Define & Assess Skills - Smart Grid Security Specialists

SANS 2011 North American SCADA & Process Control Summit

Michael Assante
President & CEO
NBISE
michae.assante@nbise.org
208-557-8026
Cyber Security: People and Technology

- Ever-changing threats: Automated systems will always be a step behind
- Must develop front-line defenders in the public and private sectors
- Highly-complex issues require professionals with a demonstrated level of hands-on competence, performance, and intuition
- Professionals and their organizations will benefit from competency definition and skill measurement
National Board of Information Security

Mission Statement

To increase the security of information networks, computing systems, and industrial and military technology by improving the potential and performance of the cybersecurity workforce.

- Non-profits formed in June 2010, structured as a 501(c)(3) research institute and a 501(c)(6) certifications organization
- Working to identify the roles and individuals needed to secure our nation from attack
  - Competency model development, rigorous examinations, and valuable certification programs
  - Provide material to training providers, but do not conduct training
### Job Task & Competency Analysis

**Define the Job**
- What does a successful professional need to know and do?
- What methods and tools must she be familiar with?
- What defines successful performance?
- How should the job be segmented into specialties & tasks?

### Determine Scope of Measurement

**Define What Should be Measured**
- What kinds of exercises will best demonstrate a candidate’s knowledge, skills, and abilities?
- How can we best measure performance in these exercises?
- What is the appropriate level of breadth and depth for an examination?
- What areas should be weighted?

### Create & Validate Measurement

**Create the Measurement Tool**
- What specific questions should be asked?
- Is the examination statistically valid?
- Do test takers perform consistently?
- Do hands-on tasks reflect current practices?

---

NBISE defines the jobs and competency measurement tools, and makes information available to training organizations. We do not conduct training ourselves.
What is a competency?

- **Knowledge** (understanding of strategy or procedure)
- **Skills** (consistency of performance)
- **Ability** (transfer across domains)

- **Narrow** to **Broad**
- **Shallow** to **Deep**
- **Consistent** to **Inconsistent**

- **Novice**
- **Apprentice**
- **Journeyman**
- **Master**
Smart Grid Cyber Security Specialist Project
DOE Funded Smart Grid Cyber Security Specialist

- Development team forming: PNNL & NBISE
- Conduct a comprehensive job analysis necessary to guide aptitude testing, instructional design, certification, performance evaluation, and electronic performance support of security specialists.
- This analysis will detail the knowledge, skills and abilities required to perform the job, while providing tools or guidance necessary to manage the stages of maturation through which security specialists progress from applicant to trainee to mastery of the subject matter.
Potential Performance Realization Framework

Skill Measurement & Development

Performance exam development
Proficiency Assessment Development
Critical Incident Analysis
Exploratory factor analysis
Job Analysis Questionnaire
Competency Model
Job Definition
Individual Development Plan

Organizational Benefits

Ground Truth
Proficiency Ratings
Team Challenge Modules
Collaborative Learning Modules
Scenario Modules
Use Cases
Team Scoring
Performance Evaluation
Proficiency Ratings
Team Profiles
Best Practices
Use Cases

Individual Benefits

K.S.A.M.
Proficiency Ratings
Exercise Modules
Test Modules
Problem-based Learning Modules
Scored Exams
Best Practices
Use Cases
Skill Profiles
Training Syllabus
Individual Development Plan
Best Practices
Misuse Cases
Training Syllabus
Misuse Cases

Goals: Skill-Focused Utility Program

- Recruitment – Knowing what to look for and where
- Assessment – Knowing where you are (individual & Organization)
- Development – Knowing how to and how well you have developed the skills needed to be successful
- Sustainment – Knowing how to maintain ground-truth currency, developing job families tied to incentives, and maneuvering individuals up career ladders/paths
- Recognition – Identifying & recognizing individuals who have obtained expertise in valued competencies
# Project Phases

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I - Competency Analysis Study</td>
<td>Determining the full and complete set of cyber security skills needed for the Smart Grid Security Specialists to do their job effectively.</td>
</tr>
<tr>
<td>II - Critical Incident Analysis</td>
<td>The skills identified in Phase 1 of the Competency Analysis Study will be analyzed in this phase. The analysis process will examine significant events associated with exemplary success or failure by Smart Grid Specialist in performing their job duties.</td>
</tr>
<tr>
<td>III - Performance Analysis, Final Report, Recommendations</td>
<td>This phase will refine data gathered and analyze performance of the Smart Grid Specialists capabilities based on indicators of expertise. Results from traditional methods of assessment will be compared to results gathered using newer approaches to measure the strategy and consistency of task performance.</td>
</tr>
</tbody>
</table>
Key Tasks for Phase 1

- Establish a task force of subject matter experts from industry for competency model development
- Conduct literature review, research and interviews to generate a job description report
- Interview task force members for job competency analysis survey
- Develop job analysis survey and pilot
- Develop final survey based on pilot results
- Administer survey to Smart Grid Cyber Security Spec
- Analyze survey results and present findings
Project Progress

- Project work plan established
- Project research team identified
- Looking for domain experts to help develop the Job Task & Competency Analysis
- Recruiting participants in March 2011

smartgrid@nbise.org
Other Projects
Aptitude Exams: Measuring Skill

Part A. Paper-based

- Challenges
- Required Knowledge & Critical Skills Assessment
- Knowledge A.
- Knowledge B.
- Knowledge C.

Part B. Performance-based

- "Hands-on Simulation"
- Tools
- Applied Knowledge
- Methods

Measure of Knowledge, Skills, Abilities and Potential
Hands-on Performance Exams

- Operational Security and Penetration Testing
  - Partnership with CREST and CESG in the U.K.
  - Piloted in US from Nov-Jan
  - Intermediate & Expert performance-based exams
  - Released in April 2011

- Network Intrusion Analysis, Host Malware Analysis, Malware Reverse Engineering
  - CREST and CPNI are looking for a U.S. partner – NBISE seeking funding to pursue

Use developments in cognitive science to identify mature and nascent talent in cyber security professionals, incorporating knowledge of current “ground truths” into competency and certification.
Contact Information

Michael Assante
Chief Executive Officer
michael.assante@nbise.org
208.557.8026

David Tobey
Chief Scientist
david.tobey@nbise.org
540.860.9172

Kelly Ziegler
Chief Operating Officer
kelly.ziegler@nbise.org
973.766.3276