISMA)* of 2002

Questions and Answers

QUESTIONS?