Fiscal Year 2024 Budget Estimates

Defense Human Resources Activity Cyber

March 2023

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

	FY 2022 Actuals	Price Change	Program Change	FY 2023 Enacted	Price Change	Program Change	FY 2024 Estimate
DHRA Cyber	17,622	405	8,086	26,113	575	829	27,517

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 FY2024 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.

- Administer the federal responsibilities of the Uniformed and Overseas Citizens Absentee Voting Act of 1986 (UOCAVA), as most recently amended by the Military Overseas Voter Empowerment Act (MOVE Act);

- Provide assistive technology to allow DoD and federal employees with disabilities to access electronic and information technology;

DHRA - Cyber

I. <u>Description of Operations Financed</u>: (Cont.)

- 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.

<u>Narrative Explanation of Changes</u>:
The FY 2024 DHRA Cyber budget represents a net programmatic increase of $0.829 million with a price growth of $0.575 million.

<u>Cyber Funding</u>:

(Dollars in Thousands)		
FY 2022	**FY 2023**	**FY 2024**
17,622	26,113	27,517

<u>Defense Civilian Personnel Advisory Service (DCPAS)</u>:

(Dollars in Thousands)		
FY 2022	**FY 2023**	**FY 2024**
38	0	0

DCPAS's goals and objectives are in direct alignment with the DoD Strategic Goals and the National Defense Strategy goal of recruiting, developing and retaining an agile, information-advantaged, motivated, diverse and highly skilled Total Force which can react appropriately to the ever changing and dynamic threat landscape. Funding in the Cyber arena supports Cybersecurity for the Defense Competency Assessment Tool (DCAT) Cloud instance within DCPAS. The Army Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) Center as a Cybersecurity Service Provider (CSSP) will provide the necessary cybersecurity support for subscribers in

I. Description of Operations Financed: (Cont.)
accordance with DoD and the National Institute of Standards and Technology (NIST) cybersecurity standards. Cloud service offerings (CSO) are cloud services compliant as outlined in the DoD Chief Information Officer (CIO) memorandum dated November 15, 2017, titled Department of Defense Cybersecurity.

Defense Suicide Prevention Office (DSPO):

(Dollars in Thousands)		
FY 2022	**FY 2023**	**FY 2024**
14	103	103

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 tools, 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 Cybersecurity Service Provider support for supported systems.

DMDC - Defense Enrollment Eligibility Reporting System (DEERS):

(Dollars in Thousands)		
FY 2022	**FY 2023**	**FY 2024**
2,177	3,244	5,013

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.

DHRA - Cyber

I. Description of Operations Financed: (Cont.)
DMDC - Enterprise Data Service (EDS):

(Dollars in Thousands)		
FY 2022	**FY 2023**	**FY 2024**
4,926	4,924	4,548

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.

DMDC - Enterprise Human Resource Information System (EHRIS):

(Dollars in Thousands)		
FY 2022	**FY 2023**	**FY 2024**
2,183	2,080	2,116

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 2022	**FY 2023**	**FY 2024**
2,992	9,193	9,476

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 2022	**FY 2023**	**FY 2024**
2,269	2,161	2,289

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.

DHRA - Cyber

I. Description of Operations Financed: (Cont.)
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):

(Dollars in Thousands)		
FY 2022	**FY 2023**	**FY 2024**
385	**796**	**801**

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 eight DHRA programs:

- Advanced Distributed Learning (ADL)

- 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 – Advanced Distributed Learning (ADL)

The ADL program is in the process of transitioning from OSD (P&R) to DHRA and all ADL requirements to include funding will be in DHRA DSSC starting on 1 October 2022. ADL Cyber requirements and estimated funding will be included in FY 2025.

DHRA - Cyber

I. Description of Operations Financed: (Cont.)
DSSC – Computer/Electronic Accommodations Program (CAP):

(Dollars in Thousands)		
FY 2022	**FY 2023**	**FY 2024**
369	111	113

The Computer/Electronic Accommodations Program (CAP), which is recognized by the U.S. Office of Personnel Management as a model strategy to increase DoD Federal employment of individuals with disabilities, has provided over 227,000 accommodations to DoD civilian employees and Service members since its inception. CAP is widely considered the go-to source on providing effective assistive technology (AT) solutions. These functions would not be possible without the use of CAP's CAPX/Activity and Reporting Management System (ARMS) Defense Business System, which is hosted by the Defense Manpower Data Center (DMDC). DMDC's role as host includes network and cyber security support. Additionally, DMDC provides cyber security for the Exhibit Arts fulfillment contract platform used to support CAP's outreach efforts.

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

(Dollars in Thousands)		
FY 2022	**FY 2023**	**FY 2024**
280	0	330

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), Authorization to Operate (ATO) validations).

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

(Dollars in Thousands)		
FY 2022	**FY 2023**	**FY 2024**
202	266	268

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

DHRA - Cyber

I. Description of Operations Financed: (Cont.)
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 2022	**FY 2023**	**FY 2024**
361	**361**	**366**

The DTMO's cyber activities support two DTMO IT investments, DTMO Passport and Oracle Service Cloud. The DTMO Passport is DTMO's network infrastructure currently hosted at Ft. Detrick, MD and is scheduled to move to DHRA's Oracle Cloud Infrastructure (OCI) environment in FY 2023. Passport consists of DTMO's travel data repository, Commercial Travel Information Management (CTIM) database, and over 30 applications that support the travel enterprise. Oracle Service Cloud, commonly known as the Ticket Management System (TMS), is a SaaS 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: Cyber Security Service Provider (CSSP) support, Cyber Scanning Tools licenses (Passport only), Security Control Assessment – Validation (SCA-V).

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

(Dollars in Thousands)		
FY 2022	**FY 2023**	**FY 2024**
433	**343**	**347**

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. 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 cybersecurity services. Specifically, external vulnerability scans, web vulnerability scanning, malware notification protection, and attack sensing and warning. Additionally, cybersecurity functions include contractor support for DoD Risk Management Framework accreditation requirements.

DSSC – Federal Voting Assistance Program (FVAP):

(Dollars in Thousands)		
FY 2022	**FY 2023**	**FY 2024**
107	**96**	**97**

DHRA - Cyber

I. Description of Operations Financed: (Cont.)

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 C5ISR.

DSSC – Military-Civilian Transition Office (MCTO):

MCTO's mission is to continually improve the delivery of resources, information, and assistance provided through the programs, promoting their effective and efficient support of transitioning Service members and members of the National Guard and Reserve, their families, and communities worldwide. The table below reflects the MCTO combined funding beginning in FY 2023.

(Dollars in Thousands)		
FY 2022	**FY 2023**	**FY 2024**
563	1,345	1,365

- Transition Assistance Program (TAP)

- Yellow Ribbon Reintegration Program (YRRP)

The Military-Civilian Transition Office (MCTO) combined Transition Assistance Program (TAP) and Yellow Ribbon Reintegration Program (YRRP) into one program. In January 2020, the Defense Personnel and Family Support Office (DPFSO) created the Military-Civilian Transition Office (MCTO) to merge the Office for Reintegration Programs (ORP) with TVPO to develop synergies between DPFSO programs. MCTO manages both the Transition Assistance Program (TAP) and the Yellow Ribbon Reintegration Program (YRRP) to efficiently deliver resources to transitioning Service members, members of the National Guard and Reserve Component, their families and communities worldwide. Both TAP and YRRP funding were consolidated in the FY 2023 President's Budget. Resource consolidation has been effective in current operations by streamlining contracts, curriculum, and to include a projected movement to a single Information Technology (IT) platform.

DSSC – MCTO / Transition Assistance Program (TAP):

The MCTO Transition Assistance Program (TAP) provides information, training, counselling, and tools to ensure the approximately 200,000 Service Members retiring, separating, or being released from Active Duty annually are successful in their transition to civilian life. The Transition Assistance Program's Information Technology (TAP-IT) suite, put into production in 2013, is a crucial piece in the overall TAP process. The TAP-IT suite provides data collection and reporting capability to the Department of Defense (DoD) in support of Title 10, U.S. Code, Chapter 58 as well as DoD policy, "Transition Assistance for Military Personnel." The TAP-IT System is the Enterprise DoD System of Record regarding the Veterans Opportunity to Work (VOW) to Hire Heroes Act compliance, ensuring that all eligible transitioning Service Members meet the required DoD Career

I. Description of Operations Financed: (Cont.)

Readiness Standards (CRS), as well as supporting collection of required data for Service Members having a viable Individual Transition Plan or receiving a "warm handover" to the interagency partners for post-transition Services.

The TAP-IT suite is the DoD-wide source for capturing transitioning Service members' TAP course attendance and documenting transition progress on an electronic DD Form 2648 across the Services. MCTO and the military Services are currently executing FY 2019 National Defense Authorization Act (NDAA) mandated changes, the Government Accountability Office (GAO) 2018 report recommended improvements and subsequent major changes that have resulted in a DoD policy to modify the 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 pdf 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", 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. Additionally, there are cyber security efforts to safeguard personally identifiable information (PII).

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

The MCTO Yellow Ribbon Reintegration Program (YRRP) is a Department of Defense-wide effort to promote the well-being of National Guard and Reserve Component members, their families and communities, by connecting them with resources throughout the deployment cycle through in-person and/or online events. Through Yellow Ribbon Reintegration events, Service members and loved ones connect with local resources before, during, and after deployments. The EventPLUS application is a DoD-wide tool supporting Reserve Component program managers and event planners in the implementation, management, evaluation, and budgeting of in-person and online events. Additionally, the EventPLUS application provides a 24/7 resource for National Guard and Reserve Component Service members where they can access on-demand trainings, deployment-related resources, and search and register for upcoming YRRP events in their local areas.

Cybersecurity functions include prevention of, damage to, protection of, and restoration of EventPLUS to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. 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, external vulnerability scans, web vulnerability scanning, malware notification protection, and attack sensing & warning. Additionally, cybersecurity functions include contractor support for DoD Risk Management Framework accreditation requirements.

Sexual Assault Prevention and Response Office (SAPRO):

(Dollars in Thousands)		
FY 2022	**FY 2023**	**FY 2024**

DHRA - Cyber

I. Description of Operations Financed: (Cont.)

323	1,090	285

The Department, under the guidance of the Sexual Assault Prevention and Response Office (SAPRO), has worked to improve its programs in an effort 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). Funding realigned to the Defense Manpower Data Center (DMDC)/Enterprise Data Service (EDS) for Defense Sexual Assault Information Database (DSAID) System Management in support of the Independent Review Commission (IRC) on Sexual Assault in the Military recommendations.

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. NDAA FY 2015, Section 545; and DoD policy.

DHRA - Cyber

II. Force Structure Summary:
N/A

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

A. BA Subactivities	FY 2022 Actuals	Budget Request	FY 2023 Congressional Action Amount	Percent	Appropriated	Current Enacted	FY 2024 Estimate
Defense Civilian Personnel Advisory Service (DCPAS)	$38	$0	$0	0.00%	$0	$0	$0
Defense Suicide Prevention Office (DSPO)	$14	$103	$0	0.00%	$103	$103	$103
DMDC - Defense Enrollment Eligibility Reporting System (DEERS)	$2,177	$3,244	$0	0.00%	$3,244	$3,244	$5,013
DMDC - Enterprise Data Services (EDS)	$4,926	$4,924	$0	0.00%	$4,924	$4,924	$4,548
DMDC - Enterprise Human Resources Information System (EHRIS)	$2,183	$2,080	$0	0.00%	$2,080	$2,080	$2,116
DMDC - Identity Credential Management (ICM)	$2,992	$9,193	$0	0.00%	$9,193	$9,193	$9,476
DMDC - Personnel Accountability (PA)	$0	$0	$0	0.00%	$0	$0	$0
DMDC - Personnel Accountability and Security (PAS)	$2,269	$2,161	$0	0.00%	$2,161	$2,161	$2,289
DPAC - Office of People Analytics (OPA)	$385	$796	$0	0.00%	$796	$796	$801
DSSC - Computer/Electronic Accommodations Program (CAP)	$369	$111	$0	0.00%	$111	$111	$113
DSSC - Defense Activity for Non-Traditional Education Support (DANTES)	$280	$0	$0	0.00%	$0	$0	$330
DSSC - Defense Language and National Security Education Office (DLNSEO)	$202	$266	$0	0.00%	$266	$266	$268
DSSC - Defense Travel Management Office (DTMO)	$361	$361	$0	0.00%	$361	$361	$366
DSSC - Employer Support of the Guard and Reserve (ESGR)	$433	$343	$0	0.00%	$343	$343	$347
DSSC - Federal Voting Assistance Program (FVAP)	$107	$96	$0	0.00%	$96	$96	$97
DSSC - Military-Civilian Transition Office (MCTO)	$563	$1,345	$0	0.00%	$1,345	$1,345	$1,365

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

		FY 2023					
		Budget	**Congressional Action**			**Current**	**FY 2024**
	FY 2022						
A. BA Subactivities	**Actuals**	**Request**	**Amount**	**Percent**	**Appropriated**	**Enacted**	**Estimate**
Sexual Assault Prevention and Response Office (SAPRO)	$323	$1,090	$0	0.00%	$1,090	$1,090	$285
Total	**$17,622**	**$26,113**	**$0**	**0.00%**	**$26,113**	**$26,113**	**$27,517**

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

B. Reconciliation Summary	Change FY 2023/FY 2023	Change FY 2023/FY 2024
BASELINE FUNDING	**$26,113**	**$26,113**
Congressional Adjustments (Distributed)	0	
Congressional Adjustments (Undistributed)	0	
Adjustments to Meet Congressional Intent	0	
Congressional Adjustments (General Provisions)	0	
SUBTOTAL APPROPRIATED AMOUNT	**26,113**	
Fact-of-Life Changes (2023 to 2023 Only)	0	
SUBTOTAL BASELINE FUNDING	**26,113**	
Supplemental	0	
Reprogrammings	0	
Price Changes		575
Functional Transfers		0
Program Changes		829
CURRENT ESTIMATE	**26,113**	**27,517**
Less: Supplemental	0	
NORMALIZED CURRENT ESTIMATE	**$26,113**	**$27,517**

DHRA - Cyber

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

FY 2023 President's Budget Request (Amended, if applicable)..**$26,113**

1. Congressional Adjustments $0

    a) Distributed Adjustments...$0

    b) Undistributed Adjustments $0

    c) Adjustments to Meet Congressional Intent...$0

    d) General Provisions $0

FY 2023 Appropriated Amount **$26,113**

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 2023 Baseline Funding...**$26,113**

4. Reprogrammings (Requiring 1415 Actions).. $0

    a) Increases $0

DHRA - Cyber

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

      b) Decreases $0

Revised FY 2023 Estimate..**$26,113**

5. Less: Item 2, Supplemental Appropriation and Item 4, Reprogrammings $0

      a) Less: Supplemental Funding $0

FY 2023 Normalized Current Estimate **$26,113**

6. Price Change $575

7. Functional Transfers $0

      a) Transfers In $0

      b) Transfers Out...$0

8. Program Increases...$3,013

      a) Annualization of New FY 2023 Program $0

      b) One-Time FY 2024 Increases $0

      c) Program Growth in FY 2024 ....$3,013

            1) DMDC - Defense Enrollment Eligibility Reporting System (DEERS) $1,698
            +$1,680 thousand - Cyber contract cost increase due to corresponding investment into the enhancement of
            DHRA's continuous monitoring operations and Risk Management Framework (RMF) accreditation processes
            to right size DHRA's cyber capabilities.
            +$18 thousand - Increase in Cyber requirements.
            (FY 2023 Baseline: $3,244 thousand; 0 FTEs)

            2) DMDC - Enterprise Data Services (EDS)...$814

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

+$814 thousand - Funding realigned to the Defense Manpower Data Center (DMDC)/Enterprise Data Service (EDS) for Defense Sexual Assault Information Database (DSAID) System Management in support of the Independent Review Commission (IRC) on Sexual Assault in the Military recommendations.
(FY 2023 Baseline: $4,924 thousand; 0 FTEs)

3) DMDC - Identity Credential Management (ICM) $81
+$81 thousand - ICM Program costs are increasing due to deployment of additional identity-focused cybersecurity toolsets used to protect its data (such as logging/SIEM capabilities and continuous monitoring toolsets).
(FY 2023 Baseline: $9,193 thousand; 0 FTEs)

4) DMDC - Personnel Accountability and Security (PAS) $80
+$80 thousand - Cyber contract cost increase due to corresponding investment into the enhancement of DHRA's continuous monitoring operations and Risk Management Framework (RMF) accreditation processes to right size DHRA's cyber capabilities.
(FY 2023 Baseline: $2,161 thousand; 0 FTEs)

5) DSSC - Defense Activity for Non-Traditional Education (DANTES) $330
+330 thousand - Realign funding to Cyber from Voluntary Education Non-cyber per recent contract awards to reflect the proper classification.
(FY 2023 Baseline: $0 thousand; 0 FTEs)

6) DSSC - Federal Voting Assistance Program (FVAP)...$2
+$2 thousand - Increase in portal enhancements for DMDC cyber hardening.
(FY 2023 Baseline: $96 thousand; 0 FTEs)

7) DSSC - Military-Civilian Transition Office (MCTO)...$8
+$8 thousand - Increase in IT Contract Support Services.
(FY 2023 Baseline: $1,345 thousand; 0 FTEs)

9. Program Decreases ....$-2,184

a) Annualization of FY 2023 Program Decreases $0

b) One-Time FY 2023 Increases $0

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

c) Program Decreases in FY 2024 .... $-2,184

    1) Defense Suicide Prevention Office (DSPO)... $-2
-$2 thousand - Efforts to consolidate DHRA cybersecurity services across the Field Activity have begun generating efficiencies that reduced individual program spend.
(FY 2023 Baseline: $103 thousand; 0 FTEs)

    2) DMDC - Enterprise Data Services (EDS)... $-1,298
-$1,298 thousand - Cyber EDS FY 2023 budget included implementation/adoption costs. FY 2024 costs decreases as we move from implementation to maintenance and sustainment costs of cyber tools.
(FY 2023 Baseline: $4,924 thousand; 0 FTEs)

    3) DMDC - Enterprise Human Resources Information System (EHRIS) .... $-10
-$10 thousand - Program decrease is related to a reduction in the number of Authority to Operate (ATO) validations. As the EHRIS cyber program matures, ATOs will be issued for longer durations, eliminating the need for annual revalidation work.
(FY 2023 Baseline: $2,080 thousand; 0 FTEs)

    4) DPAC - Office of People Analytics (OPA) .... $-13
-$13 thousand - Small decrease in annual Risk Management Framework (RMF) audit across all accredited platforms.
(FY 2023 Baseline: $796 thousand; 0 FTEs)

    5) DSSC - Defense Language and National Security Education Office (DLNSEO) .... $-4
-$4 thousand - Efforts to consolidate DHRA cybersecurity services across the Field Activity have begun generating efficiencies that reduced individual program spend.
(FY 2023 Baseline: $266 thousand; 0 FTEs)

    6) DSSC - Defense Travel Management Office (DTMO) .... $-3
-$3 thousand - Reduction in cyber support services as a result of the migration to an enterprise cloud environment.
(FY 2023 Baseline: $361 thousand; 0 FTEs)

    7) DSSC - Employer Support of the Guard and Reserve (ESGR) .... $-4

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

-$4 thousand - Efforts to consolidate DHRA cybersecurity services across the Field Activity have begun generating efficiencies that reduced individual program spend.
(FY 2023 Baseline: $343 thousand; 0 FTEs)

8) DSSC - Federal Voting Assistance Program (FVAP)... $-3
-$3 thousand - Efforts to consolidate DHRA cybersecurity services across the Field Activity have begun generating efficiencies that reduced individual program spend.
(FY 2023 Baseline: $96 thousand; 0 FTEs)

9) DSSC - Military-Civilian Transition Office (MCTO)... $-18
-$18 thousand - Efforts to consolidate DHRA cybersecurity services across the Field Activity have begun generating efficiencies that reduced individual program spend.
(FY 2023 Baseline: $1,345 thousand; 0 FTEs)

10) Sexual Assault Prevention and Response Office (SAPRO) .... $-829
-$814 thousand - Funding realigned to the Defense Manpower Data Center (DMDC)/Enterprise Data Service (EDS) for Defense Sexual Assault Information Database (DSAID) System Management in support of the Independent Review Commission (IRC) on Sexual Assault in the Military recommendations.
 (FY 2023 Baseline: $1,090 thousand; 0 FTEs)

FY 2024 Budget Request **$27,517**

DHRA - Cyber

IV. <u>Performance Criteria and Evaluation Summary</u>:

<u>Defense Suicide Prevention Office (DSPO)</u>
DSPO / 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 DSPO/DHRA networks; an increased number of these longer ATOs demonstrates a more secure environment.

Benchmarks	FY 2022 Estimate	FY 2023 Estimate	FY 2024 Estimate
	1	1	1

Remarks: DSPO, in conjunction with DMDC, maintains one ATO.

FY 2022: DSPO should receive a three-year ATO for the Military Mortality Database (MMDB).

FY 2023: The MMDB will be two years into a three-year ATO.

FY 2024: Continuing to get to three-year ATO

<u>Defense Manpower Data Center (DMDC)</u>
Defense Enrollment Eligibility Reporting System (DEERS) / Cyber

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

Performance Evaluation: 50 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 2022 Estimate	FY 2023 Estimate	FY 2024 Estimate
Three-year ATOs issued	10 percent	20 percent	30 percent

Remarks: Current FY 2022 at 0 percent

DHRA - Cyber

IV. <u>**Performance Criteria and Evaluation Summary**</u>:

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

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

Performance Evaluation: 50 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 2022 Estimate	FY 2023 Estimate	FY 2024 Estimate
Three-year ATOs issued	10 percent	20 percent	30 percent

Remarks: Current FY 2022 at 18 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 2022 Estimate	FY 2023 Estimate	FY 2024 Estimate
Cybersecurity tool coverage	85 percent	95 percent	95.5 percent

Remarks:

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 2022 Estimate	FY 2023 Estimate	FY 2024 Estimate

DHRA - Cyber

IV. <u>Performance Criteria and Evaluation Summary</u>:

Percent Compliant privileged user accounts	Not Available	100 percent	100 percent

Remarks:

Performance Statement: Reduce number of security breaches.

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

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

Benchmarks	FY 2022 Estimate	FY 2023 Estimate	FY 2024 Estimate
Root-level or User-Level Intrusions	1	0	0

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: 50 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 2022 Estimate	FY 2023 Estimate	FY 2024 Estimate
Three-year ATOs issued	10 percent	20 percent	30 percent

Remarks: Current FY 2022 at 13 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: Receive three year ATO for all programs in ICM that require an ATO.

DHRA - Cyber

IV. <u>Performance Criteria and Evaluation Summary</u>:

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 2022 Estimate	FY 2023 Estimate	FY 2024 Estimate
Three-year ATOs issued	10 percent	20 percent	30 percent

Remarks: Current FY 2022 at 20 percent

Defense Manpower Data Center (DMDC)
Personnel Accountability and Security (PAS) / Cyber

Performance Evaluation: Receive one year ATOs for Personnel Accountability NIPR programs.

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 2022 Estimate	FY 2023 Estimate	FY 2024 Estimate
Three-year ATOs issued	10 percent	20 percent	30 percent

Remarks: Current FY 2022 at 25 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.

DHRA - Cyber

IV. Performance Criteria and Evaluation Summary:

Benchmarks	FY 2022 Estimate	FY 2023 Estimate	FY 2024 Estimate
100 percent of OPA accreditation boundaries have an active ATO	100 percent	100 percent	100 percent

Defense Support Service Center (DSSC) manages eight DHRA programs

- Advanced Distributed Learning (ADL)

- 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 – Advanced Distributed Learning (ADL)
Advanced Distribute Learning (ADL)/Cyber

The ADL program is in the process of transitioning from OSD (P&R) to DHRA and all ADL requirements to include funding will be in DHRA DSSC beginning on 1 October 2022. ADL Cyber Performance Statements, Evaluations and Outcomes will be included in FY 2025.

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 is able to 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.

DHRA - Cyber

IV. Performance Criteria and Evaluation Summary:

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

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

Benchmarks	FY 2022 Estimate	FY 2023 Estimate	FY 2024 Estimate
Submit Assessment Scans.	2	4	4

Remarks: None.

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 2022 Estimate	FY 2023 Estimate	FY 2024 Estimate
Submit full DoD MOU/JST RMF artifacts/documentation into eMASS for DMDC review.	0	2	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 3 year ATO without conditions.

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

DHRA - Cyber

IV. Performance Criteria and Evaluation Summary:

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.

Benchmarks	FY 2022 Estimate	FY 2023 Estimate	FY 2024 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 were issued three-year ATOs in FY 2019.

FY 2022: Both systems will be targeted for three-year ATO renewal this FY.

FY 2023: Both ATOs will be maintained.

FY 2024: Both ATOs will be maintained.

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

Performance Statement: Sustain ATOs in accordance to RMF & DHRA guidelines to maintain a secure and achieve 3-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 2022 Estimate	FY 2023 Estimate	FY 2024 Estimate
# of ATOs approved	3	1	0

Remarks: As of FY 2022, DTMO maintains three ATOs, DTMO Passport/Ft. Detrick, DTMO Passport/OCI, and Oracle Service Cloud (also known as Ticket Management System). FY 2023, DTMO will submit an ATO extension for the Passport/Ft. Detrick.

DHRA - Cyber

IV. Performance Criteria and Evaluation Summary:

FY 2022: The DTMO successfully achieved a 1-year ATO for the Passport Ft. Detrick environment to allow for time to complete migration to OCI. However, the Passport OCI migration was delayed until FY 2023. An external ATO validation was not conducted in FY 2022 for Passport OCI environment (as previously forecasted), because a determination was made that an external ATO validation will was required.

The DTMO successfully achieved a 3-year ATO for the Passport OCI environment, it will expire May 12, 2025.

The Oracle Service Cloud external ATO validation was conducted, an ATO package was submitted and resulted in a 3-year ATO, expiring in March 21, 2025.

FY 2023: The DTMO will request an ATO extension for the Passport Ft. Detrick environment due to the delay in migration schedule.

FY 2024: DTMO will be in sustainment mode for both ATOs, DTMO Passport OCI and Oracle Service Cloud, and begin preparation for an ATO package submissions 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, Center, then works with appropriate offices to resolve issues identified.

Benchmarks	FY 2022 Estimate	FY 2023 Estimate	FY 2024 Estimate
Complete two WVS assessment scans and provide associated reports	2	2	2

DHRA - Cyber

IV. Performance Criteria and Evaluation Summary:

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 RMF documents to include: System Security Plan, Security Design, Network Architecture, Hardware/Software Inventory, Plan of Action and Milestones (POA&Ms), 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. All Information Technology Systems will compliance DoD Risk Management Framework (RMF) guidance.

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

Benchmarks	FY 2022 Estimate	FY 2023 Estimate	FY 2024 Estimate
RMF documentation uploaded and validated in eMass	95 percent	95 percent	95 percent

Remarks:
Support contractor has uploaded required documentation and Defense Manpower Data Center staff is scheduled to conduct validation during the fourth quarter of FY 2022.

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 the CSSP

DHRA - Cyber

IV. <u>Performance Criteria and Evaluation Summary</u>:

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 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.

Benchmarks	FY 2022 Estimate	FY 2023 Estimate	FY 2024 Estimate
Complete two WVS assessment scans	2	2	2

Remarks:
FVAP is working on assessing POAMs with cyber hardening in Software Security Center and meeting other conditions such as adhering to DMDC central logging. 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 RMF documents to include: System Security Plan, Security Design, Network Architecture, Hardware/Software Inventory, Plan of Action and Milestones (POA&Ms), 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 Risk Management Framework (RMF) as documented in the Enterprise Mission Assurance Support Service (eMASS).

Benchmarks	FY 2022 Estimate	FY 2023 Estimate	FY 2024 Estimate
RMF documentation uploaded and validated in eMass	100 percent	100 percent	100 percent

Remarks:

IV. Performance Criteria and Evaluation Summary:

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)

The Military – Civilian Transition Office (MCTO) combines Transition Assistance Program (TAP) and Yellow Ribbon Reintegration Program (YRRP) into one program. In January 2020, DPFSO created the Military-Civilian Transition Office (MCTO) to merge the Office for Reintegration Programs (ORP) with TVPO to develop synergies between DPFSO programs. MCTO manages both the Transition Assistance Program (TAP) and the Yellow Ribbon Reintegration Program (YRRP) to efficiently deliver resources to transitioning Service members, members of the National Guard and Reserve, their families and communities worldwide. Both TAP and YRRP funding consolidated in FY 2023. Resource consolidation has been effective in current operations by streamlining contracts, curriculum, and to include a projected movement to a single Information Technology (IT) platform.

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. CSSP is able to provide defensive cyber operations in support of network command/control, ensuring secure communications, 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 TVPO with vulnerabilities with respect to public facing web presence.

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

Benchmarks	FY 2022 Estimate	FY 2023 Estimate	FY 2024 Estimate
Complete Assessment Scans.	100 percent	100 percent	100 percent

DSSC – Military-Civilian Transition Office (MCTO)
Yellow Ribbon Reintegration Program (YRRP) / Cyber

DHRA - Cyber

IV. Performance Criteria and Evaluation Summary:

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 leading to 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 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 2022 Estimate	FY 2023 Estimate	FY 2024 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 RMF documents for EventPLUS to include: System Security Plan, Security Design, Network Architecture, Hardware/Software Inventory, POA&Ms, 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 EventPLUS security classification.

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

Benchmarks	FY 2022 Estimate	FY 2023 Estimate	FY 2024 Estimate

IV. <u>Performance Criteria and Evaluation Summary</u>:

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 2022.

<u>Sexual Assault Prevention and Response Office (SAPRO)</u>
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 2022 Estimate**	**FY 2023 Estimate**	**FY 2024 Estimate**
	1	1	1

Remarks:
SHL current ATO expires May 31, 2023.

DHRA - Cyber

V. Personnel Summary:

	FY 2022	**FY 2023**	**FY 2024**	**Change FY 2022/ FY 2023**	**Change FY 2023/ FY 2024**

N/A

DHRA - Cyber

VI. <u>OP 32 Line Items as Applicable (Dollars in thousands)</u>:

| | | FY 2022 Program | Change from FY 2022 to FY 2023 | | FY 2023 Program | Change from FY 2023 to FY 2024 | | FY 2024 Program |
			Price Growth	Program Growth		Price Growth	Program Growth	
671	DISA DISN SUBSCRIPTION SERVICES (DSS)	3,037	98	-3,135	0	0	0	0
0699	**TOTAL OTHER FUND PURCHASES**	**3,037**	**98**	**-3,135**	**0**	**0**	**0**	**0**
922	EQUIPMENT MAINTENANCE BY CONTRACT	118	2	-120	0	0	0	0
925	EQUIPMENT PURCHASES (NON-FUND)	3,335	70	-3,405	0	0	0	0
932	MGT PROF SUPPORT SVCS	1,409	30	-1,439	0	0	0	0
987	OTHER INTRA-GOVT PURCH	0	0	710	710	16	-458	268
989	OTHER SERVICES	364	8	24,130	24,502	539	-22,163	2,878
990	IT CONTRACT SUPPORT SERVICES	9,359	197	-8,655	901	20	23,450	24,371
0999	**TOTAL OTHER PURCHASES**	**14,585**	**307**	**11,221**	**26,113**	**575**	**829**	**27,517**
9999	**GRAND TOTAL**	**17,622**	**405**	**8,086**	**26,113**	**575**	**829**	**27,517**

DHRA - Cyber