

Operationally Focused CYBER Training Framework

Deputy Director, Field Security Operations

9 May 2012

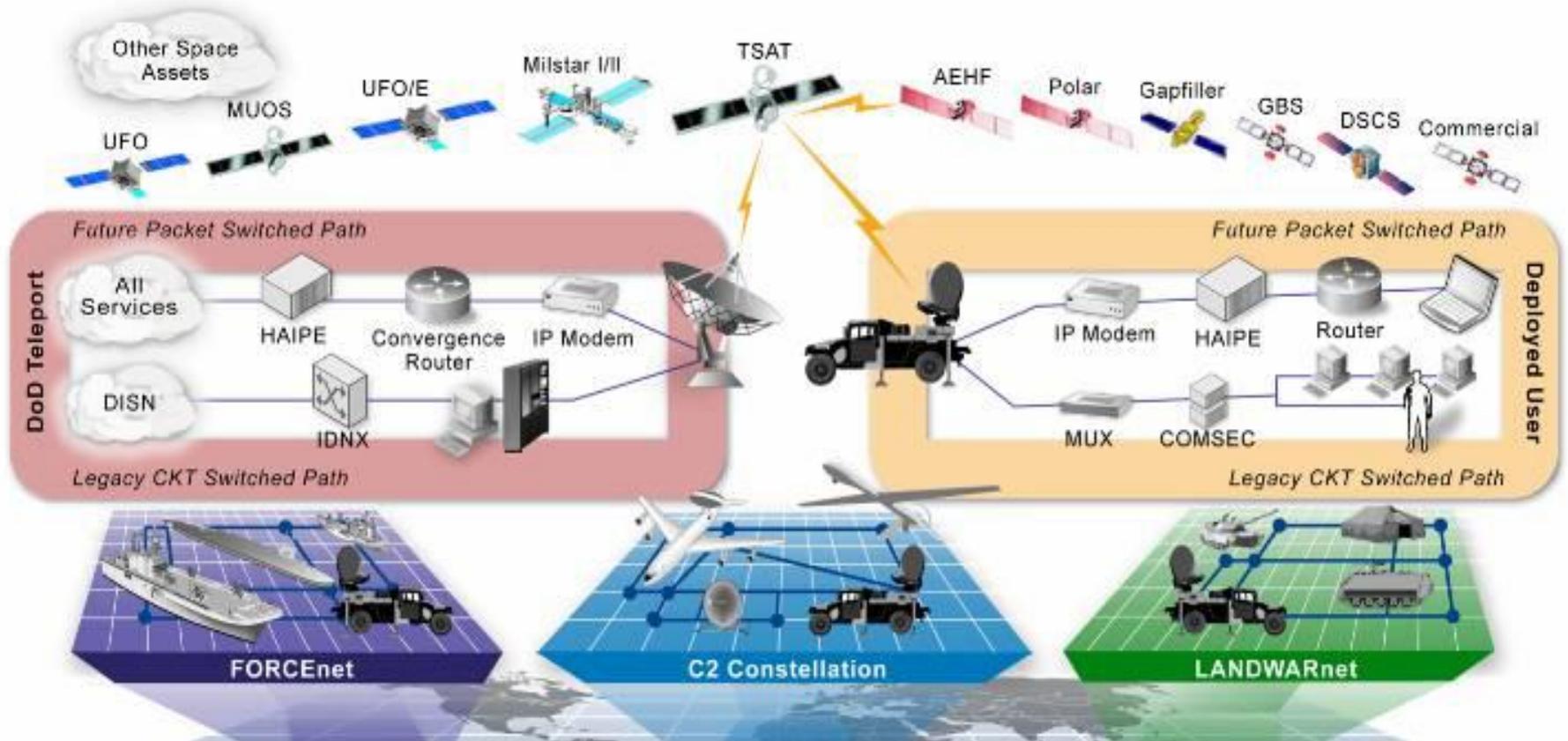
Agenda

- DISA Cyber Workforce Training Vision
- Basic Tenets
- Role-based Educational/Assessment implementation plan
- Documentation & Product Development
- Examples
- Related DoD Initiatives
- Way Ahead

Vision

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

One Standard



“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

	Combat Element	Combat Support					
CYBER ROLES	Server Administrator	Technical Support Specialist	Systems Developer	I & W Analyst	Administration	Logistic	Finance
	Systems Security Analyst	Systems Test & Eval Specialist	Software Engineer	CND Analyst			
	Network Operations Manager	Knowledge Manager	Systems Architect	Intel Analyst			
	CND Incident Responder	Data Administer	IA Compliance Agent	CND Forensic Analyst			
	Cyber Security/ IS Professional	System Requirements Plan	Net Infrastructure Spec	Endpoint Exploit Analyst			
	CND Manager	Technical Support Specialist	Systems Developer	Cryptographic Cyber Planner			
	Interactive Operator	CND Auditor	Test & Eval Engineer	BDA Analyst			
	Production Operator	Assessment Analyst	Partner Ops Planner	Forensic Analyst			
	Close Access Network Operator	Network Warfare Cyber Planner	R&D Engineer	Operational Target Dev Analyst			
		Legal Advisor/ SJA	Cyber Policy & Strategy Planner	Digital Network Exploit Analyst			
			Target Digital Network Analyst				
			Target Analyst Reporter				

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

National Initiative for Cybersecurity Education (NICE)

ENGAGING AMERICANS IN SECURING CYBERSPACE



NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

INTRODUCTION
The National Initiative for Cybersecurity Education (NICE) is a nationally coordinated effort focused on cybersecurity awareness, education, training, and professional development. Two Executive Branch initiatives, in 2008 and 2010, founded the NICE. [\[full text version\]](#)

DEFINING CYBERSECURITY
Defining the cybersecurity population in common terms is one of the major steps in building a robust workforce and providing meaningful training and professional development. NICE is working in collaboration with numerous federal government agencies, subject matter experts internal and external to the government, and industry partners. [\[full text version\]](#)

SECURELY PROVISION

OPERATE AND MAINTAIN

PROTECT AND DEFEND

ANALYZE

SUPPORT

INVESTIGATE

OPERATE AND COLLECT

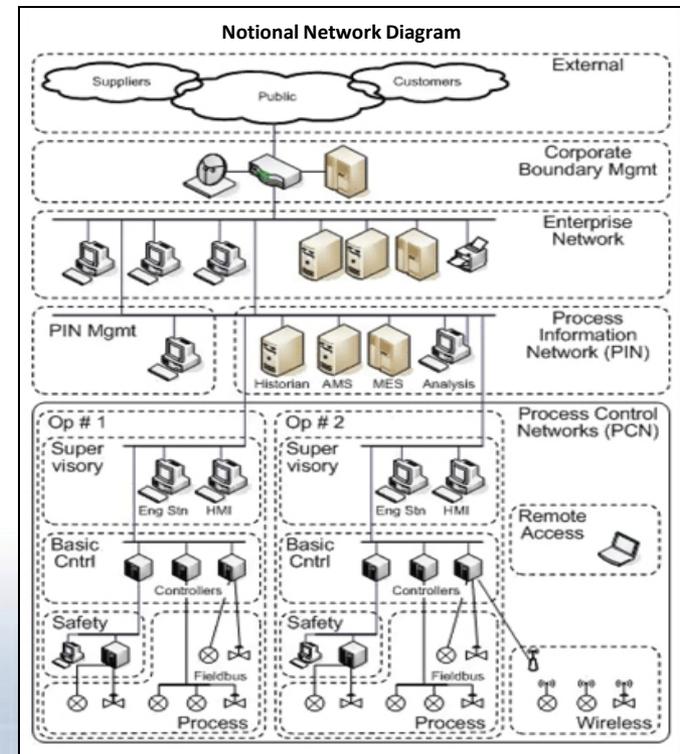
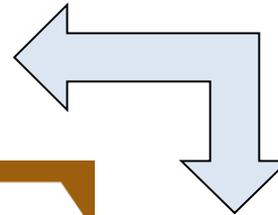
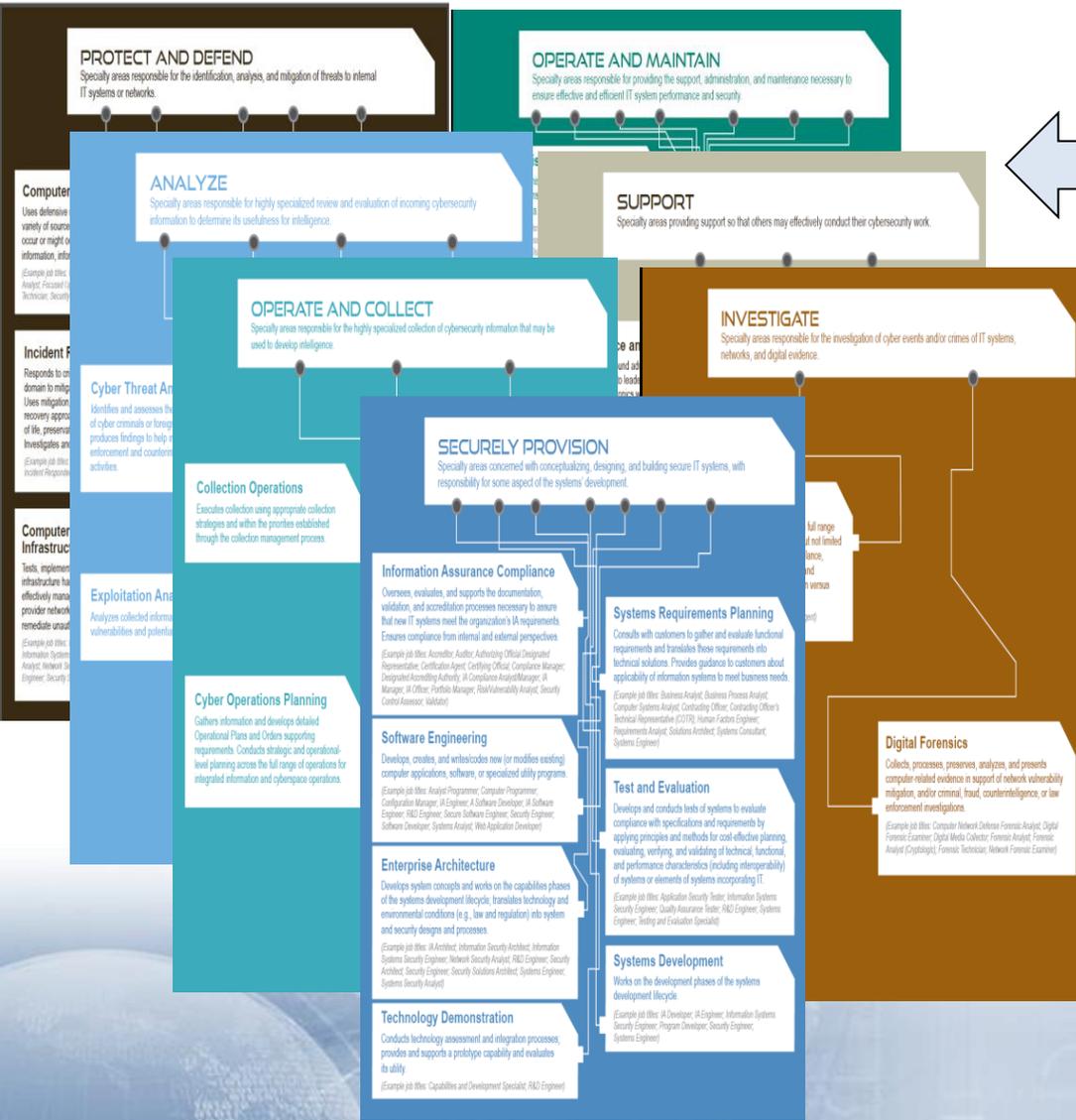
CYBERSECURITY WORKFORCE FRAMEWORK

Home | Instructions | Feedback | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Operate and Collect | Analyze | Support

- 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

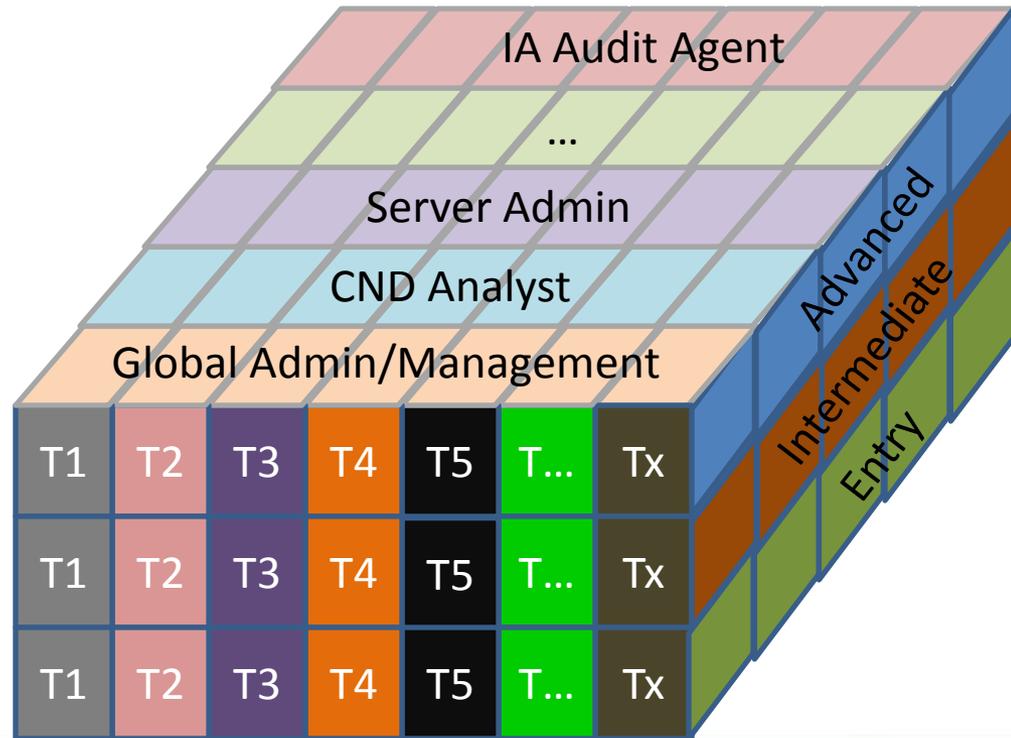


Documentation and Product Development



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 (T_n) training focused on
 - Roles to tools
 - Tools to tools
 - Roles to roles



Crosswalk KSAs to Training Module

	A	B	C	D	E	F	G
1	Role	Work Role	Task #	Task	Entry	Intermediate	Advanced
2	CND	KSA	1	(U) Ability to analyze malware			
3	CND-A	KSA	1	(U) Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.			
4	SWE	KSA	1	(U) Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.			
5	CND-A	KSA	2	(U) Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.			
6	SWE	KSA	2	(U) Ability to use and understand mathematical concepts (e.g., discrete math).			
7	CND	KSA	2	(U) Knowledge of access authentication methods		C	C
				(U) Knowledge of applicable business			



KSA	Role
24	- CND
24	- CND-A
21	- SA
14	- NO
23	- DBA
31	- SWE
22.83 Average	

138 KSAs containing 19 matches

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



	A	B	C	D	E	F	G
8	NO	KSA					
9	CND-A	KSA					
10	DBA	KSA					
11	CND	KSA					
12	CND-A	KSA	2				
13	CND-A	KSA					
14	SWE	KSA					
15	SWE	KSA					
16	CND	KSA					
17	DBA	KSA					
18	CND-A	KSA					
19	DBA	KSA					

1	JC&CS Role Definition	Abbreviation used	Candidate Role
	CND Analyst—Uses data collected from a variety of CND tools (including intrusion detection system alerts, firewall and network traffic logs, and host system logs) to analyze events that occur within their environments for the purposes of mitigating threats.	CND	
	Network Operations Manager—Plans, organizes, and directs the operation, administration, maintenance, and provisioning of network systems in order to ensure availability and integrity of information.	NO	Network Services
	CND Auditor—Performs assessments of systems and networks within the NE or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy.	CND-A	IA Compliance
	Data Administrator—Develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data.	DBA	Data Admin
	Server Administrator—Installs, configures, troubleshoots, and maintains server hardware and software to ensure their confidentiality, integrity, and availability.	SA	System Admin
	Software Engineer—Develops, creates, and writes/codes new (or modifies 1310 existing) computer applications, software, or specialized utility programs.	SWE	Software Engineer

6 of 9 Targeted Roles

- ### 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

Raw Content

Development

Delivery

Assessment

INPUTS

Tactics
Techniques
Procedures

- DoD focused
- Operational Focused

Vendor
Delivered
Course
Training

- Capability Specific

Operation
Orders/
Policies

- Capability Specific Orders
- Threat TTPs

Cyber Training Coordinators

Roles

Tools

Cyber Course Developers

TTPs

(Entry –Intermediate-Advance)

Cyber Trainers/Instructors

Trainers

Trainers

Classroom

- Training rooms
- Local Training Area

VTE

- AGILE
- FedVTE.gov

CBT/WBT

- Web Based
- Computer Based

Collaborative

- DCO/VTC
- Cyber Range

1. Observations
2. Interviews
3. Surveys
4. Tests
5. Live Fire Exercises
6. Unit Level Exercises for Crew Certifications

Commercial Training
Delivery

DoDize/Operationalize
Training

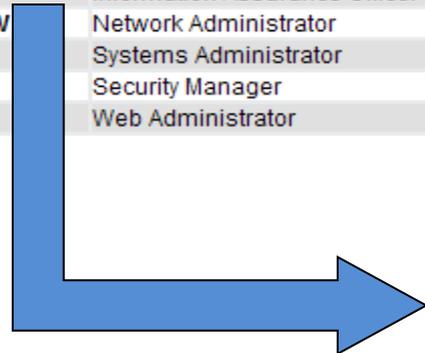
Effective Training Delivery

Training Evaluation/Course
Follow up

Role-based Curriculum Home Page

- Specialty Home
- Expand Specialty and select level
 - ▶ Awareness and General Audience
 - ▶ Computer Net Defense Operator
 - ▶ Computer Net Defense Service Provider
 - ▶ Designated Approving Authority
 - ▶ Database Administrator
 - ▶ Information Assurance Manager
 - ▶ Information Assurance Officer
 - ▶ Network Administrator
 - ▶ Systems Administrator
 - ▶ Security Manager
 - ▶ Web Administrator

Specialty	Date Last Modified			
	Basic	Intermediate	Mastery	
GEN	Awareness and General Audience	21 Jul 10		
CND-OP	Computer Net Defense Operator	21 Jul 10	21 Jul 10	21 Jul 10
CND-SP	Computer Net Defense Service Provider	21 Jul 10	21 Jul 10	21 Jul 10
DAA	Designated Approving Authority	21 Jul 10	21 Jul 10	21 Jul 10
DBA	Database Administrator	21 Jul 10	21 Jul 10	21 Jul 10
IAM	Information Assurance Manager	21 Jul 10	21 Jul 10	21 Jul 10
IAO	Information Assurance Officer	21 Jul 10	21 Jul 10	21 Jul 10
NETW	Network Administrator	21 Jul 10	21 Jul 10	21 Jul 10
SA	Systems Administrator	21 Jul 10	21 Jul 10	21 Jul 10
SEC	Security Manager	21 Jul 10	21 Jul 10	21 Jul 10
WEB	Web Administrator	21 Jul 10	21 Jul 10	21 Jul 10



Training Resources For Assigned Role

IA Compliance Agent

IA COMPLIANCE AGENT				
KSA	Provider	Course	Audience	Type
1. Knowledge of identified vulnerabilities, alerts, and bulletins (IAVA, IAVB).	Schoolhouse Offerings			
	No Courses Identified			
	Other			
2. Knowledge of IT security certification and accreditation requirements.	No Courses Identified			
	Schoolhouse Offerings			
	USAF	Cyber Surety	3D0X3	Initial
	USAF	Undergraduate Cyber Training Course	17D	Initial
	USMC	Information Assurance Managers Course	0689	Advanced
	Other			
	DISA	DIACAP v1.0	Open	Functional
	DISA	IA for Auditors and IG's v1.0	Open	Functional
	DISA	IA HOT Subjects v1.1	Open	Functional
	DISA	Information Assurance Policy & Technology (ASP&T) v4.0	Open	Functional
3. Knowledge of IT security principles and regulations.	Schoolhouse Offerings			
	Army	Network Management Technician Basic Course	250N	Initial
	Army	Signal Systems Support Technician Advanced Course	254A	Initial
	Army	Advanced Leader Course	25B	Advanced
	Army	Network Management Technician Advanced Course	250N	Advanced
	Army	Senior Leader Course	25B	Advanced
	Army	CAW SA/ISSO Course	Open	Functional
	Army	Cisco Certified Network Professional	Open	Functional
	Army	CISSP Information Assurance Level III Course	Open	Functional

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:
 - a. Develop and Issue Security Procedures Governing Information Systems Operations
 - 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).

Example – CCRI Reviewer Certification

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](mailto: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

