CYBERSPACE WORKFORCE

DoD Cyberspace Workforce Framework (DCWF) Overview

February 2016

Cybersecurity Demands of the 21st Century

Trends and Key Challenges

- **Growing Reliance on Technology** – Technological advancements have increased the role of cybersecurity across the government and private sector. Technology is now relied upon to realize business strategies, enable innovation, create competitive advantage, protect and defend resources, and improve sales, marketing, and customer service areas.

- **Increasingly Complex Operating Environment** – Today's workers must deal with rising global competition, rapid technological advancement, and emerging threats to national and organizational security.

- **Increasing Amount of Governance** – Cyber threat is considered one of the most serious economic and national security challenges the nation is facing. As a result, today's Federal cybersecurity workers must adhere to an increasing amount of guidance, regulations, policies, and standards related to cybersecurity.

Cybersecurity Workforce Demands

Trends and Key Challenges

- **Inconsistent Lexicon** – While strides have been made, the language used to discuss cybersecurity work and skill requirements is inconsistent. This hinders the nation's ability to assess capabilities, identify skill gaps, and prepare the pipeline of future cyber talent.

- **Lack of Cybersecurity Professionals** – A recent report by the Partnership for Public Service and Booz Allen Hamilton stated, "There is a nationwide shortage of highly qualified cybersecurity experts, and the government has fallen behind in the race for this talent."

- **Disjointed Professional Development** – There is a lack of clearly defined roles and career paths for cybersecurity work. Efforts to establish accreditation standards for cyber curricula and certifications have been inconsistent.

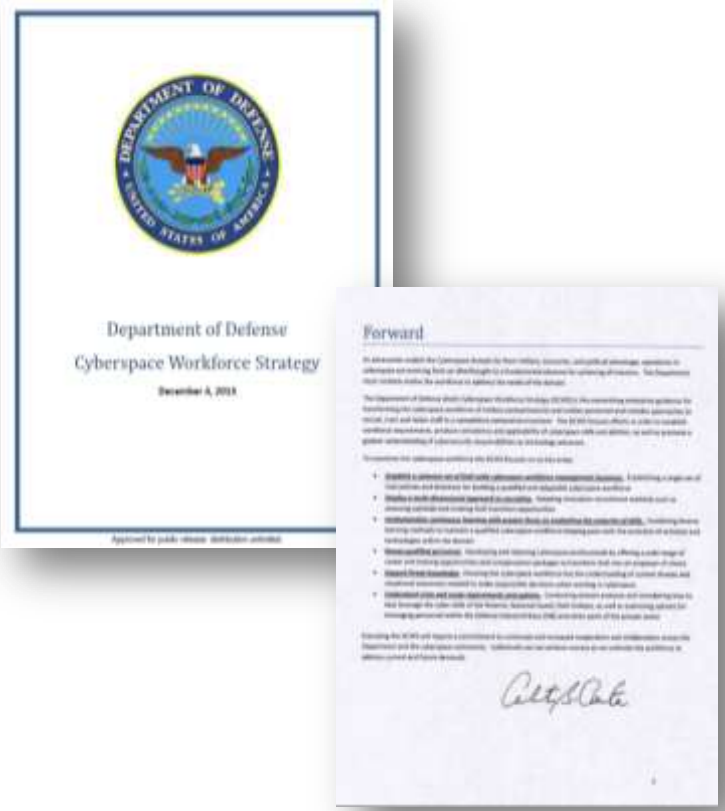
- **Cybersecurity Viewed as Separate Function** – There is often a perception that cybersecurity is a stand alone function performed by specific cybersecurity professionals. As a result, cybersecurity is not recognized by many in the broader cyber workforce as being a part of daily work.

DoD Cyberspace Workforce Strategy

- The DoD Cyberspace Workforce Strategy was signed by the Deputy Secretary of Defense, Ashton Carter, in 2013

- The Strategy serves as the overarching guidance for transforming the cyberspace workforce and includes approaches to recruit, train, and retain staff in a competitive national environment

- A critical element of the Strategy is Focus Area 1, which requires the development of the DoD Cyberspace Workforce Framework (DCWF)



DCWF Overview

- On behalf of the DoD, the DoD CIO is developing the DCWF to establish a standard lexicon for cyberspace work
- The DCWF is based on the:
  - National Initiative for Cybersecurity Education (NICE) Workforce Framework (see right)
  - Joint Cyberspace Training and Certification Standards (JCT&CS)
- The DCWF includes work role descriptions, as well as baseline tasks, knowledge, skills, and abilities (KSAs) aligned by work role

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

** Oversight and Development was changed to Oversee and Govern in NICE 2.0*

High-Level DCWF Methodology

Phase 1
Shaping & Validation
Completed

- Conducted Subject Matter (SME) Panels to develop work role titles and descriptions, as well as align tasks and KSAs to each work role
- Conducted Working Group Sessions to review and validate SME Panel recommendations

Phase 2
Criticality Analysis
In-Progress

- The DoD CIO is currently facilitating criticality analysis to determine which tasks and KSAs are core versus optional

Phase 3
Proficiency Analysis
Completed

- The DoD CIO developed descriptions for a 3 level skills maturity model: Foundational, Journeyman, Mastery

High-Level DCWF Structure

Securely Provision

Specialty Areas	Work Roles
Risk Management	• Authorizing Official/Designating Representative • Security Control Assessor
Software Development	• Software Developer • Secure Software Assessor
Systems Architecture	• Enterprise Architect • Security Architect
Technology Research & Development	• Research & Development Specialist
Systems Requirements Planning	• Requirements Planner
Test and Evaluation	• Testing and Evaluation Specialist
Systems Development	• Information Systems Security Developer • Systems Developer

DCWF Applications

- The DCWF will be leveraged to:
  - Establish a standard lexicon for cyberspace work
  - Identify, code, and track cyberspace personnel with increased accuracy
  - Develop qualification requirements for cyberspace work roles
  - Facilitate the development of targeted recruitment and retention strategies
  - Facilitate the development of career paths
  - Standardize Civilian position descriptions

Related Workforce Issuances

DoD Cyberspace Workforce Strategy

↓

Current **- DoD Directive 8140.01**
Cyberspace Workforce Management

↓

Planned **- DoD Instruction 8140.aa**
Cyber Workforce
Identification, Tracking, & Report Requirements

DoD Cyber Workforce Framework
(Lexicon of Cyber Work Roles)

↓

Current **–**
DoD 8570.01-M remains in effect until it is replaced

Planned **- DoD Manual(s) - Cyber Workforce Qualification Requirements**

Conceptual Qualification Methodology

Education	Training	Residency		Credentials*	Continuous Development
		O-J-T	Supervisor Evaluation	Certifications*	Knowledge, Exercises, Skills Labs
		Performance-based Assessments*			

*Where applicable

Other Key Cyber Initiatives

DoD Cyber Strategy

- Signed by Secretary of Defense Carter in April 2015
- The Office of the PCA, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, and Joint Staff will oversee the implementation of the Strategy
- The strategy outlines five strategic goals to mitigate cyber risks and defend US interests
- The DoD CIO is responsible for Strategic Goal 1: Build and Maintain Ready Forces and Capabilities to Conduct Cyber Operations

DoD Cybersecurity Culture and Compliance Initiative (DC3I)

- Signed by General Dempsey and Secretary of Defense Carter in September 2015
- USSTRATCOM and USCYBERCOM will lead implementation, with involvement from the DoD CIO
- DC3I outlines 11 tasks to transform DoD cybersecurity culture in mutual support of the DoD Cyber Strategy
- The DoD CIO is supporting the implementation for 3 of the 11 tasks outlined

Questions?

CYBERSPACE WORKFORCE

Back-Up Slides

DCWF Interpretation

DCWF Interpretation

- The DCWF leverages the NICE numbering scheme to maintain traceability
  - Task and KSAs below 2000 = NICE 2.0 content
  - Task and KSAs above 2000 = JCT&CS content, newly developed content
  - Task and KSAs noted with letters = (e.g., 123A, 2345A) NICE 2.0 or JCT&CS minimally modified content

CYBERSPACE WORKFORCE

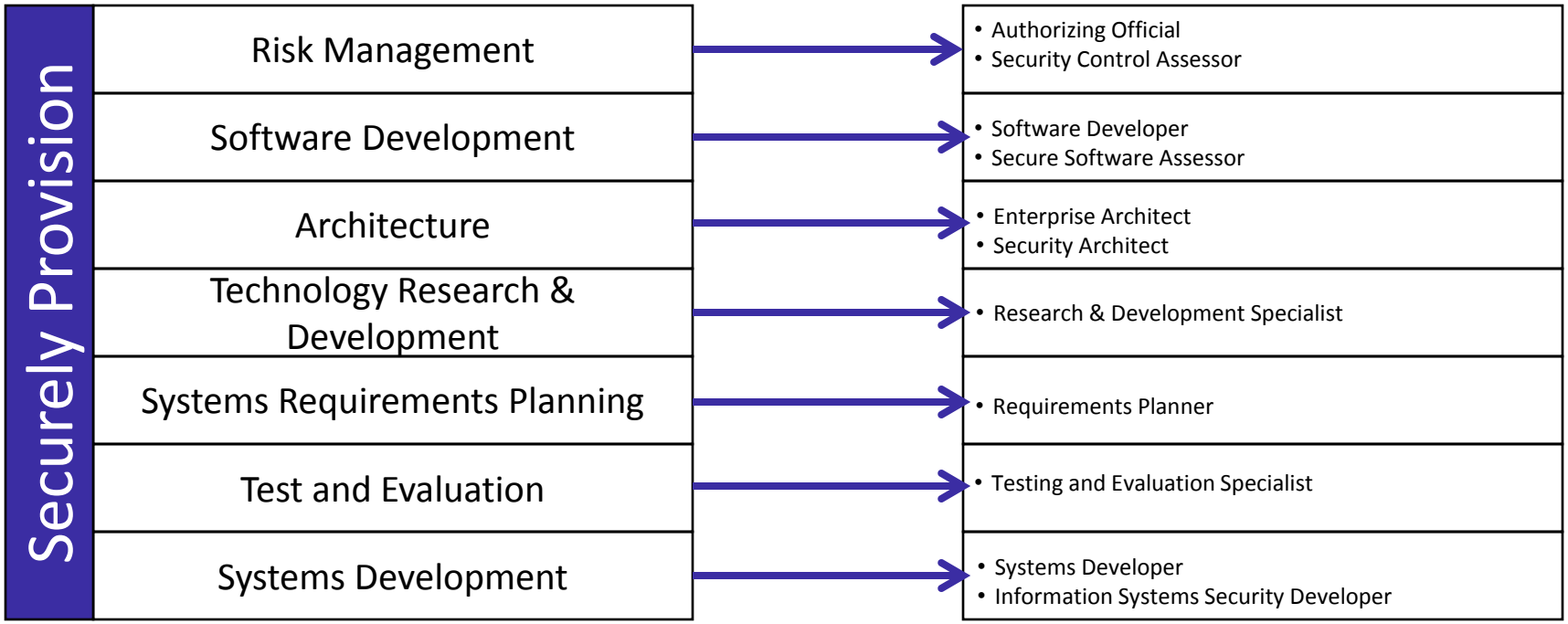
Back-Up Slides

DCWF Alignment of Roles

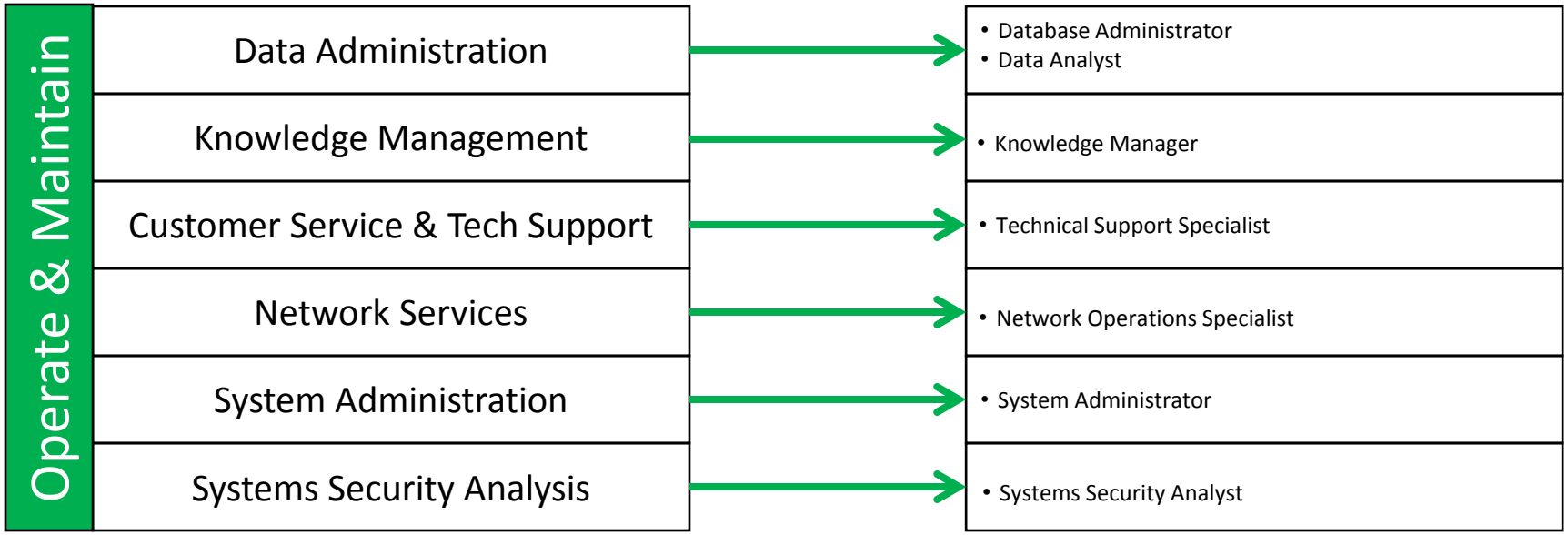
Participation

- Air Force
- Army
- Navy
- Marine Corps
- Coast Guard
- Joint Staff
- USCYBERCOM
- USSTRATCOM
- USSOCOM
- OSD(P) Cyber
- OSD(P&R)
- OUSD(AT&L)
- OUSD(I)
- CAPE
- DARPA
- DoD CIO
- DC-3
- DCAA
- DCMA
- DECA
- DFAS
- DHRA
- DIA
- DISA
- DLA
- DMA
- DoD IG
- DoD EA
- DSCA
- DTIC
- DTRA
- MDA
- NDU
- NGB
- NGA
- NRO
- NSA
- PFPA
- TMA
- UCDMO

Role Alignment



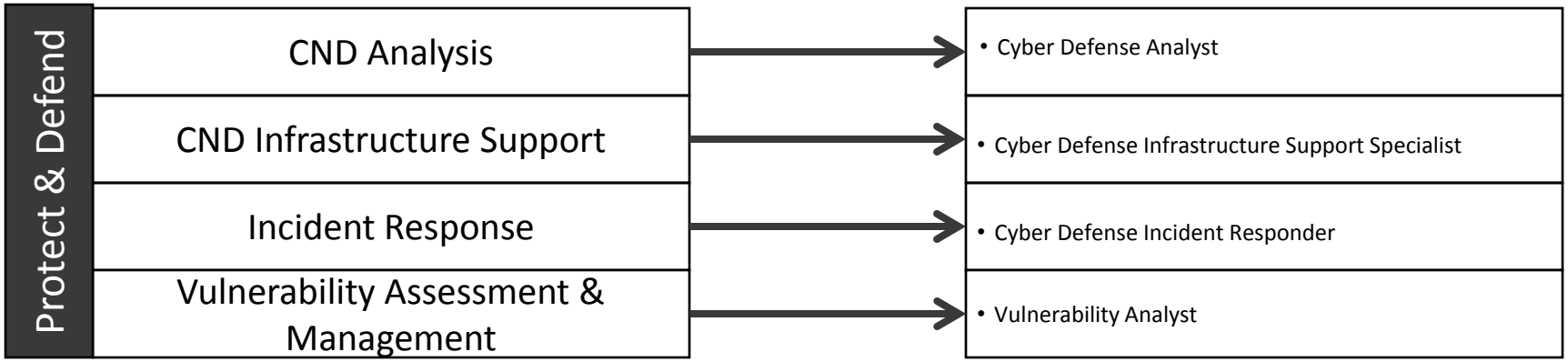
Role Alignment



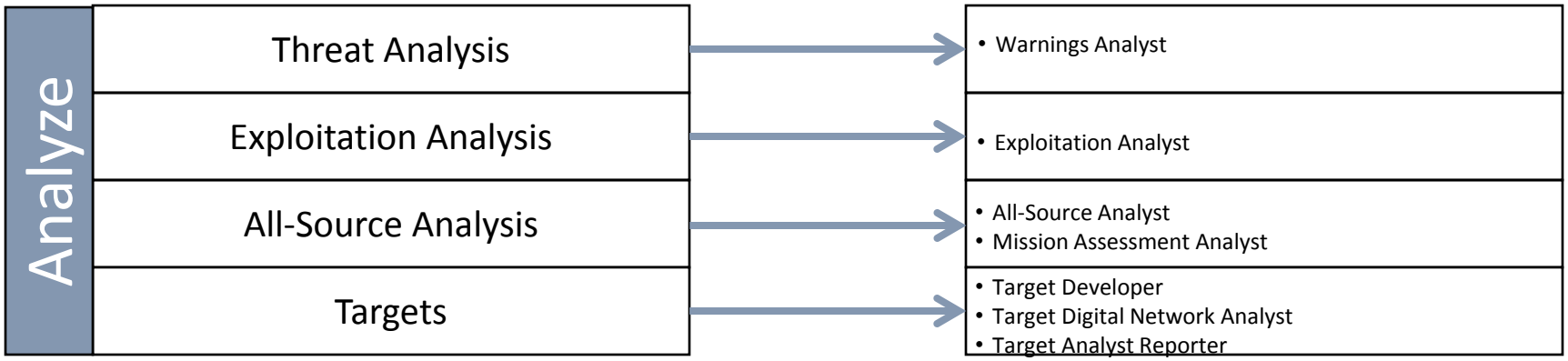
Role Alignment

Oversee & Govern	Legal Advocacy & Advice	• Legal Advisor
	Training, Education, and Awareness	• Cyber Instructor • Instructional Curriculum Developer
	Cybersecurity Management	• Information Systems Security Manager • COMSEC Manager
	Strategic Planning & Policy	• Cyberspace Workforce Developer & Manager • Cyberspace Policy and Strategy Planner
	Executive Cyberspace Leadership	• Executive Cyberspace Leadership
	Acquisition and Program/Project Management	• Program Manager • IT Project Manager • IT Investment/Portfolio Manager • IT Program Auditor • Product Support Manager

Role Alignment



Role Alignment



Role Alignment

Operate & Collect	Collection Operations	• All-Source Collection Mgr • All-Source Collect. Reqs Mgr
	Cyber Operational Planning	• Cyber Ops Planner • Cyber Intel Planner • Interagency/International Integration Planner
	Cyber Operations	• Interactive Operator

Role Alignment

Investigate	Investigation	• Cyber Crime Investigator
	Digital Forensics	• Cyber Defense Forensics Analyst • Forensics Analyst