

Department of the Air Force

DAFITC 2023 DoD Cyber Workforce Panel





UNCLASSIFIED

DoD Cyber Workforce Framework Panel

- **Ms. Venice M. Goodwine, SES, DAF Chief Information Officer, Office of the Secretary of the Air Force (SAF/CN)**
- **Col Joy M. Kaczor, AF/A2/6, Director, Cyber Operations & Warfighter Communications**
- **Mr. Patrick Johnson, Director, Workforce Innovation Directorate, DoD CIO**
- **Mr. Anthony O. Dillard, GS-15, Cyberspace and Information Technology Career Field Manager, Office of the Secretary of the Air Force (SAF/CN)**

UNCLASSIFIED



- **DoD Talent Management**
- **Special Salary Rate vs Work Role**
- **DoD 2023-2027 Cyber Workforce Strategy and Implementation Plan**
- **DoD Cyber Workforce Framework (DCWF)**
- **DoD 8140 Workforce Management Series**
- **Cyber Excepted Service (CES)**



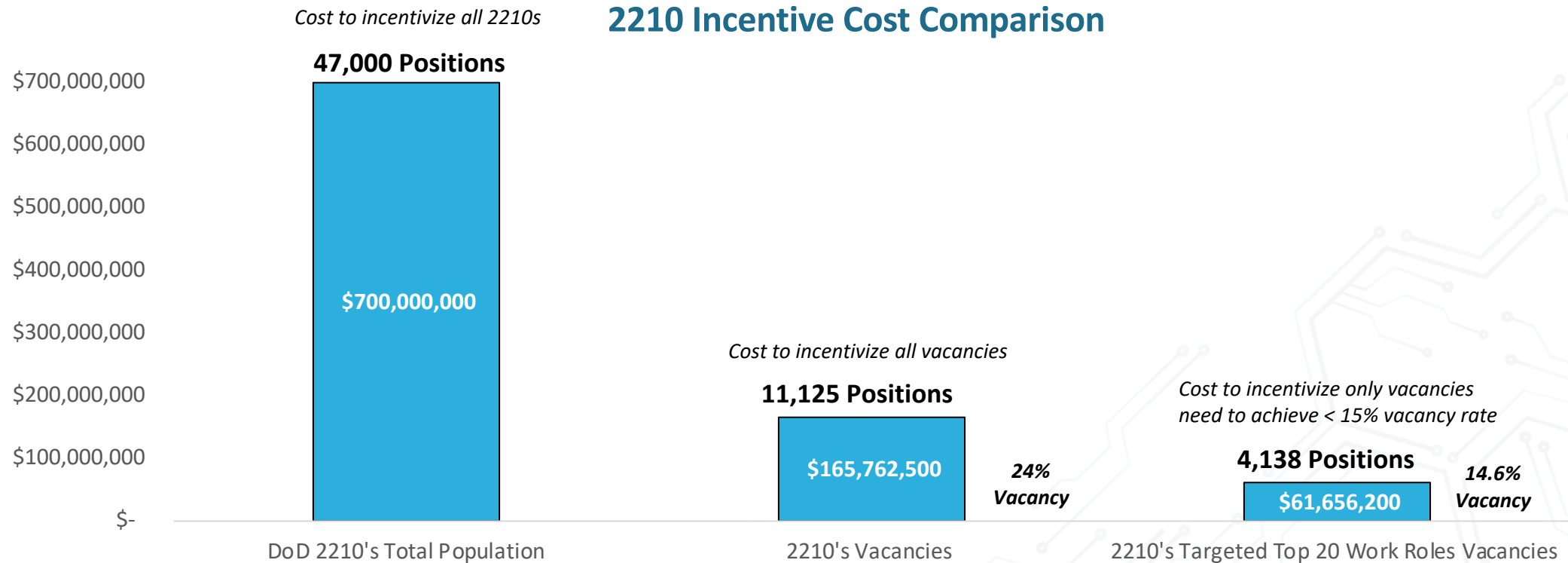
DoD Talent Management

- **Establishment of the Chief Talent Management Officer (19 Apr 23)**
 - Lead a comprehensive review to look for ways to improve how the Department attracts, develops, and retains talent
 - Develop a DoD Talent Acquisition and Management Strategy that will consider current and future Department-wide mission requirements
 - Develop a DoD-wide approach to talent acquisition and management based on the imperatives of the NDS and the knowledge, skills, and abilities required to accomplish the objectives of the NDS
- **Development of Labor Market Framework**
 - Provides a lens through which organizations view the supply and demand of talent



Benefits of Work Role-based Incentive

01100011 01111001 01100010 01100101 01110010 00100000 01110111 01101111 01110010 01101011 01100110 01101111 01110010 01100011 01100101 00001010



Focusing incentives on the 20 work roles in the 2210 occupational series with the highest vacancy rates brings the vacancy rate for 2210 under the 15% threshold (14.6% or 6,862 vacancies). That's an 88% (\$638,343,800) savings vs incentivizing all 2210's.

Introduction

To ensure the Department of Defense (DoD) deploys an agile, capable and ready cyber workforce¹, the Office of the Department of Defense Chief Information Officer (DoD CIO) in collaboration with other Office of the Secretary of Defense (OSD) Component heads; the Joint Staff; United States Cyber Command (USCYBERCOM); and the military services, released the **2023–2027 DoD Cyber Workforce Strategy**² (CWF Strategy) in March 2023.

The CWF Strategy sets the foundation for how the Department will foster a cyber workforce capable of executing the Department's complex and varied cyber mission and provides a unifying direction for civilian and military workforce management activities. Specifically, it identifies goals and associated objectives, which will aid the Department in identifying, recruiting, developing and retaining a more agile, and effective cyber workforce.

The CWF Strategy Implementation Plan (Implementation Plan) will assist the Department in advancing talent management initiatives for a more diverse and effective cyber workforce. The successful execution of the CWF Strategy, through this Implementation Plan and follow-on actions, will empower the Department and its components to foster the most capable and dominant force in the world.





Implementation Plan Purpose

The CWF Strategy is aligned to the Department's strategic goals within the 2022 National Defense Strategy³, the Fiscal Year 2022 - Fiscal Year (FY) 2026 DoD Civilian Human Capital Operating Plan⁴ and Strategic Human Capital Management Goals (see Figure 1). The Implementation Plan is a supplement to the CWF Strategy to ensure the goals and objectives of the CWF Strategy are achieved. The Implementation Plan will help bound activities and assist the Department in support of the four human capital pillars and the management of a more diverse and effective cyber workforce. To realize success of the Implementation Plan, the activities outlined within must be measurable and monitored on a recurring basis. In support of this objective, a series of activities, milestones and key performance indicators (KPIs) are identified to measure progress and assess program effectiveness [Implementation Plan Initiatives, Roles and Responsibilities and Measurement section].

DoD Offices of Primary Responsibility (OPR) and Offices of Coordinating Responsibility (OCR) will use the information outlined in this Implementation Plan as a guide in future action planning sessions where they will execute activities directly supporting initiatives they are assigned. Working together, the Department will be best positioned to overcome cyber workforce challenges and advance our critical mission sets.

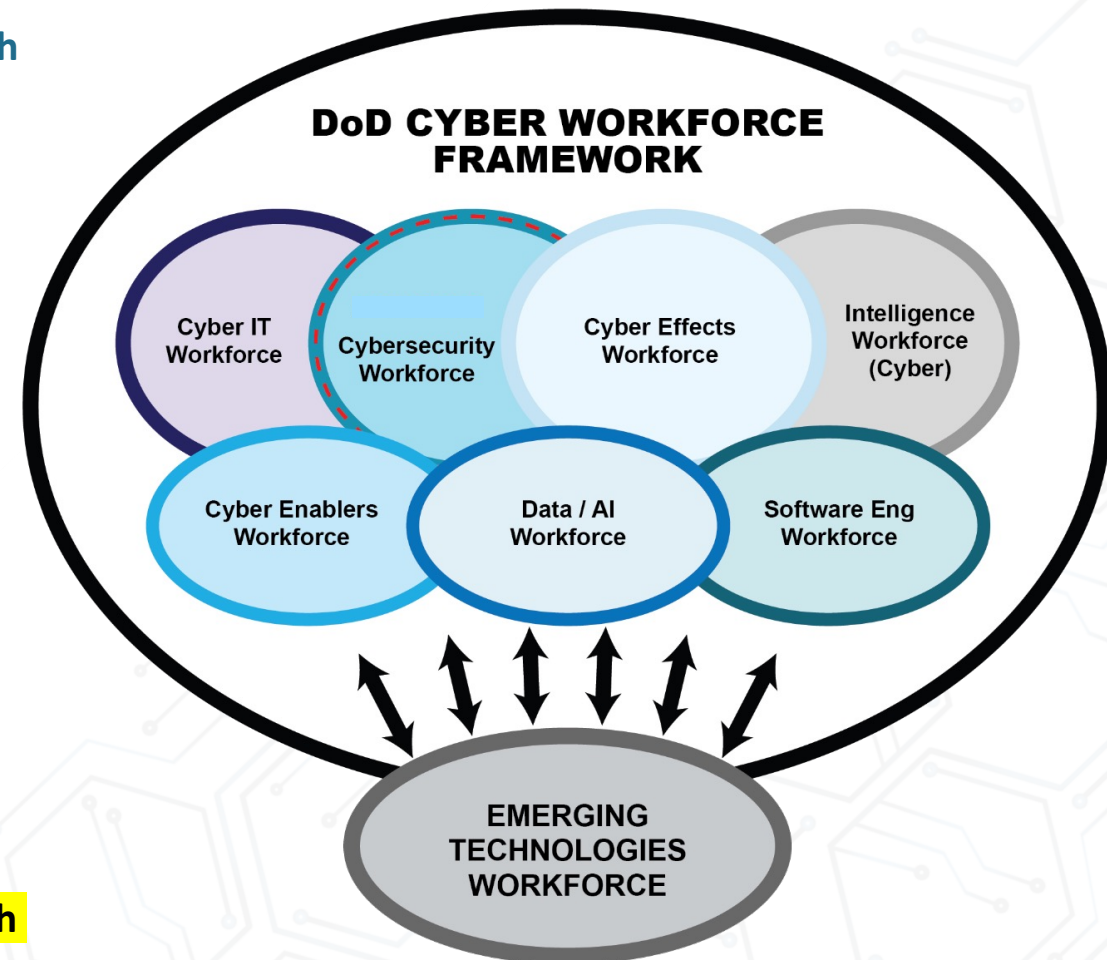


Work Roles Vs. Occupational Series

01100011 01111001 01100010 01100101 01110010 00100000 01110111 01101111 01110010 01101011 01100110 01101111 01110010 01100011 01100101 00001010

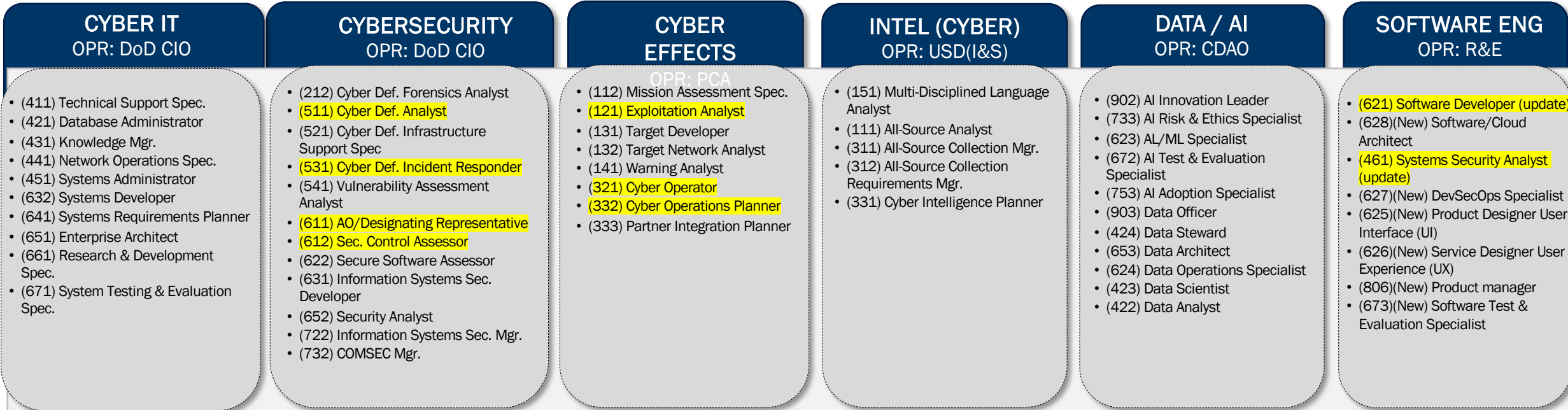
The DoD Cyber Workforce Framework (DCWF) provides the Department with an enterprise baseline standards using Work Roles, which offer greater fidelity than historical occupational structures (e.g. civilian occupational series, military occupational specialties).

- **Agile and responsive process that can incorporate the ever-changing requirements to align to evolving technical threat landscape:**
 - Updated 39 work roles to include Cloud and DevSecOps
 - Added a Control Systems unique work role
 - The Framework now consists of 71 work roles to include Artificial Intelligence (AI), Data, and Software Engineering
- **Among it's many applications, the Department is using the DCWF to:**
 - Conduct strategic workforce planning
 - Develop tailored training and education materials
 - Qualification requirements and career progression
 - **Targeted recruitment and retention incentives**
 - **Identification of critical recruiting and retention shortfalls (i.e., high vacancy rates & attrition rates)**

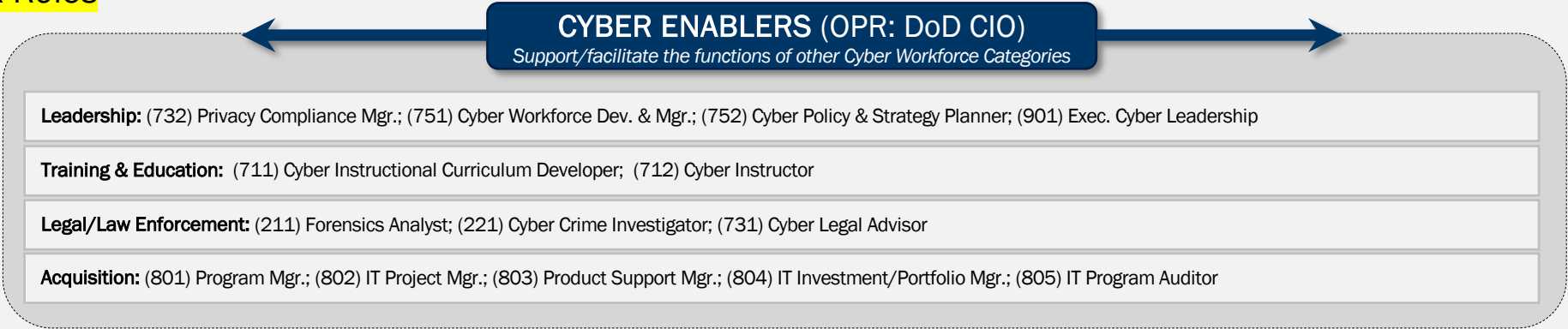




DCWF Expansion



*CES TLMS Work Roles





DoD 8140 Workforce Management Series

- **DOD DIRECTIVE 8140.01: CYBERSPACE WORKFORCE MANAGEMENT**

- Authorizes establishment of a DoD Cyberspace Workforce Management Board (CWMB) as the governing body to ensure that the requirements of this issuance are met
- Establishes the DoD Cyberspace Workforce Framework (DCWF) as the authoritative reference for the identification, tracking, and reporting of DoD cyberspace positions and foundation for developing enterprise baseline cyberspace workforce qualifications
- Unifies the overall cyberspace workforce and establishes specific workforce elements (e.g., information technology (IT), cybersecurity, cyberspace effects, intelligence, and enablers) to align and manage the cyberspace workforce under the CWMB

- **DOD INSTRUCTION 8140.02: IDENTIFICATION, TRACKING, AND REPORTING OF CYBERSPACE WORKFORCE REQUIREMENTS**

- Establishes policy, assigns responsibilities, and provides guidance for the identification, tracking, data collection, and reporting requirements of DoD Cyberspace Workforce Framework (DCWF) work roles

- **DOD MANUAL 8140.03: CYBERSPACE WORKFORCE QUALIFICATION AND MANAGEMENT PROGRAM**

- Implements policy, assigns responsibilities, and prescribes procedures for the qualification of personnel identified as members of the DoD cyberspace workforce
- Identifies members of the DoD cyberspace workforce based on the cyberspace work role(s) of the position(s) assigned, as described in DoD Instruction (DoDI) 8140.02



DoD 8140 Foundational Qualification Options

(652) Security Architect					
		Basic	Intermediate	Advanced	NOTES
Foundational Qualification Options	Education	Associate degree or higher from an accredited college or university	Associate degree or higher from an accredited college or university	Bachelor degree or higher from an accredited college or university	When Education is listed, recommend an accredited Computer Science, Cyber Security, Information Technology, Software Engineering, Information Systems, or Computer Engineering degree; or a degree in a Mathematics or Engineering field.
		OR	OR	OR	
	Training	Offerings listed in DoD 8140 Training Repository	Offerings listed in DoD 8140 Training Repository	Offerings listed in DoD 8140 Training Repository	
		OR	OR	OR	
	Personnel Certification	GSEC	CASP+ or CCSP or Cloud+ or CSSLP	CISSP-ISSAP or CISSP-ISSEP	See the Certification Index tab at the end of this document for certification vendor information.
Foundational Qualification Alternative	Experience	Conditional Alternative	Conditional Alternative	Conditional Alternative	Refer to Section 3 of the DoD 8140 Manual for more information.
Residential Qualification	On-the-Job Qualification	Always Required	Always Required	Always Required	Individuals must demonstrate capability to perform their duties in their resident environment.
	Environment-Specific Requirements	Component Discretion	Component Discretion	Component Discretion	
Annual Maintenance	Continuous Professional Development	Minimum of 20 hours annually or what is required to maintain certification; whichever is greater.	Minimum of 20 hours annually or what is required to maintain certification; whichever is greater.	Minimum of 20 hours annually or what is required to maintain certification; whichever is greater.	



Cyber Excepted Service Personnel System



*An Enterprise approach for
managing the DoD cyber
workforce*

Mission-focused Personnel System

Aligned to both Title 10 and Title 5 provisions, that supports the human capital lifecycle for civilian employees engaged in or in support of a cyber-related mission

Promotes a Culture of Excellence

Based upon mission requirements and employee capabilities

Offers Flexibilities

For Recruitment, Development & Retention of cyber professionals across DoD

Advances Strategic Goals

Of the Office of the DoD Chief Information Officer, Principal Cyber Advisor, and U.S. Cyber Command



CES Attributes

CES

Attributes

One Common Occupational Structure

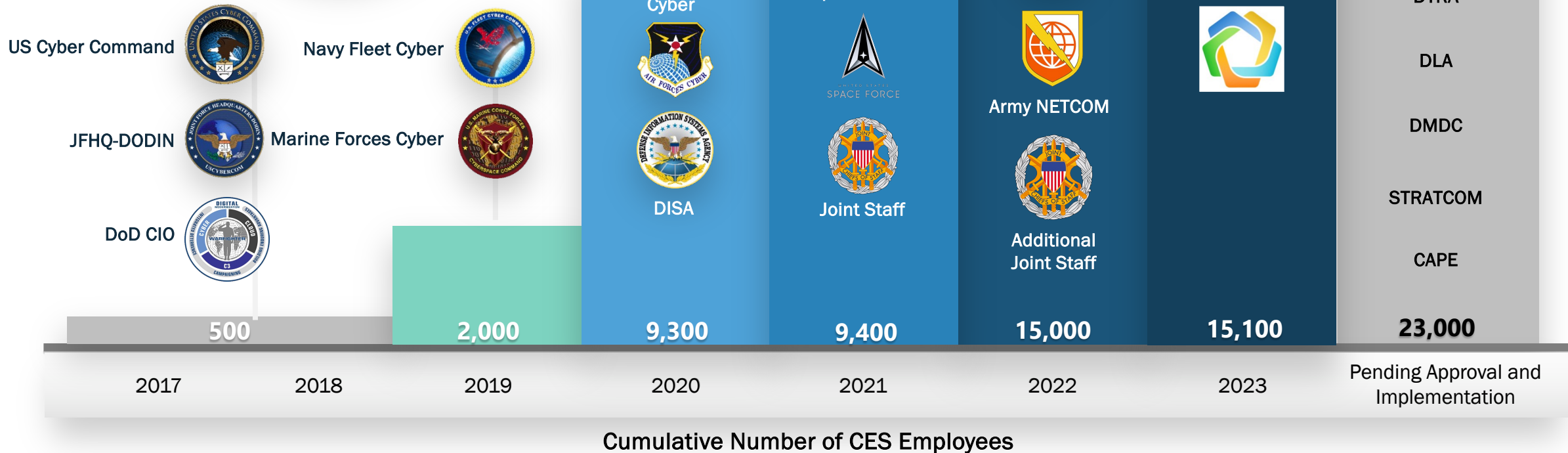
Facilitates voluntary employee conversions from Competitive to Excepted Service

- ✓ Agile Recruitment Sourcing Flexibilities
- ✓ “On the Spot” Appointments
- ✓ Enhanced Pay-Setting Flexibilities
- ✓ Non-Competitive & Competitive Lateral Movements
- ✓ Probationary Periods Carry Over
- ✓ Modified Veterans Preference
- ✓ Qualification-based Professional Development and Advancement Opportunities (no Time-in-Grade)

Cyber Excepted Service Snapshot

CES

Conversion
Timeline





Employee

Competitive Service

OR

CES



Keep Current Grade and Salary

Maintain Attained Career Status

Completed Probationary Periods

Temporary Promotions

Federal Retirements, Retirement, Leave Accrual Rate

Protections, Appeal Rights, Collective Bargaining

Performance Management (DPMAP)

Enhanced Compensation Flexibilities

Qualification-based Promotions (no time-in-grade)

Quality Step Increase up to Step 12





CES TLMS Update Criteria

01100011 01111001 01100010 01100101 01110010 00100000 01110111 01101111 01110010 01101011 01100110 01101111 01110010 01100011 01100101 00001010

Current Rules to Add Work Roles to TLMS

- Vacancy Rate greater than 15%
- Attrition Rate greater than 10%
- Enterprise Relevance – Work Role has been identified by a majority of CES organizations
- CWMB Approval

Proposed Rules to Add Work Roles to TLMS

- Vacancy Rate greater than 15%
- Attrition Rate greater than 10%
- Refresh Rate (Hires/Losses) greater than 1 is healthy (example: 120 Hires/80 Losses = 1.5, work role is healthy)
- Military Vacancy Rate greater than 15%
- Additional CES work role health considerations
 - *Candidate for other compensation Tools/Incentives? (Yes/No)*
 - *Maximized use of 3R Incentives? (Yes/No)*
- CWMB Decision (Yes/No/Defer)

Proposed Rules to Remove Work Roles from TLMS

- Staffing level greater than 110%
- *Military workforce staffing levels not critically short (Yes/No)*
- CWMB Decision (Yes/No/Defer)

Process

- Coordination with CES PMs and AOs prior to CWMB
- Coordination with OUSD I&S and OUSD P&R prior to CWMB
- CES TLMS refreshed quarterly
- CES TLMS Changes formalized with P&R during staffing process