Fiscal Year 2024 Budget Estimates

Defense Counterintelligence and Security Agency

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
DCSA	941,189	18,789	38,155	998,133	48,917	15,073	1,062,123

I. Description of Operations Financed:
Operational Activities

A. Industrial Security (IS) Directorate:

The Industrial Security (IS) directorate, formerly the Critical Technology Protection mission, contributes to national security by serving as the primary interface between the Federal Government and cleared industry under DoD cognizance. Mandated by guidance set forth in DoD Instruction 5220.22 and Executive Order 12829, the DCSA administers and implements the defense portion of the National Industrial Security Program (NISP) on behalf of the DoD and 34 other federal executive branch agencies. The IS directorate vets and provides oversight, direction, and assistance to cleared contractors, their security programs and associated classified information systems, and the analysis and mitigation of foreign ownership, control or influence (FOCI) at over 10,000 cleared companies with approximately 12,500 contractor facilities and approximately 6,500 classified systems. The IS directorate plays a key role providing oversight to cleared industry and mitigating potential insider threats and intrusions by adversaries attempting to gain access to classified information. Additionally, pursuant to DoD Instruction 5100.76, the IS directorate also assesses security measures for the physical security of sensitive conventional Arms, Ammunition and Explosives (AA&E) at contractor facilities.

The IS directorate also provides operational and administrative support to field operations, which includes guidance, policy interpretation regarding industrial and personnel security policy, and international programs. This support is accomplished by assessing and mitigating foreign interest risk, conducting holistic business intelligence analysis, and collaborating with experts in security, finance, business structures, and governance to analyze FOCI in U.S. companies performing classified work. The IS directorate conducts analysis on covered transactions involving cleared industry under FOCI mitigations to the Office of the Under Secretary of Defense, Acquisition and Sustainment (OUSD(A&S)) in support of the Committee on Foreign Investment in the United States (CFIUS), which requires coordination with senior members of foreign, civilian, and military organizations, who represent more than 65 foreign governments that are signatories of bilateral security agreements for the timely and secure international movement of both U.S. and foreign classified information related to international security requirements.

The IS directorate has expanded into three new mission areas following the publication of multiple polices and regulations set forth by DoD Instruction 5200.48. These areas include responsibility for the Department's efforts to manage the Controlled Unclassified Information (CUI) program, which assigns the IS directorate responsibility for supporting the agency's efforts to comply with program policies and regulations. Section 847 of the National Defense Authorization Act of Fiscal Year (FY) 2020 names the DCSA as the lead agency to conduct FOCI analysis, mitigation, and management of beneficial ownerships for certain DoD contracts over $5M in support of the Department’s acquisition programs. The mission supports

I. Description of Operations Financed: (Cont.)
the Office of the Under Secretary of Defense, Intelligence and Security (OUSD(I&S)), OUSD(A&S), and the Office of the Under Secretary of Defense, Research and Engineering (OUSD(R&E)) in enabling the protection of DoD supply chains to further reduce Defense Industrial Base FOCI risks. Lastly, in support of the NISP mission, the DCSA established a formal program for Secure Internet Protocol Router

Network (SIPRNet) Command Cyber Readiness Inspections (CCRIs). Addressing requirements in CJCSI 6211.02D and DoDI 8010.01, the formal program allows the DCSA to improve the Department's cybersecurity readiness posture through the detection, mitigation, and resolution of vulnerabilities in Defense contractor SIPRNet enclaves.

1. Critical Technology Protection Integration Cell (CTPIC)

The CTPIC is a whole-of-government engagement effort to deter, detect, and disrupt the unauthorized technology transfer activities of our adversaries. The CTPIC serves as the DoD focal point for assessments, coordination, integration, and operational information sharing related to critical technology protection across all phases of research, development, and sustainment. The CTPIC also encompasses Blue Advantage, which provides assessments on DoD and interagency efforts to safeguard critical and emerging technology with defense and defense intelligence applications.

2. Applied Research Laboratory for Intelligence and Security (ARLIS)

The ARLIS program management office oversees the University Affiliated Research Center (UARC) on behalf of the Defense Intelligence and Security Enterprises to provide strategic research and development to solve intelligence and security problems. The ARLIS overlays human behavior, social science and culture, and language expertise with proficiency, research, and development in emerging and advanced technologies to solve increasingly technical, and human-centered intelligence and security challenges.

B. Personnel Vetting:

1. Consolidated Adjudications Services (CAS)
Funds support the DoD Personnel Security, Suitability/Fitness, and Credentialing (SSC) Adjudications Program used for overall incoming adjudication requirements and derogatory information developed as part of the Continuous Vetting (CV) mission. The DoD Adjudications program delivers informed and timely adjudicative decisions supporting a Trusted Workforce to enable operational readiness and risk management. Adjudication is the foundation to supporting personnel readiness and warfighter lethality. The program protects national security information by clearing appropriate personnel, supporting the hiring of trusted personnel into the federal workforce, and vetting personnel for logical and physical access to DoD facilities. The DoD Adjudications program proactively identify risks to protect national security information and further enable the DoD to apply innovative technologies to detect, deter, and mitigate insider threats critical to DoD mission readiness. The CAS remains committed to maintaining compliance with Intelligence Reform and Terrorism Prevention Act (IRTPA) timeliness standards.

I. Description of Operations Financed: (Cont.)

2. Vetting Risk Operations (VRO)
Provides personnel security support and oversight of National Industrial Security Program (NISP) contractor personnel by executing the Personnel Security Investigation – Industry (PSI-I) funding, and granting interim determinations for national security clearances. Provides personnel security oversight for industry personnel having access to U.S. and foreign classified information. Manages approximately 1.3 million cleared contractors during the lifecycle of their time having access to classified information. The VRO CV mission will transfer to the DCSA Defense Working Capital Fund in FY 2024.

3. Publicly Available Social Media Information (PASMI)
In FY 2024, the DCSA will pursue multiple efforts to implement a scalable capability to include PASMI into background investigations in accordance with Security Executive Agent Directive 5 (SEAD 5) and aligned to the Trusted Workforce 2.0 personnel vetting reform initiative. The investment being implemented includes collection, analysis, and reporting tools for PASMI in support of national security eligibility determinations. The DCSA's Personnel Security missions [Background Investigations (BI) and VRO] are managing research projects with the ARLIS and the Defense Advanced Research Projects Agency (DARPA) as part of the discovery learning process. Additionally, these missions are conducting multiple pilots to test different capabilities, which will enable PASMI to be included in the initial vetting for the accessions population and to be expanded to all initial investigations of the DCSA personnel, as well as the CV populations. The DCSA's DoD Insider Threat Management and Analysis Center (DITMAC) is expanding a proof of concept to continue exploring ad hoc PASMI capabilities to support the insider threat mission. In addition, the DCSA's VRO access to PASMI also fulfills the Secretary's requirements to improve the vetting of International Military Students who intend to or are currently receiving training within the continental U.S.

The DoD studies have identified PASMI as a unique data source to identify key behaviors that are potentially derogatory under the Allegiance, Foreign Influence, Foreign Preference, Personal Conduct, and other guidelines of the National Security Adjudication Guidelines. Data received from PASMI is often not found anywhere else in the course of the personnel vetting cycle. The PASMI will not be the sole source of information guiding a decision. It adds a data layer, supplementing an already wide-ranging compilation of information contributing to common sense determinations about an individual's suitability. The DCSA continues exploration to determine the most efficient and cost-effective means by which to integrate social media checks into BI and CV, in a manner which yields the most productive outcomes while not exponentially increasing product costs.

C. DoD Insider Threat Management and Analysis Center (DITMAC):

The DITMAC provides an integrated capability to collect and analyze information for insider threat detection and mitigation. The program gathers, integrates, reviews, assesses, and responds to information derived from DoD Insider Threat hubs, Counterintelligence (CI), security, cybersecurity, civilian and military personnel management, workplace violence, anti-terrorism risk management, law enforcement, user activity monitoring (UAM) on DoD information networks, and other sources as necessary and appropriate to identify, mitigate, and counter insider threats to address current and emerging threats to DoD personnel, assets and information. Continuing in FY 2024, the DITMAC will provide program management for the Department's Non-Secure Internet Protocol Router Network (NIPRnet) UAM program to identify, validate, or corroborate behaviors that could be

I. Description of Operations Financed: (Cont.)
indicative of an insider threat on DoD unclassified networks. The DITMAC will offer a centralized capability to comply with the NIPRnet UAM Program, including a tool capability and analytical support. The NIPR UAM capability provides the Department an ability to proactively detect and monitor indicators of concern for a limited population set on the unclassified IT system. Starting in FY 2024, and in compliance with Executive Order 13587, the DCSA will expand the UAM analytic capabilities to the Office of the Secretary of Defense and 4th Estate Organizations on the SIPRnet domain.

D. Training Directorate:

1. Security Training (ST)

Delivers security education, training, and certification products and services to the DoD and other federal agencies and industry under the National Industrial Security Program (NISP). The ST directorate utilizes an agile delivery platform to maximize accessibility from in-person, instructor-led courses, online courses, webinars, video presentations, toolkits, and job aids. Develops and manages the Security Professional Education Development Certification Program, which provides a series of National Commission for Certifying Agencies accredited professional certifications across multiple security disciplines designed to professionalize the security workforce via a common set of competencies that promote interoperability and facilitate professional development and training.

2. National Center for Credibility Assessments (NCCA)

The NCCA is the sole provider of credibility assessment education and training; audits of agencies' quality assurance programs against federal standards; and research, development, testing and evaluation of credibility assessment equipment and protocols within the federal government. The NCCA provides services to 30 federal partner agencies by conducting three 12-week initial polygraph examiner training courses per year and multiple continuing education courses, to include required countermeasures training. The NCCA has the oversight responsibility to ensure federal programs consisting of approximately 1,100 polygraph examiners conduct their examinations in accordance with federal and agency policies and requirements. These federally trained examiners conduct more than 103,000 screening, operational, and criminal specific examinations per year.

E. Counterintelligence (CI) Analysis:

Detects and deters attempts by the nation’s adversaries to steal sensitive national security information and technologies from cleared industry and keep U.S. Government leaders informed of the threat. The CI Special Agents work extensively with companies and other U.S. Government agencies to quickly and efficiently identify, share, and refer actionable threat information. The CI Analysis Division authors the premier publication, “Targeting U.S. Technologies: An Assessment of Threats to Cleared Industry,” which is a culmination of suspicious contact reports from across the cleared national industrial base, describing suspicious foreign activity targeting U.S. personnel, technologies, and export-controlled products. The Cyber Operations Division employs tools and processes to aggressively address threats to cleared contractors in the cyber domain. The Cyber team’s proficiencies in cyber, CI, and technical analysis create a work center capable of implementing innovative solutions to identify, assess, and neutralize the cyber threat from foreign intelligence entities.

I. Description of Operations Financed: (Cont.)

F. Personnel Security:

1. Personnel Security Investigations for Industry (PSI-I):
The centrally managed PSI-I Program budget is used to execute requests for initial and periodic reinvestigations for contractor personnel security clearance in support of all DoD components and 36 other Federal Agencies participating in the National Industrial Security Program (NISP). Budgetary requirements are based on anticipated industry investigations by case type, in accordance with the DCSA Working Capital Fund published rates, and adjusted to include costs on a case by case basis for Triggered Enhanced Subject Interviews (TESI) and Reimbursable Security Investigations (RSI). The DCSA manages requests for initial and periodic reinvestigations for contractor personnel. The PSI-I requirements and budgets are impacted by changes in security policy, investigation pricing, and demand for research, development, and acquisition programs supporting DoD components and Federal agencies participating in the NISP.

2. International Military Student (IMS) Screening

The IMS provides centralized screening and vetting of International Military Student training in the U.S. as a result of the December 2019 Pensacola Naval Air Station Shooting. The DoD procedures for IMS vetting were established in accordance with Section 1090 of the National Defense Authorization Act (NDAA) of FY 2021. Budgetary requirements are based on the anticipated number of initial and continuing or periodic reviews. The IMS population is vetted through the Expedited Screen Protocol (ESP) products and services offered by the DCSA Working Capital Fund. This capability optimizes intelligence data sources, other classified and unclassified U.S. Government data systems and human analytics to provide multi-point identity detection of potential foreign risks and high risk, which includes association with international terrorism, foreign intelligence entities, and international crime.

Operational Support Activities

A. Management Headquarters:

1. The DCSA Headquarters enables mission execution through centralized management of enterprise strategic priorities to provide direct service support to field operations. These functions provide critical common services support devoted to the daily operations by enabling industry's delivery of uncompromised capabilities and leveraging advanced technologies and innovation. The support consists of financial management, acquisitions, human capital management, legal advice and assistance through the general counsel and inspector general, public affairs, strategic management, and equal employment opportunity.

The Chief Strategy Office (CSO) is the primary source for the development and implementation of the DCSA strategy and transformation efforts, and provides specialized strategic advice to the Director, DCSA, on these matters. The CSO is responsible for strategy development, for enabling and overseeing strategy implementation and monitoring, measuring achievement of the DCSA strategic objectives through key performance indicators, and aligning strategy to mission and staff support functions, to include finance, talent, technology, acquisition, and establishing the agency's policy

I. Description of Operations Financed: (Cont.)

doctrine. The CSO leads the DCSA's enterprise data management, analytics, operational performance metrics management, and knowledge management. The CSO drives enterprise transformation efforts that enable maturation and optimization of the Agency's business processes and leverages enterprise data and infrastructure to increase mission performance. The CSO manages enterprise policy and governance, leads DCSA requirements generation activities, executes Component Acquisition Executive (CAE) functions, and leads process improvement initiatives in coordination with relevant stakeholders.

B. Facilities and Physical Security:

The Logistics Management Office (LMO) and Security Programs Office (SPO) conduct facility acquisition, maintenance, property management, logistical management, physical security, and access control for 167 field offices distributed across the U.S. for FY 2024. The DCSA established formal programs for these offices allowing proper planning to address increased physical space requirements associated with the mission expansion and transfers. The requirements include additional sensitive compartmented information facilities (SCIFs) for the Counterintelligence and Industrial Security missions, improvements to existing physical space, leasing government vehicles, and the implementation of a regional field structure to reduce costs while optimizing information sharing across mission areas. Funding for this function is being requested for the first time in FY 2024.

C. Office of the Chief Information Officer (OCIO):

The OCIO drives how best to assure information technology (IT) fully and economically supports the DCSA's business operations, customer needs on all matters relating to the DCSA information enterprise. The OCIO provides wide-ranging network protection and security of DCSA network and information systems. The OCIO comprehensively coordinates with the National Institutes of Standards and Technology, Defense Information Systems Agency, National Security Agency, Committee on National Security Systems, Office of the Director of National Intelligence, Joint Forces Headquarters, Department of Defense Information Network (DoDIN), and others relative to information technology and cybersecurity policies and procedures affecting the DCSA’s automation initiatives.

D. National Background Investigations Service (NBIS):

The NBIS is transitioning to the DCSA’s Working Capital Fund in FY 2024.

E. Program Executive Office (PEO)

The PEO provides a portfolio of enterprise-wide IT programs that employ best practice methodologies for the delivery of innovative IT solutions, advancing DCSA’s broad-spectrum National Security capabilities to better serve the DoD, the U.S. Government and cleared industry. Essential programs within the PEO include:

I. Description of Operations Financed: (Cont.)

1. DITMAC System of Systems (DSoS)

The DCSA's insider threat mission uses the DITMAC System of Systems (DSoS) to enable information sharing, collaboration, analysis, and risk mitigation to address current and emerging threats insiders pose to DoD personnel, assets, and information across over 50 insider threat hubs and programs supporting DoD Components, Specialized Missions, and the Intelligence Community (IC). Hubs report insider threat cases to the DITMAC via the DSoS that correlates this information with additional data sources and historical data. Funding sustains activities including hosting, licenses, engineering, service desk, user support services, operational support, and cybersecurity/risk management framework support associated with the insider threat mission.

2. National Industrial Security System (NISS)

The NISS provides industrial security capabilities to include the systems of record for facilities clearance information and industrial security oversight, improved risk assessment and mitigation related to contractors under Foreign Ownership, Control, or Influence (FOCI), and identification of clearances requirements for contracting companies. Funding supports software sustainment activities to include system updates to meet emerging DoD and DCSA policy (e.g. migration to new cloud environments, data sharing with DoD stakeholders, etc.), cybersecurity updates to remain compliant with emerging accreditation requirements (e.g. Security Technical Implementation Guides, application and platform configurations, etc.), continuous monitoring along with annual security reviews for NIPR and SIPR, software licenses and system vulnerability assessments, and mitigation plans.

3. Security Education Training Systems (SETS)

The DCSA requires up to eleven independent and semi-independent systems to meet its missions of providing security education and training to government, industry, and public workforces. Funding ensures the continued operations, maintenance, and essential enhancements of those training platforms. Further, it will facilitate the rationalization and consolidation of the DCSA's education and training platforms while enhancing the capabilities that learners, instructors, administrators, and agency leaders depend upon to properly transfer knowledge to the learner. Finally, the FY 2024 request will enable the future instantiation of a security education and training ecosystem by leveraging agency enterprise tools while providing the essential education and learning

II. Force Structure Summary:
N/A

III. Financial Summary ($ in Thousands):

		FY 2023					
			Congressional Action				
A. BA Subactivities	FY 2022 Actuals	Budget Request	Amount	Percent	Appropriated	Current Enacted	FY 2024 Estimate
Counterintelligence Program	$60,063	$53,197	$15,000	28.20%	$68,197	$68,197	$67,318
Facilities and Physical Security	$0	$0	$0	0.00%	$0	$0	$45,368
Industrial Security	$101,086	$122,272	$0	0.00%	$122,272	$122,272	$155,360
Insider Threat - DITMAC	$21,937	$64,823	$0	0.00%	$64,823	$64,823	$89,423
Management HQ Activities	$82,788	$53,660	$0	0.00%	$53,660	$53,660	$57,787
National Background Investigative Service (NBIS)	$74,198	$8,502	$0	0.00%	$8,502	$8,502	$0
Office of Chief Information Officer	$63,944	$58,430	$0	0.00%	$58,430	$58,430	$50,926
Personnel Vetting	$172,994	$228,423	$0	0.00%	$228,423	$228,423	$172,202
Program Executive Office (PEO)	$49,291	$29,688	$0	0.00%	$29,688	$29,688	$27,974
PSI for Industry	$283,683	$322,185	$0	0.00%	$322,185	$322,185	$353,350
Training	$31,205	$41,953	$0	0.00%	$41,953	$41,953	$42,415
Total	**$941,189**	**$983,133**	**$15,000**	**1.53%**	**$998,133**	**$998,133**	**$1,062,123**

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

B. Reconciliation Summary	Change FY 2023/FY 2023	Change FY 2023/FY 2024
BASELINE FUNDING	**$983,133**	**$998,133**
Congressional Adjustments (Distributed)	15,000	
Congressional Adjustments (Undistributed)	0	
Adjustments to Meet Congressional Intent	0	
Congressional Adjustments (General Provisions)	0	
SUBTOTAL APPROPRIATED AMOUNT	**998,133**	
Fact-of-Life Changes (2023 to 2023 Only)	0	
SUBTOTAL BASELINE FUNDING	**998,133**	
Supplemental	0	
Reprogrammings	0	
Price Changes		48,917
Functional Transfers		0
Program Changes		15,073
CURRENT ESTIMATE	**998,133**	**1,062,123**
Less: Supplemental	0	
NORMALIZED CURRENT ESTIMATE	**$998,133**	**$1,062,123**

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

FY 2023 President's Budget Request (Amended, if applicable)	**$983,133**
1. Congressional Adjustments	$15,000
a) Distributed Adjustments	$15,000
1) Joint Cyber Intelligence Tool Suite	$15,000
b) Undistributed Adjustments	$0
c) Adjustments to Meet Congressional Intent	$0
d) General Provisions	$0
FY 2023 Appropriated Amount	**$998,133**
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	**$998,133**
4. Reprogrammings (Requiring 1415 Actions)	$0

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

a) Increases $0

b) Decreases $0

Revised FY 2023 Estimate $998,133

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

a) Less: Supplemental Funding $0

FY 2023 Normalized Current Estimate $998,133

6. Price Change $48,917

7. Functional Transfers $0

a) Transfers In $0

b) Transfers Out $0

8. Program Increases $112,963

a) Annualization of New FY 2023 Program $0

b) One-Time FY 2024 Increases $581

1) Civilian Compensable - One Additional Compensable Workday $581
One additional compensable day is included in FY 2024. The number of compensable days for FY 2023 is 260 days (2080 hours), and for FY 2024 is 261 days (2088 hours)
(FY 2023 Baseline: $293,353 thousand)

c) Program Growth in FY 2024 ..... $112,382

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

1) Consolidated Adjudications Services $10,475
Increase is a result of IT support for the increasing derogatory nature of the personnel security, suitability and credential adjudication mission.
(FY 2023 Baseline: $115,118 thousand)

2) Facilities and Physical Security $44,787
The increase will improve planning for current and future agency physical space requirements for facilities, logistics, and security in support of new and expanded missions.
(FY 2023 Baseline: $0 thousand)

3) Industry Security $26,557
Supports the implementation of section 847 of the FY 2020 NDAA requiring Foreign Ownership, Control, and Influence (FOCI) pre-award analysis of all Defense contracts valued at $5M or more.
(FY 2023 Baseline: $122,271 thousand; 435 FTEs; +79 FTEs)

4) Insider Threat $22,655
Expand upon insider threat analysis capacity and NIPRnet User Activity Monitoring (UAM) IT capability and analytic capacity, and expand analysis to the SIPR domain. Increase program capacity through delivery of Prevention, Assistance, and Response (PAR) capability to joint military installations.
(FY 2023 Baseline: $64,823 thousand; 69 FTEs; +22 FTEs)

5) Management Headquarters $2,517
Provides resources for recruitment and retention incentives to improve the DCSA's ability to attract, recruit, and retain personnel with cyber; science, technology, engineering, and math (STEM); high demand/low density skills;, and advanced certifications in key mission areas.
(FY 2023 Baseline: $53,660 thousand)

6) Personnel Security Investigations for Industry $5,391
Increase supports the Trusted Workforce implementation which will increase Continues Vetting (CV) expenses such as time base checks, and alert resolution.
(FY 2023 Baseline: $322,185 thousand)

9. Program Decreases ..... $-97,890

a) Annualization of FY 2023 Program Decreases $0

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

b) One-Time FY 2023 Increases ..... $-15,000

1) Joint Cyber Intelligence Tool Suite ..... $-15,000

c) Program Decreases in FY 2024 ..... $-82,890

1) Office of Chief Information Officer ..... $-9,257
Funding realigned to address the Department of Defense-directed higher priority requirements for Industrial Security CCRI) and Personnel Vetting (PSMOI)
(FY 2023 Baseline: $58,430 thousand)

2) Enterprise Training ..... $-797
Decrease in courseware delivery through use of technology such as video teleconference, and other cost-efficient course options supporting creditability assessments (polygrapher training).
(FY 2023 Baseline: $41,953 thousand)

3) Personnel Vetting - Vetting Risk Operation (VRO) ..... $-58,324
Reduced funding and FTEs for VRO as the Continuous Vetting (CV) missions converts to WCF for the implementation of the Trusted Workforce 2.0 requirements.
(FY 2023 Baseline: $105,805 thousand; 251 FTEs; -58 FTEs)

4) Program Executive Office ..... $-2,605
Reduced funds for legacy IT systems supporting execution of the Personnel Vetting mission (the Defense Central Index of Investigations and Investigative Records Repository). Transitioned Secure Web Fingerprint Transmission (SWFT) capability to working capital funds in accordance with transition of other personnel vetting mission areas.
(FY 2023 Baseline: $29,688 thousand)

5) National Background Investigation Service (NBIS) ..... $-8,757
Reduction is due to the transition of the National Background Investigation System (NBIS) to the DCSA working capital fund in FY 2024.
(FY 2023 Baseline: $8,502 thousand; 52 FTEs; -27 FTEs)

6) Counterintelligence Program ..... $-2,925
Decreases contractor support that produce and disseminate raw reporting requirements in relation to classified technology due to emphasis on threat vulnerability technology reporting.

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

(FY 2023 Baseline: $68,197 thousand)

7) International Military Student ..... $-225
The decrease is due to a new pricing model for costs associated with access to controlled unclassified information and suitability clearances.
(FY 2023 Baseline: $7,500 thousand)

FY 2024 Budget Request $1,062,123

IV. Performance Criteria and Evaluation Summary:

1. Industrial Security (IS) Directorate

A. National Industrial Security Program (NISP) Performance Measure: Protection of Classified Information

Comments: The 12,500 cleared facilities for which the Defense Counterintelligence and Security Agency Industrial Security (DCSA IS) Directorate provides oversight are geographically dispersed across the United States. These facilities range from small consulting firms with part-time, inexperienced security managers to large manufacturing facilities and research and development plants with professional security staffs. Some of the larger facilities possess vast amounts of classified information and have very complex security requirements.

The DCSA IS intentionally engages with industry and individual members of the Defense Industrial Base (DIB) on a regular basis and on a wide range of issues. These touchpoints and actions contribute to the DCSA's oversight of the National Industrial Security Program (NISP) and the protection of classified information in cleared industry. At the front-end of the process, the DCSA IS makes a risk-based determination as to the trustworthiness of a facility and whether or not they can become a member of the NISP and hold a facility clearance. If a facility does get admitted to the NISP, there are numerous activities the DCSA IS conducts to determine the security posture of a facility and whether or not it is eligible to remain in the NISP. The DCSA IS uses sound risk management principles to prioritize the appropriate level of engagement with a facility.

The core of the NISP is the Security Review; the DCSA is the only agency providing security review oversight on classified contracts. The security review evaluates and rates cleared facilities' security programs to check for compliance with 32 CFR Part 117 requirements and uses a risk-based approach to determine if the facility is applying appropriate mitigation measures to minimize the potential compromise, loss, or damage of classified information. As the NISP moved into FY 2022 under the new 32 CFR Part 117, the DCSA also unveiled and applied a new security review and rating process. To date, the DCSA has effectively conducted 2,000 reviews under this process in the return to on-site engagements, identifying and mitigating risks throughout industry. During COVID-19 operations, the DCSA IS had created a supplemental remote oversight process called Continuous Monitoring Engagements (CMEs). Due to the impactful nature of this remote oversight, both as a health check on the security posture of facilities, and as a flag for identifying when an on-site visit was warranted, this process was further codified into what is now known as Security Monitoring Actions (SMAs). While SMAs do not replace the value and purpose of on-site security reviews, they do provide a valuable supplement and indicator and will continue to be used as an oversight capability.

IV. Performance Criteria and Evaluation Summary: (Cont.)

The following metrics track engagement with industry across a variety of activities and report on various meaningful outcomes of those activities.

FY 2022 Actions	
Security Reviews	1,964
Security Monitoring Actions (SMAs)	1,303
Facility Clearances Issued	458
Information Systems Authorized to Process Classified Information	2,465
FY 2022 Findings	
Total Vulnerabilities Identified	827
Total Administrative Findings Identified	4,261
Security Violations Processed	637
Cases Involving Loss/Compromise of Classified Information	353
Number of Invalidations / Revocations	44 / 0

2. Training Directorate

A. Security Training (ST)

Performance Measure #1: Requested Seats in Center for Development of Security Excellence (CDSE) FY 2022 Scheduled Courses

Comments: This performance measure is used to compare the number of "student seats" (throughput capacity) available for Instructor-led classroom and virtual Instructor-led courses vs. "student seats" requested by the security community in FY 2022. During FY 2022, the CDSE increased virtual instructor-led training offerings to manage the community needs and continuity of operations during the evolving COVID-19 Pandemic. Alternative delivery methods were produced and courses redesigned to continue delivery of traditional classroom courses in a virtual format for continuity of mission. Overall access/completions of CDSE online courses/products continue to significantly increase from previous pre-pandemic years.

IV. Performance Criteria and Evaluation Summary: (Cont.)

FY22 Seats Available in Courses Scheduled	**21-Oct**	**21-Nov**	**21-Dec**	**22-Jan**	**22-Feb**	**22-Mar**	**22-Apr**	**22-May**	**22-Jun**	**22-Jul**	**22-Aug**	**22-Sep**	**Total**
Monthly Available Seats As Scheduled	19	160	101	90	126	23	75	181	95	54	197	157	1278
Requested Total Seats	20	204	114	223	184	25	116	238	100	126	297	160	1807
% of Seat Requests	95%	78%	89%	40%	68%	92%	65%	76%	95%	43%	66%	98%	71%

ST Performance Measure #2: Required Active Course Inventory. **Comments:** This output performance measure provides the actual number of active training courses (Virtual and Instructor Led Courses, eLearning Courses and Short Format Learning Courses) in the inventory compared with the total number of CDSE courses in maintenance due to new/updated policy, updated Defense Security Skill Standards, changing security landscape, new mission areas and/or security community requests. The goal is to make sure all courses continue to be current, accurate and relevant with the current security environment which requires continuous maintenance and sustainment of courses. An emphasis is being put on online learning products vs. classroom today, where possible, to meet the exponential growth in the demand for CDSE products.

IV. Performance Criteria and Evaluation Summary: (Cont.)

Active Products FY 2022	***Oct-21***	***Nov-21***	***Dec-21***	***Jan-22***	***Feb-22***	***Mar-22***	***Apr-22***	***May-22***	***Jun-22***	***Jul-22***	***Aug-22***	***Sep-22***
Active Products	*525*	*527*	*527*	*531*	*535*	*536*	*545*	*550*	*554*	*554*	*562*	*565*
Products in Maintenance or Development	*61*	*51*	*40*	*43*	*43*	*46*	*45*	*40*	*39*	*35*	*35*	*34*
% of Total Inventory in Maintenance or Development	*12%*	*10%*	*8%*	*8%*	*8%*	*9%*	*8%*	*7%*	*7%*	*6%*	*6%*	*6%*

3. Counterintelligence (CI)

A. (CUI) CI Performance Measures: Annual processing of intelligence information reports (IIRs) and relevance of analytic products (output and impact) to the community. The CI identifies threats to personnel, facilities, information, and technology resident in the cleared U.S. industrial base, the DCSA enterprise, and is charged to identify threats targeting the federal government's trusted workforce. In all three instances, the CI articulates those threats to stakeholders and action agencies for potential mitigation, investigative, or operational consideration. The DCSA continually updates and aligns activities to detect, deter, and disrupt National Intelligence Priorities Framework (NIPF) actors targeting critical defense technologies, the DCSA enterprise, and the federal government's trusted workforce. Production targets are: (1) release ≥ 90% of the annual IIR production target and (2) ≥ 95% of all analytic products produced will address NIPF CI Tier 1-3 countries and non-state actors – Foreign intelligence Entities (FIE) (output/impact).

4. Personnel Vetting

A. Consolidated Adjudications Services (CAS)

DCSA CAS Performance Measure: To determine security clearance eligibility of non-Intelligence Agency Department of Defense (DoD) personnel occupying sensitive positions and/or requiring access to classified material including Sensitive Compartmented Information (SCI). These determinations involve all military service members, applicants, civilian employees, and consultants affiliated with the DoD, to include DoD Personnel at the White House and contractor personnel under the National Industrial Security Program (NISP). The DCSA CAS also adjudicates security clearance eligibility for staff of the United States Senate and House of Representatives, the Congressional Budget Office, the United States Capitol Police and selected judicial staff. Additionally, the DCSA CAS renders favorable adjudicative determinations for employment suitability of DoD civilian employees and Common Access Card (CAC) or Fitness eligibility of non-cleared DoD contractors.

IV. Performance Criteria and Evaluation Summary: (Cont.)

	FY 2020	FY 2021	FY 2022	FY 2023
Number of Personnel Serviced	3,600,000	3,600,000	3,600,000	3,600,000
Number of suitability/credential (Tier 1) background investigation decisions	78,250	68,188	68,188	68,188
Number of national security (Tier 3, 5, 3R, and 5R) investigation decisions	763,150	665,012	665,012	665,012
Number of on-going security management actions (customer service requests, Continuous Evaluation (CE) alerts, incident reports)	105,700	154,450	151,500	151,500

B. Personnel Security Investigation-Industry (PSI-I) Performance Measure: The PSI-I budget is based on total number of forecasted investigations, by case type, and the DCSA rate, and adjusted to include costs on a case by case basis for Triggered Enhanced Subject Interviews (TESI) and Reimbursable Security Investigations (RSI). The DCSA administers requests for initial and periodic reinvestigations for contractor personnel to include Tier 5 for Top Secret/SCI, and Tier 3 for Secret and Confidential clearances. To manage risk in enterprise insider threat mitigation, the PSI-I program budget funds Continuous Vetting (CV) on an estimated 1.2 million cleared contractors using CV related investigative products and services, to include time-based checks and alert resolution. To manage risk in enterprise insider threat mitigation, the PSI-I program budget funds Continuous Vetting (CV) on an estimated 1.2 million cleared contractors using CV related investigative products and services, to include time-based checks and alert resolution. The Vetting and Risk Operations (VRO) has developed metrics below to evaluate the number of personnel serviced by their multiple lines of business when executing the PSI-I budget.

	FY 2018	FY 2019	FY 2020	FY 2021	FY 2022	FY 2023
Personnel Serviced Cleared Contractors	839,500	847,650	950,657	1,064,895	1,144,849	1,251,319
e-QIPs Processed	139,246	226,601	188,499	163,713	165,458	187,697
Interims Issued	79,569	100,662	86,760	96,847	101,801	103,233
Periodic Review/Continuous Vetting	85,399	88,350	74,904	70,737	65,903	87,189

IV. Performance Criteria and Evaluation Summary: (Cont.)

C. International Military Service (IMS) Performance Measure: The IMS budget is based on total number of forecasted screenings, by case type, and the DCSA rate. The Defense Security Cooperation Agency administers requests for the IMS. The DCSA has developed metrics below to evaluate the number of the IMS when executing the IMS budget.

	FY 2023	FY 2024
Initial	21,777	22,846
Continuous Review	67,832	72,584

V. Personnel Summary:

	FY 2022	FY 2023	FY 2024	Change FY 2022/ FY 2023	Change FY 2023/ FY 2024
Civilian End Strength (Total)	**1,651**	**2,174**	**2,121**	**523**	**-53**
U.S. Direct Hire	1,651	2,174	2,121	523	-53
Total Direct Hire	**1,651**	**2,174**	**2,121**	**523**	**-53**
Civilian FTEs (Total)	**1,839**	**1,950**	**1,966**	**111**	**16**
U.S. Direct Hire	1,839	1,950	1,966	111	16
Total Direct Hire	**1,839**	**1,950**	**1,966**	**111**	**16**
Average Annual Civilian Salary ($ in thousands)	**157.1**	**150.4**	**170.0**	**-6.6**	**19.5**
Contractor FTEs (Total)	**312**	**312**	**312**	**0**	**0**

Personnel Summary Explanations:

*Note: FY 2022 End Strength Total

DCSA management decision to transfer personnel from the appropriated fund billets to DCSA Wide Working Capital Fund (DWCF) billets in Q4 FY 2022 to increase DWCF personnel supporting the Agency mission. The transfer resulted in a reduction to the FY 2022 End Strength.

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

			Change from FY 2022 to FY 2023			Change from FY 2023 to FY 2024		
		FY 2022 Program	Price Growth	Program Growth	FY 2023 Program	Price Growth	Program Growth	FY 2024 Program
101	EXEC, GEN'L & SPEC SCHEDS	288,229	11,904	-7,379	292,754	14,720	26,104	333,578
121	PCS BENEFITS	600	25	-26	599	30	-29	600
0199	**TOTAL CIVILIAN PERSONNEL COMPENSATION**	**288,829**	**11,929**	**-7,405**	**293,353**	**14,750**	**26,075**	**334,178**
308	TRAVEL OF PERSONS	6,722	141	-4,799	2,064	45	58	2,167
0399	**TOTAL TRAVEL**	**6,722**	**141**	**-4,799**	**2,064**	**45**	**58**	**2,167**
683	PURCHASES FROM DWCF DEFENSE COUNTERINTELLIGENCE & SECURITY AGENCY	328,298	0	-6,113	322,185	25,775	5,390	353,350
696	DFAS FINANCIAL OPERATION (OTHER DEFENSE AGENCIES)	1,625	89	93	1,807	14	-14	1,807
0699	**TOTAL OTHER FUND PURCHASES**	**329,923**	**89**	**-6,020**	**323,992**	**25,789**	**5,376**	**355,157**
771	COMMERCIAL TRANSPORT	590	12		602	12	1	615
0799	**TOTAL TRANSPORTATION**	**590**	**12**	**0**	**602**	**12**	**1**	**615**
912	RENTAL PAYMENTS TO GSA (SLUC)	1,380	29	-1	1,408	31	-3	1,436
913	PURCHASED UTILITIES (NON-FUND)	11	0		11	0		11
914	PURCHASED COMMUNICATIONS (NON-FUND)	8,425	177	-8	8,594	189	-14	8,769
915	RENTS (NON-GSA)	4,525	95	-4	4,616	102	-10	4,708
917	POSTAL SERVICES (U.S.P.S)	31	1	-1	31	1	-1	31
920	SUPPLIES & MATERIALS (NON-FUND)	7,028	148	811	7,987	176	-959	7,204
921	PRINTING & REPRODUCTION	298	6		304	7	-2	309
922	EQUIPMENT MAINTENANCE BY CONTRACT	43,909	922	6,657	51,488	1,133	260	52,881
923	FACILITIES SUST, REST, & MOD BY CONTRACT	2,308	48	-2	2,354	52	-46	2,360
925	EQUIPMENT PURCHASES (NON-FUND)	10,680	224	-296	10,608	233	-121	10,720
932	MGT PROF SUPPORT SVCS	145,078	3,047	43,966	192,091	4,226	-15,116	181,201
934	ENGINEERING & TECH SVCS	908	19	6	933	21	-9	945
987	OTHER INTRA-GOVT PURCH	83,699	1,758	5,345	90,802	1,998	-1,392	91,408
989	OTHER SERVICES	6,845	144	-94	6,895	152	976	8,023

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

			Change from FY 2022 to FY 2023			Change from FY 2023 to FY 2024		
		FY 2022 Program	Price Growth	Program Growth	FY 2023 Program	Price Growth	Program Growth	FY 2024 Program
0999	TOTAL OTHER PURCHASES	315,125	6,618	56,379	378,122	8,321	-16,437	370,006
9999	GRAND TOTAL	941,189	18,789	38,155	998,133	48,917	15,073	1,062,123