GROWING THE NEXT GENERATION OF CYBER TALENT

Patrick Johnson

Director, Workforce Innovation Directorate

DoD CIO

September 2023

AGENDA

- Mission Statement
- DoD CWF Strategy Implementation Plan
- Cultivating Tomorrow's Talent Pool
- Cyber Academic Engagement Central Program Office
- What is the DoD Cyber Scholarship Program?
- DoD 8140 Qualification Model Example
- DoD Foundational Qualification Option: Education
- Questions

MISSION STATEMENT

The Department of Defense is one of the Nation's largest employers with approximately:

- 1.3 million active-duty service members
- 750,000 National Guard and Reserve service members
- 750,000 civilian personnel
- 600,000 contractors

Growing Our Talent:

To remain the strongest fighting force in the world, we must **recruit** and **retain** the best of America. That means we must continue:

- Building pathways of opportunity for all qualified American's.
- Deepening the Department's partnerships with America's best universities.
- Continuing to invest in training and education and create programs that focus on science, technology, engineering, and math.
- Providing exceptional opportunities for service and professional development for our total force.

DoD CWF STRATEGY IMPLEMENTATION PLAN

CWF Strategy

- Aims to 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.

Implementation Plan

- Sets the foundation for how the Department will execute the 22 objective and 38 initiatives aligned with the 4 overarching goals in the CWF Strategy.

- 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.

CULTIVATING TOMORROW'S TALENT POOL

CWF Strategy Goal 4:

- Foster collaboration and partnerships to enhance capability development, operational effectiveness and career broadening experiences.

Objective 4.3:

- Enhance collaboration with academia to cultivate a talent pipeline and support important areas of research.

Initiative 4.3.1:

- Establish a centralized program office to manage cyber-focused student and employee developmental programs across the Department.

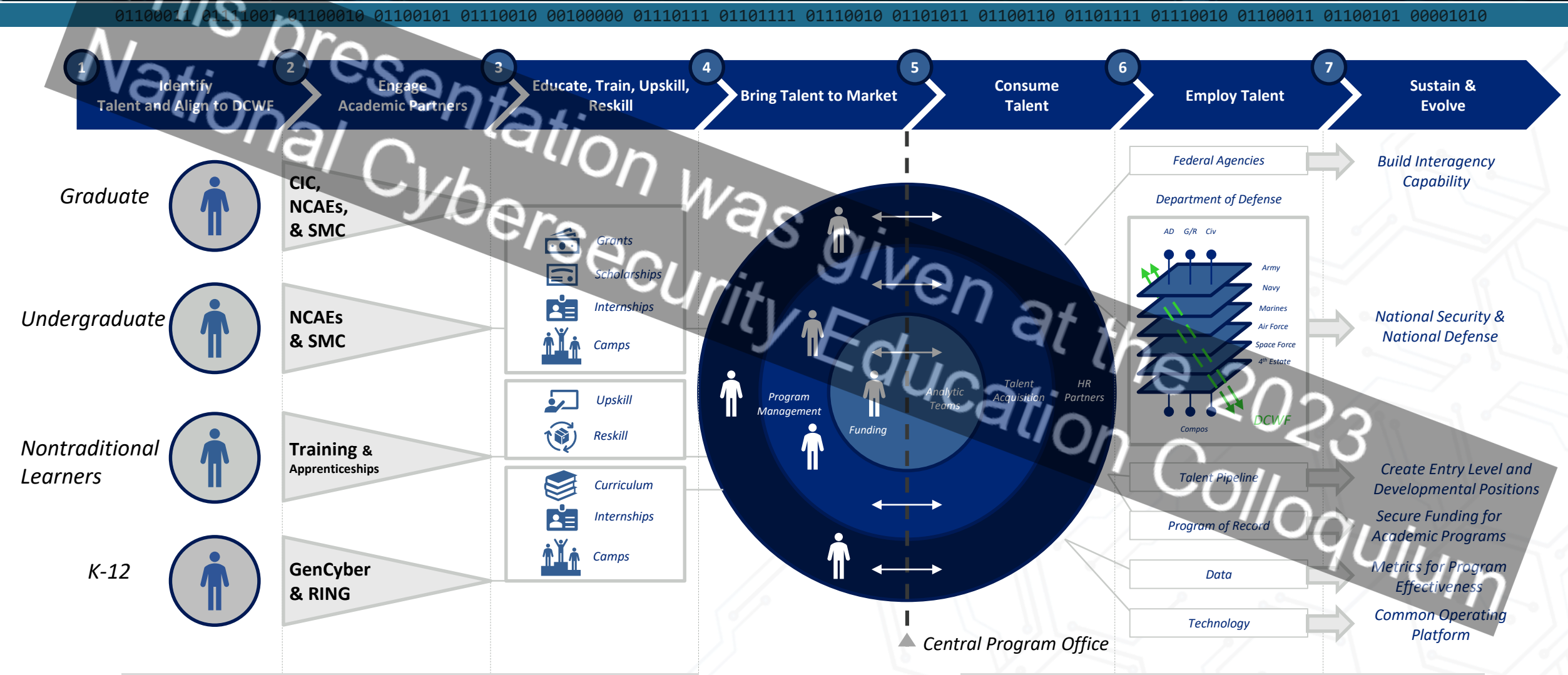
Initiative 4.3.2:

- Ensure NCAE-C curriculum aligns with Department-wide cyber standard.

Initiative 4.3.3:

- Increase return on investment of scholarship programs and effectively track participation to customize recruitment and outreach efforts.

CYBER ACADEMIC ENGAGEMENT CENTRAL PROGRAM OFFICE



WHAT IS THE DoD CYBER SCHOLARSHIP PROGRAM?

01100011 01111001 01100010 01100101 01110010 00100000 01110111

The DoD Cyber Scholarship Program (DoD CySP)

(Formerly the Information Assurance Scholarship Program) is designed to encourage the recruitment of the nation's top cyber talent and the retention of DoD personnel who have skills necessary to meet DoD's cyber requirements and help secure our nation against the threats of information systems and networks.

Grants awarded for scholarships and capacity building to NCAE-Cs:

Scholarships

Recruitment: Targets students who are not current DoD or Federal employees and who are enrolled at designated CAEs; may be undergraduate or graduate students
Retention: Targets Military and Civilian DoD personnel for Associates or Graduate (Certificates, Masters, and PhD programs)

NCAE-Cs

National Centers of Academic Excellence in Cybersecurity (NCAE-C)

National Centers of Academic Excellence in Cyber Defense (CAE-CD)

National Centers of Academic Excellence in Cyber Defense Research (CAE-R)

National Centers of Academic Excellence in Cyber Operations (CAE-CO)

DoD 8140 QUALIFICATION MODEL EXAMPLE

(621) Software Developer				
		Basic	**Intermediate**	**Advanced**
Foundational Qualification Options	**Education**	Associate degree or higher from an accredited college or university	Bachelor degree or higher from an accredited college or university	Bachelor degree or higher from an accredited college or university
		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	CSSLP	CISSP-ISSAP
Foundational Qualification Alternative	**Experience**	Conditional Alternative	Conditional Alternative	Conditional Alternative
Residential Qualification	**On-the-Job Qualification**	Always Required	Always Required	Always Required
	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.

DoD 8140 FOUNDATIONAL QUALIFICATION OPTION: Education

DoD CYBER EXCHANGE NIPR

DOD WORKFORCE INNOVATION DIRECTORATE

- 8140 Home
- Documents Library
- DoD Approved 8570 Baseline Certifications
- Frequently Asked Questions - FAQs
- Steps to Obtain a DoD 8570 Baseline Certification
- Summary of IA Workforce Qualification Requirements
- Help
- Workforce Innovation Directorate Home
- Qualifications Matrices

DoD 8140 Policy Requirements

Degree Achievement within 5 Years
Degree conferred within the past 5 years by an institution of higher education unless continuous work in a relevant discipline can be demonstrated.

Demonstration of Continuous Work
Considered documentation of employment covering any cyber work role with no more than three consecutive years lapse in cyber work.

DoD 8140 Qualification Approval Process

Academic Programs Mapped to DCWF Work Role Codes
Emphasis on ABET Accredited and CAE Designated Programs.
Example Programs: Computer Science, Cybersecurity, Data Science, Information Technology, Electrical Engineering, Information Systems, Software Engineering, Computer Engineering.

Basic, Intermediate, and Advanced Proficiency Levels for each Work Role Code
Associates, Bachelors, Masters, Doctoral Degrees, Masters Certificate mapped to proficiency level.

Survey on Cyber Education Requirements

Sponsor: Institute for Defense Analyses (IDA)
(on behalf of the DoD)

Purpose: To gather perspectives on how to best educate the DoD's cyber workforce to protect the Nation from future cyber threats (findings will be included in a report requested by Congress).

Survey Question Focus:

- Student capacity in cyber programs of study
- Educator staffing levels
- Cyber education preferences and requirements
- Perceptions of future cyber threats
- The need for a National Cyber Academy

SHARE YOUR THOUGHTS ON CYBER EDUCATION BY TAKING A BRIEF SURVEY

(visit the URL or Scan the QR Code below)

https://idaorg.gov1.qualtrics.com/jfe/form/SV_251iRbldGNIdmUC

QUESTIONS

SCAN TO VIEW THE CYBER WORKFORCE STRATEGY