Fiscal Year 2025 Budget Estimates

Defense Human Resources Activity Cyber

March 2024

Operation and Maintenance, Defense-Wide Summary ($ in thousands)
Budget Activity (BA) 4: Administration and Service-wide Activities

	FY 2023 Actuals	Price Change	Program Change	FY 2024 Estimate	Price Change	Program Change	FY 2025 Estimate
DHRA Cyber	36,043	1,128	-9,654	27,517	578	11,686	39,781

- FY 2023 includes $0 in Overseas Operations Costs (OOC) Actuals. FY 2024 includes $0 in OOC Estimate. FY 2025 includes $0 for the OOC Budget Estimate. OOC were financed previously with former Overseas Contingency Operations (OCO) funding.
- This DoD component is a budget line item in the Operation and Maintenance Defense-wide account and therefore, the FY 2024 Estimate does not reflect a CR adjustment. The overall Operation and Maintenance, Defense-wide account CR adjustment for FY 2024 may be found in the O-1 document.

I. Description of Operations Financed:

The Defense Human Resources Activity (DHRA) is a Field Activity of the Under Secretary of Defense (Personnel & Readiness), (USD (P&R)) that consists of a headquarters and multiple direct reporting organizations. DHRA by design gives USD (P&R) greater capability and flexibility in managing the work of a diverse set of activities supporting the department’s human resources mission. Each direct reporting organization within DHRA has a unique, but complementary mission set. Headquarters DHRA serves as an intermediate headquarters, planning, programming, and budgeting for all activities within the DHRA enterprise and in executing, coordinating, and providing direct oversight to the work of its direct reporting organizations. DHRA ensures that the Department’s warfighters present and past along with their families and civilian members of the Department receive the care and support they deserve, fairly, and in a timely fashion, through benefits administration, program execution and policy enforcement.

The DHRA FY 2025 cybersecurity budget is used to support the secure operation of the information systems that enable DHRA to successfully execute its mission to:

- Organize, direct, and manage all assigned resources, to include the programs described herein;
- Maintain a central repository of the Department of Defense (DoD) Human Resource (HR) information, both current and historic;
- Provide rapid data-driven analytic solutions to support the decision-making needs to effectively maintain the readiness of the All-Volunteer Force;
- Administer the sexual assault prevention and response policies and programs for DoD;
- Administer transition assistance programs for the DoD Service members leaving active duty;
- Serve as the single focal point for commercial travel within the DoD and centrally manage all commercial travel programs;
- Administer the program that distributes DoD identification cards to members of the Military, DoD civilians, contractors, and other eligible personnel;
- Serve as the authoritative source of identification and authentication of DoD-affiliated personnel for credentialing, identity protection, security, entitlements, and benefits verification;

I. Description of Operations Financed: (Cont.)

- Administer the federal responsibilities of the Uniformed and Overseas Citizens Absentee Voting Act of 1986, as most recently amended by the Military Overseas Voter Empowerment Act;
- Provide assistive technology to allow DoD and federal employees with disabilities to access electronic and information technology;
- Provide assistance to Service members and Veterans to pursue their educational goals and earn degrees or certifications during and after their service.

In particular, the DHRA Cybersecurity budget is used to deliver and enhance a cybersecurity program that safeguards DHRA information infrastructure and data assets from unauthorized use, disclosure, modification, damage or loss by implementing standardized security practices in planning, implementation, management, and operations that foster a secure operating environment by:

- Defending, mitigating and securing current and future systems, networks and infrastructure against cyber threats;
- Operating continuous monitoring and assessment tools, such as network and host vulnerability scanners, compliance scanners, and intrusion detection systems;
- Strengthening technical measures to maintain an agile and resilient network and infrastructure;
- Provide incident response for identified cybersecurity incidents;
- Developing and enforcing policy to support this mission and educating DHRA associates about security requirements;
- Regularly assessing systems using Risk Management Framework (RMF) methodologies;
- Providing security architecture consulting to DHRA programs requiring additional guidance.

Narrative Explanation of Changes:
The FY 2025 DHRA Cyber budget represents a net programmatic increase of $11.686 million with a price growth of $0.578 million.

Cyber Funding:

(Dollars in Thousands)		
FY 2023	**FY 2024**	**FY 2025**
36,043	**27,517**	**39,781**

Defense Suicide Prevention Office (DSPO):

(Dollars in Thousands)		
FY 2023	**FY 2024**	**FY 2025**
77	**103**	**106**

I. Description of Operations Financed: (Cont.)

This is for DSPO's Military Mortality Database (MMDB). This is to fund on-going cyber services, to include contracts and procurements to establish policy, procedures, process controls, compliance with orders and directives, incident response, system protections and tools. This includes capabilities to detect, monitor, analyze, respond to, report on, and prevent cybersecurity incidents.

Defense Manpower Data Center (DMDC) manages five DHRA programs:

- Defense Enrollment Eligibility Reporting System (DEERS)
- Enterprise Data Service (EDS)
- Enterprise Human Resource Information System (EHRIS)
- Identity Credential Management (ICM)
- Personnel Accountability and Security (PAS)

Cybersecurity funding supports the sustainment of DMDC's cyber toolsets, enterprise security engineering, auditing, continuous monitoring, incident response, and compliance reporting. These costs and services are shared across all of DMDC's Programs to provide efficiencies of scale and allow the specialization of the cybersecurity professionals that provide the support. Cybersecurity funding is also used to acquire DoD-mandated Cybersecurity Service Provider support for each program's systems.

DMDC – Defense Enrollment Eligibility Reporting System (DEERS):

(Dollars in Thousands)		
FY 2023	**FY 2024**	**FY 2025**
4,995	**5,013**	**12,393**

Cybersecurity funding provides the DEERS portfolio with access to DMDC's continuous monitoring program, cybersecurity tools, audits, incident response, risk management support, and security engineering services.

DMDC – Enterprise Data Service (EDS):

(Dollars in Thousands)		
FY 2023	**FY 2024**	**FY 2025**
7,660	**4,548**	**8,855**

Cybersecurity funding provides the EDS portfolio with access to DMDC's continuous monitoring program, cybersecurity tools, audits, incident response, risk management support, and security engineering services.

I. Description of Operations Financed: (Cont.)

DMDC – Enterprise Human Resource Information System (EHRIS):

(Dollars in Thousands)		
FY 2023	FY 2024	FY 2025
2,997	2,116	2,185

Cybersecurity funding provides the EHRIS portfolio with access to DMDC's continuous monitoring program, cybersecurity tools, audits, incident response, risk management support, and security engineering services.

DMDC – Identity Credential Management (ICM):

(Dollars in Thousands)		
FY 2023	FY 2024	FY 2025
14,320	9,476	9,797

Cybersecurity funding provides the ICM portfolio with access to DMDC's continuous monitoring program, cybersecurity tools, audits, incident response, risk management support, and security engineering services.

DMDC – Personnel Accountability and Security (PAS):

(Dollars in Thousands)		
FY 2023	FY 2024	FY 2025
3,330	2,289	2,358

Cybersecurity funding provides the PAS portfolio with access to DMDC's continuous monitoring program, cybersecurity tools, audits, incident response, risk management support, and security engineering services.

Defense Personnel Analytics Center (DPAC) manages two DHRA programs:

- DoD Office of the Actuary (OACT)
- Office of People Analytics (OPA)

The Office of the Actuary does not have any specific cyber requirements.

I. Description of Operations Financed: (Cont.)

DPAC – Office of People Analytics (OPA):

(Dollars in Thousands)		
FY 2023	**FY 2024**	**FY 2025**
484	**801**	**819**

Cyber funding is used by OPA for necessary annual audits under the Risk Management Framework (RMF) and for Cyber Security Service Provider (CSSP) support for our testing and recruiting related applications.

Defense Support Service Center (DSSC) manages the following DHRA programs:

- Computer/Electronic Accommodations Program (CAP)
- Defense Activity for Non-Traditional Education Support (DANTES)
- Defense Language and National Security Education Office (DLNSEO)
- Defense Travel Management Office (DTMO)
- Employer Support of the Guard and Reserves (ESGR)
- Federal Voting Assistance Program (FVAP)
- Military-Civilian Transition Office (MCTO)

DSSC – Computer/Electronic Accommodations Program (CAP):

(Dollars in Thousands)		
FY 2023	**FY 2024**	**FY 2025**
408	**113**	**117**

The Computer/Electronic Accommodations Program (CAP) is recognized by the U.S. Office of Personnel Management as a model program to increase DoD Federal employment of individuals with Targeted and Specific disabilities. The program has provided over 233,000 accommodations to more than 95,000 DoD civilian employees and Service members since its inception. CAP is widely recognized as the principal source on providing disability employment subject matter expertise, assistive technology solutions, and employment support services. These functions would not be possible without the use of CAP's Defense Business System (DBS), CAPX. CAPX is comprised of CAP's website and secure portal, Activity and Reporting Management System (ARMS). CAPX is hosted by the Defense Manpower Data Center (DMDC). DMDC's role as the hosting provider includes network and cybersecurity support and to assist CAP with managing/supporting CAPX's Authority to Operate (ATO).

I. Description of Operations Financed: (Cont.)

DSSC – Defense Activity for Non-Traditional Education Support (DANTES):

(Dollars in Thousands)		
FY 2023	FY 2024	FY 2025
319	330	337

DANTES cyber activities support two IT investments: DoD Voluntary Education Partnership Memorandum of Understanding (DoD MOU) and the Joint Services Transcript (JST). DoD policy requires educational institutions that wish to participate in the DoD Tuition Assistance (TA) Program to sign the MOU conveying the commitments and agreements between the educational institution and the DoD prior to an educational institution receiving funds from a service's TA program. JST is an official academic record that provides colleges and universities with documented evidence of professional military education, training, prior learning, and occupation experiences achieved by service members and veterans. Cyber security activities to support these two IT investments include contractor support to complete DoD Risk Management Framework accreditation requirements (e.g. Cyber Security Service Provider (CSSP) and Authorization to Operate (ATO) validations).

DSSC – Defense Language and National Security Education Office (DLNSEO):

(Dollars in Thousands)		
FY 2023	FY 2024	FY 2025
202	268	274

Supports the cybersecurity requirements for DLNSEO's information technology systems. Funding is used to ensure compliance with Risk Management Framework (RMF) responsibilities and activities for DLNSEO's information technology systems, and to obtain cybersecurity services including continuous monitoring, incident response and compliance reporting for DLNSEO's information technology systems and users.

DSSC – Defense Travel Management Office (DTMO):

(Dollars in Thousands)		
FY 2023	FY 2024	FY 2025
262	366	379

The DTMO’s cyber activities support two DTMO IT investments: DTMO Passport and Oracle Service Cloud. The DTMO hosts the DTMO Passport boundary within the Oracle Cloud infrastructure. This boundary is divided into three environments: lower, middle, and higher regions, and it encompasses a total of 60 servers. To support the DTMO's infrastructure needs, the Defense Manpower Data Center (DMDC) procures

I. Description of Operations Financed: (Cont.)
Infrastructure as a Service (IaaS) from Oracle Cloud Infrastructure (OCI). In turn, DMDC provides DTMO with Platform as a Service (PaaS) service support for a fee. This PaaS support encompasses enterprise services, CSSP, cybersecurity management, infrastructure support, networking, server management, and database support for DTMO applications. DTMO Passport consists of DTMO's travel data repository, Commercial Travel Information Management database, and over 30 applications that support the travel enterprise. Oracle Service Cloud, commonly known as the Ticket Management System, is a Software as a Service product used by the Travel Assistance Center to manage travel help desk ticket submitted by the DoD travel community. Cyber security activities to support these two IT investments, include: CSSP support, Cyber Scanning Tools licenses (Passport only), and Security Control Assessment – Validation.

DSSC – Employer Support of the Guard and Reserve (ESGR):

(Dollars in Thousands)		
FY 2023	FY 2024	FY 2025
340	347	356

Cybersecurity functions supporting ESGR include prevention of, damage to, protection of, and restoration of ESGR's web applications to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Additionally, cybersecurity functions include specialized contractor support for DoD Risk Management Framework accreditation requirements. ESGR's systems are hosted at the Defense Information Systems Agency (DISA), which provides comprehensive services for monitoring and analysis of network traffic entering and exiting network boundaries. ESGR also shares in the costs for EventPLUS and Exhibit Arts Fulfillment System through CSSP, is covered by the Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance (C5ISR) Center.

DSSC – Federal Voting Assistance Program (FVAP):

(Dollars in Thousands)		
FY 2023	FY 2024	FY 2025
108	97	101

FVAP's cyber needs are integrated into our entire core mission of being able to provide information and assistance to those in the military, their spouses, and overseas citizens to make sure they have the tools and knowledge to be able to vote anywhere in the world. Our website is an integrated content management system. The online assistant, also called R3, directly assists voters with completing two FVAP-prescribed forms, the Federal Post Card Application and the Federal Write-In Absentee Ballot. The FVAP Portal also consists of a database back end to support reporting of voting assistance metrics from voting assistance officers all over the world on U.S. military bases. With all of our functions we make updates and enhancements as needed to better the functionality and security of the system. Our enhancements are covered by IT Coalition and our security, through CSSP, is covered by the Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance (C5ISR) Center.

I. Description of Operations Financed: (Cont.)
DSSC – Military-Civilian Transition Office (MCTO):

MCTO's mission is to provide full-spectrum program management that continuously improves design, content, and delivery of timely, relevant, and meaningful information, support, services, and resources to transitioning and reintegrating Service members and their families worldwide.

(Dollars in Thousands)		
FY 2023	**FY 2024**	**FY 2025**
402	**1,365**	**1,411**

- Transition Assistance Program (TAP)
- Yellow Ribbon Reintegration Program (YRRP)
- Department of Defense (DoD) SkillBridge
- Beyond Yellow Ribbon (BYR)

MCTO provides TAP, YRRP, BYR, and SkillBridge program management including research, strategy, policy development, program design, budget and contract management, grant management, curriculum development, program evaluation, program assessment, program compliance, Information Technology (IT), public affairs, strategic communications, and outreach. MCTO ensures a common level of support, across all Military Departments and components, to respective program eligible service members and their families at over 200 locations around the globe. MCTO manages formal DoD and federal interagency governance of transition and reintegration services and support while coordinating and collaborating with diverse stakeholders including the Department of Veterans Affairs/Department of Defense Joint Executive Committee, TAP Interagency, DoD Manpower & Reserve Affairs (M&RA), Joint Staff, National Guard Bureau, Military Departments, employers, institutions of higher learning, entrepreneurial activities, and other governmental and non-governmental entities. TAP and YRRP are programs of record with consolidated funding in the President's Budget. SkillBridge is a program of record with FY 2024/2025 funding programmed through DoD M&RA. MCTO resource consolidation provides streamlined program management and supports planned development of a single source, authoritative Enterprise Transition & Reintegration IT System enabling seamless management of transition and reintegration requirements across the Services and supporting federal agencies while ensuring full statutory and policy compliance.

DSSC – MCTO / Enterprise Transition & Reintegration IT System:

In FY 2024, MCTO will initiate development of a single source, authoritative Transition & Reintegration IT Enterprise System that will host a secure Client Tracking System which: (1) captures reported data as defined in the new statue, (2) enable seamless management of Service member transition across all Military Services and installations; (3) provides Installation and Unit Commanders performance reports and (4) introduces a streamlined way to provide person-based "data as a service" and "analytics as a service" to all of DoD Military Services and other Federal Agencies; (5) provides a Learning Management System for Active Duty and Reserve Component Service members with relevant curricula tailored to their individual transition and/or reintegration requirements. Lastly, these enhancements fulfill requirements within Section 1144(f) of Title 10,

I. <u>Description of Operations Financed</u>: (Cont.)
United States Code and applicable Congressional mandates requiring updating, modifying, and developing new curriculum to account for new statutorily required topics and framework for delivery.

<u>DSSC – MCTO / Transition Assistance Program (TAP)</u>:

TAP is codified in Sections 1142 and 1144 of Title 10, United States Code, and Department of Defense Instruction 1332.35. MCTO absorbed SkillBridge and other programs midyear which drove increases across the programmatic portfolio with the highest increases in IT enhancements, curriculum development, training, contract support, and manpower requirements. TAP provides streamlined and effective transition assistance that effectively supports individualized transition preparation for approximately 200,000 eligible Service members who separate, retire, or are released from active duty each year.

The TAP-IT suite is the DoD-wide source for capturing transitioning Service members' TAP course attendance and documenting transition progress on an electronic Department of Defense (DD)Form 2648 across the Services. MCTO and the Military Services are currently executing FY 2019 – FY 2022 National Defense Authorization Act (NDAA) mandated changes, the 2018 Government Accountability Office (GAO), report number 18-23, recommended improvements and subsequent major changes that have resulted in a DoD policy to modify the Career Readiness Standards (CRS). DoD requires Service Members to meet with a TAP Counselor for their initial counseling prior to their pre-separation counseling and transition from Service if they have served on active duty for 180 continuous days. The mandated NDAA changes as well as the DoD and GAO recommendations require modification to both the electronic and portable document format DD Form 2648 "Pre-separation Counseling Checklist for Active Component (AC), Active Guard Reserve (AGR), Active Reserve (AR), Full Time Support (FTS), and Reserve Program Administrator (RPA) Service Members", to increase reporting requirements, and necessitate new development for adding a client management capability to the TAP-IT suite. These functions would not be possible without the use of TAP-IT, which is hosted by the Defense Manpower Data Center (DMDC). DMDC's role as host includes cyber security support for the network and system applications. Additionally, there are cyber security efforts to safeguard personally identifiable information.

<u>DSSC – MCTO / Yellow Ribbon Reintegration Program (YRRP)</u>:

YRRP is codified in Public Law 110-181, Section 582 and Department of Defense Instruction 1342.28. YRRP is a DoD-wide effort to promote the well-being of National Guard and Reserve Component Service members, their families, and communities, by connecting them with resources throughout and beyond the deployment cycle.

Cybersecurity functions include prevention of, damage to, protection of, and restoration of EventPLUS to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation, including contractor support for DoD Risk Management Framework accreditation requirements EventPLUS is hosted through Amazon Web Services (government) and actively monitored by the Combat Capabilities Development Command (CCDC) C5ISR Center, which provides comprehensive services for monitoring and analysis of network traffic entering and exiting network boundaries. Specifically, CCDC C5ISR services are external vulnerability scans, web vulnerability scanning, malware notification protection, and attack sensing & warning.

I. Description of Operations Financed: (Cont.)
DSSC – MCTO / SkillBridge:

SkillBridge is codified in 10 U.S. Code, Chapter 58, § 1143, and Department of Defense Instruction 1322.29. SkillBridge provides eligible transitioning Service members with job training and employment skills training, including apprenticeship programs, to help prepare them for employment in the civilian sector. Participating service members gain valuable civilian work experience through specific industry training, apprenticeships, or internships during the last 180 days of service.

MCTO assumed programmatic responsibility for SkillBridge in May 2023. From May through July 2023, MCTO prioritized elimination of backlogged potential employer MOU requests. The MOU serves as an agreement between the employer and the DoD stipulating the services the employer offers to the separating Service members to facilitate readiness for employment in the civilian sector. During the same time period, MCTO conducted an internal programmatic review to develop a baseline understanding of “as is” cyber requirements and capabilities. That internal assessment identified significant cyber vulnerabilities with the current IT platform with no cost-effective mitigation under the current contract. MCTO developed a cyber vulnerabilities corrective action plan for implementation between July-September 2024 aligned with the end date of the current contract support.

Sexual Assault Prevention and Response Office (SAPRO):

(Dollars in Thousands)		
FY 2023	**FY 2024**	**FY 2025**
101	**285**	**293**

The Department, under the guidance of the Sexual Assault Prevention and Response Office (SAPRO), has worked to improve its programs to provide military sexual assault survivors with a full range of best-in-class support services. Funding for the Defense Sexual Assault Incident Database (DSAID) greatly assists the Military Service sexual assault prevention and response (SAPR) program management and DoD SAPRO oversight activities. DSAID serves as the DoD’s SAPR source for internal and external requests for statistical data on sexual assault in accordance with Section 563 of Fiscal Year (FY) 2009 National Defense Authorization Act (NDAA).

DoD Safe Helpline is codified in Public Law 113-291, Section 545 and Department of Defense Instruction 6495.02. DoD Safe helpline is the Department’s sole 24/7, anonymous, confidential hotline for members of the DoD community affected by sexual assault. The Safe Helpline offers specialized services including crisis intervention support and resource referrals to survivors, their families, and other DoD Stakeholders.

II. Force Structure Summary:

N/A

III. **Financial Summary ($ in Thousands):**

		FY 2024				
			Congressional Action			
A. BA Subactivities	**FY 2023 Actuals**	**Budget Request**	**Amount**	**Percent**	**Current Estimate**	**FY 2025 Estimate**
Defense Civilian Personnel Advisory Service (DCPAS)	$38	$0	$0	0.00%	$0	$0
Defense Suicide Prevention Office (DSPO)	$77	$103	$0	0.00%	$103	$106
DMDC - Defense Enrollment Eligibility Reporting System (DEERS)	$4,995	$5,013	$0	0.00%	$5,013	$12,393
DMDC - Enterprise Data Services (EDS)	$7,660	$4,548	$0	0.00%	$4,548	$8,855
DMDC - Enterprise Human Resources Information System (EHRIS)	$2,997	$2,116	$0	0.00%	$2,116	$2,185
DMDC - Identity Credential Management (ICM)	$14,320	$9,476	$0	0.00%	$9,476	$9,797
DMDC - Personnel Accountability and Security (PAS)	$3,330	$2,289	$0	0.00%	$2,289	$2,358
DPAC - Office of People Analytics (OPA)	$484	$801	$0	0.00%	$801	$819
DSSC - Computer/Electronic Accommodations Program (CAP)	$408	$113	$0	0.00%	$113	$117
DSSC - Defense Activity for Non-Traditional Education Support (DANTES)	$319	$330	$0	0.00%	$330	$337
DSSC - Defense Language and National Security Education Office (DLNSEO)	$202	$268	$0	0.00%	$268	$274
DSSC - Defense Travel Management Office (DTMO)	$262	$366	$0	0.00%	$366	$379
DSSC - Employer Support of the Guard and Reserve (ESGR)	$340	$347	$0	0.00%	$347	$356
DSSC - Federal Voting Assistance Program (FVAP)	$108	$97	$0	0.00%	$97	$101
DSSC - Military-Civilian Transition Office (MCTO)	$402	$1,365	$0	0.00%	$1,365	$1,411
Sexual Assault Prevention and Response Office (SAPRO)	$101	$285	$0	0.00%	$285	$293
Total	**$36,043**	**$27,517**	**$0**	**0.00%**	**$27,517**	**$39,781**

III. Financial Summary ($ in Thousands): (Cont.)

B. Reconciliation Summary	**Change FY 2024/FY 2024**	**Change FY 2024/FY 2025**
BASELINE FUNDING	**$27,517**	**$27,517**
Congressional Adjustments (Distributed)	0	
Congressional Adjustments (Undistributed)	0	
Adjustments to Meet Congressional Intent	0	
Congressional Adjustments (General Provisions)	0	
Fact-of-Life Changes (2024 to 2024 Only)	0	
SUBTOTAL BASELINE FUNDING	**27,517**	
Supplemental	0	
Reprogrammings	0	
Price Changes		578
Functional Transfers		0
Program Changes		11,686
CURRENT ESTIMATE	**27,517**	**39,781**
Less: Supplemental	0	
NORMALIZED CURRENT ESTIMATE	**$27,517**	**$39,781**

III. Financial Summary ($ in Thousands): (Cont.)

FY 2024 President's Budget Request (Amended, if applicable)		**$27,517**
1. Congressional Adjustments		$0
a) Distributed Adjustments	$0	
b) Undistributed Adjustments	$0	
c) Adjustments to Meet Congressional Intent	$0	
d) General Provisions	$0	
2. Supplemental Appropriations		$0
a) Supplemental Funding	$0	
3. Fact-of-Life Changes		$0
a) Functional Transfers	$0	
b) Technical Adjustments	$0	
c) Emergent Requirements	$0	
FY 2024 Baseline Funding		**$27,517**
4. Reprogrammings (Requiring 1415 Actions)		$0
a) Increases	$0	
b) Decreases	$0	

III. Financial Summary ($ in Thousands): (Cont.)

Revised FY 2024 Estimate	**$27,517**
5. Less: Item 2, Supplemental Appropriation and Item 4, Reprogrammings	$0
a) Less: Supplemental Funding	$0
FY 2024 Normalized Current Estimate	**$27,517**
6. Price Change	$578
7. Functional Transfers	$0
a) Transfers In	$0
b) Transfers Out	$0
8. Program Increases	$11,809
a) Annualization of New FY 2024 Program	$0
b) One-Time FY 2025 Increases	$0
c) Program Growth in FY 2025	$11,809
1) Defense Suicide Prevention Office (DSPO)	$1

+$1 thousand - Increases are due to the costs of deploying, operating and maintaining the cyber tools that allow us to meet the mandates of DoDI 8530.01 “Cybersecurity Activities Support to DoD Information Network Operations”, USCYBERCOM TASKORD 17-0019 “Assured Compliance Assessment Solution (ACAS) Operation Guidance” and CJCSM 6510.01B, “Cyber Incident Handling Program”, December 18, 2014, among other Department policies, Operational Orders, and Task Orders. The cost of many of these tools has increased, and in FY2025 we will no longer receive DoD Enterprise licensing for one of our primary tools (Endpoint Security Suite), further increasing operational costs for the program.
(FY 2024 Baseline: $103 thousand; 0 FTEs)

III. Financial Summary ($ in Thousands): (Cont.)

2) DMDC - Defense Enrollment Eligibility Reporting System (DEERS)... $7,275
+$7,205 thousand - Increase for Cloud Hosting to allow DMDC to architect, deploy and maintain cybersecurity toolsets to its cloud environments and supports cloud-specific cybersecurity mandates such as cybersecurity service provider (CSSP) support.
+$70 thousand - Increases are due to the costs of deploying, operating and maintaining the cyber tools that allow us to meet the mandates of DoDI 8530.01 “Cybersecurity Activities Support to DoD Information Network Operations”, USCYBERCOM TASKORD 17-0019 “Assured Compliance Assessment Solution (ACAS) Operation Guidance” and CJCSM 6510.01B, “Cyber Incident Handling Program”, December 18, 2014, among other Department policies, Operational Orders, and Task Orders. The cost of many of these tools has increased, and in FY2025 we will no longer receive DoD Enterprise licensing for one of our primary tools (Endpoint Security Suite), further increasing operational costs for the program.
(FY 2024 Baseline: $5,013 thousand; 0 FTEs)

3) DMDC - Enterprise Data Services (EDS).. $4,211
+$4,120 thousand - Increase for Cloud Hosting to allow DMDC to architect, deploy and maintain cybersecurity toolsets to its cloud environments and supports cloud-specific cybersecurity mandates such as cybersecurity service provider (CSSP) support.
+$91 thousand - Increases are due to the costs of deploying, operating and maintaining the cyber tools that allow us to meet the mandates of DoDI 8530.01 “Cybersecurity Activities Support to DoD Information Network Operations”, USCYBERCOM TASKORD 17-0019 “Assured Compliance Assessment Solution (ACAS) Operation Guidance” and CJCSM 6510.01B, “Cyber Incident Handling Program”, December 18, 2014, among other Department policies, Operational Orders, and Task Orders. The cost of many of these tools has increased, and in FY2025 we will no longer receive DoD Enterprise licensing for one of our primary tools (Endpoint Security Suite), further increasing operational costs for the program.
(FY 2024 Baseline: $4,548 thousand; 0 FTEs)

4) DMDC - Enterprise Human Resources Information System (EHRIS) $25
+$25 thousand - Increases are due to the costs of deploying, operating and maintaining the cyber tools that allow us to meet the mandates of DoDI 8530.01 “Cybersecurity Activities Support to DoD Information Network Operations”, USCYBERCOM TASKORD 17-0019 “Assured Compliance Assessment Solution (ACAS) Operation Guidance” and CJCSM 6510.01B, “Cyber Incident Handling Program”, December 18, 2014, among other Department policies, Operational Orders, and Task Orders. The cost of many of these tools has increased, and in FY2025 we will no longer receive DoD Enterprise licensing for one of our primary tools (Endpoint Security Suite), further increasing operational costs for the program.
(FY 2024 Baseline: $2,116 thousand; 0 FTEs)

III. <u>Financial Summary ($ in Thousands)</u>: (Cont.)

5) DMDC - Identity Credential Management (ICM) $122
+$122 thousand - Increases are due to the costs of deploying, operating and maintaining the cyber tools that allow us to meet the mandates of DoDI 8530.01 "Cybersecurity Activities Support to DoD Information Network Operations", USCYBERCOM TASKORD 17-0019 "Assured Compliance Assessment Solution (ACAS) Operation Guidance" and CJCSM 6510.01B, "Cyber Incident Handling Program", December 18, 2014, among other Department policies, Operational Orders, and Task Orders. The cost of many of these tools has increased, and in FY2025 we will no longer receive DoD Enterprise licensing for one of our primary tools (Endpoint Security Suite), further increasing operational costs for the program.
(FY 2024 Baseline: $9,476 thousand; 0 FTEs)

6) DMDC - Personnel Accountability and Security (PAS) $21
+$21 thousand - Increases are due to the costs of deploying, operating and maintaining the cyber tools that allow us to meet the mandates of DoDI 8530.01 "Cybersecurity Activities Support to DoD Information Network Operations", USCYBERCOM TASKORD 17-0019 "Assured Compliance Assessment Solution (ACAS) Operation Guidance" and CJCSM 6510.01B, "Cyber Incident Handling Program", December 18, 2014, among other Department policies, Operational Orders, and Task Orders. The cost of many of these tools has increased, and in FY2025 we will no longer receive DoD Enterprise licensing for one of our primary tools (Endpoint Security Suite), further increasing operational costs for the program.
(FY 2024 Baseline: $2,289 thousand; 0 FTEs)

7) DPAC - Office of Personnel Analytics (OPA) $1
+$1 thousand - Increase to Risk Management Framework (RMF) audit costs.
(FY 2024 Baseline: $801 thousand; 0 FTEs)

8) DSSC - Computer/Electronic Accommodations Program (CAP) $117
+$117 thousand - Increase in IT Contract Support Services and internal realignment from Other Services to accurately reflect use of funds for IT contract support for ongoing and emerging cyber requirements.
(FY 2024 Baseline: $113 thousand; 0 FTEs)

9) DSSC - Defense Travel Management Office (DTMO) $5
+$5 thousand - Increase attributed to movement from web-based to cloud environment.
(FY 2024 Baseline: $366 thousand; 0 FTEs)

10) DSSC - Employer Support of the Guard and Reserve (ESGR) $2
+$2 thousand - Increase due to Defense Information System Agency (DISA) inflation rate increases.
(FY 2024 Baseline: $347 thousand; 0 FTEs)

III. Financial Summary ($ in Thousands): (Cont.)

11) DSSC - Federal Voting Assistance Program (FVAP)....................$2
+$2 thousand - Increase in DMDC Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) Center Cybersecurity Service Provider (CSSP) costs.
(FY 2024 Baseline: $97 thousand; 0 FTEs)

12) DSSC - Military-Civilian Transition Office (MCTO)....................$25
+$25 thousand - Internal realignment to IT Contract Support Services from Other Services to support EventPlus contract modifications.
(FY 2024 Baseline: $1,365 thousand; 0 FTEs)

13) Sexual Assault Prevention and Response Office (SAPRO) $2
+$2 thousand - Increase due to continued support for Defense Sexual Assault Incident Database (DSAID) migration to DHRA from DISA Joint Service Provider.
(FY 2024 Baseline: $285 thousand; 0 FTEs)

9. Program Decreases ....$-123

a) Annualization of FY 2024 Program Decreases $0

b) One-Time FY 2024 Increases $0

c) Program Decreases in FY 2025 .... $-123

1) DSSC - Computer/Electronic Accommodations Program (CAP) .... $-115
-$115 thousand - Internal realignment from Other Services to IT Contract Support Services to accurately reflect use of funds for IT contract support for ongoing and emerging cyber requirements.
(FY 2024 Baseline: $113 thousand; 0 FTEs)

2) DSSC - Military-Civilian Transition Office (MCTO).................... $-8
-$8 thousand - Internal realignment from Other Services to IT Support Contract Services to support EventPlus contract modifications.
(FY 2024 Baseline: $1,365 thousand; 0 FTEs)

FY 2025 Budget Request $39,781

IV. Performance Criteria and Evaluation Summary:

Defense Suicide Prevention Office (DSPO)

DSPO / Cyber

Performance Statement: Increase the number of Authorities to Operate (ATO) issued for a period greater than one year.

Performance Evaluation: 50 percent of ATOs issued for a period greater than one year.

Performance Outcome: ATOs issued for greater than one year indicate systems that present less risk to DSPO/DHRA networks; an increased number of these longer ATOs demonstrates a more secure environment.

Benchmarks	FY 2023 Enacted	FY 2024 Estimate	FY 2025 Estimate
	1	1	1

Remarks: DSPO, in conjunction with DMDC, maintains one ATO for the Military Mortality Database (MMDB). This ATO was issued a three-year approval in October 2023, valid through October 2026.

FY 2023: MMDB Receives a three-year ATO.

FY 2024: MMDB is two years into a three-year ATO.

FY 2025: MMDB is on final year of three-year ATO. Work will be ongoing to ensure issuance of follow-on three-year ATO.

Defense Manpower Data Center (DMDC)

Defense Enrollment Eligibility Reporting System (DEERS) / Cyber

Performance Statement: Increase number of Authority to Operate (ATO) issued for more than one year.

Performance Evaluation: 75 percent of ATOs issued for greater than one year.

Performance Outcome: ATOs issued for greater than one year indicate systems that present less risk to the DMDC/DHRA networks; an increased total of these longer ATOs demonstrates a more secure environment.

Benchmarks	FY 2023 Enacted	FY 2024 Estimate	FY 2025 Estimate
ATOs issued for more than one year	75 percent	75 percent	75 percent

IV. Performance Criteria and Evaluation Summary:

Defense Manpower Data Center (DMDC)
Enterprise Data Services (EDS) / Cyber

Performance Statement: Increase number of ATOs issued for more than one year.

Performance Evaluation: 75 percent of ATOs issued for greater than one year.

Performance Outcome: ATOs issued for greater than one year indicate systems that present less risk to the DMDC/DHRA networks; an increased total of these longer ATOs demonstrates a more secure environment.

Benchmarks	FY 2023 Enacted	FY 2024 Estimate	FY 2025 Estimate
ATOs issued for more than one year	75 percent	75 percent	75 percent

Performance Statement: Increase deployment of Cybersecurity Monitoring Tools.

Performance Evaluation: 85 percent coverage for all cyber tools.

Performance Outcome: Increased tool coverage will correspond with increased ability to detect and respond to cybersecurity risks, threats and vulnerabilities.

Benchmarks	FY 2023 Enacted	FY 2024 Estimate	FY 2025 Estimate
Cybersecurity tool coverage	85 percent	85 percent	85 percent

Performance Statement: Increase privileged user account compliance with Account Management Policy requirements.

Performance Evaluation: 90 percent compliance with policy requirements.

Performance Outcome: User accounts that comply with organizational and Departmental account policies present lower risk to the network and indicate a more robust privileged account program.

Benchmarks	FY 2023 Enacted	FY 2024 Estimate	FY 2025 Estimate
Percent compliant privileged user accounts	90 percent	90 percent	90 percent

Performance Statement: Reduce number of security breaches.

Performance Evaluation: No more than one root or user-level intrusion.

IV. Performance Criteria and Evaluation Summary:

Performance Outcome: Reducing the number of security breaches protects Department data and networks.

Benchmarks	**FY 2023 Enacted**	**FY 2024 Estimate**	**FY 2025 Estimate**
Root-level or User-Level Intrusions	1	1	1

Defense Manpower Data Center (DMDC)
Enterprise Human Resource Information Systems (EHRIS) / Cyber

Performance Statement: Increase number of ATOs issued for more than one year.

Performance Evaluation: 75 percent of ATOs issued for greater than one year.

Performance Outcome: ATOs issued for greater than one year indicate systems that present less risk to the DMDC/DHRA networks; an increased total of these longer ATOs demonstrates a more secure environment.

Benchmarks	**FY 2023 Enacted**	**FY 2024 Estimate**	**FY 2025 Estimate**
ATOs issued for more than one year	75 percent	75 percent	75 percent

Defense Manpower Data Center (DMDC)
Identity Credential Management (ICM) / Cyber

Performance Statement: Increase number of ATOs issued for more than one year.

Performance Evaluation: 75 percent of ATOs issued for greater than one year.

Performance Outcome: ATOs issued for greater than one year indicate systems that present less risk to the DMDC/DHRA networks; an increased total of these longer ATOs demonstrates a more secure environment.

Benchmarks	**FY 2023 Enacted**	**FY 2024 Estimate**	**FY 2025 Estimate**
ATOs issued for more than one year	75 percent	75 percent	75 percent

IV. Performance Criteria and Evaluation Summary:

Defense Manpower Data Center (DMDC)

Personnel Accountability and Security (PAS) / Cyber

Performance Statement: Increase number of ATOs issued for more than one year.

Performance Evaluation: 75 percent of ATOs issued for greater than one year.

Performance Outcome: ATOs issued for greater than three years indicate systems that present less risk to the DMDC/DHRA networks; an increased total of these longer ATOs demonstrates a more secure environment.

Benchmarks	FY 2023 Enacted	FY 2024 Estimate	FY 2025 Estimate
ATOs issued for more than one year	75 percent	75 percent	75 percent

Defense Personnel Analytics Center (DPAC) manages two DHRA programs:

- DoD Office of the Actuary (OACT)
- Office of People Analytics (OPA)

The Office of the Actuary does not have any specific cyber requirements.

DPAC - Office of People Analytics (OPA)

OPA / Cyber

Performance Statement: Maintain active Authority to Operate (ATO) across all OPA accreditation boundaries.

Performance Evaluation: 100 percent of OPA accreditation boundaries have an active ATO.

Performance Outcome: ATOs are required to continue to provide recruiting, testing, and analytic support to the Department and present less risk to DMDC/DHRA networks and supported enclaves.

Benchmarks	FY 2023 Enacted	FY 2024 Estimate	FY 2025 Estimate
100 percent of OPA accreditation boundaries have an active ATO	100 percent	100 percent	100 percent

IV. Performance Criteria and Evaluation Summary:

Defense Support Service Center (DSSC) manages the following DHRA programs:

- Computer/Electronic Accommodations Program (CAP)
- Defense Activity for Non-Traditional Education Support (DANTES)
- Defense Language and National Security Education Office (DLNSEO)
- Defense Travel Management Office (DTMO)
- Employer Support of the Guard and Reserves (ESGR)
- Federal Voting Assistance Program (FVAP)
- Military-Civilian Transition Office (MCTO)

DSSC - Computer/Electronic Accommodations Program (CAP)

Computer/Electronic Accommodations Program (CAP)/Cyber

Performance Statement: Defense Manpower Data Center (DMDC) Cybersecurity Service Provider (CSSP) provides 24/7 network defense, vulnerability assessment, and incident response services. CSSP can provide defensive cyber operations in support of network command/control, ensuring secure communications, and cyber intelligence support. DMDC identifies vulnerabilities in the CAP web applications, database, and public-facing website. DMDC CSSP helps to achieve DoD policy compliance support and provides situational awareness of organization web application vulnerability posture and correlation of vulnerabilities to threats. CAP supports DMDC cyber operations by submitting scan requests at specified intervals in support of Enterprise Mission Assurance Support Services (eMASS).

Performance Evaluation: Successful CSSP certification for CAP Public Website and Internal Management Portal that provides Web Vulnerability Scanning (WVS) support to assist CAP with public facing web presence vulnerabilities.

Performance Outcome: DMDC conducts required scans and reports any identified vulnerabilities.

Benchmarks	FY 2023 Enacted	FY 2024 Estimate	FY 2025 Estimate
Submit Fortify/Sonatype Code Assessment Scans.	4	4	4
Submit and/or Review Assured Compliance Assessment Solution Scans.			4

Remarks: None.

IV. Performance Criteria and Evaluation Summary:

DSSC - Defense Activity for Non-Traditional Education Support (DANTES)

Defense Activity for Non-Traditional Education Support (DANTES)/Cyber

Defense Activity for Non-Traditional Education Support (DANTES) DoD Voluntary Education Partnership Memorandum of Understanding (DoD MOU) and the Joint Services Transcript (JST)/Cyber

Performance Statement: Increase the number of Authority to Operate (ATO) decisions issued.

Performance Evaluation: 50 percent of ATOs issued for a period greater than one year.

Performance Outcome: ATOs issued for greater than one year indicate systems that present less risk to DANTES/DMDC/DHRA networks; an increased number of these longer ATOs demonstrates a more secure environment.

Benchmarks	FY 2023 Enacted	FY 2024 Estimate	FY 2025 Estimate
Submit full DoD MOU/JST Risk Management Framework (RMF) artifacts/documentation into eMASS for DMDC review.	2	1	1

FY 2023: DANTES DoD MOU program will undergo an external ATO validation and submit a request for a one year ATO with conditions. The migration to the contractor government cloud will be complete and the ATO package submitted to DMDC. JST will begin the process of drafting their ATO package.

FY 2024: DoD MOU will undergo an additional review to obtain a three-year ATO without conditions.

FY 2025: JST will obtain a three-year ATO without conditions.

DSSC - Defense Language and National Security Education Office (DLNSEO)

Defense Language and National Security Education Office (DLNSEO)/Cyber

Performance Statement: Increase the number of Authority to Operate (ATO) decisions issued for a period greater than one year.

Performance Evaluation: 50 percent of ATOs issued for a period greater than one year.

Performance Outcome: ATOs issued for greater than one year indicate systems that present less risk to DLNSEO/DHRA networks; an increased number of these longer ATOs demonstrates a more secure environment.

IV. Performance Criteria and Evaluation Summary:

Benchmarks	FY 2023 Enacted	FY 2024 Estimate	FY 2025 Estimate
Active ATOs issued for greater than one year	100 percent	100 percent	100 percent

Remarks: DLNSEO maintains two ATOs, for its National Language Service Corps and National Security Education Program systems. Both systems were issued one-year ATOs in FY 2023.

FY 2023: Both systems received ATO with conditions. A three-year ATO will be requested during this year's renewal.

FY 2024: Both systems will resubmit RMF package to obtain three-year ATOs.

FY 2025: Both three-year ATOs will be sustained.

DSSC - Defense Travel Management Office (DTMO)
Defense Travel Management Office (DTMO)/Cyber

Performance Statement: Sustain ATOs in accordance with RMF & DHRA guidelines to maintain a secure environment and achieve three-year ATOs.

Performance Evaluation: 50 percent of ATOs issued for a period greater than one year.

Performance Outcome: ATOs issued for greater than one year indicate systems that present less risk to DoD networks; an increased number of longer ATOs demonstrates a more secure environment.

Benchmarks	FY 2023 Enacted	FY 2024 Estimate	FY 2025 Estimate
# of ATOs approved	1	0	2

FY 2023: Passport Ft. Detrick environment was decommissioned and the ATO retired.

The DTMO successfully achieved a three-year ATO for the Passport OCI environment till May 12, 2025.

The Oracle Service Cloud external ATO validation was conducted, an ATO package was submitted, and a three-year ATO achieved till March 21, 2025.

FY 2024: DTMO will sustain the DTMO Passport OCI and Oracle Service Cloud ATOs, and begin preparation for an ATO package submissions in FY 2025.

IV. Performance Criteria and Evaluation Summary:

FY 2025: DTMO will obtain and maintain two 3-year ATO packages in FY 2025.

DSSC - Employer Support of the Guard and Reserve (ESGR)
Employer Support of the Guard and Reserve (ESGR)/Cyber

Performance Statement:
Cybersecurity Service Provider (CSSP) Services Vulnerability Analysis and Assessment (VAA) Support services are vital, proactive activities to help determine the vulnerability posture of DoD assets. Vulnerability assessments apply a variety of techniques to identify vulnerabilities in web applications and the CSSP office helps achieve DoD policy compliance. VAA support provides situational awareness of organization web application vulnerability posture and correlation of vulnerabilities to threats.

Performance Evaluation:
Provide Web Vulnerability Scanning (WVS) support to assist ESGR with vulnerability identification of DoD Whitelisted websites in accordance with USCYBERCOM TASKORD 13-0613 with respect to public facing web presence.

Performance Outcome:
Defense Information Systems Agency (DISA) conduct required scans and report any vulnerabilities identified. ESGR receives scan results from DISA, ESGR, then works with appropriate offices to resolve issues identified.

Benchmarks	FY 2023 Enacted	FY 2024 Estimate	FY 2025 Estimate
Complete two WVS assessment scans and provide associated reports	2	2	2

Remarks:
ESGR works with partners to ensure software meets DoD security requirements, applying vendor and custom code patches to improve security posture.

Performance Statement:
The Exhibit Arts Fulfillment System contractor will create, write and edit the Risk Management Framework (RMF) documents to include: System Security Plan, Security Design, Network Architecture, Hardware/Software Inventory, Plan of Action and Milestones (POAMs), Risk Assessments, Security Controls, Contingency Planning, Patch Management Plans, Incident Response Plans, Continuous Monitoring Plans, Security Categorization, and Common Control Identifiers (CCIs) including Privacy Controls to ensure the overall security posture of the network/information system.

IV. Performance Criteria and Evaluation Summary:

Performance Evaluation:
Establish appropriate administrative, technical, and physical safeguards to protect all nonpublic Government data to ensure the confidentiality, integrity, and availability of government data. All Information Technology Systems will comply with DoD Risk Management Framework (RMF) guidance.

Performance Outcome:
Required documentation uploaded and validated against security control checks per DoD standards concerning RMF as documented in the Enterprise Mission Assurance Support Service (eMASS).

Benchmarks	FY 2023 Enacted	FY 2024 Estimate	FY 2025 Estimate
RMF documentation uploaded and validated in eMass	95 percent	95 percent	95 percent

Remarks:
ESGR IT Specialist and a support contractor have uploaded required documentation and Defense Manpower Data Center staff conducted validation during the first quarter of FY 2023.

DSSC - Federal Voting Assistance Program (FVAP)
Federal Voting Assistance Program (FVAP)/Cyber

Performance Statement: The C5ISR Center Cybersecurity Service Provider (CSSP) is one of twenty-three approved CSSPs that provide 24/7 network defense, vulnerability assessment, and incident response services. Cybersecurity is a rapid moving field, both within the public and private sectors, and the CSSP is able to provide defensive cyber operations in support of network command/control, ensuring secure communications, and cyber intelligence support. Simultaneously, CSSP is able to utilize these operational datasets as a baseline for continuous transformation with research/development and thus, further modernization. C5ISR identifies vulnerabilities in web applications and helps to achieve DoD policy compliance support. It also provides situational awareness of organization web application vulnerability posture and correlation of vulnerabilities to threats.

Performance Evaluation: Successful CSSP certification for FVAP Portal and Procurement IDIQ Portal that provides Web Vulnerability Scanning (WVS) support to assist FVAP with vulnerabilities with respect to public facing web presence.

Performance Outcome: C5ISR conducts required scans and reports any vulnerabilities identified.

IV. Performance Criteria and Evaluation Summary:

Benchmarks	FY 2023 Enacted	FY 2024 Estimate	FY 2025 Estimate
Complete two WVS assessment scans	2	2	2

Remarks:
FVAP is working on assessing Plan of Action and Milestones (POAMs) with cyber hardening in Software Security Center and meeting other conditions. Other compliance tasks and remediation will be dealt with from the controls that were found to need updates in the last Authority to Operate (ATO) assessment in support of the next cycle of approval for the FVAP Portal ATO.

Performance Statement:
The contractor and government lead will work to create, write and edit the Risk Management Framework (RMF) documents to include: System Security Plan, Security Design, Network Architecture, Hardware/Software Inventory, POAMs, Risk Assessments, Security Controls, Contingency Planning, Patch Management Plans, Incident Response Plans, Continuous Monitoring Plans, Security Categorization, and Common Control Identifiers (CCIs) including Privacy Controls to ensure the overall security posture of the network/ IS.

Performance Evaluation:
Establish appropriate administrative, technical, and physical safeguards to protect any and all nonpublic Government data to ensure the confidentiality, integrity, and availability of government data appropriate to the FVAP Portal security classification.

Performance Outcome:
Required documentation uploaded and validated against security control checks per DoD standards concerning RMF as documented in the Enterprise Mission Assurance Support Service (eMASS).

Benchmarks	FY 2023 Enacted	FY 2024 Estimate	FY 2025 Estimate
RMF documentation uploaded and validated in eMass	100 percent	100 percent	100 percent

Remarks:
Support contractor is working on meeting conditions laid out in the last ATO. The government lead is tracking the progress of remediation of ATO conditions and contractor will be required to correct any discrepancies identified by the submission deadline.

DSSC – Military-Civilian Transition Office (MCTO):

- Transition Assistance Program (TAP)
- Yellow Ribbon Reintegration Program (YRRP)

IV. Performance Criteria and Evaluation Summary:

- Department of Defense (DoD) SkillBridge
- Beyond Yellow Ribbon (BYR)

MCTO's mission is to provide full-spectrum program management that continuously improves design, content, and delivery of timely, relevant, and meaningful information, support, services, and resources to transitioning and reintegrating Service members and their families worldwide.

MCTO provides TAP, YRRP, and SkillBridge program management including research, strategy, policy development, program design, budget and contract management, grant management, curriculum development, program evaluation, program assessment, program compliance, information technology (IT), public affairs, strategic communications, and outreach. MCTO ensures a common level of support, across all Military Departments and components, to respective program eligible service members and their families at over 200 locations around the globe. MCTO manages formal DoD and federal interagency governance of transition and reintegration services and support while coordinating and collaborating with diverse stakeholders including the Department of Veterans Affairs/Department of Defense Joint Executive Committee, TAP Interagency, DoD Manpower & Reserve Affairs (M&RA), Joint Staff, National Guard Bureau, Military Departments, employers, institutions of higher learning, entrepreneurial activities, and other governmental and non-governmental entities. TAP and YRRP are programs of record with consolidated funding in the President's Budget. SkillBridge is a program of record with FY24/25 funding programmed through DoD M&RA. MCTO resource consolidation provides streamlined program management and supports planned development of a single authoritative source, Enterprise Transition & Reintegration IT System, which enables seamless management of transition and reintegration requirements across the Services and supports federal agencies while ensuring full statutory and policy compliance.

DSSC – Military-Civilian Transition Office (MCTO)
Transition Assistance Program (TAP) / Cyber

Performance Statement: Defense Manpower Data Center (DMDC) Cybersecurity Service Provider (CSSP) provides 24/7 network defense, vulnerability assessment, and incident response services. The CSSP provides defensive cyber operations in support of network command/control, ensuring secure communications, assured data integrity, and cyber intelligence support. DMDC identifies vulnerabilities in the TAP-IT web applications, database, and public-facing website. DMDC CSSP helps to achieve DoD policy compliance support and provides situational awareness of organization web application vulnerability posture and correlation of vulnerabilities to threats.

Performance Evaluation: Successful CSSP certification for TAP-IT that provides Web Vulnerability Scanning (WVS) support to assist MCTO with vulnerabilities with respect to public facing web presence.
Performance Outcome: DMDC conducts required scans and report any vulnerabilities identified.

Benchmarks	FY 2023 Enacted	FY 2024 Estimate	FY 2025 Estimate
Complete Assessment Scans.	100 percent	100 percent	100 percent

IV. Performance Criteria and Evaluation Summary:

DSSC – Military-Civilian Transition Office (MCTO)

Yellow Ribbon Reintegration Program (YRRP) / Cyber

Performance Statement: The contractor and government will coordinate with C5ISR Center Cybersecurity Service Provider (CSSP) to ensure and provide 24/7 network defense, vulnerability assessment, and incident response services for EventPLUS. Cybersecurity is a rapid moving field, both within the public and private sectors, and the CSSP is able to provide defensive cyber operations in support of network command/control, ensuring secure communications, and cyber intelligence support. Simultaneously, CSSP is able to utilize these operational datasets as a baseline for continuous transformation with research/development and thus, further modernization. C5ISR identifies vulnerabilities in web applications and protects, defends, and responds to suspicious behavior that is then repaired by MCTO and put back into compliance with DoD policy.

Performance Evaluation: Successful CSSP certification for EventPLUS provides Web Vulnerability Scanning (WVS) support to assist EventPLUS with vulnerabilities with respect to public facing web presence.

Performance Outcome: The contractor and C5ISR conducts required scans and reports any vulnerabilities identified to government and contractor in coordination with DMDC.

Benchmarks	FY 2023 Enacted	FY 2024 Estimate	FY 2025 Estimate
Vulnerability Scanning	100 percent	100 percent	100 percent

Remarks: The government and contractor began implementing CSSP for EventPLUS in FY 2020 and completed partial scanning and estimates 40 percent compliance with required vulnerability scanning. The government reached 100 percent of required scanning in FY 2021 and continues to coordinate with the contractor and DMDC personnel to conduct ongoing scans, review, and provide remediation efforts as part of EventPLUS's vulnerability management program.

Performance Statement: The contractor and government lead, in coordination with DMDC, will work to create, write and edit Risk Management Framework (RMF) documents for EventPLUS to include: System Security Plan, Security Design, Network Architecture, Hardware/Software Inventory, Plan of Action and Milestones , Risk Assessments, Security Controls, Contingency Planning, Patch Management Plans, Incident Response Plans, Continuous Monitoring Plans, Security Categorization, and Common Control Identifiers (CCIs) including Privacy Controls to ensure the overall security posture of the network information system.

Performance Evaluation: Establish appropriate administrative, technical, and physical safeguards to protect any and all nonpublic Government data to ensure the confidentiality, integrity, and availability of government data appropriate to the EventPLUS security classification.

Performance Outcome: Required documentation uploaded and validated against security control checks per DoD standards concerning RMF as documented in the Enterprise Mission Assurance Support Service (eMASS) and in coordination with DMDC.

IV. Performance Criteria and Evaluation Summary:

Benchmarks	FY 2023 Enacted	FY 2024 Estimate	FY 2025 Estimate
RMF documentation uploaded and validated in eMass	100 percent	100 percent	100 percent

Remarks: The government continues to coordinate with the contractor and DMDC personnel to maintain up-to-date RMF documentation as part of the RMF assessment and compliance for EventPLUS. The government achieved 100 percent compliance with RMF documentation requirements in FY 2023.

DSSC – Military-Civilian Transition Office (MCTO)
SkillBridge / Cyber

Remarks: MCTO assumed programmatic responsibility for SkillBridge in May 2023. From May through July 2023, MCTO prioritized elimination of backlogged employer MOU requests. During the same time period, MCTO conducted an internal programmatic review to develop a baseline understanding of “as is” cyber requirements and capabilities. That internal assessment identified significant cyber vulnerabilities with the current IT platform with no cost-effective mitigation under the current contract. MCTO developed a cyber vulnerabilities corrective action plan for implementation between July-September 2024 aligned with the end date of the current contract support.

Sexual Assault Prevention and Response Office (SAPRO)
DoD Safe Helpline (SHL)/Cyber

Performance Statement: Maintain SHL Authority to Operate (ATO) per requirements and security controls outlined by DMDC.

Performance Evaluation: Annually assess the security controls to determine their effectiveness.

Performance Outcome: Increased security posture of SHL to further enable SAPRO to accomplish its mission.

Benchmarks	FY 2023 Enacted	FY 2024 Estimate	FY 2025 Estimate
	1	1	1

Remarks:
SHL current ATO expires March 31, 2026.

V. **Personnel Summary**:

	FY 2023	FY 2024	FY 2025	Change FY 2023/ FY 2024	Change FY 2024/ FY 2025

N/A

VI. OP 32 Line Items as Applicable (Dollars in thousands):

			Change from FY 2023 to FY 2024			Change from FY 2024 to FY 2025		
		FY 2023	Price	Program	FY 2024	Price	Program	FY 2025
		Program	Growth	Growth	Program	Growth	Growth	Program
671	DISA DISN SUBSCRIPTION SERVICES (DSS)	7,843	507	-8,350	0	0	337	337
677	DISA TELECOMM SVCS - REIMBURSABLE	14	1	-15	0	0	0	0
0699	**TOTAL OTHER FUND PURCHASES**	**7,857**	**508**	**-8,365**	**0**	**0**	**337**	**337**
922	EQUIPMENT MAINTENANCE BY CONTRACT	235	5	-240	0	0	0	0
925	EQUIPMENT PURCHASES (NON-FUND)	994	22	-1,016	0	0	0	0
932	MGT PROF SUPPORT SVCS	609	13	-622	0	0	0	0
987	OTHER INTRA-GOVT PURCH	0	0	268	268	6	0	274
989	OTHER SERVICES	944	21	1,913	2,878	60	-447	2,491
990	IT CONTRACT SUPPORT SERVICES	25,404	559	-1,592	24,371	512	11,796	36,679
0999	**TOTAL OTHER PURCHASES**	**28,186**	**620**	**-1,289**	**27,517**	**578**	**11,349**	**39,444**
9999	**GRAND TOTAL**	**36,043**	**1,128**	**-9,654**	**27,517**	**578**	**11,686**	**39,781**