TRANSFORMING TALENT MANAGEMENT

DoD Chief Information Officer, Workforce Innovation Directorate

May 2023

Agenda

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

⚡ Mission and Vision Statement

⚡ Human Capital Pillar Connection

⚡ Work Roles Improve Workforce Management

⚡ DoD Cyber Workforce Framework (DCWF) Impact

⚡ Benefits of Work Role-based Incentives

⚡ DCWF Alignment to Elements

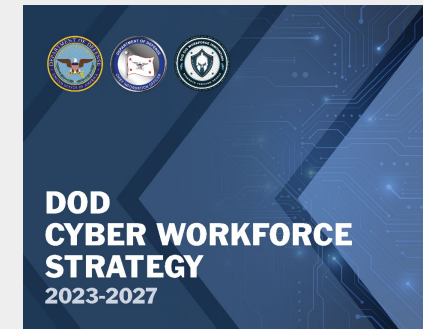⚡ 8140 Qualification Program Overview

⚡ Questions

Mission and Vision Statement

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

MISSION – Provide the tools, resources, policies and programs that enable the Department's cyber workforce stakeholders to identify, recruit, develop and retain a more agile and effective cyber workforce. This includes developing Department-wide policies, championing interagency workforce development initiatives and supporting components with meeting Department-wide cyber requirements to provide a unified direction for the individual communities that comprise this workforce.

VISION – Develop a cyber workforce that is the most capable and dominant force in the world.

DOD CYBER WORKFORCE STRATEGY 2023-2027

- Identification
- Recruitment
- Development
- Retention

GOAL 1: Execute consistent capability assessment and analysis processes to stay ahead of force needs.

GOAL 2: Establish an enterprise-wide talent management program to better align force capabilities with current and future requirements.

GOAL 3: Facilitate a cultural shift to optimize Department-wide personnel management activities.
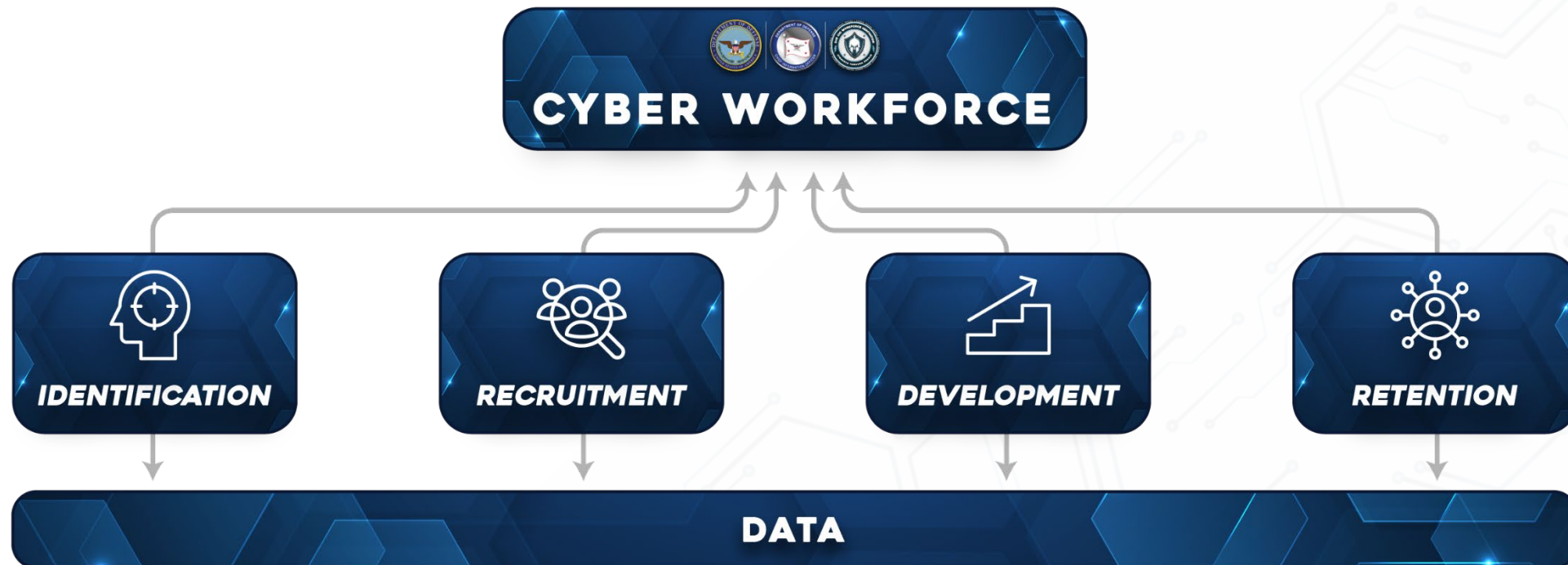
GOAL 4: Foster collaboration and partnerships to enhance capability development, operational effectiveness and career broadening experiences.

Human Capital Pillar Connection

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

This strategy utilizes four human capital pillars – Identification, Recruitment, Development and Retention – to identify and group cyber workforce challenges. The four pillars also serve as the catalyst for targeted workforce development goals, which aid the Department in achieving the mission and vision of this strategy.
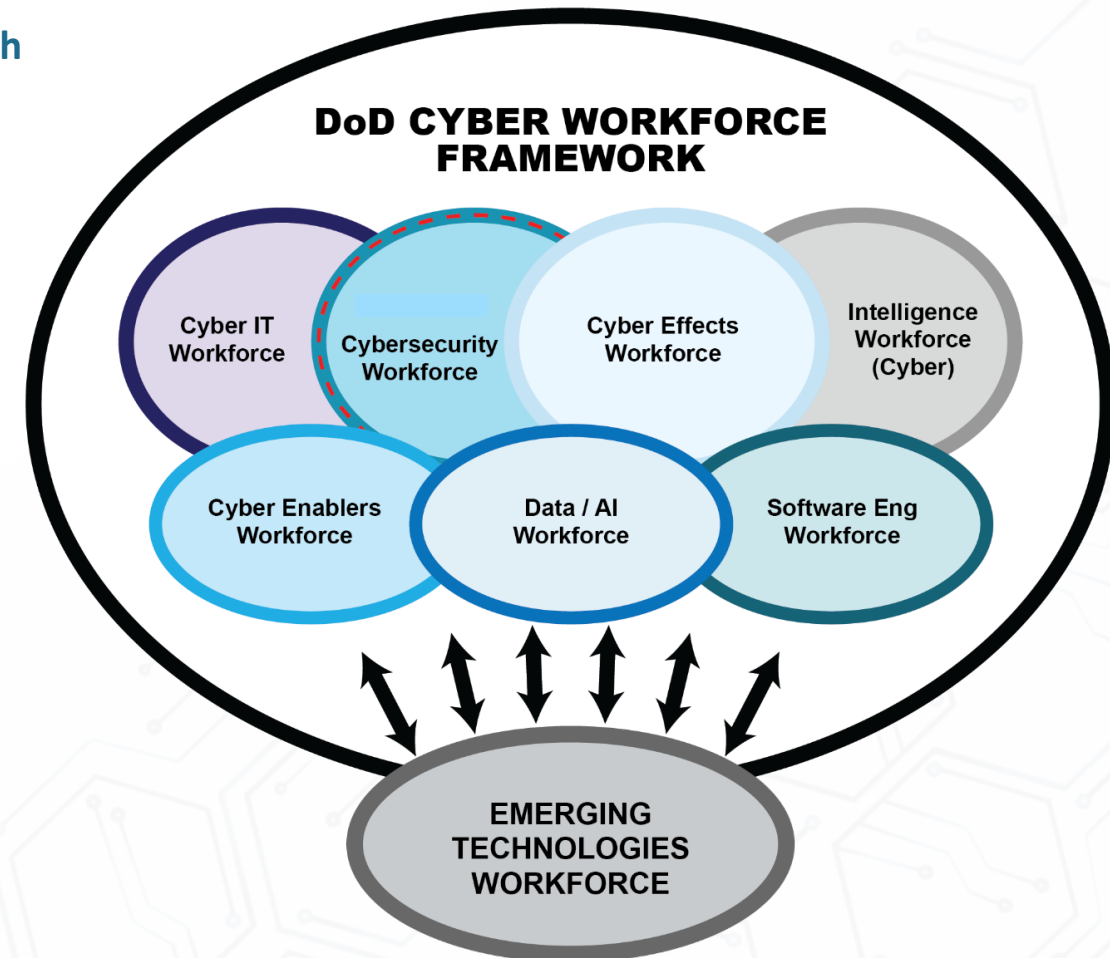
Work Roles Improve Workforce Management

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)

DoD CYBER WORKFORCE FRAMEWORK

Cyber IT Workforce • Cybersecurity Workforce • Cyber Effects Workforce • Intelligence Workforce (Cyber) • Cyber Enablers Workforce • Data / AI Workforce • Software Eng Workforce • EMERGING TECHNOLOGIES WORKFORCE
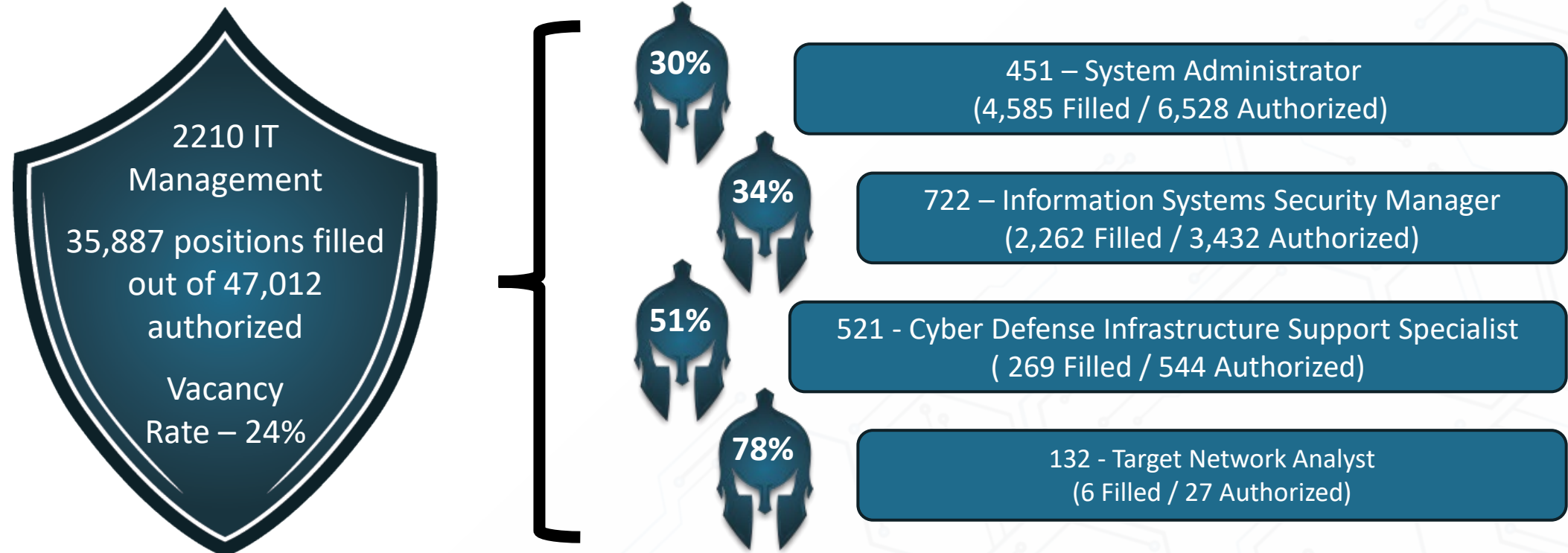
DoD Cyber Workforce Framework Impact

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

Comparing Vacancy Rates by Occupational Series and Coded Work Roles

Viewing the workforce by Occupational Series vs. DCWF work roles can tell you two difference stories. For example, if you were to view Occupational Series (i.e. 2210 IT Management) you would see a vacancy rate of 24%, but if you were to drill down by coded work roles (i.e. 132 Target Network Analyst or 212 Cyber Defense Forensics Analyst) you would see much higher vacancy rates among segments of the workforce. Using coded work roles allows for more detailed analysis.

2210 IT Management

35,887 positions filled out of 47,012 authorized

Vacancy Rate – 24%

30% — 451 – System Administrator (4,585 Filled / 6,528 Authorized)

34% — 722 – Information Systems Security Manager (2,262 Filled / 3,432 Authorized)

51% — 521 - Cyber Defense Infrastructure Support Specialist (269 Filled / 544 Authorized)

78% — 132 - Target Network Analyst (6 Filled / 27 Authorized)

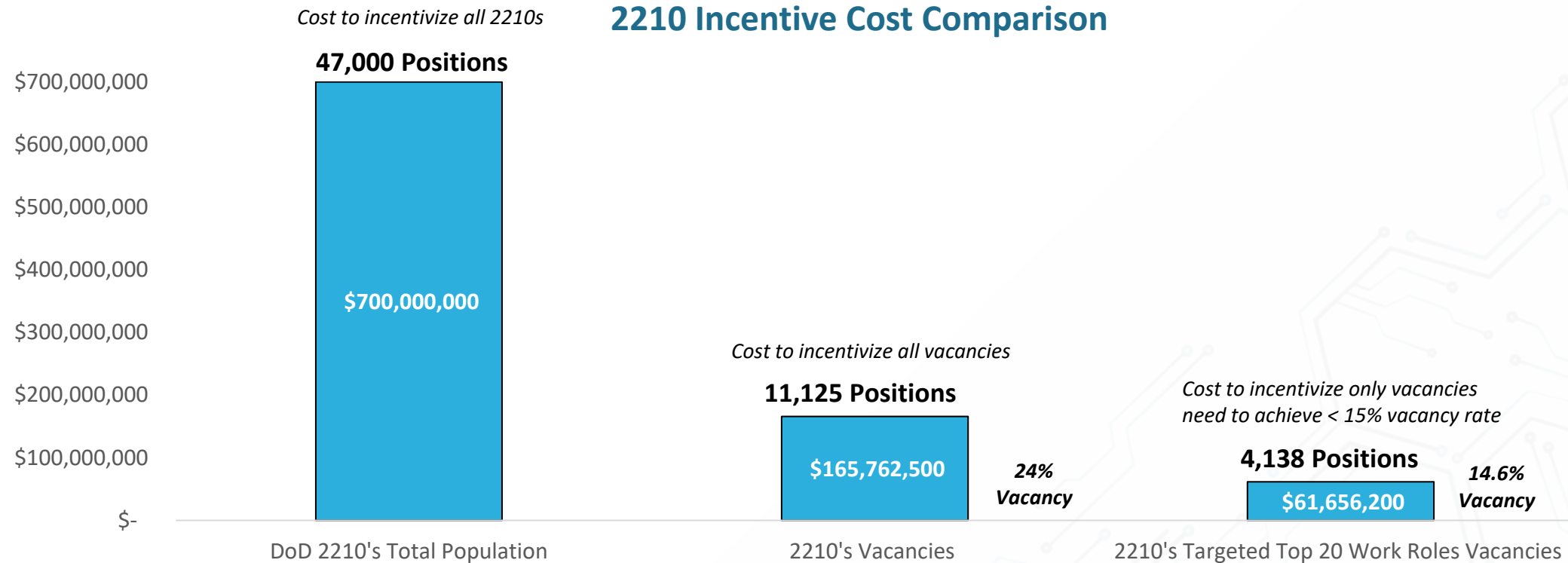# 52 Work Roles Within 2210 Occupational Series

- Displayed data is aggregated from across the department

- The 20 work roles in the 2210 occupational series with the highest vacancy rates

- 4138 vacancies in these work roles

- Work roles allow for more targeted decision making

Work Role Code	Authorized	Personnel	Vacancies	Vacancy Rate	Hires	External	Internal	Losses	Turnover Rate
MULTI-DISCIPLINED LANGUAGE ANALYST 151	8	0	8	100.0%	0	0	0	0	-
TARGET NETWORK ANALYST 132	27	6	21	77.8%	0	0	0	0	0.0%
TARGET DEVELOPER 131	14	4	10	71.4%	1	0	1	0	0.0%
PRIVACY COMPLIANCE MANAGER 732	59	20	39	66.1%	1	1	0	0	0.0%
CYBER DEFENSE FORENSICS ANALYST 212	63	25	38	60.3%	0	0	0	0	0.0%
RESEARCH & DEVELOPMENT SPECIALIST 661	309	139	170	55.0%	12	8	4	3	2.2%
WARNING ANALYST 141	39	18	21	53.8%	2	1	1	2	11.1%
CYBER DEFENSE INFRASTRUCTURE SUPPORT SPECIALIST 521	544	269	275	50.6%	17	12	5	6	2.2%
KNOWLEDGE MANAGER 431	986	515	471	47.8%	17	3	14	8	1.6%
FORENSICS ANALYST 211	79	42	37	46.8%	0	0	0	2	4.8%
PARTNER INTEGRATION PLANNER 333	47	25	22	46.8%	3	1	2	1	4.0%
SECURITY ARCHITECT 652	235	126	109	46.4%	3	0	3	4	3.2%
INFORMATION SYSTEMS SECURITY DEVELOPER 631	427	232	195	45.7%	7	2	5	5	2.2%
SYSTEMS REQUIREMENTS PLANNER 641	1969	1091	878	44.6%	46	17	29	19	1.7%
IT PROGRAM AUDITOR 805	147	83	64	43.5%	4	2	2	5	6.0%
CYBER POLICY AND STRATEGY PLANNER 752	1551	984	567	36.6%	55	12	43	21	2.1%
MISSION ASSESSMENT SPECIALIST 112	81	53	28	34.6%	3	1	2	0	0.0%
INFORMATION SYSTEMS SECURITY MANAGER 722	3432	2262	1170	34.1%	141	59	82	48	2.1%
CYBER LEGAL ADVISOR 731	3	2	1	33.3%	0	0	0	0	0.0%
CYBER INSTRUCTOR 712	43	29	14	32.6%	4	4	0	2	6.9%

Benefits of Work Role-based Incentive

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

2210 Incentive Cost Comparison

Cost to incentivize all 2210s

47,000 Positions

$700,000,000

Cost to incentivize all vacancies

11,125 Positions

$165,762,500

24% Vacancy

Cost to incentivize only vacancies need to achieve < 15% vacancy rate

4,138 Positions

$61,656,200

14.6% Vacancy

DoD 2210's Total Population	2210's Vacancies	2210's Targeted Top 20 Work Roles Vacancies

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.

DCWF Alignment to Elements

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

CYBER IT
OPR: DoD CIO

- (411) Technical Support Spec.
- (421) Database Administrator
- (431) Knowledge Mgr.
- (441) Network Operations Spec.
- (451) Systems Administrator
- (632) Systems Developer
- (641) Systems Requirements Planner
- (651) Enterprise Architect
- (661) Research & Development Spec.
- (671) System Testing & Evaluation Spec.

CYBERSECURITY
OPR: DoD CIO

- (212) Cyber Def. Forensics Analyst
- (511) Cyber Def. Analyst
- (521) Cyber Def. Infrastructure Support Spec
- (531) Cyber Def. Incident Responder
- (541) Vulnerability Assessment Analyst
- (611) AO/Designating Rep.
- (612) Sec. Control Assessor
- (622) Secure Software Assessor
- (631) Information Systems Sec. Developer
- (652) Security Analyst
- (722) Information Systems Sec. Mgr.
- (732) COMSEC Mgr.

CYBER EFFECTS
OPR: PCA

- (112) Mission Assessment Spec.
- (121) Exploitation Analyst
- (131) Target Developer
- (132) Target Network Analyst
- (141) Warning Analyst
- (321) Cyber Operator
- (332) Cyber Operations Planner
- (333) Partner Integration Planner

INTEL (CYBER)
OPR: USD(I&S)

- (151) Multi-Disciplined Language Analyst
- (111) All-Source Analyst
- (311) All-Source Collection Mgr.
- (312) All-Source Collection Requirements Mgr.
- (331) Cyber Intelligence Planner

DATA / AI
OPR: CDAO

- (902) AI Innovation Leader
- (733) AI Risk & Ethics Specialist
- (623) AL/ML Specialist
- (673) AI Test & Evaluation Specialist
- (753) AI Adoption Specialist
- (903) Data Officer
- (424) Data Steward
- (653) Data Architect
- (624) Data Operations Specialist
- (423) Data Scientist
- (422) Data Analyst

SOFTWARE ENG
OPR: R&E

- (621) Software Developer (update)
- (628)(New) Software/Cloud Architect
- (461) Systems Security Analyst (update)
- (627)(New) DevSecOps Specialist
- (625)(New) Product Designer User Interface (UI)
- (626)(New) Service Designer User Experience (UX)
- (806)(New) Product manager
- (673)(New) Software Test & Evaluation Specialist

CYBER ENABLERS (OPR: DoD CIO)
Support/facilitate the functions of other Cyber Workforce Categories

Leadership: (732) Privacy Compliance Mgr.; (751) Cyber Workforce Dev. & Mgr.; (752) Cyber Policy & Strategy Planner; (901) Exec. Cyber Leadership

Training & Education: (711) Cyber Instructional Curriculum Developer; (712) Cyber Instructor

Legal/Law Enforcement: (211) Forensics Analyst; (221) Cyber Crime Investigator; (731) Cyber Legal Advisor

Acquisition: (801) Program Mgr.; (802) IT Project Mgr.; (803) Product Support Mgr.; (804) IT Investment/Portfolio Mgr.; (805) IT Program Auditor

8140 Qualification Program Overview

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

The DoD 8140 Qualification Program establishes a **comprehensive approach** for cyber workforce talent management. It establishes Enterprise **baseline standards for qualification** that directly support operational needs and **workforce readiness**.

Key Benefits
1. Leverages and improves upon DoD 8570
2. Allows for Component customization
3. Supports integration of cyber workforce elements

DoD 8140 Qualification Program Tenets

The DoD 8140 Qualification Program was built to set cyber workforce standards for the Department while allowing for flexibility in Component implementation and workforce management.

Role-Based Progression

Qualifications are outlined based on DoD Cyber Workforce Framework (DCWF) work roles, according to three levels of proficiency, to enable career progression

Verification of Knowledge

Requisite knowledge is verified through Education or Training or Personnel Certification, providing both personnel and Components flexibility

Verification of Capability

Requisite capability is verified through On-the-Job Qualification and Environment Specific Requirements to ensure cyber personnel can meet mission needs

Continuous Professional Dev.

Personnel must complete at least 20 hours of professional development each year to ensure skillsets evolve along with changes in the environment

8140 Qualification Training & Certification

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

Fill out your Application of Intent

AI logic review scores the application, if approved, you move forward in the process.

Get your account via a Statement of Interest

Your application is sent to a DoD panel for final approval or adjudication.

Outreach to Interested Parties

Continuous monitoring and re-certification.

QUESTIONS

SCAN TO VIEW THE CYBER
WORKFORCE STRATEGY