CYBERSPACE WORKFORCE

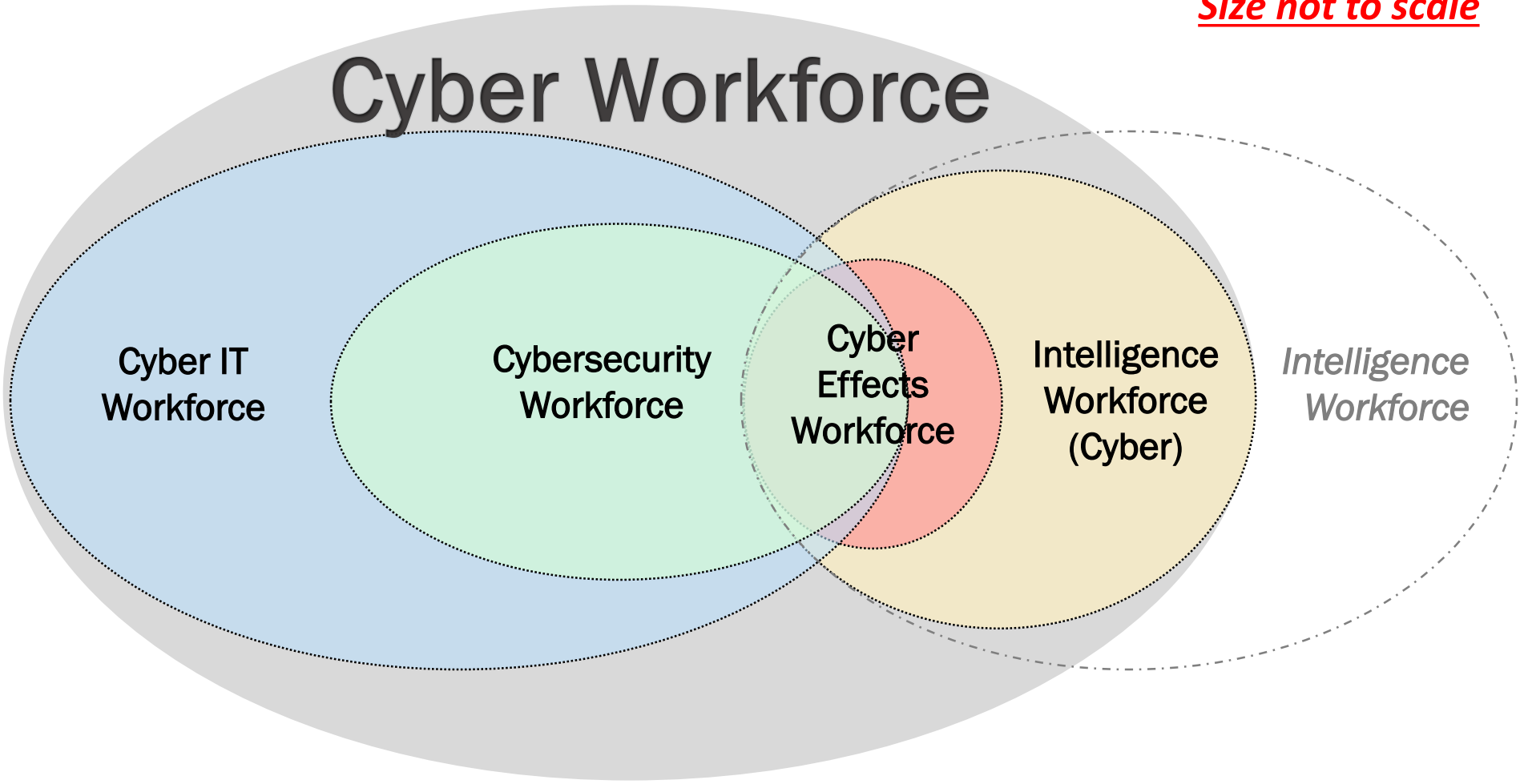
# Department of Defense Cyber Workforce Initiatives

November 2016

# Cyber Workforce & Skill Communities

## Notional Representation

***Size not to scale***



# Work Role Examples

# DCWF Elements

| Cybersecurity Analysis Results | | Category | Specialty Area | Roles |
|---|---|---|---|---|
| | | Operate & Maintain | System Administration | System Administrator |
| | | | Installs, configures, troubleshoots, and maintains server and systems configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Administers server-based systems, security devices, distributed applications, network storage, messaging, and performs systems monitoring. Consults on network, application, and customer service issues to support computer systems' security and sustainability. | Installs, configures, troubleshoots, and maintains hardware, software, and administers system accounts. |

| No | Yes | | | Tasks |
|---|---|---|---|---|
| | X | 434A | Task | Check system hardware availability, functionality, integrity, and efficiency. |
| | X | 452 | Task | Conduct functional and connectivity testing to ensure continuing operability. |
| | X | 683 | Task | Maintain baseline system security according to organizational policies. |
| | X | 695 | Task | Manage accounts, network rights, and access to systems and equipment. |
| | X | 701A | Task | Manage system/server resources including performance, capacity, availability, serviceability, a recoverability. |
| | X | 763A | Task | Diagnose faulty system/server hardware. |
| | X | 835A | Task | Troubleshoot hardware/software interface and interoperability problems. |
| | | | | KSAs |
| X | | 219A | KSA | Skill in operating system administration. |
| | X | 892 | KSA | Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, anti-virus software, anti-spyware). |
| | X | 986 | KSA | Knowledge of organizational information technology (IT) user security policies (e.g., account creat password rules, access control). |
| | | 22 | KSA | * Knowledge of computer networking concepts and protocols, and network security methodo |
| | | [illegible] | KSA | * Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). |
| | X | 1157 | KSA | * Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity. |
| | X | 1158 | KSA | * Knowledge of cybersecurity principles. |
| | X | 1159 | KSA | * Knowledge of cyber threats and vulnerabilities. |
| | X | 6900 | KSA | * Knowledge of specific operational impacts of cybersecurity lapses. |

**Cybersecurity Analysis:** Tasks and KSAs having direct cybersecurity implications

**Role Definitions:** Define a broad set of responsibilities required to execute key functions

**Numbering Scheme:** Provides traceability to the NICE Framework and the JCT&CS

**Tasks:** Describe work assigned or completed as part of standard responsibilities

**Core Cybersecurity Knowledge Statements:** Cybersecurity Knowledge statements applied to all roles within the DCWF

**KSAs:** Standalone statements that describe the attributes required for a job or task

# DC3I – Task 2
# Cybersecurity Task Analysis

- Each task was analyzed to determine whether or not the task is to be considered a cybersecurity task based on the following criteria:
  1) The subject task is inherently a cybersecurity task or is directly cybersecurity related;
  2) The impact of not performing the subject task or performing the subject task incorrectly could result in damage or loss of system or network capabilities resulting in a vulnerability or incident.
  3) Additional Designation – Requires Advocacy – Cybersecurity tasks without an obvious security impact; requires cybersecurity experts to work with curriculum developers to identify and implement cybersecurity impacts into training requirements.

  - 91% of Provider tasks are cybersecurity; 20% of cybersecurity tasks require advocacy

- Analysis was conducted in support of the DoD CIO and distributed for review through USCYBERCOM to Component Cyber Command representatives

- Output from this session will be provided to the DoD Cyber Training Advisory Council (CyTAC) for coordinated development of training requirements

# Cyber Workforce Skill Categories

## *Preliminary Alignment of DCWF (NCWF) Work Roles*

### Cyber IT

Data Analyst
Database Administrator
Enterprise Architect
Knowledge Manager
Network Ops Specialist
Requirements Planner
R&D Specialist
Software Developer
System Administration
Systems Developer
Tech Support Specialist
T&E Specialist

12

### Cybersecurity

Authorizing Official
COMSEC Manager
Cyber Defense Analyst
Cyber Def Forensics Analyst
Cyber Def. Incident Responder
Cyber Defense Infra Spt Spec.
Exploitation Analyst
Info Sys Sec Developer
Info Sys Sec Mgr
Secure SW Assessor
Security Architect
Security Control Assessor
Systems Security Analyst
Vulnerability Analyst
Warning Analyst

15

### Cyber Effects

Cyber Operator
Cyber Ops Planner
Partner Integration Planner
Mission Assessment Specialist
Target Digital Net. Analyst
Target Developer

6

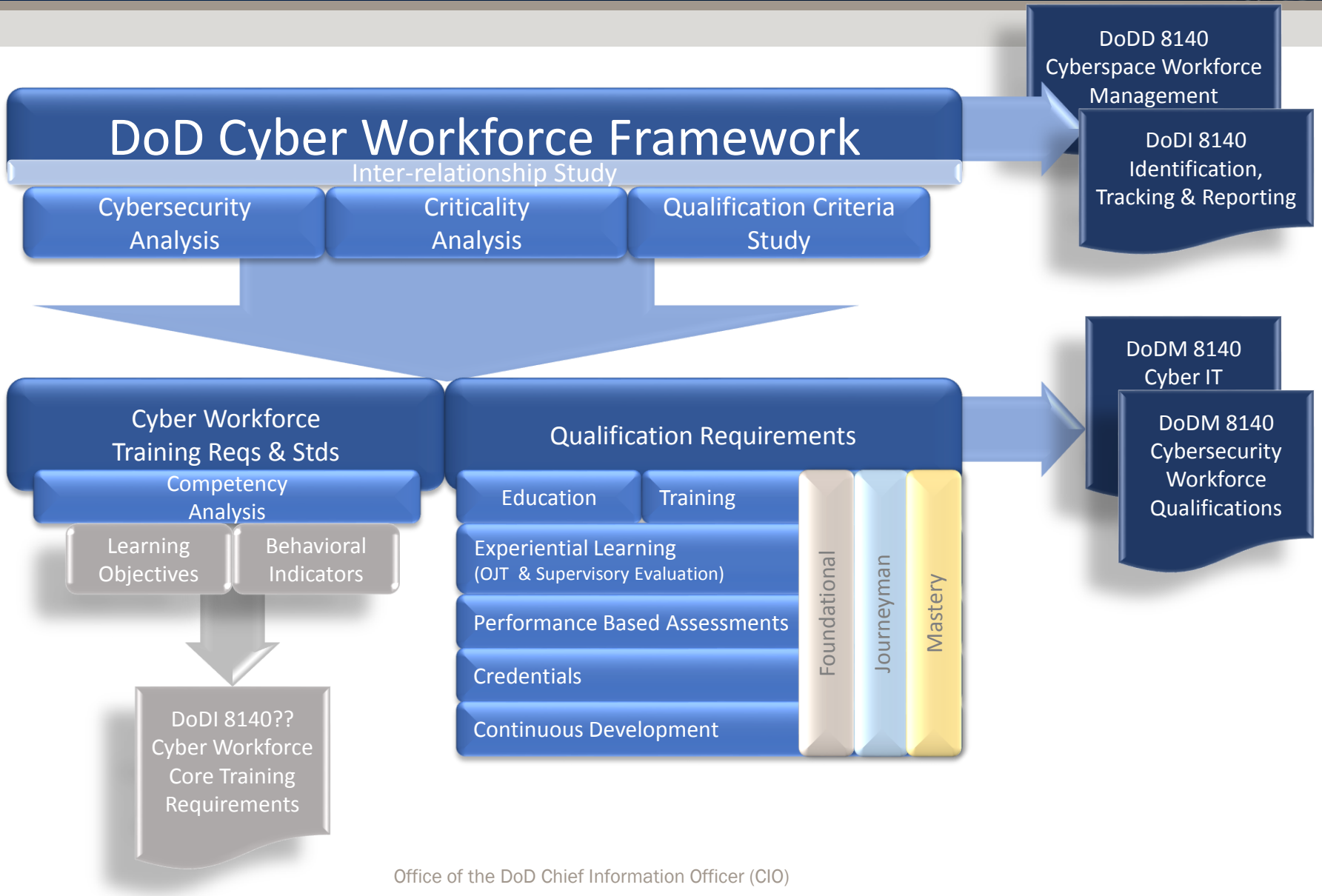
### Intel

All Source Analyst
All Source Collection Mgr
All Source Collection Reqs Mgr
Cyber Intelligence Planner
Multi Disc Language Analyst

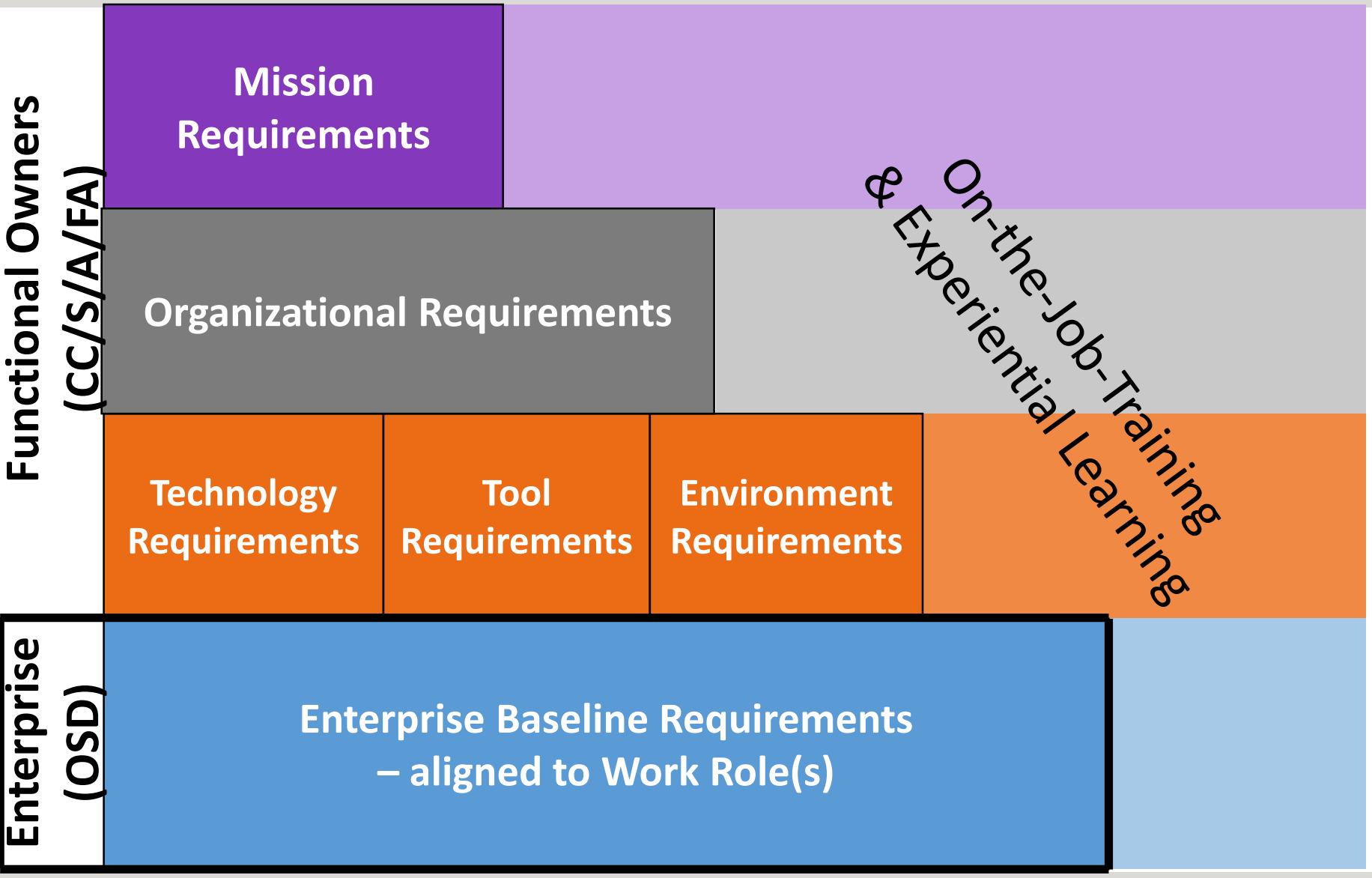
5

| | |
|---|---|
| **Acquisition:** IT Invest/Portfolio Manager, IT Project Manager, Program Manager, Product Support Manager, IT Program Auditor | 5 |
| **Training & Education:** Cyber Instructor, Cyber Instr./Curriculum Dev., Cyber WF Developer & Manager | 3 |
| **Legal/Law Enforcement:** Legal Advisor, Cyber Crime Investigator, Forensics Analyst | 3 |
| **Leadership:** Cyber Policy/Strat Planner, Executive Cyber Leadership | 2 |

# The Keystone



# Enterprise Baseline Requirements



# Cyber Workforce Qualifications Process

***Conceptual Model***

## Security Control Assessor

| | *Foundational* | *Journeyman* | *Mastery* |
|---|---|---|---|
| **Educate** | No | Yes | Yes |
| **Train** | Yes – Basic Concepts | Yes – Complex Concepts | No |
| **Practicums*** **Performance-Based Assessments** | Yes – 70% | Yes – 80% | Yes – 90% |
| **Residency** – **On The Job Training** | Yes | Yes | No |
| **Residency** – **Supervisor Evaluation** | Yes | Yes | Yes |
| **Credentials*** **Certifications** | No | No | Yes |
| **Continuous Development** **Knowledge/Exercise /Skills Labs** | Yes – 20 hrs/yr | Yes – 20 hrs/yr | Yes – 20 hrs/yr |

EXAMPLE

# Cyber Workforce Qualifications Process

***Conceptual Model***

## Vulnerability Analyst

| | *Foundational* | *Journeyman* | *Mastery* |
|---|---|---|---|
| **Educate** | No | Yes | Yes |
| **Train** | Yes – Basic Concepts | Yes – Complex Concepts | No |
| **Practicums*** **Performance-Based Assessments** | Yes – 70%<br>CMF Req (75%) | Yes – 80%<br>CMF Req (85%) | Yes – 90%<br>CMF Req (95%) |
| **Residency** – **On The Job Training** | Yes | Yes | No |
| **Residency** – **Supervisor Evaluation** | Yes | Yes | Yes |
| **Credentials*** **Certifications** | No | No | Yes |
| **Continuous Development** **Knowledge/Exercise /Skills Labs** | Yes – 20 hrs/yr<br>CMF Req - 30 hrs/yr | Yes – 20 hrs/yr<br>CMF Req - 30 hrs/yr | Yes – 20 hrs/yr<br>CMF Req -30 hrs/yr |

# Questions?

# Contact Information

**DoD CIO Key Point of Contact:**
Stephanie Keith
Chief, Cyber Workforce Strategy & Policy Division

**All DoD Cyberspace Workforce related inquiries and questions should be sent to:**
OSD.CyberspaceWorkforce-TAG@mail.mil

**DoD Cyberspace Workforce Strategy**
http://dodcio.defense.gov/Portals/0/Documents/DoD%20Cyberspace%20Workforce%20Strategy_signed(final).pdf

**DoD Directive 8140.01 – Cyberspace Workforce Management**
http://www.dtic.mil/whs/directives/corres/pdf/814001_2015_dodd.pdf

**National Initiative for Cybersecurity Education (NICE) Workforce Framework**
http://csrc.nist.gov/nice/framework/