CYBERSPACE WORKFORCE

DoD Cyberspace Workforce Framework (DCWF) Overview

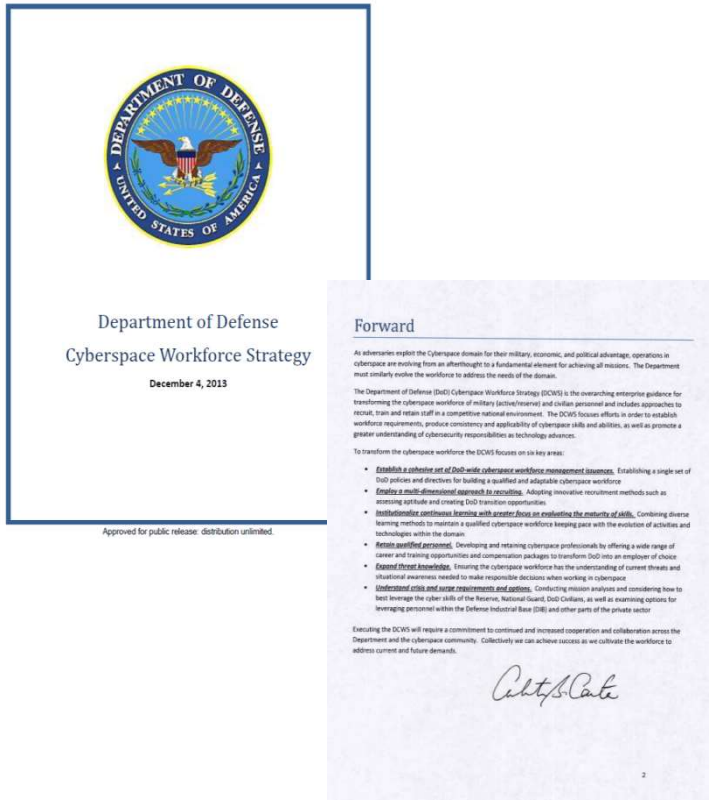
April 2016

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)



Department of Defense

Cyberspace Workforce Strategy

December 4, 2013

Approved for public release: distribution unlimited.

Forward

As adversaries exploit the Cyberspace domain for their military, economic, and political advantage, operations in cyberspace are evolving from an afterthought to a fundamental element for achieving all missions. The Department must similarly evolve the workforce to address the needs of the domain.

The Department of Defense (DoD) Cyberspace Workforce Strategy (DCWS) is the overarching enterprise guidance for transforming the cyberspace workforce of military (active/reserve) and civilian personnel and includes approaches to recruit, train and retain staff in a competitive national environment. The DCWS focuses efforts in order to establish workforce requirements, produce consistency and applicability of cyberspace skills and abilities, as well as promote a greater understanding of cybersecurity responsibilities as technology advances.

To transform the cyberspace workforce the DCWS focuses on six key areas:

- ***Establish a cohesive set of DoD-wide cyberspace workforce management issuances.*** Establishing a single set of DoD policies and directives for building a qualified and adaptable cyberspace workforce
- ***Employ a multi-dimensional approach to recruiting.*** Adopting innovative recruitment methods such as assessing aptitude and creating DoD transition opportunities
- ***Institutionalize continuous learning with greater focus on evaluating the maturity of skills.*** Combining diverse learning methods to maintain a qualified cyberspace workforce keeping pace with the evolution of activities and technologies within the domain
- ***Retain qualified personnel.*** Developing and retaining cyberspace professionals by offering a wide range of career and training opportunities and compensation packages to transform DoD into an employer of choice
- ***Expand threat knowledge.*** Ensuring the cyberspace workforce has the understanding of current threats and situational awareness needed to make responsible decisions when working in cyberspace
- ***Understand crisis and surge requirements and options.*** Conducting mission analyses and considering how to best leverage the cyber skills of the Reserve, National Guard, DoD Civilians, as well as examining options for leveraging personnel within the Defense Industrial Base (DIB) and other parts of the private sector

Executing the DCWS will require a commitment to continued and increased cooperation and collaboration across the Department and the cyberspace community. Collectively we can achieve success as we cultivate the workforce to address current and future demands.

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

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

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

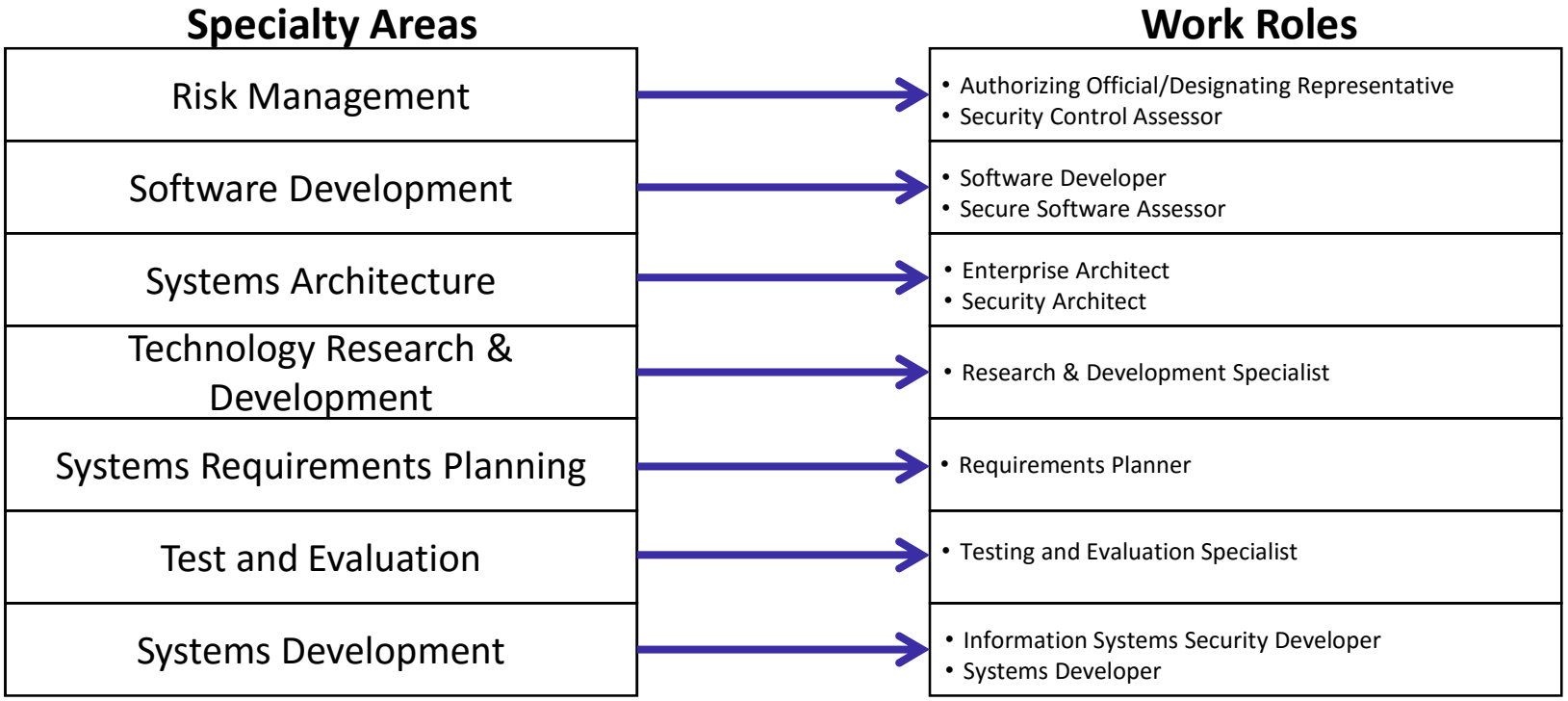
- The DCWF is also being published in a National Institute of Standards and Technology (NIST) Special Publication, to serve as a national standard for Private industry, the Federal government, and academia

High-Level DCWF Methodology

Phase 0	Phase 1	Phase 2	Phase 3
Role Alignment	Shaping & Validation	Criticality Analysis	Proficiency Analysis
Completed	*Completed*	*In-Progress*	*Completed*
• Identified work roles that align to each Specialty Area • Conducted a pilot with Defense Information Systems Agency (DISA) to validate alignments	• 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 validate SME Panel recommendations	• The DoD CIO is currently facilitating criticality analysis to determine which tasks and KSAs are core versus optional	• The DoD CIO developed descriptions for a 3 level skills maturity model: Foundational, Journeyman, Mastery

Phase 0: Role Alignment

Securely Provision



Phase 1: Shaping and Validation

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.

		Tasks
434A	Task	Check system hardware availability, functionality, integrity, and efficiency.
452	Task	Conduct functional and connectivity testing to ensure continuing operability.
456A	Task	Conduct periodic system maintenance including cleaning (both physically and electronically), disk checks, routine reboots, data dumps, and testing.
499	Task	Design group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.
518	Task	Develop and document systems administration standard operating procedures.
518A	Task	Comply with organization systems administration standard operating procedures.
		KSAs
1072	KSA	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth).
22	KSA	* Knowledge of computer networking concepts and protocols, and network security methodol
108	KSA	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
	KSA	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to
	KSA	* Knowledge of cybersecurity principles.
1153		* Knowledge of cyber threats and vulnerabilities.
6900	KSA	* Knowledge of specific operational impacts of cybersecurity lapses.

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

DCWF Phase 2: Criticality Analysis

Criticality Analysis

- The DoD CIO released a tasker to facilitate the DCWF Criticality Analysis
- The criticality analysis is being used to identify the tasks and KSAs that are:
  - **Core:** Critical for successful performance
  - **Optional :** Somewhat or not important for successful performance

DCWF Phase 3: Proficiency Analysis

Proficiency Analysis

- Conducted internal and external research to complete Phase 3 of DCWF development
- The proficiency analysis resulted in definitions for a three level skills maturity model: Foundational, Journeyman, Mastery
- Qualification requirements will be aligned to each of the three levels in the DoD 8140 Manual

DCWF Phase 3:
Skills Maturity Model Definitions

Level	Description
Foundational	At this level, the role requires an individual to have familiarity with basic concepts and processes and the ability to apply these with frequent, specific guidance. An individual must be able to perform successfully in routine, structured situations.
Journeyman	At this level, the role requires an individual to have extensive knowledge of basic concepts and process and experience applying these with only periodic-high level guidance. An individual must be able to perform successfully in non-routine and sometimes complicated situations.
Mastery	At this level, the role requires an individual to have an in-depth understanding of advanced concepts and processes and experience applying these with little to no guidance. An individual must be able to serve as a resource and provide guidance to others. An individual must also be able to perform successfully in complex, unstructured situations.

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

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

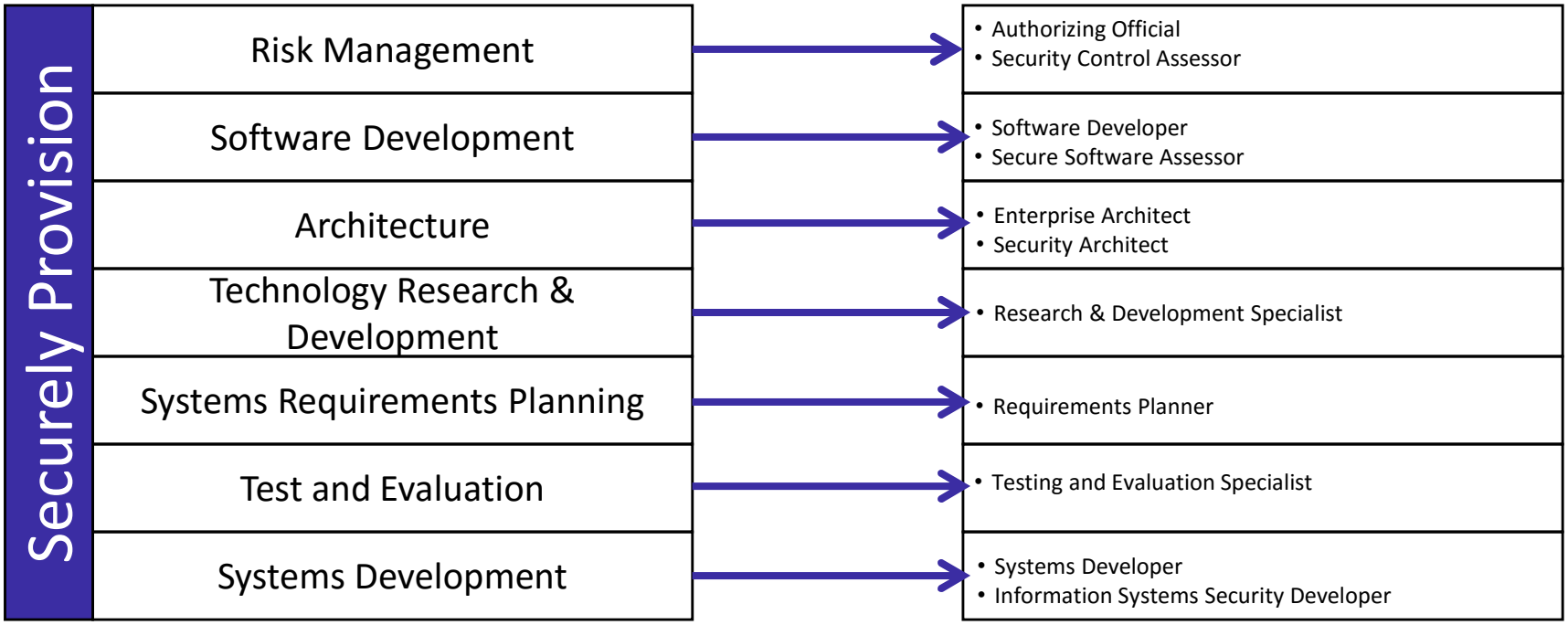
Back-Up Slides

DCWF Alignment of Roles

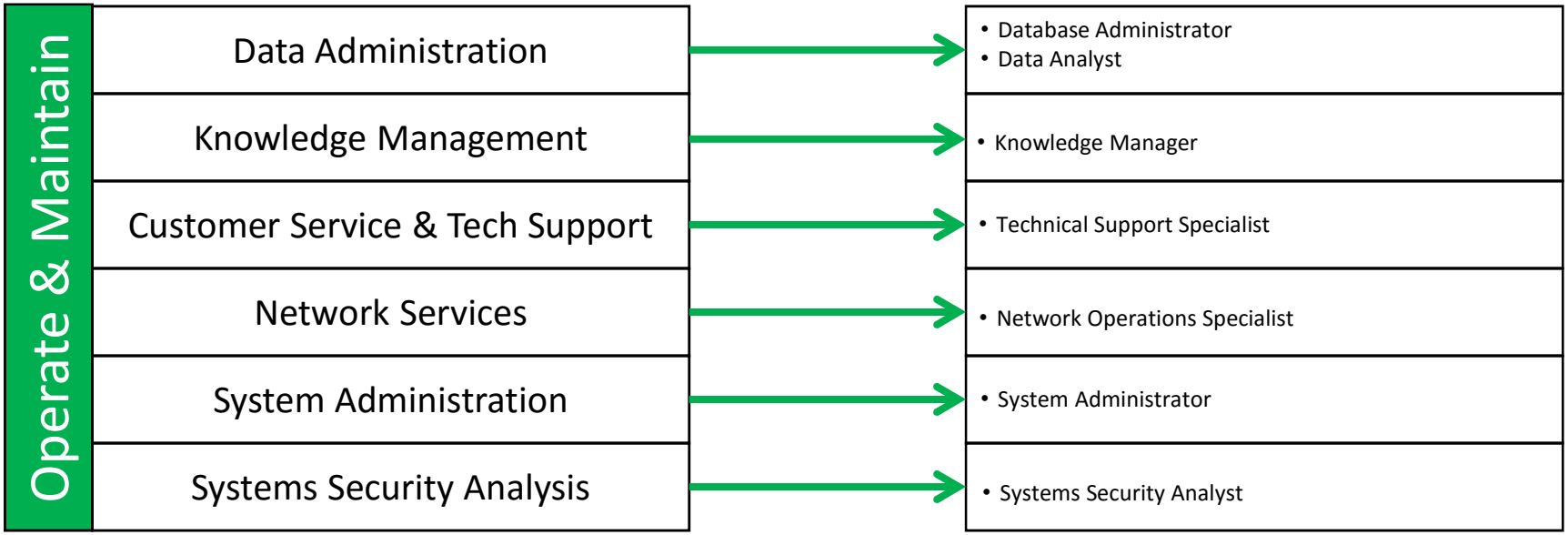
Participation

- 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

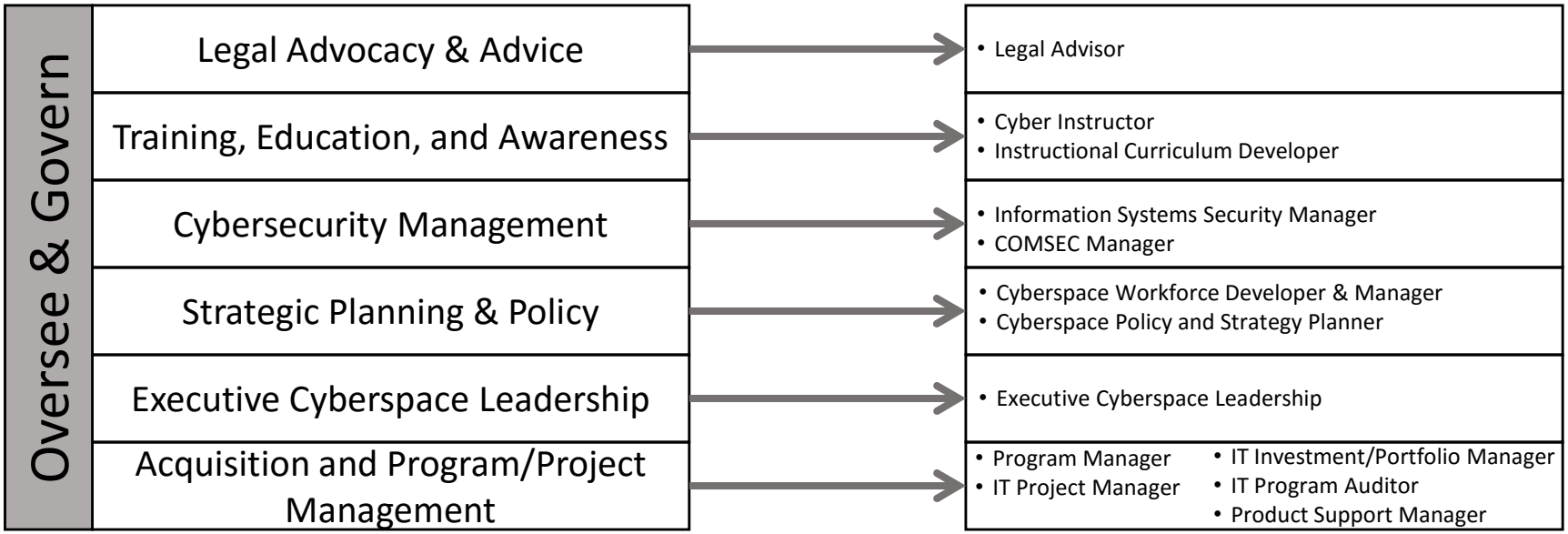
Role Alignment



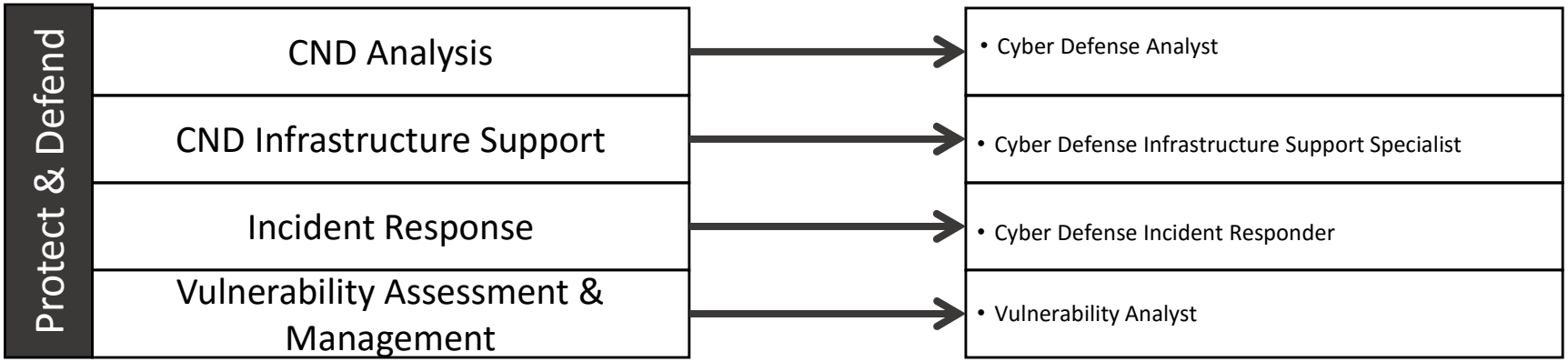
Role Alignment



Role Alignment



Role Alignment



Role Alignment