Fiscal Year 2022 President's Budget

Defense Human Resources Activity Cyber

May 2021

Operation and Maintenance, Defense-Wide Summary ($ in thousands)
Budget Activity (BA) 1: Operating Forces/Combat Development Activities

	FY 2020 Actuals	Price Change	Program Change	FY 2021 Enacted	Price Change	Program Change	FY 2022 Request
DHRA Cyber	0	0	20,670	20,670	393	-3,408	17,655

*FY 2020 includes Division A, Title IX and X of the Consolidated Appropriations Act, 2020 (P.L. 116-93), Division F, Title IV and V from the Further Consolidated Appropriations Act, 2020 (P.L. 116-94) and the Coronavirus Aid, Relief, and Economic Security Act (P.L. 116-136).
*FY 2021 includes Division C, Title IX and Division J, Title IV of the Consolidated Appropriations Act, 2021 (P.L. 116-260).

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 2022 budget funds execution of the Field Activity’s mission to:

- Organize, direct, and manage all assigned resources, to include the programs described herein;
- Design and manage DHRA programs and activities to improve standards of performance, economy, and efficiency;
- Maintain a central repository of the Department of Defense (DoD) Human Resource (HR) information, both current and historic;
- Provide program and policy support and associated information management and administrative services to the DoD Components on civilian HR matters;
- Provide DoD-wide guidance on civilian personnel policy implementation and professional development programs (except with regard to Defense Civilian Intelligence Personnel System, where guidance is developed by the Under Secretary of Defense for Intelligence in conjunction with the USD (P&R));
- Provide rapid data-driven analytic solutions to support the decision making needs to effectively maintain the readiness of the All-Volunteer Force.
- Support the development of policy and administer the sexual assault prevention and response policies and programs for DoD;
- Support the development of policy and administer the suicide prevention policies and programs for the DoD;
- Support the development of policy and administer transition assistance programs for the DoD Service members leaving active duty;

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

- Develop policy and administer the combating trafficking in persons' policies and programs for the DoD;
- Support the development DoD civilian personnel policies While providing consulting/advisory services, programs, and solutions that strengthen the mission readiness and morale of DoD HR professionals and directly impact the more than 900,000 civilian employees that make up the DoD civilian workforce.
- Assist in the establishment and administration of policy regarding the development, maintenance, and utilization of language capabilities; monitor trends in the promotion, accession, and retention of individuals with critical skills; and explore innovative concepts to expand language capabilities;
- Serve as the single focal point for commercial travel within the DoD; assist in establishing strategic direction and in establishing and administering travel policy; centrally manage all commercial travel programs;
- Develop policy for DoD identification cards distributed to members of the Military, DoD civilians, contractors, and other eligible personnel and execute associated programs and capabilities;
- 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;
- Provide assistance to Service members and Veterans to pursue their educational goals and earn degrees or certifications during and after their service.
- Perform the technical research support needed to assess the impact and effectiveness of many P&R programs and policies which provides both evidence for DoD Leadership to base decisions on, and researched findings that identify opportunities to strengthen the All-Volunteer Force.
- Provide a Center of Excellence for training, education, research, and consultation in matters related to diversity and inclusion; military and civilian equal opportunity; and the prevention and response to sexual harassment, harassment, hazing and bullying across the total force.

The Field Activity is comprised of operational programs that support the OUSD (P&R) in its mission to develop policies, plans, and programs that will ensure the readiness of the Total Force and the well-being of military families. The Field Activity supports the USD (P&R) vision of creating an organization dedicated and committed to the readiness of the Department's Service men and women, their families, and civilian employees.

<u>Narrative Explanation of Changes</u>:
The FY 2022 DHRA Cyber budget represents a net programmatic decrease of -$3.4 million with a price growth of +$.4 million.

<u>Cyber Funding:</u>

(Dollars in Thousands)

I. Description of Operations Financed: (Cont.)

FY 2020	FY 2021	FY 2022
0	20,670	17,655

Beginning in FY 2021, DHRA identified and transferred $20,670 thousand in cyber funding, from within the direct reporting organizations and programs, to a newly established cyber funding line for increased visibility and tracking purposes.

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

(Dollars in Thousands)		
FY 2020	FY 2021	FY 2022
0	0	428

The Department of Defense Voluntary Education System (DoDVES) supports the DANTES Examination program which takes incoming credit-by-exam score data and provides it to the appropriate Service Voluntary Education (VolEd) management systems. Cyber activity funding enables completion of risk management framework (RMF) requirements to maintain an Authority to Operate (ATO). Requirements include completing Assured Compliance Assessment Solution (ACAS) scans, Security Technical Implementation Guide (STIGs), maintaining boundary drawings, hardware and software lists and security of the host activity. Continuous monitoring also requires resources to keep all of these events and the associated documents (artifacts) up to date and compliant. Funding also provides SaaS (Software as a Service)/PaaS (Platform as a Service) support.

Defense Language and National Security Education Office (DLNSEO):

(Dollars in Thousands)		
FY 2020	FY 2021	FY 2022
0	254	248

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.

DHRA Enterprise Operations Center (DEOC):

(Dollars in Thousands)		
FY 2020	FY 2021	FY 2022
0	1,551	0

I. <u>Description of Operations Financed</u>: (Cont.)
Funding in FY 2021 was misidentified as cyber, DEOC has no cyber requirements as reflected in FY 2022.

<u>Defense Manpower Data Center (DMDC) manages five DHRA programs:</u>

- Defense Enrollment Eligibility Reporting System (DEERS)
- Enterprise Data Service (EDS)
- Enterprise Human Resource Information System (EHRIS)
- Identity Credential Management (ICM), formerly known as Real-Time Automated Personnel Identification System (RAPIDS)
- Personnel Accountability and Security (PAS), formerly known as Personnel Accountability (PA) and Personnel Security Assurance (PSA)

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.

<u>DMDC - Defense Enrollment Eligibility Reporting System (DEERS):</u>

(Dollars in Thousands)		
FY 2020	**FY 2021**	**FY 2022**
0	**2,731**	**1,941**

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

<u>DMDC - Enterprise Data Service (EDS):</u>

(Dollars in Thousands)		
FY 2020	**FY 2021**	**FY 2022**
0	**2,489**	**4,393**

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

<u>DMDC - Enterprise Human Resource Information System (EHRIS):</u>

(Dollars in Thousands)

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

FY 2020	FY 2021	FY 2022
0	2,157	1,945

Cybersecurity funding provides the sustainment of EHRIS portfolio with access to DMDC's Cyber cybersecurity tools, enterprise security engineering, auditing, continuous audits, monitoring, incident response, and compliance reporting. Risk management and security engineering support.

DMDC - Identity Credential Management (ICM):

(Dollars in Thousands)		
FY 2020	FY 2021	FY 2022
0	2,197	2,698

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

DMDC - Personnel Accountability and Security (PAS):

(Dollars in Thousands)		
FY 2020	FY 2021	FY 2022
0	1,460	2,023

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

Department of Defense Personnel and Family Support Center (DPFSC) manages four DHRA programs:

- Computer/Electronic Accommodations Program (CAP)
- Employer Support of the Guard and Reserve (ESGR)
- Federal Voting Assistance Program (FVAP)
- Transition to Veterans Program Office (TVPO)
- Yellow Ribbon Reintegration Program (YRRP)

DPFSC - Computer/Electronic Accommodations Program (CAP):

I. Description of Operations Financed: (Cont.)

(Dollars in Thousands)		
FY 2020	FY 2021	FY 2022
0	278	104

Recognizing that the cost of technology often remained a barrier to employment, the DoD established CAP in 1990 as a centrally funded program to provide assistive technology (AT) and support services to DoD civilian employees with disabilities at no cost to employing components or field activities. Since its inception, CAP's scope has significantly expanded to provide active duty Service members with assistive technology and allowing those who are wounded, injured or ill to retain equipment (AT) upon separation. Today, approximately 2.8 million DoD employees, wounded, ill and injured Service members, as well as active duty and reserve military personnel are potentially eligible for products and services at no additional cost to the requestor for products and services through this 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, provides over 221,000 accommodations to DoD civilian employees and Service members, and is widely considered the go-to source on providing effective AT solutions. These functions would not be possible without the use of CAP's Portal Defense Business System, 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 related to the platform used in executing the fulfillment contract providing materials in support of outreach efforts.

DPFSC - Employer Support of the Guard and Reserve (ESGR):

(Dollars in Thousands)		
FY 2020	FY 2021	FY 2022
0	1,797	322

The ESGR program fosters a culture in which all employers support and value the employment of members of the National Guard and Reserve Components (RC) in the United States and Territories, thereby increasing the readiness of the RCs. ESGR develops and promotes supportive work environments for Service members in the RCs through outreach, recognition, and educational opportunities that increase awareness of applicable laws and resolves employer conflicts between the Service members and their employers. ESGR operates in every state, territory, and the District of Columbia through a network of more than 3,500 volunteers and approximately 57 support staff members to increase the readiness of the RCs.

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. Specifically, external vulnerability scans, web vulnerability scanning, malware notification protection, and attack sensing & warning (DoDI 8500.01 and DoDI 8530.01). Additionally, cybersecurity functions include contractor support for DoD Risk Management Framework (DoDI 8510.01) accreditation requirements.

I. Description of Operations Financed: (Cont.)
DPFSC - Federal Voting Assistance Program (FVAP):

(Dollars in Thousands)		
FY 2020	**FY 2021**	**FY 2022**
0	**273**	**92**

FVAP's cyber needs are integrated in to 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 backend 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.

DPFSC – Transition to Veterans Program (TVPO)/Transition Assistance Program (TAP):

(Dollars in Thousands)		
FY 2020	**FY 2021**	**FY 2022**
0	**3,188**	**843**

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, DoD Instruction (DoDI) 1332.35, "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 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. TVPO and the military Services are currently processing 2019 National Defense Authorization Act (NDAA) mandated changes, the Government Accountability Office (GAO) 2018 report recommended improvements and subsequent major changes that have result a DoDI 1332.35 rewrite that modifies the CRS. DoD requires Service Members to meet with a TAP Counsellor for their initial counseling prior to their pre-separation counseling and transition from Service if they have served on active duty for more than 180 continuous days. The mandated NDAA changes as well as the DoDI and GAO recommendations require modification to both the electronic and pdf DD Form 2648, increase reporting requirements, and necessitate new development for adding a client management capability

I. Description of Operations Financed: (Cont.)

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).

DPFSC – Yellow Ribbon Reintegration Program (YRRP):

(Dollars in Thousands)		
FY 2020	**FY 2021**	**FY 2022**
0	**2,245**	**415**

The Yellow Ribbon Reintegration Program (YRRP) is a Department of Defense-wide effort to promote the well-being of National Guard and Reserve members, their families and communities, by connecting them with resources throughout the deployment cycle both in-person and online. Through Yellow Ribbon 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 manager 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 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 supporting 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 (DoDI 8500.01 and DoDI 8530.01). Additionally, cybersecurity functions include contractor support for DoD Risk Management Framework (DoDI 8510.01) accreditation requirements.

Defense Suicide Prevention Office (DSPO):

(Dollars in Thousands)		
FY 2020	**FY 2021**	**FY 2022**
0	**0**	**97**

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.

I. Description of Operations Financed: (Cont.)

Defense Travel Management Office (DTMO):

(Dollars in Thousands)		
FY 2020	FY 2021	FY 2022
50	50	338

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. 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).

Office of People Analytics (OPA):

(Dollars in Thousands)		
FY 2020	FY 2021	FY 2022
0	0	750

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.

Sexual Assault Prevention and Response Office (SAPRO):

(Dollars in Thousands)		
FY 2020	FY 2021	FY 2022
0	0	1,018

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 assist the Military Service sexual assault prevention and response (SAPR) program management and DoD

I. Description of Operations Financed: (Cont.)

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 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 FY15, Section 545; DoD Instruction (DoDI) 6495.02; DoDI 6495.03

II. Force Structure Summary:

N/A

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

		FY 2021					
			Congressional Action				
A. BA Subactivities	**FY 2020 Actuals**	**Budget Request**	**Amount**	**Percent**	**Appropriated**	**Current Enacted**	**FY 2022 Request**
Defense Activity for Non-Traditional Education Support (DANTES)	$0	$0	$0	0.00%	$0	$0	$428
Defense Language and National Security Education Office (DLNSEO)	$0	$256	$-2	-0.78%	$254	$254	$248
Defense Suicide Prevention Office (DSPO)	$0	$0	$0	0.00%	$0	$0	$97
Defense Travel Management Office (DTMO)	$0	$50	$0	0.00%	$50	$50	$338
DHRA Enterprise Operations Center (DEOC) (Formerly HQ - Operations)	$0	$1,561	$-10	-0.64%	$1,551	$1,551	$0
DMDC - Defense Enrollment Eligibility Reporting System (DEERS)	$0	$2,749	$-18	-0.65%	$2,731	$2,731	$1,941
DMDC - Enterprise Data Services (EDS)	$0	$2,505	$-16	-0.64%	$2,489	$2,489	$4,393
DMDC - Enterprise Human Resources Information System (EHRIS)	$0	$2,171	$-14	-0.64%	$2,157	$2,157	$1,945
DMDC - Identity Credential Management (ICM) - (Formerly RAPIDS)	$0	$2,211	$-14	-0.63%	$2,197	$2,197	$2,698
DMDC - Personnel Accountability (PA)	$0	$1,470	$-10	-0.68%	$1,460	$1,460	$0
DMDC - Personnel Accountability and Security (PAS)	$0	$0	$0	0.00%	$0	$0	$2,023
DPFSC - Computer/Electronic Accommodations Program (CAP)	$0	$280	$-2	-0.71%	$278	$278	$104
DPFSC - Employer Support of the Guard and Reserve (ESGR)	$0	$1,809	$-12	-0.66%	$1,797	$1,797	$322
DPFSC - Federal Voting Assistance Program (FVAP)	$0	$275	$-2	-0.73%	$273	$273	$92
DPFSC - Transition to Veterans Program Office (TVPO)	$0	$3,209	$-21	-0.65%	$3,188	$3,188	$843
DPFSC - Yellow Ribbon Reintegration Program (YRRP)	$0	$2,260	$-15	-0.66%	$2,245	$2,245	$415
Office of People Analytics (OPA)	$0	$0	$0	0.00%	$0	$0	$750

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

		FY 2021					
			Congressional Action				
A. BA Subactivities	**FY 2020 Actuals**	**Budget Request**	**Amount**	**Percent**	**Appropriated**	**Current Enacted**	**FY 2022 Request**
Sexual Assault Prevention and Response Office (SAPRO)	$0	$0	$0	0.00%	$0	$0	$1,018
Total	**$0**	**$20,806**	**$-136**	**-0.65%**	**$20,670**	**$20,670**	**$17,655**

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

B. Reconciliation Summary	Change FY 2021/FY 2021	Change FY 2021/FY 2022
BASELINE FUNDING	**$20,806**	**$20,670**
Congressional Adjustments (Distributed)	0	
Congressional Adjustments (Undistributed)	-136	
Adjustments to Meet Congressional Intent	0	
Congressional Adjustments (General Provisions)	0	
SUBTOTAL APPROPRIATED AMOUNT	**20,670**	
Fact-of-Life Changes (2021 to 2021 Only)	0	
SUBTOTAL BASELINE FUNDING	**20,670**	
Supplemental	0	
Reprogrammings	0	
Price Changes		393
Functional Transfers		0
Program Changes		-3,408
CURRENT ESTIMATE	**20,670**	**17,655**
Less: Wartime Supplemental	0	
NORMALIZED CURRENT ESTIMATE	**$20,670**	**$17,655**

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

FY 2021 President's Budget Request (Amended, if applicable)			**$20,806**
1. Congressional Adjustments			$-136
a) Distributed Adjustments		$0	
b) Undistributed Adjustments		$-136	
1) Undistributed Reduction - Excess to need - Non NIP	$-136		
c) Adjustments to Meet Congressional Intent		$0	
d) General Provisions		$0	
FY 2021 Appropriated Amount			**$20,670**
2. War-Related and Disaster Supplemental Appropriations			$0
a) OCO Supplemental Funding		$0	
3. Fact-of-Life Changes			$0
a) Functional Transfers		$0	
b) Technical Adjustments		$0	
c) Emergent Requirements		$0	
FY 2021 Baseline Funding			**$20,670**
4. Reprogrammings (Requiring 1415 Actions)			$0

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

a) Increases	$0
b) Decreases	$0
Revised FY 2021 Estimate	**$20,670**
5. Less: Item 2, War-Related and Disaster Supplemental Appropriation and Item 4, Reprogrammings	$0
a) Less: OCO Supplemental Funding	$0
FY 2021 Normalized Current Estimate	**$20,670**
6. Price Change	$393
7. Functional Transfers	$0
a) Transfers In	$0
b) Transfers Out	$0
8. Program Increases	$8,043
a) Annualization of New FY 2021 Program	$0
b) One-Time FY 2022 Increases	$0
c) Program Growth in FY 2022	$8,043
1) Defense Activity for Non-Traditional Education (DANTES)	$428

+$428 thousand - Realign DANTES non-Cyber program funds to DANTES Cyber for risk management framework and authority to operate costs. Planned costs include completing Assured Compliance Assessment Solution (ACAS) scans, Security Technical Implementation Guide (STIGs), maintaining boundary drawings, hardware and software lists and security of the host activity.

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

(FY 2021 Baseline: $0 thousand; 0 FTEs)

2) Defense Suicide Prevention Office (DSPO).. $97
+$97 thousand - Realign DSPO's Suicide Data Repository program funding to DSPO's Military Mortality Database (MMDB) DHRA Cyber program. To fund on-going cyber services such as the Annual Risk Management Framework (RMF) audit in order to achieve/maintain the system's Authority to Operate (ATO) and maintain and implement a host of cybersecurity scan tools to monitor the system for any vulnerabilities, intrusions, malware, end-of-life software/code, etc.
(FY 2021 Baseline: $0 thousand; 0 FTEs)

3) Defense Travel Management Office (DTMO) $287
+$199 thousand - Increased funding to support the new cybersecurity measures for the transition of DTMO Passport to an enterprise cloud environment. Cybersecurity measures include: Authorization to Operate (ATO) Security Control Assessor-Validator (SCA-V), Cyber Security Service Provider (CSSP), and cybersecurity scanning tools.
+88 thousand - Increased funding to support the new cybersecurity measures for the DTMO Oracle Service Cloud, also known as the Ticket Management System (TMS). Cybersecurity measures include: Authorization to Operate (ATO) Security Control Assessor-Validator (SCA-V) and Cyber Security Service Provider (CSSP).
(FY 2021 Baseline: $50 thousand; 0 FTEs)

4) DMDC - Enterprise Data Services (EDS)... $2,981
+$2,981 thousand - Realign program funds from EDS non-Cyber to EDS Cyber to support authority to operation and risk management framework costs associated with cloud migration.
(FY 2021 Baseline: $2,489 thousand; 0 FTEs)

5) DMDC - Identity Credential Management (ICM) - (Formerly RAPIDS)... $459
+$459 thousand - Cybersecurity Upgrades. Supports ongoing investment in Cyber hardening efforts of the Identity Credential Management (ICM) software portfolio. DMDC continues to invest in cybersecurity scanning software and mature vulnerability management processes, leading to the identification of additional cybersecurity vulnerabilities that require mitigation. Funds will be used to contract for software development, business analysis, and system architecture support to remediate systems within the Identity Credential Management (ICM) portfolio and provide improvements to reduce the rate of new Cyber findings and code vulnerabilities.
(FY 2021 Baseline: $2,197 thousand; 0 FTEs)

6) Office of People Analytics (OPA) $750

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

+$750 thousand - Increase funds to support cyber requirements for Cyber Security Support Provider (CSSP) support and Authority to Operate (ATO) related audits.
(FY 2021 Baseline: $0 thousand; 0 FTEs)

7) Personnel Accountability and Security (PAS) $2,023
+$1,488 thousand – Realign funding from Personnel Accountability (PA) to PAS.
+$535 thousand – Increased funding to support cloud migration as applications now have separate accreditation boundaries and additional funds are required to support the Risk Management Framework (RMF) and the Authority To Operate (ATO) processes.
(FY 2021 Baseline: $0 thousand; 0 FTEs)

8) Sexual Assault Prevention and Response Office (SAPRO) $1,018
+$1,018 thousand - Realign program funds from SAPRO non-cyber to SAPRO cyber to support Authority To Operate (ATO) and Risk Management Framework (RMF) costs associated with cybersecurity and infrastructure.
(FY 2021 Baseline: $0 thousand; 0 FTEs)

9. Program Decreases ....$-11,451

a) Annualization of FY 2021 Program Decreases $0

b) One-Time FY 2021 Increases .... $-842

1) DMDC - Defense Enrollment Eligibility Reporting System (DEERS)... $-842
-$842 thousand - funding decrease is a result of a one-time increase in FY 2021 to support the DEERS Authority to Operate (ATO) and audit.
(FY 2021 Baseline: $2,371 thousand; 0 FTEs)

c) Program Decreases in FY 2022 .... $-10,609

1) Defense Language and National Security Education Office (DLNSEO).. $-11
-$11 thousand - cost reductions due to consolidation of cyber costs and re-assessment of DHRA cyber costs.
(FY 2021 Baseline: $254 thousand; 0 FTEs)

2) DHRA Enterprise Operations Center (DEOC) (Formerly HQ - Operations) .... $-1,580

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

-$1,580 thousand - Funding in FY 2021 was misidentified as cyber, DEOC has no cyber requirements in FY 2022.
(FY 2021 Baseline: $1,551 thousand; 0 FTEs)

3) DMDC - Enterprise Data Services (EDS).. $-1,124
-$1,124 - decreased cyber toolset costs due to lower cost of ongoing sustainment licensing versus initial acquisition.
(FY 2021 Baseline: $2,489 thousand)

4) DMDC - Enterprise Human Resources Information System (EHRIS) .... $-253
-$253 thousand - Cost decrease as a result of migration to SaaS solutions and inherent security controls.
(FY 2021 Baseline: $2,157 thousand; 0 FTEs)

5) DMDC - Personnel Accountability (PA)... $-1,488
-$1,488 thousand - Realign funding to new program Personal Accountability and Security (PAS).

(FY 2021 Baseline: $1,460 thousand; 0 FTEs)

6) DPFSC - Computer/Electronic Accommodations Program (CAP)... $-179
-$179 thousand - Realigned funding from CAP Cyber to CAP non-Cyber program due to misidentification of initial Cyber costs.

(FY 2021 Baseline: $278 thousand; 0 FTEs)

7) DPFSC - Employer Support of the Guard and Reserve (ESGR)... $-1,509
-$1,509 thousand - Funding realignment from ESGR Cyber to ESGR non-Cyber program due to prior year misidentification.

(FY 2021 Baseline: $1,797 thousand; 0 FTEs)

8) DPFSC - Federal Voting Assistance Program (FVAP) .... $-186
-$186 thousand - Funding realignment from FVAP Cyber to FVAP non-Cyber program due to prior year misidentification.
(FY 2021 Baseline: $273 thousand; 0 FTEs)

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

9) DPFSC - Transition to Veterans Program Office (TVPO) .... $-2,406
-$2,406 thousand - Funding realignment from TVPO Cyber to TVPO non-Cyber program due to prior year misidentification.

(FY 2021 Baseline: $3,188 thousand; 0 FTEs)

10) DPFSC - Yellow Ribbon Reintegration Program (YRRP) .... $-1,873
-$1,873 thousand - Funding realignment from YRRP Cyber to YRRP non-Cyber program due to prior year misidentification.

(FY 2021 Baseline: $2,245 thousand; 0 FTEs)

FY 2022 Budget Request $17,655

IV. Performance Criteria and Evaluation Summary:

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

The OP-5, Part IV for Cyber is a new requirement for FY 2022. Currently no data collection efforts have been in place and there are no metrics to present at this time. DHRA has begun this process for the FY 2023 budget.

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

The OP-5, Part IV for Cyber is a new requirement for FY 2022. Currently no data collection efforts have been in place and there are no metrics to present at this time. DHRA has begun this process for the FY 2023 budget.

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 1 year

Performance Evaluation: 50% 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.

Performance Statement: Reduce the ratio of the number of Program Manager (PM) and Product Owners (PO) needing Risk Management Framework (RMF)/eMASS training to the number of PMs/POs that have been trained

Performance Evaluation: 90% of Program Managers/Product Owners complete RMF/eMASS training

Performance Outcome: More informed PMs/POs result in stronger accreditation packages and a lower risk posture for the DMDC network

Benchmarks	FY 2020 Actual	FY 2021 Estimate	FY 2022 Estimate
	0	0	1

IV. Performance Criteria and Evaluation Summary:

Remarks:

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

Performance Statement: Increase number of ATOs issued for more than 1 year

Performance Evaluation: 50% 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.

Performance Statement: Reduce the ratio of the number of Program Manager and Product Owners needing RMF/eMASS training to the number of PMs/POs that have been trained

Performance Evaluation: 90% of Program Managers/Product Owners complete RMF/eMASS training

Performance Outcome: More informed PMs/POs result in stronger accreditation packages and a lower risk posture for the DMDC network

Benchmarks	FY 2020 Actual	FY 2021 Estimate	FY 2022 Estimate
	0	0	1

Remarks:

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

Performance Statement: Increase number of ATOs issued for more than 1 year

Performance Evaluation: 50% 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.

IV. Performance Criteria and Evaluation Summary:

Benchmarks	FY 2020 Actual	FY 2021 Estimate	FY 2022 Estimate
	0	0	1

Remarks:

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

Performance Statement: Increase number of ATOs issued for more than 1 year

Performance Evaluation: Receive 3 year ATO for all programs in ICM that require an ATO.

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.

Performance Statement: Increase the percent of Product Owners that have completed RMF/eMASS training

Performance Evaluation: 100% of Product Owners complete RMF/eMASS training

Performance Outcome: More informed Product Owners result in stronger accreditation packages and a lower risk posture for the DMDC network.

Benchmarks	FY 2020 Actual	FY 2021 Estimate	FY 2022 Estimate
	0	0	3

Remarks:

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

Performance Evaluation: Receive 3 year ATOs for Personnel Accountability NIPR programs

IV. Performance Criteria and Evaluation Summary:

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 2020 Actual	FY 2021 Estimate	FY 2022 Estimate
	0	0	3

Remarks:
FY22 ATOs expected:

- Synchronized Predeployment and Operational Tracker (SPOT) Enterprise Suite/Total Operational Picture Support System (TOPSS) Non-Secure Internet Protocol Router (NIPR)
- Neo Tracking System (NTS)

Personnel Accountability NIPR Applications (Personnel Location Web Service (PLWS), Personnel Accountability Reporting System (PARS), Personnel Location Accountability Check Online (PLACO)

Defense Personnel Family Support Center (DPFSC)
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 DoDI 8530.01 compliance support and provides situational awareness of organization web application vulnerability posture and correlation of vulnerabilities to threats.

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 2020 Actual	FY 2021 Estimate	FY 2022 Estimate
Complete Assessment Scans.	0	2	2

Remarks: None.

IV. **Performance Criteria and Evaluation Summary**:

Performance Statement: The DOD Cybersecurity service evaluation process begins with the submission of a formal application package in the Enterprise Mission Assurance Support Service (eMASS). As outlined in Department of Defense Manual (DODM) 8530.01, the application package must contain a letter of request for an evaluation of cybersecurity activities (only for prospective CSSPs), a completed self-assessment utilizing the current ESM, cybersecurity service alignment matrix and supporting artifacts. Insignia/Excentium will assist CAP with the completion of RMF artifacts, develop Plan of Action and Milestones (POA&Ms) for all findings (technical and policy/documentation) that cannot be remediated prior to DMDC review, submit artifacts and application package into eMass, and provide all pertinent guidance to CAP.

Performance Evaluation: Successful completion of DMDC Risk Management Framework (RMF) artifacts in support of CAPX Authority to Operate (ATO) requirements.

Performance Outcome: Insignia/Excentium completes DMDC RMF requirements and submits full CAPX package into eMass.

Benchmarks	FY 2020 Actual	FY 2021 Estimate	FY 2022 Estimate
Submit full CAPX RMF artifacts/documentation into eMass for DMDC review.	0	100%	0

Remarks: Insignia/Excentium has uploaded required documentation and DMDC staff is scheduled to conduct validation during the second quarter of FY21. Once the validation is complete the contractor and CAP will be required to correct any discrepancies identified.

Defense Personnel Family Support Center (DPFSC)

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 DoDI 8530.01 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 IAW 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.

IV. Performance Criteria and Evaluation Summary:

Benchmarks	FY 2020 Actual	FY 2021 Estimate	FY 2022 Estimate
Complete two WVS assessment scans and provide associated reports	0	2	2

Remarks:
ESGR is migrating 6 servers hosted at DISA to update Windows operating system in the second and third quarters of FY21. Once the migration is complete, web vulnerability scans will be requested. Once reports are provided, ESGR will work with DISA and support contractors to correct any vulnerabilities identified.

Performance Statement:
The 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 2020 Actual	FY 2021 Estimate	FY 2022 Estimate
RMF documentation uploaded and validated in eMass	0	95%	95%

Remarks:
Support contractor has uploaded required documentation and Defense Manpower Data Center staff is scheduled to conduct validation during the third quarter of FY21. Once the validation is complete the contractor will be required to correct any discrepancies identified.

Defense Personnel Family Support Center (DPFSC)
Federal Voting Assistance Program (FVAP) / Cyber

IV. Performance Criteria and Evaluation Summary:

Performance Statement: The C5ISR Center Cybersecurity Service Provider (CSSP) is one of 23 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 helps to achieve DoDI 8530.01 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 2020 Actual	FY 2021 Estimate	FY 2022 Estimate
Complete two WVS assessment scans	0	2	2

Remarks:
FVAP will be changing over Tomcat servers and updating versions of other security software like Splunk in FY 2021. Other compliance tasks and remediation will be dealt with from the controls that were found to need updates in the Risk Management Framework (RMF) Audit in support of the FVAP Portal Authority to Operate.

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:

IV. Performance Criteria and Evaluation Summary:

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 2020 Actual	FY 2021 Estimate	FY 2022 Estimate
RMF documentation uploaded and validated in eMass	0	100%	100%

Remarks:
Support contractor has uploaded required documentation and Defense Manpower Data Center (DMDC) staff is scheduled to conduct validation during the third quarter of FY21. Once the validation is complete the contractor will be required to correct any discrepancies identified.

Defense Personnel Family Support Center (DPFSC)
Transition to Veterans Program Office (TVPO) /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 DoDI 8530.01 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 2020 Actual	FY 2021 Estimate	FY 2022 Estimate
Complete Assessment Scans.	100%	100%	100%

Defense Personnel Family Support Center (DPFSC)
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,

IV. Performance Criteria and Evaluation Summary:

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 helps to achieve DoDI 8530.01 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 2020 Actual	FY 2021 Estimate	FY 2022 Estimate
Vulnerability Scanning	40%	100%	100%

Remarks: The government and contractor began implementing CSSP for EventPLUS in FY 2020 and completed partial scanning and estimates 40% compliance with required vulnerability scanning. The government anticipates to reach 100% of required scanning by FY 2021 and continues to coordinate with the contractor and DMDC personnel to conduct 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 2020 Actual	FY 2021 Estimate	FY 2022 Estimate
RMF documentation uploaded and validated in eMass	40%	90%	100%

IV. Performance Criteria and Evaluation Summary:

Remarks: The government is coordinating with the contractor and DMDC personnel to update all RMF documentation as part of the RMF assessment for EventPLUS slated to being in 3rd Quarter FY21. The government anticipates being 100% compliant with RMF documentation requirements by FY 2022.

Defense Suicide Prevention Office (DSPO)

DSPO / Cyber

The OP-5, Part IV for Cyber is a new requirement for FY 2022. Currently no data collection efforts have been in place and there are no metrics to present at this time. DHRA has begun this process for the FY 2023 budget.

Defense Travel Management Office (DTMO)

DTMO / Cyber

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

Performance Evaluation: 50% 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 DTMO/DMDC/DHRA networks; an increased number of these longer ATOs demonstrates a more secure environment.

Benchmarks	FY 2020 Actual	FY 2021 Estimate	FY 2022 Estimate
	0	0	2

Remarks: DTMO maintains two ATOs, DTMO Passport and Oracle Service Cloud (also known as Ticket Management System).

FY2021: DTMO Passport was granted a 1-year ATO in January 2021; Oracle Service Cloud was granted a 1-year extension until April 7, 2022, due to contract constraints to perform the ATO audit.

FY2022: DTMO Passport is scheduled to migrate to DHRA/DMDC’s cloud environment (a new ATO will be required); the audit of Oracle Service Cloud will be completed and the ATO package submitted; Oracle Service Cloud is Software as a Service with no issues anticipated.

Office of People Analytics (OPA)

IV. Performance Criteria and Evaluation Summary:

OPA / Cyber

The OP-5, Part IV for Cyber is a new requirement for FY 2022. Currently no data collection efforts have been in place and there are no metrics to present at this time. DHRA has begun this process for the FY 2023 budget.

Sexual Assault Prevention and Response Office (SAPRO)

Defense Sexual Assault Incident Database (DSAID) / Cyber

Performance Statement: Maintain DSAID Authority to Operate (ATO) per requirements and security controls outlined by the Joint Service Provider (JSP).

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

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

Benchmarks	FY 2020 Actual	FY 2021 Estimate	FY 2022 Estimate
	0	2	1

Remarks:
DSAID current ATO-C expires September 8, 2021. SAPRO is actively working with JSP to resolve outstanding issues identified.

*Increase in FY21 and FY22 due to the need to maintain JSP ATO and obtain new DMDC ATO for DSAID concurrently.

V. Personnel Summary:

	FY 2020	FY 2021	FY 2022	Change FY 2020/ FY 2021	Change FY 2021/ FY 2022

Personnel Summary Explanations:

N/A

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

			Change from FY 2020 to FY 2021			Change from FY 2021 to FY 2022		
		FY 2020 Program	Price Growth	Program Growth	FY 2021 Program	Price Growth	Program Growth	FY 2022 Program
987	OTHER INTRA-GOVT PURCH	0	0	532	532	10	-190	352
989	OTHER SERVICES	0	0	16,950	16,950	322	-812	16,460
991	FOREIGN CURRENCY VARIANCE	0	0	3,188	3,188	61	-2,406	843
0999	**TOTAL OTHER PURCHASES**	**0**	**0**	**20,670**	**20,670**	**393**	**-3,408**	**17,655**
9999	**GRAND TOTAL**	**0**	**0**	**20,670**	**20,670**	**393**	**-3,408**	**17,655**

*FY 2020 includes Division A, Title IX and X of the Consolidated Appropriations Act, 2020 (P.L. 116-93), Division F, Title IV and V from the Further Consolidated Appropriations Act, 2020 (P.L. 116-94) and the Coronavirus Aid, Relief, and Economic Security Act (P.L. 116-136).
*FY 2021 includes Division C, Title IX and Division J, Title IV of the Consolidated Appropriations Act, 2021 (P.L. 116-260).