DOD CYBER WORKFORCE STRATEGY

2023-2027

TABLE OF CONTENTS

FOREWORD

The Department of Defense's (DoD) cyber workforce plays a prominent role in safeguarding our Nation against current and future threats. To ensure the DoD deploys an agile, capable, and ready cyber workforce, the Office of the Department of Defense Chief Information Officer (DoD CIO) created the 2023-2027 DoD Cyber Workforce Strategy. This strategy establishes a unified direction for DoD cyber workforce management and, as the cyber domain continues to expand, the inclusion of emerging technology workforces. This strategy also provides a roadmap for how the cyber workforce will grow and adapt to guarantee our Nation's security.

More specifically, this strategy enables the Department to stay ahead of workforce trends by applying standardized workforce analysis tools and processes; continuing to develop cyber personnel to meet current and future requirements; championing the utilization of workforce-related authorities in non-traditional ways; and building strategic relationships in support of growing, diversifying and strengthening the cyber workforce.

This strategy will be followed by a cyber workforce implementation plan to ensure that the strategy's talent identification, recruitment, development, retention, and management objectives are achieved.

The successful implementation of the Cyber Workforce strategy will help the Department recruit and maintain the most talented, diverse, and dominant cyber workforce in the world.

Dr. Kathleen H. Hicks
United States Deputy Secretary of Defense

EXECUTIVE SUMMARY

The scope and pace of malicious cyber activity continues to grow with new threats and attacks to the Nation's infrastructure emerging daily. As a result of these threats and other cyber-related challenges, there is an enterprise-wide need to drive cultural change and further the development and sustainment of the cyber workforce. To meet this requirement, the DoD CIO, in close coordination with other Office of the Secretary of Defense (OSD) Component heads; the Joint Staff; United States Cyber Command (USCYBERCOM); and the military services, created this 2023–2027 DoD CIO Cyber Workforce Strategy. This strategy sets the foundation for how the Department will foster a cyber workforce capable of executing the Department's complex and varied cyber missions.

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 goals, which aid the Department in unifying efforts to achieve the mission and vision of this strategy. The four workforce goals are:

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.

A forthcoming implementation plan will outline a prioritized list of implementation activities the DoD CIO will lead to achieve the goals and objectives of this strategy. This strategy, along with the implementation plan, will enable the Department to identify and qualify its military and civilian personnel while also developing plans for recruiting and retaining our highly effective cyber workforce.

INTRODUCTION

> "To recruit and retain the most talented workforce, we must advance our institutional culture and reform the way we do business. The Department must attract, train and promote a workforce with the skills and abilities to tackle national security challenges, creatively and capably, in a complex global environment."
>
> — Mr. Lloyd Austin, III,
> Secretary of Defense

As the principal staff assistant and senior information technology advisor to the Secretary of Defense, the DoD CIO oversees national security and defense business systems, manages information resources and finds efficiencies. The DoD CIO develops tools, resources and programs for the governance, recruitment, retention and professional development of the DoD cyber workforce.

The DoD CIO developed this strategy to provide focus to cyber-related human capital initiatives in support of the 2022 National Defense Strategy that states the Department must "Cultivate the Workforce We Need." However, we believe the Department must also consider the future and lay the ground work to "Build the Workforce We Anticipate." This strategy identifies the need for a cultural shift to reform the management of the Department's most valuable asset: its people.

CHALLENGES

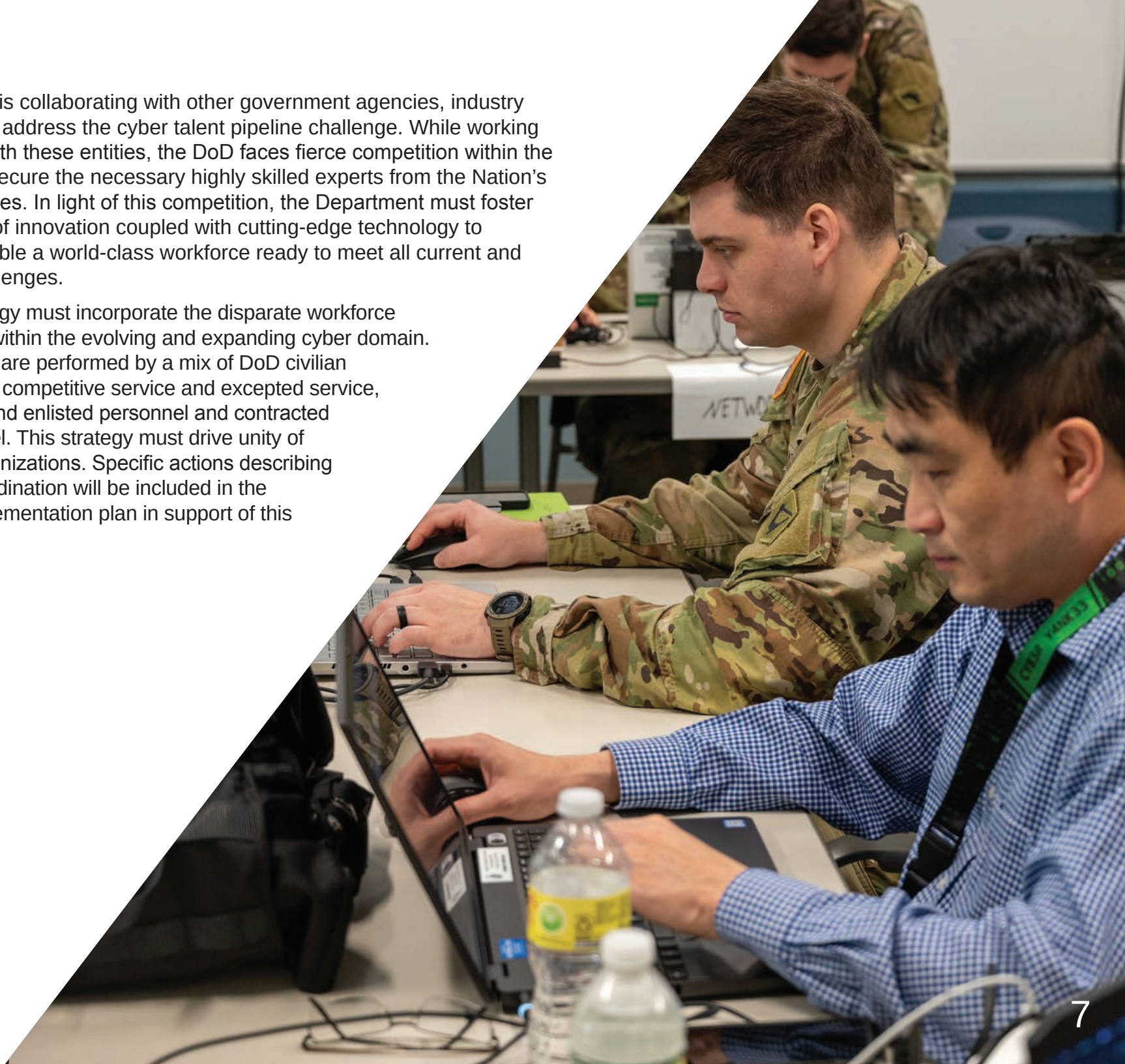
> To address the numerous workforce challenges DoD faces, we must take a unified and coordinated approach that takes meaningful action to reduce the talent pipeline gap, increase the quality and diversity of our cyber workforce, and prioritize the personal and professional needs of our cyber practitioners.
>
> — Mr. John Sherman, DoD CIO

The scope and pace of malicious cyber activities continues to grow, even after the COVID-19 pandemic created a significant amount of disruption and resulted in lasting impacts on the global work environment. The World Economic Forum—Global Technology 2021 Report estimated a 238% increase in cyber attacks due to the massive uptick in and shift to remote work and cloud-based solutions. Additionally, state actors and affiliated hacker groups have increased their attacks targeting the federal government and private industry. Some recent cyber attacks from foreign actors that threaten the Nation's security are the SolarWinds hack, which was directed by the Russian Intelligence Service, the ransomware attack on the Colonial Pipeline by a Russia-linked cybercrime group, and cyber espionage and other malicious cyber operations targeting a range of government and private-sector organizations across industries from Iranian-linked hackers.

To combat current and future cyber threats and attacks, the DoD must employ an agile, highly skilled and diverse cyber workforce. The Department must also expand its cyber workforce with various roles and develop talent to securely build, operate and maintain its digital and critical infrastructures and protect and defend our data against cyber adversaries at home and abroad. However, there is a recognized shortage of skilled cyber personnel that could potentially impact operational readiness across the Department and put national security at risk. Despite the vast expansion of cyber educational and experiential opportunities, the Nation's cyber talent pipeline remains limited.

The Department is collaborating with other government agencies, industry and academia to address the cyber talent pipeline challenge. While working collaboratively with these entities, the DoD faces fierce competition within the labor market to secure the necessary highly skilled experts from the Nation's finite talent sources. In light of this competition, the Department must foster an environment of innovation coupled with cutting-edge technology to produce and enable a world-class workforce ready to meet all current and future cyber challenges.

Finally, this strategy must incorporate the disparate workforce supporting DoD within the evolving and expanding cyber domain. Cyber work roles are performed by a mix of DoD civilian employees in the competitive service and excepted service, military officers and enlisted personnel and contracted support personnel. This strategy must drive unity of effort across organizations. Specific actions describing the required coordination will be included in the forthcoming implementation plan in support of this strategy.



The DoD Cyber Workforce

DEFINITION

The DoD cyber workforce is defined in DoDD 8140.01 as, “Personnel who build, secure, operate, defend and protect DoD and U.S. cyberspace resources; conduct related intelligence activities; enable future operations; and project power in or through cyberspace.” It is comprised of personnel assigned to the following workforce elements: Information technology (IT), cybersecurity, cyberspace effects, intelligence workforce (cyberspace) and cyberspace enablers.

With the cyber landscape continuing to evolve, the Department is working to expand the scope of the cyber workforce to include the technological areas pertaining to artificial intelligence (AI), cloud, data and secure software development. The Department is also ensuring the skills required for building, securing, operating, defending and protecting control systems are embedded into the Department’s approach to human capital efforts outlined in this strategy.

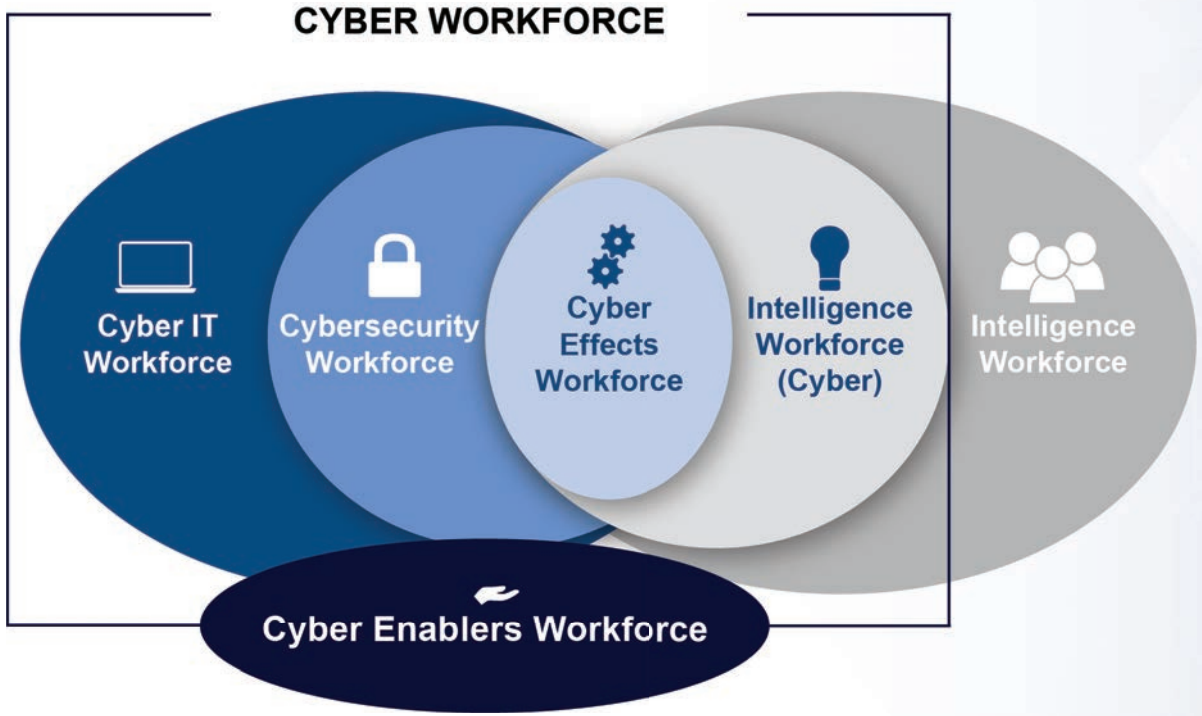


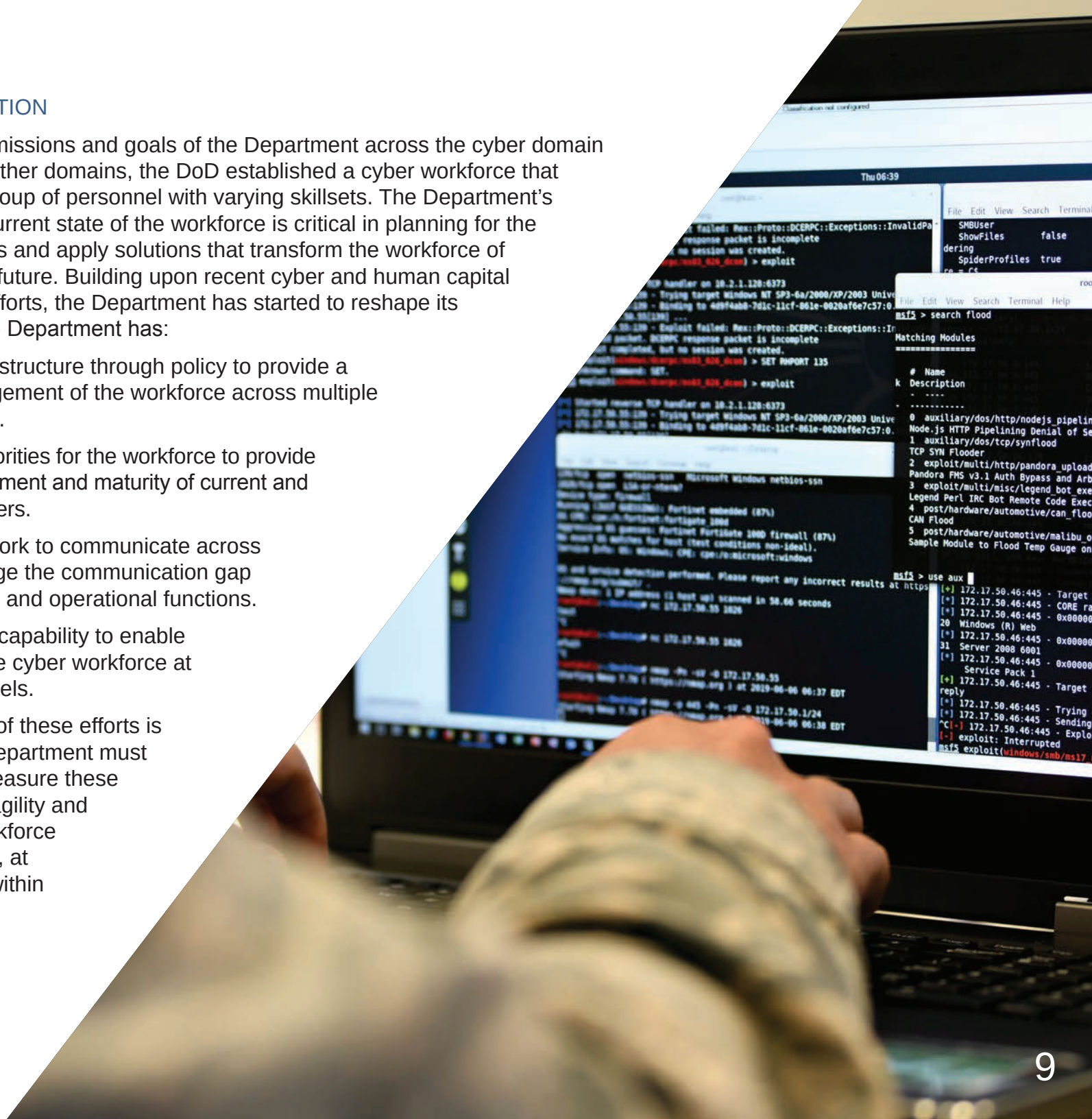
Figure 1 – DoD Cyber Workforce

CURRENT IMPLEMENTATION

To accomplish the varied missions and goals of the Department across the cyber domain and its intersections with other domains, the DoD established a cyber workforce that encompasses a diverse group of personnel with varying skillsets. The Department's ability to understand the current state of the workforce is critical in planning for the future to allocate resources and apply solutions that transform the workforce of today into the force of the future. Building upon recent cyber and human capital strategy implementation efforts, the Department has started to reshape its workforce. Specifically, the Department has:

- Created a governance structure through policy to provide a standard for the management of the workforce across multiple functional communities.
- Implemented new authorities for the workforce to provide flexibility in the management and maturity of current and future workforce members.
- Implemented a framework to communicate across the total force and bridge the communication gap between administrative and operational functions.
- Developed an analytic capability to enable an understanding of the cyber workforce at macro and granular levels.

However, implementation of these efforts is in the initial stages. The Department must continue to mature and measure these initiatives to advance the agility and capability of the cyber workforce across the DoD enterprise, at the component level and within individual commands.



PURPOSE

There is a need to further the development and sustainment of the cyber workforce required to maintain a U.S. advantage in a contested and rapidly evolving cyberspace. To meet this requirement, the 2023–2027 DoD Cyber Workforce Strategy takes a proactive approach in setting unifying direction and guidance for the Department to foster a cyber workforce that will be ready to execute cyber missions.

This strategy will underpin Department efforts to:

- Close workforce management gaps (e.g., limited developmental positions and training opportunities).
- Resource workforce management and development initiatives in accordance with updated capability planning guidance.
- Stay at the forefront of technological advances (e.g., AI, cloud, cyber, data, secure software development, embedded systems, quantum computing, advanced cryptography and zero-trust).
- Securely and rapidly deliver resilient systems.
- Transform into a data-centric organization with optimized data analytics to build cyber workforce requirements and proactively address the cyber workforce at the speed and scale for operational advantage.

The Department strives to be an “employer of choice” among cyber professionals and works to attract the best cyber warriors, given our unique and important mission set. Now more than ever, it is essential that we expand our cyber workforce with diverse roles and develop talent to securely build, operate and maintain our digital and critical infrastructures and protect and defend our data against cyber adversaries at home and abroad.

As the DoD looks to the future, this strategy lays the foundation for how the Department will establish the direction and supporting mechanisms for the unified management of different communities and workforce types that

make up the cyber workforce. This will ensure the Department is strongly positioned and equipped to identify, recruit, retain and develop the world-class cyber talent necessary to match the requirements created by emerging technology, tactics and procedures in this transformational, digital age. To overcome identified challenges, we will align our strategic goals and implementation efforts to four human capital management pillars, which will provide the foundation for unified management and empowerment of the DoD cyber workforce.

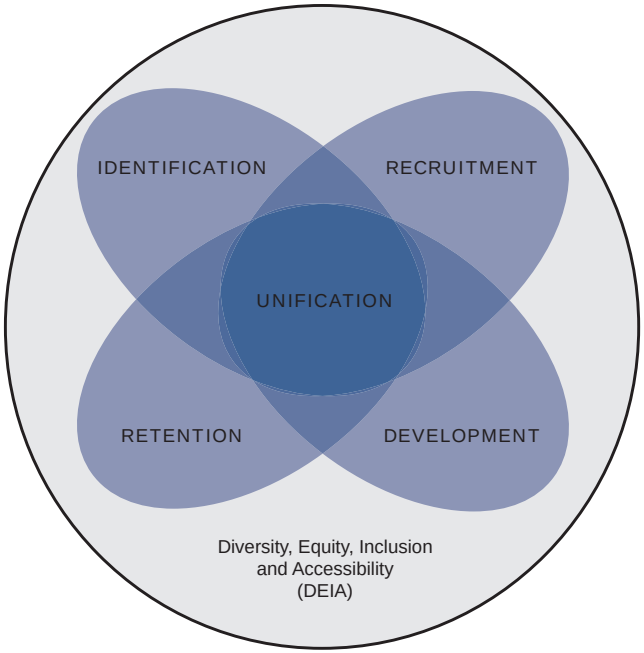


Figure 2 – Four Human Capital Pillars

FOUR PILLARS

The four pillars are: Identification, Recruitment, Development and Retention. The pillars provide a unifying direction to accomplish the mission, vision and goals laid out in this strategy. Utilization of the four pillars helps the DoD identify and group current cyber workforce challenges along with the human capital initiatives the DoD is implementing to address them. The four pillars are defined as follows:

Identification — The processes of determining workforce needs or requirements and the potential or incumbent workforce to meet them.

Recruitment — Identifying and attracting the talent needed to meet mission requirements and the process of evaluating the effectiveness of recruiting efforts.

Development — Understanding individual and team performance requirements and providing the necessary opportunities and resources to satisfy those performance requirements.

Retention — The incentive programs the Department employs to retain talent and the process of evaluating the effectiveness of the incentive programs.

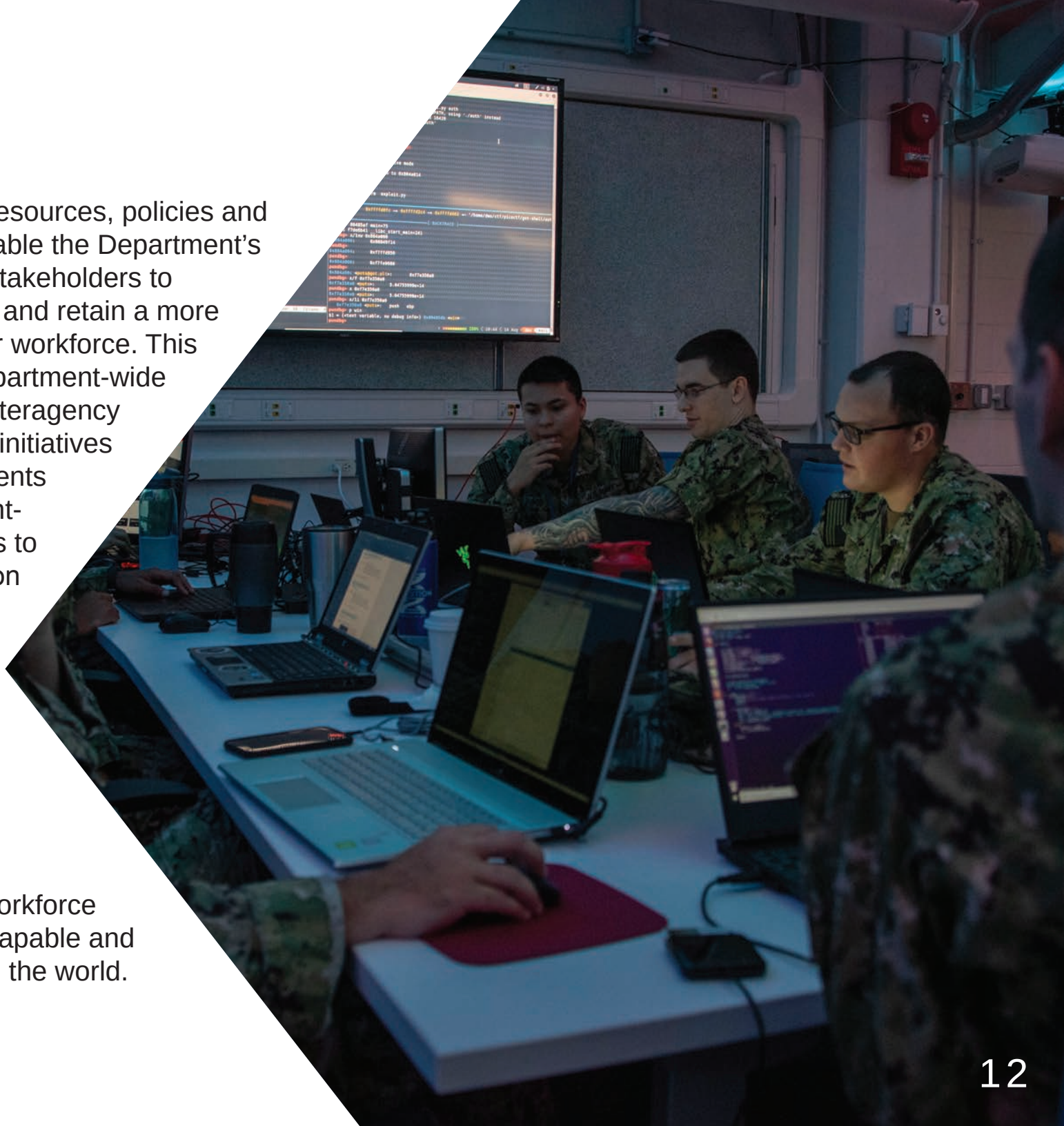
Diversity, equity, inclusion and accessibility (DEIA) ensures the Department consists of cyber professionals with diverse backgrounds, skillsets, thought processes and worldviews. If the Department's cyber workforce is to become the most capable and dominant force in the world, it must champion DEIA. Doing so mitigates the risk of the Department becoming an echo chamber of likeminded thought leaders who are unable to implement innovative solutions to cyber problems. The Department intends to cultivate a workforce that draws from the full diversity of the Nation.

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.



GOALS

The following workforce goals have been identified to achieve the mission and vision of this strategy.

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.

Each goal is described further in the following sections.

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

The Department must continue to develop processes that align workforce metrics to mission requirements while operationalizing risk-based decisions that can be tailored to key workforce segments at each echelon of the enterprise. This is required to maintain a clear understanding of capability needs across the Department and drive agile decision making in today's complex threat environment. To effectively address this goal, the Department should compel the use of a common foundation for workforce evaluations, as well as expand the use of proven capability assessment processes and supporting analytical tools with built-in quality assurance mechanisms. Together, these activities will ensure the Department is able to assess current capabilities, project future workforce trends and proactively adjust resources to support leadership priorities and varied DoD mission sets.

Goal 1 Objectives:

1.1 Implement a repeatable capability and workforce requirement review process to ensure identified needs reflect environmental demands.

1.2 Expand and refine frameworks to better support requirements identification.

1.3 Utilize advanced analytic capabilities to increase the speed, accuracy and efficiency of capability and requirement reviews.

1.4 Establish a repository of organizations with known capabilities to better identify partnership

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

The Department requires a holistic approach to talent management that ensures there are targeted mechanisms in place to recruit, develop and retain critical cyber talent. This approach must include multiple feeder systems to address identified needs, close capability gaps and drive the evolution of skill sets to maintain an advantage against our adversaries. It is imperative that the Department establish an enterprise-wide talent management program to unify the broader cyber workforce under a common umbrella that allows for enhanced interoperability and workforce planning opportunities.

Goal 2 Objectives:

2.1 Develop and implement assessments to align talent with development programs and training pipelines for the roles best suited.

2.2 Develop enhanced guidance for talent acquisition to include previously untapped or under-represented sources of talent.

2.3 Manage as a unified functional community. Compel development, employment and resourcing decisions with a whole of community perspective.

2.4 Drive continuous development to foster capability advancement across all proficiency and experience levels.

2.5 Improve and expand new employee development programs as a part of talent management.

2.6 Include changing mission requirements in development pipelines to match talent management to mission.

2.7 Evaluate capability demonstration programs, including performance-based assessments to maximize reach and effectiveness.

Facilitate a cultural shift to optimize Department-wide personnel management activities

The COVID-19 pandemic caused a shift in the future of work (e.g., expansion of telework, holistic views of work and worker health). What might seem like a challenge is an opportunity, which if fully embraced and properly communicated, will provide a competitive advantage to recruit, develop and retain world-class cyber talent. Specifically, the Department needs to facilitate a cultural shift in how it optimizes personnel management authorities and their application. This must involve utilizing existing authorities in nontraditional ways that consider agility, flexibility, responsiveness and innovation. Additionally, the Department should focus on enhancing personnel management authorities and, when possible, expanding their scope to facilitate broad impact. Facilitating a cultural shift will enable to Department to draw from a more expansive talent pool to meet current and future mission needs.

Goal 3 Objectives:

3.1 Establish a Cyber Workforce Development Fund to accelerate implementation activities and enable training throughout to match demand.

3.2 Champion remote work flexibilities and policies to expand opportunities across the cyber workforce.

3.3 Review the application of existing authorities to include and attract a broader pool of talent.

3.4 Apply security clearance requirements appropriately for cyber positions, billets and personnel to increase positional flexibility.

3.5 Establish a mechanism for part-time surge support based on emergent mission need.

3.6 Expand Cyber Excepted Service (CES) authorities to optimize program capabilities and increase attractiveness for talent.

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

Collaboration, both internal and external (e.g., other government agencies, industry, academia, allied nations) to the Department, are critical engagements that should be leveraged to grow and enhance workforce capabilities. The Department must continue to prioritize these engagements, allocate the necessary resources to support these efforts and proactively ensure a mutual benefit. Additionally, the Department must continuously seek opportunities to strengthen critical alliances and further DoD's role as a domestic and global leader of cyber expertise.

Goal 4 Objectives:

4.1 Pilot an apprenticeship program to develop dedicated employment exchanges with the private sector.

4.2 Leverage talent exchanges to attract experienced talent and provide career broadening opportunities for existing cyber workforce members.

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

4.4 Strengthen partnerships with federal agencies, specifically partnerships focused on career broadening opportunities, cross-training and information sharing.

4.5 Leverage partnerships with allies and partner nations to strengthen force development capabilities and interoperability.

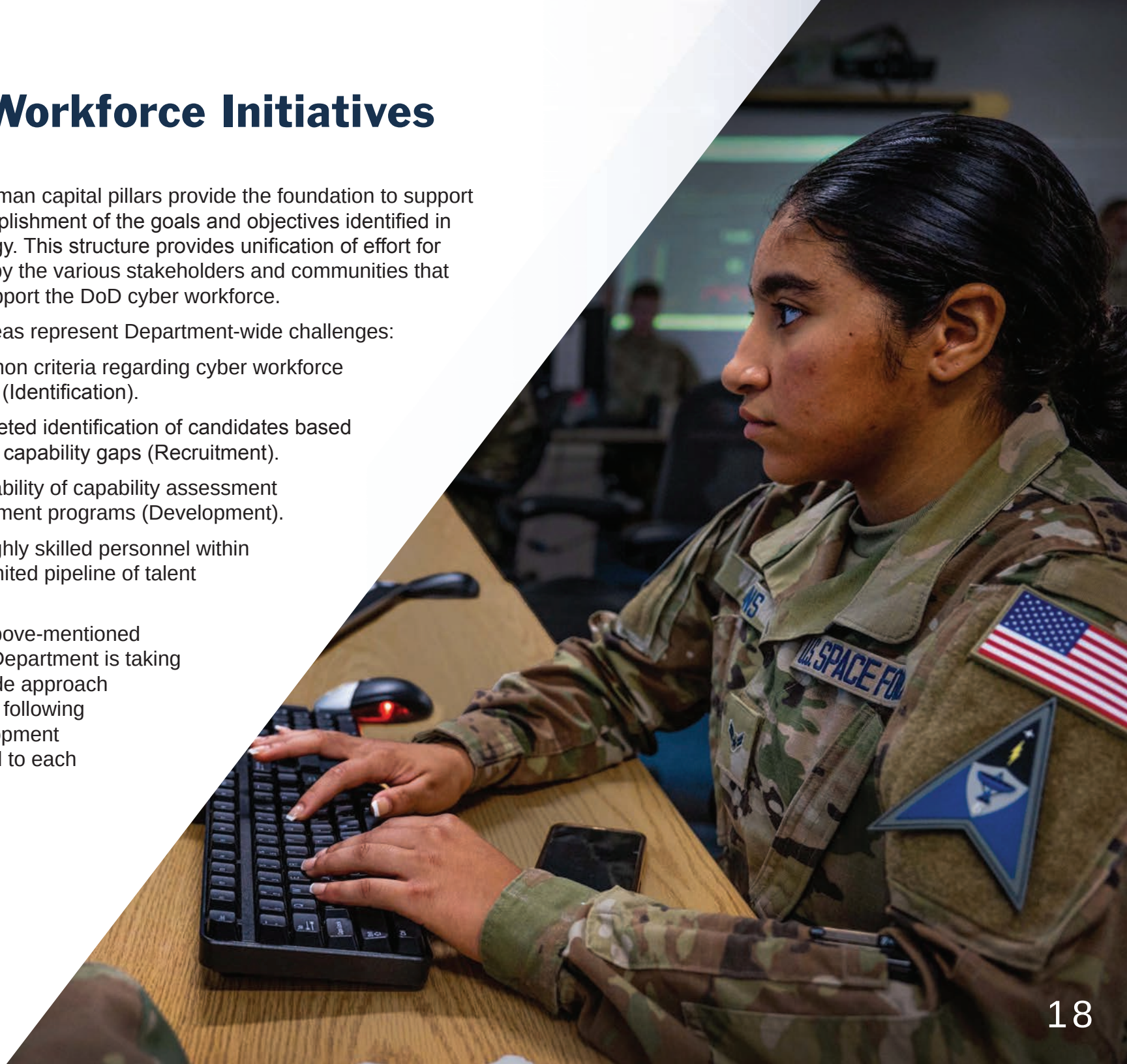
Cyber Workforce Initiatives

The four human capital pillars provide the foundation to support the accomplishment of the goals and objectives identified in this strategy. This structure provides unification of effort for implementation by the various stakeholders and communities that make up and support the DoD cyber workforce.

The following areas represent Department-wide challenges:

- Lack of common criteria regarding cyber workforce requirements (Identification).
- Need for targeted identification of candidates based on skills to fill capability gaps (Recruitment).
- Limited availability of capability assessment and enhancement programs (Development).
- Attrition of highly skilled personnel within an already limited pipeline of talent (Retention).

To resolve the above-mentioned challenges, the Department is taking an enterprise-wide approach to implement the following workforce development initiatives aligned to each strategic goal.



These initiatives will enable the Department to meet the cyber challenges of today and tomorrow. Further details on the initiatives listed in Table 1 will be provided in the forthcoming implementation plan for this strategy.

Human Capital Pillars				Initiatives
✓	✓	✓	✓	Prescribe standards and assign responsibilities for the management of the DoD cyber workforce to include the identification, tracking, qualification and reporting of the workforce through the DoD 8140 Policy Series.
	✓	✓	✓	Code cyber workforce positions using the DoD Cyber Workforce Framework (DCWF).
	✓	✓		Establish a repeatable review process that will examine cyber workforce requirements and capabilities.
	✓		✓	Seek additional authorities to extend and further refine the DoD CES and the Targeted Local Market Supplement (TLMS), helping to provide incentives and flexible capabilities to recruit and retain employees for civilian cyber positions.
✓	✓	✓	✓	Further develop and educate the cyber workforce on the current and future programs offered to help attract, retain and develop the cyber workforce (e.g., DoD Cyber Workforce Rotational Program (CWRP), DoD Cyber Scholarship Program (CySP) and the Cyber Information Technology Exchange Program (CITEP)).
	✓	✓	✓	Integrate and further advance the data analytics capabilities across the Department to support senior level leadership during crucial policy and program development. Continue building the Advana use case to help the DoD CIO evolve from a compliance role to a center of excellence for enterprise-wide cyber workforce analytics that integrate with and inform risk assessments.

IDENTIFICATION RECRUITMENT DEVELOPMENT RETENTION

Table 1 – Cyber Workforce Initiatives

CLOSING SUMMARY

"Whether supporting our warfighters in today's challenging threat environment, or creating efficiencies in the department, DoD needs highly skilled military and civilian workforces. We need individuals to support rapidly-evolving areas from nanotechnology to robotics. And we need people with digital skillsets, including data scientists, software developers and machine learning experts."

— Dr. Kathleen H. Hicks,
Deputy Secretary of Defense

This strategy sets the direction for the Department to develop and grow the cyber workforce in a unified and intentional manner, bridging the gap between the current state of the cyber workforce and the outcome described in the strategic vision. It provides a unifying direction for the Department in identifying, recruiting, developing and retaining high-demand cyber talent capable of achieving and sustaining dominance in a highly contested domain. This strategy also identifies targeted workforce goals and objectives, which in conjunction with the forthcoming implementation plan, will support the DoD in achieving the enclosed mission and vision. The current and future state of the Department's cyber workforce and capabilities is crucial in building, securing, operating, defending and protecting DoD and U.S. cyberspace resources, conducting related intelligence activities, enabling future operations, preserving the Nation's well-being and projecting power in and through cyberspace.

APPENDICES

APPENDIX A — 2023–2027 DOD CYBER WORKFORCE STRATEGY GOALS & OBJECTIVES

DoD Strategic Goals	
2022 National Defense Strategy (NDS)	Strategic Goal 4: Cultivate the Workforce We Need
FY22-FY26 DOD Civilian Human Capital (HC) Operating Plan	Human Capital Objectives (HCOs) HCO 1: Manage People HCO 2: Cultivate a Culture of Engagement and Inclusion HCO 3: Advance Human Resources
Strategic Human Capital Management (SHCM) Goals	1. Invest in our national security workforce by 1) recruiting; 2) developing; 3) retaining; and 4) inspiring an existing and new generation to remain in public service. 2. Ensure the workforce is agile, information-advantaged, motivated, diverse and highly-skilled.
2023–2027 DoD Cyber Workforce Strategy Goals & Objectives	
Goal 1: Execute consistent capability assessment and analysis processes to stay ahead of force needs.	
Objectives:	1.1 Implement a repeatable capability and workforce requirement review process to ensure identified needs reflect environmental demands. 1.2 Expand and refine frameworks to better support requirements identification. 1.3 Utilize advanced analytic capabilities to increase the speed, accuracy and efficiency of capability and requirement reviews. 1.4 Establish a repository of organizations with known capabilities to better identify partnership or pipeline sources. Include nontraditional or under-represented capability sources to bring in new solutions.
Goal 2: Establish an enterprise-wide talent management program to better align force capabilities with current and future requirements.	
Objectives:	2.1 Develop and implement assessments to align talent with development programs and training pipelines for the roles best suited. 2.2 Develop enhanced guidance for talent acquisition to include previously untapped or under-represented sources of talent. 2.3 Manage as a unified functional community. Compel development, employment and resourcing decisions with a whole of community perspective. 2.4 Drive continuous development to foster capability advancement across all proficiency and experience levels. 2.5 Improve and expand new employee development programs as a part of talent management. 2.6 Include changing mission requirements in development pipelines to match talent management to mission. 2.7 Evaluate capability demonstration programs including performance based assessments to maximize reach and effectiveness.

APPENDICES

APPENDIX A — 2023–2027 DOD CYBER WORKFORCE STRATEGY GOALS & OBJECTIVES

DoD Cyber Workforce Strategy Goals & Objectives (Continued)	
Goal 3: Facilitate a cultural shift to optimize Department-wide personnel management activities.	
Objectives:	3.1 Establish a Cyber Workforce Development Fund to accelerate implementation activities and enable training throughout to match demand. 3.2 Champion remote work flexibilities and policies to expand opportunities across the cyber workforce. 3.3 Review the application of existing authorities to include and attract a broader pool of talent. 3.4 Apply security clearance requirements appropriately for cyber positions, billets and personnel to increase positional flexibility. 3.5 Establish a mechanism for part-time surge support based on emergent mission need. 3.6 Expand CES authorities to optimize program capabilities and increase attractiveness for talent.
Goal 4: Foster collaboration and partnerships to enhance capability development, operational effectiveness and career broadening experiences.	
Objectives:	4.1 Pilot an apprenticeship program to develop dedicated employment exchanges with the private sector. 4.2 Leverage talent exchanges to attract experienced talent and provide career broadening opportunities for existing cyber workforce members. 4.3 Enhance collaboration with academia to cultivate a talent pipeline and support important areas of research. 4.4 Strengthen partnerships with federal agencies, specifically partnerships focused on career broadening opportunities, cross-training and information sharing. 4.5 Leverage partnerships with international allies and partners to strengthen force development capabilities and interoperability.

Table 2 - 2023–2027 DoD Cyber Workforce Strategy Goals & Objectives

APPENDICES

APPENDIX B – ACRONYM GLOSSARY

Acronym Glossary	
AI	Artificial Intelligence
CES	Cyber Excepted Service
CIO	Chief Information Officer
CITEP	Cyber Information Technology Exchange Program
CWRP	Cyber Workforce Rotational Program
CySP	Cyber Scholarship Program
DCWF	DoD Cyber Workforce Framework
DEIA	Diversity, Equity, Inclusion and Accessibility
DoD	Department of Defense
IT	Information Technology
NDS	National Defense Strategy
OSD	Office of the Secretary of Defense
TLMS	Targeted Local Market Supplement
USCYBERCOM	United States Cyber Command