Operationally Focused CYBER Training Framework
Agenda

• DISA Cyber Workforce Training Vision
• Basic Tenets
• Role-based Educational/Assessment implementation plan
• Documentation & Product Development
• Examples
• Related DoD Initiatives
• Way Ahead
Establish a robust workforce training and certification program that will better prepare DoD cyber warriors to operate and defend our networks in an increasingly threat-based environment.
“Whether we do our cyber training at one school or at multiple schools, the training will have to be executed to one standard. I think that’s what we need to do so that the combatant commanders and the forces in the field know that whether they get a soldier, marine, airman or sailor, that person is trained to a standard and can accomplish the mission that is expected of them.” - GEN Keith Alexander
Basic Tenets

• Provide a “Training Strategy Roadmap” for Role-Based & Crew Certification
• Commercial certifications broader than what is often needed
• DISA can produce focused, relevant qualifications and certifications for our Cyber warriors
• Crew certification is a grouping of qualified Role-Based operators who obtain the desired effects necessary to defend and operate in cyberspace
• A “Cyber Defense Academy” will qualify role-based individuals to work effectively as part of crews and teams
• Joint Cyberspace Training & Certification Standard (JCT&CS) is the current baseline for work role definition
• National Initiative for Cybersecurity Education (NICE) will be baseline for Federal and DoD work role definitions
Role-Based Educational/Assessment Implementation Plan
## Joint Cyberspace Training and Certification Standards

**Joint Training Requirements**
- Procedures & Guidelines
- Individual, staff and collective tasks

**3 Lines of Operations**
- DGO
- DCO
- OCO

**Each Work Role**
- Associated Tasks
- Requisite
  - Knowledge
  - Skill
  - Abilities
- Proficiency Levels
  - Entry
  - Intermediate
  - Advance
- Training Products
  - Role Based
  - TTPS

### CYBER Roles

<table>
<thead>
<tr>
<th>CYBER Roles</th>
<th>Combat Element</th>
<th>Combat Support</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Administrator</strong></td>
<td>Technical Support Specialist</td>
<td>I &amp; W Analyst</td>
</tr>
<tr>
<td><strong>Systems Security Analyst</strong></td>
<td>Systems Test &amp; Eval Specialist</td>
<td>CND Analyst</td>
</tr>
<tr>
<td><strong>Network Operations Manager</strong></td>
<td>Knowledge Manager</td>
<td>Intel Analyst</td>
</tr>
<tr>
<td><strong>CND Incident Responder</strong></td>
<td>Data Administrator</td>
<td>CND Forensic Analyst</td>
</tr>
<tr>
<td><strong>Cyber Security/ IS Professional</strong></td>
<td>System Requirements Plan</td>
<td>Endpoint Exploit Analyst</td>
</tr>
<tr>
<td><strong>CND Manager</strong></td>
<td>Technical Support Specialist</td>
<td>Cryptographic Cyber Planner</td>
</tr>
<tr>
<td><strong>Interactive Operator</strong></td>
<td>CND Auditor</td>
<td>BDA Analyst</td>
</tr>
<tr>
<td><strong>Production Operator</strong></td>
<td>Assessment Analyst</td>
<td>Forensic Analyst</td>
</tr>
<tr>
<td><strong>Close Access Network Operator</strong></td>
<td>Network Warfare Cyber Planner</td>
<td>Operational Target Dev Analyst</td>
</tr>
<tr>
<td></td>
<td>Legal Advisor/ SJA</td>
<td>Digital Network Exploit Analyst</td>
</tr>
<tr>
<td></td>
<td>Cyber Policy &amp; Strategy Planner</td>
<td>Target Digital Network Analyst</td>
</tr>
<tr>
<td></td>
<td>Target Analyst Reporter</td>
<td>Target Analyst Reporter</td>
</tr>
</tbody>
</table>
National Initiative for Cybersecurity Education (NICE)

- Federal Gov’t effort
  - Overarching Framework
    - Taxonomy
    - Lexicon
- Focused on
  - Awareness
  - Education
  - Training
  - Professional Development
- Population
  - Information Technology
  - Information Assurance
  - Computer Science
- Structure
  - 7 High Level Categories
  - 31 Specialty Areas/Roles
    - Knowledge
    - Skills
    - Abilities
- End Result
  - Better trained & equipped workforce with the “cyber” skills required for a position
Cyber Security Training
Relationships

- Roles to Roles
- Roles to Tools
- Tools to Tools
Documentation and Product Development
### Training Matrix

- **Roles require tools and function training at various levels depending on mission need**
  - Roles will need training on how to interface with other Roles and how their tools interface with other tools and roles

- **Tools and Functions (Tn) training focused on**
  - Roles to tools
  - Tools to tools
  - Roles to roles

<table>
<thead>
<tr>
<th>Advanced</th>
<th>Intermediate</th>
<th>Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Admin/Management</td>
<td>CND Analyst</td>
<td>Server Admin</td>
</tr>
<tr>
<td>T1</td>
<td>T2</td>
<td>T3</td>
</tr>
<tr>
<td>T1</td>
<td>T2</td>
<td>T3</td>
</tr>
<tr>
<td>T1</td>
<td>T2</td>
<td>T3</td>
</tr>
</tbody>
</table>
Crosswalk KSAs to Training Module

138 KSAs containing 19 matches

(U) Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.

Training Module Steps

• Complete TTP
• Identify training objectives
  – Conduct vulnerability scans
  – Recognize vulnerability
• Build Storyboards/content
  – Instructional design
  – Graphics
  – Programming
• Test final product – Objective?
• Post/link to TTP on IASE
## Training Product Delivery

<table>
<thead>
<tr>
<th>Raw Content</th>
<th>Development</th>
<th>Delivery</th>
<th>Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Training Coordinators</td>
<td>Roles</td>
<td>Tools</td>
<td>Classroom</td>
</tr>
<tr>
<td>Cyber Course Developers</td>
<td>TTPs (Entry–Intermediate–Advance)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber Trainers/Instructors</td>
<td>Trainers</td>
<td>Trainers</td>
<td></td>
</tr>
<tr>
<td>Tactics Techniques Procedures</td>
<td>• DoD focused</td>
<td>• Training rooms</td>
<td>1. Observations</td>
</tr>
<tr>
<td>• Operational Focused</td>
<td>• Local Training Area</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vendor Delivered Course Training</td>
<td>• Capability Specific</td>
<td>VTE</td>
<td>2. Interviews</td>
</tr>
<tr>
<td>• Capability Specific Orders</td>
<td>• AGILE</td>
<td></td>
<td>3. Surveys</td>
</tr>
<tr>
<td>• Threat TTPs</td>
<td>• FedVTE.gov</td>
<td></td>
<td>4. Tests</td>
</tr>
<tr>
<td>Operation Orders/ Policies</td>
<td>CBT/WBT</td>
<td></td>
<td>5. Live Fire Exercises</td>
</tr>
<tr>
<td>• Capability Specific Orders</td>
<td>• Web Based</td>
<td></td>
<td>6. Unit Level</td>
</tr>
<tr>
<td>• Threat TTPs</td>
<td>• Computer Based</td>
<td>Exercises for Crew</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Collaborative</td>
<td></td>
<td>Certifications</td>
</tr>
</tbody>
</table>

| Commercial Training Delivery | DoDize/Operationalize Training | Effective Training Delivery | Training Evaluation/Course Follow up |

INPUTS

- TTTs

- DoD focused

- Operational Focused

- Vendor Delivered

- Course Training

- Capability Specific

- Threat TTPs

- Operation Orders/Policies

- Capability Specific Orders

- Threat TTPs

- DoDize/Operationalize

- Training

- Effective Training Delivery

- Training Evaluation/Course Follow up
Role-based Curriculum
Home Page

Training Resources For Assigned Role
Examples
Example – Tactics, Techniques and Procedures (TTPs)

• FRAGO 13 TTP for HBSS

- Marriage of HBSS Capabilities to IAM/O Responsibilities
- Ensure Compliance with Info System Security Policies and Procedures
- Monitor and Audit Information Systems
- Report information System Security Violations and Intrusions
- Establish Information System Configuration Management Procedures
FRAGO 13 For HBSS
IAM/O Roles and Responsibilities

• Taken from IAO Duty Appointment document:
  b. Ensure Compliance with Information System Security Policies and Procedures
  c. Monitor and Audit Information Systems
  d. Report information System Security Violations and Intrusions
  e. Establish Information System Configuration Management Procedures
  f. Ensure Education, Training, and Awareness Program is operational

• Act as bridge between IA personnel and IA mandates (external/internal)
• Provide oversight to IA personnel and system administrators in technical security tool policy creation
FRAGO 13 for HBSS TTP

• Asset Awareness
  – Deployment of HBSS components and Point Products to current HBSS Baseline. Begin “Tuning” process and enable configuration of reporting capabilities. Target workstations and servers. Enable SIM reporting.

• Minimum Protection
  – Builds on Asset Awareness, continue “Tuning” process, Block High and Log Medium severity IPS signatures.

• Protected Site
  – Builds on Minimum Protection, continue “Tuning” process, Block High, Block Medium, and Log Low severity IPS signatures. Enable Application Monitoring in a “adaptive” mode, Enable host-based Firewall in “adaptive” mode.

• Secure Site
  – Builds on Protected Site, continue “Tuning” process, Block High, Block Medium, and Block Low severity IPS signatures. Enforce Application Blocking, enforce Firewall policy to include a Connection Aware Group (CAG).
Reviewer Certification Program (RCP)

Program goals:

• Increase the number of Command Cyber Readiness Inspections (CCRIs) -- thus increasing inspection footprint on the DISN
• Improve overall technical knowledge of agency and service personnel and maintain their skill sets
• Increase job satisfaction and obtain operational awareness
• Supports USCYBERCOM requirement for services to conduct CCRIs
RCP Training Process

Application & Approval
- Interested candidate reviews program requirements and applies for program
- DISA FSO reviews candidate qualifications and approves entry

Training
- Candidates complete applicable training, including CBTs, classroom training, and training trips (OJT and Checkride)

Certification & Accreditation
- FSO certifies candidates upon successful completion of all training requirements and recommends candidates for accreditation by USCYBERCOM

Recertification
- Reviewers are required to maintain certification through refresher training courses
Related DoD Initiatives

- DoD 8140 workforce requirements initiative
- Learning Management System selection by OSD P&R
- JCT & CS CONOPs and Implementation Plan
- DHS and NSA Centers for Academic Excellence
- Associate Director for Education and Training
- DISA Cyber Workforce Developments
Way Ahead

• Focus on delivery of “Operationalizing” DISA delivered Cyber Tool Suites that support Role & Crew qualifications
  – Entry to Advance level use of tool
  – Entry to Advance level use for a Role(s)
  – Integration to other tools and Roles
  – Prioritize the effort

• Provide Tactics, Techniques, Procedures (TTPs) template and repository

• Move forward on the development of the foundation for a DoD “Cyber Defense University Academy”
  – Cyber Role-Based training & assessments products, and qualification standards
  – Coordinate with other education leaders
  – Coordinate with operations leads
Way Ahead

• Develop procedure roadmaps for roles
  – Observe, describe and document role
  – Map training to knowledge, skills and abilities (KSAs)
  – Map KSAs to training for creating Individual Development Plans (IDPs)

• Review current 8570 approved certifications and make recommendations on objectives for creation of “new” DoD Role-Based certification
  – Education
  – Testing
  – Experience
  – Continuing education
Resource Information

• Information Assurance Support Environment (IASE)
  – iase.disa.mil

• Training Framework Working Group
  – !FSOTrainingFramew@disa.mil

• Reviewer Certification Program
  – E-mails address: FSO_RCP_Coordinator@disa.mil
  – URL: https://www.us.army.mil/suite/page/643689 (must request access)

• TTP location
  – SIPR URL: cybercom.smil.mil (look for tools on right side of screen)

• IA Symposium, Nashville, 27-30 Aug 12
Questions