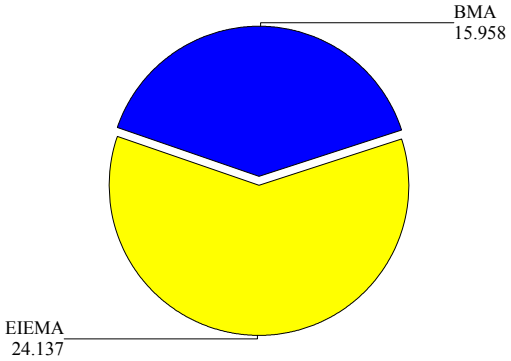
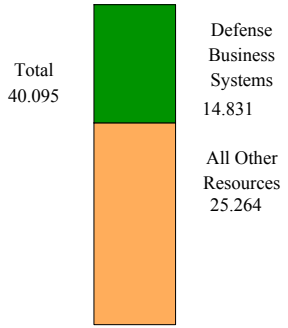
Department of Defense
Fiscal Year (FY) 2016 President's Budget Request
Defense Security Service Overview

Mission Area



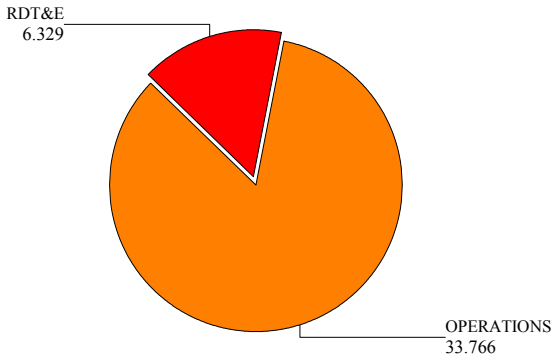
FY 2016 ($M)

Business System Breakout



FY 2016 ($M)

Appropriation



FY 2016 ($M)

FY15 to FY16 Comparison ($M)

	FY2015	Inflation	Program Change	FY2016
PB FY2016:	36.060	0.613	3.422	40.095

See Significant Changes section for explanation of Progam Change

FY15PB/FY16PB Comparison ($M)

	FY2015	FY2016	Delta
PB FY2015:	42.125	34.626	-7.499
PB FY2016:	36.060	40.095	
Delta:	-6.065	5.469	

See Significant Changes section for explanation

Page left intentionally blank

Executive Summary

The Defense Security Service (DSS) supports national security and the war fighter missions, secures the nation's technological base, and oversees the protection of US and foreign classified information within the industry. This mission is accomplished by: Clearing industrial facilities; Accrediting cleared industry information systems; Delivering security education training; and Providing information technology services that support the industrial security missions of the Department of Defense (DoD) and its partnering agencies. In addition, on 12 December 2014, the Under Secretary of Defense directed DSS to incubate the DoD Insider Threat Management and Analysis Center (DITMAC) reported in the classified volume.

Key DSS strategic goals are to enable successful protection of national assets and interests on behalf of DoD and to consistently meet expanding industrial security mission requirements by providing centralized, secure access to information resources. Key strategic objectives to support these goals include: The development, enhancement, and provision of security and information sharing tools and services; Building strategic and tactical partnerships with customers; Recognizing, communicating, and managing risks; and Developing effective and efficient information technology architecture to support critical processes.

DSS Information Technology (IT) systems provide service critical to the major DSS mission areas: Industrial Security Oversight and Security Education. DSS performs these critical functions through operation of its Enterprise Security Systems (ESS). DSS manages the ESS to provide an effective, real-time, security support capability for the Military Departments, DoD Agencies, the National Industrial Security Program (NISP), and other Federal Agencies. In compliance with the DoD Enterprise Architecture Framework, ESS is the unified offering of security mission systems which facilitate and automate improved national investigative and adjudicative standards, streamline security processes, and increase DoD community collaboration.

ESS is the secure, authoritative source for management, storage, and timely dissemination of industrial security and security training information with flexibility and support structure for future DoD security process growth. ESS is comprised of the Industrial Security Facilities Database (ISFD), the Security Training, Education and Professionalization Portal (STEPP), the NISP Contract Classification System (NCCS), the Office of the Designated Approving Authority (ODAA) Business Management System (OBMS), and the National Industrial Security System (NISS).

ESS strengthens agency performance through enhanced automation and oversight of the industrial security facility clearance process, improvement of the DSS ODAA Industrial Security accreditation process, and effective delivery of security education and awareness training.

Significant Changes (Explanations of Change by Appropriation Group. Dollars are in thousands unless otherwise noted.)

OPERATIONS

Horizontal Change (Delta 894)

Horizontal change of $1.444M ($0.894M with Inflation) to continue portfolio maintenance.

Vertical Change (Delta 2,684)

Vertical change of $2.684M due to the planned merger of ISFD into NISS, which requires the decoupling of the Electronic Facility Clearance System (eFCL) from ISFD and establishes eFCL as a separate resource reporting entity. In addition, funding allocated for Defense Information System Network (DISN) services reflected in this budget submission establishes DSS as a Contributing Component in compliance with IT service reporting requirements.

RDT&E

Horizontal Change (Delta 2,528)
Horizontal change of $2.591M ($2.528M with Inflation) due to the rephrasing of funding to begin development of NISS Increment-1 for consolidation of ISFD and eFCL functions.

Vertical Change (Delta 2,785)
Vertical change of $2.785M to continue development of NISS Increment-1 for consolidation of ISFD and eFCL functions.

Major Accomplishments

In compliance with the Deputy Secretary of Defense Memorandum, "Defense Security Service Future Options Study Recommendations, January 15, 2009," and the DSS mission to offer IT system services critical to its major mission areas: Industrial Security Oversight and Security Education; DSS has accomplished the following activities aligned to Agency goals articulated in the Fiscal Year (FY) 2015 Organizational Execution Plan (OEP):

• The DSS Office of the Designated Approving Authority (ODAA) Business Management System (OBMS) is the Defense Security Service (DSS) system of record for the management of the information assurance accreditation of Contractor Information Systems under the National Industrial Security Program (NISPOM). Major accomplishments for OBMS are: Successfully deployed Identity and Access Management module; Successfully deployed latest Production Release 2.1; and, Deployed a solution to meet customer-reporting requirements. These accomplishments streamlined process and increased efficiency for certifications and accreditations of cleared contractor information systems.

• The National Industrial Security Program (NISP) Contract Classification System (NCCS) establishes the centralized repository mechanism with standardized procedures in managing the security classification specification data. Major accomplishments for NCCS are: Successfully deployed Production Release 5.7 to establish Invoices Receipt Acceptance and Property Transfer (iRAPT (formerly Wide Area Workflow (WAWF)) system interoperability; and, Initiated Release 5.8 to incorporate iRAPT workflow enhancement requirements. These accomplishments improve the effective submission of the DD Form 254 for contract security classification specifications.

• The National Industrial Security System (NISS) is the next generation functional replacement for the Industrial Security Facility Database system. Major accomplishments for NISS are: Completed the Market Analysis for the NISS Acquisition; Completed essential activities for Pre-Milestone A approval of the Business Capability Lifecycle (BCL); Received Milestone Decision Authority (MDA) approval to proceed with NISS development; and, Completed acquisition preparation for development contract award on-schedule for Fiscal Year (FY) 2015. These accomplishments facilitate the timely development of NISS and will provide a centralized web-based platform for NISP personnel to manage the industrial security facility clearance process; therefore, achieving material and non-material efficiencies for the NISP.

• The Industrial Security Facility Database (ISFD) is a centralized web-based platform for all National Industrial Security Program personnel to manage the industrial security facility clearance process from request to approval or rejection, and storage of all investigative data associated with that process. Major accomplishments for ISFD are: Completed assessment of ISFD application code with automated and manual checks; and, Planning of legacy ISFD incorporation into the NISS. These accomplishments facilitate the next stage evolution of the NISP support systems.

• The Security Training, Education and Professionalization Portal (STEPP) is a web-based application accessible to DoD security professionals, DoD contractors, Federal agencies, and selected foreign governments for security education and awareness. Major accomplishments for STEPP are: Automated Security Professional Certification business processes with a global commercial testing provider to further the Department of Defense's (DoD) initiative to professionalize the security workforce; Automated the exchange of

Security Professional high stakes certification data from the test centers, STEPP, and the Defense Workforce Certification (DWC) system, while maintaining data integrity and legal defensibility for the DoD Security Professional Workforce; and, Integrated STEPP with our Common Access Card (CAC) Portal, allowing students to access STEPP via CAC and PIV. These accomplishments increase the effective delivery of security education and awareness training.

Major Planned Activities

The DSS Office of the Chief Information Officer (OCIO) will focus on pre-planned product improvements to the ESS applications, researching and improving assured information sharing, better posturing systems and networks against vulnerabilities, ensuring self-defense of systems and networks, and safeguarding data at all stages. These enhancements are necessary for the DSS OCIO to increase efficiency, capabilities, and security of ESS Applications.

In keeping with efficient and effective capture of emerging industrial security system requirements, compliance with Federal/DoD mandates, and performance improvements, DSS will implement the following ESS system enhancements and major activities in FY15 and FY16:

• The DSS Office of the Designated Approving Authority (ODAA) Business Management System (OBMS): Continued development of next release and migration planning to implement a DSS Enterprise Service Oriented Architecture (SOA) solution; Continued customer enhancement planning and post deployment support; and, Process development and planning for transition to sustainment.

• The National Industrial Security Program (NISP) Contract Classification System (NCCS): Complete Release 5.8 planning, testing, and deployment for iRAPT workflow enhancement requirements; and, Initiate planning and requirements gathering for next release.

• The National Industrial Security System (NISS): Award NISS development contract; Begin Development of NISS Increment-1 for consolidation of ISFD and Electronic Facility Clearance System (eFCL) functions; and, Implemented BPR future state workflows, dashboard, notification and native mobile capabilities.

• The Industrial Security Facility Database (ISFD): Initiate code transition activities required for ISFD merger with NISS; and, Complete Lightweight Directory Access Protocol (LDAP) and Discoverer (OBIEE) Upgrades.

• The Security Training, Education and Professionalization Portal (STEPP): Upgrade the STEPP LMS software and improve contingency operations capabilities of the platform; Automate data exchanges with the Defense Manpower Data Center (DMDC) and the DCPDS system to improve data accuracy, save on manual rework, and validation; and, Automate Security Professional Certification eligibility determination, grouping, processing, resubmission, assignment of certificate numbers, and reporting of conferred candidates.

Infrastructure Modernization/Joint Information Environment (JIE)

The following six areas represent DSS JIE participation in response to policy and guidance:

1. Application migration to the Core Data Centers: Where evidenced by sound business investment decisions through the agency governance processes, DSS will continue to look at application (e.g. systems) migration to consolidated data centers or cloud infrastructure (MilCloud or commercial). In FY14, The OCIO established the IT Strategy Committee, a board designed to assist the agency with making sound information technology investment decisions. In FY15/16, the OCIO will continue to evolve the committee, further integrating it with the agency governance framework and align the IT strategy to the agency mission.

2. Ensure Internet Facing Applications meet DISA DMZ STIG requirements: All DSS systems and web-based applications already comply with DISA STIG requirements. These applications will continue to evolve to maintain pace with STIG updates and changes as risks evolve and are mitigated through the DoD Risk Management Framework (RMF). In FY15/16, DSS will continue to implement STIG requirements and require the same level of adherence of our data center and cloud service providers.

3. SIPR PKI implementation for servers and workstations: In FY15/16, DSS will complete SIPR PKI implementation.

4. Migration to DISA Enterprise Email: In FY15/16, DSS will complete SIPR and NIPR email migration.

5. Leverage DISA Enterprise Directory Service (EDS) for populating directory attributes: the DoD CIO memorandum titled "Mandating Use of the DoD Enterprise Directory Services (EDS)" mandates the use of EDS, and requires DoD Components to: 1) Populate and maintain authoritative organizational and contact data in DMDC's authoritative data source; 2) Use EDS provisioning and synchronization services to populate directories with enterprise attributes; and, 3) Use EDS provisioning and synchronization services to populate all Global Address Lists. In FY14, The National Industrial Security Program (NISP) Central Access Information Security System (NCAISS) uses the Authentication Gateway Service (AGS) to validate DoD CACs. However, NCIASS goes a step further, implementing PKI-PKE interoperability by supporting DOD-approved External Certificate Authority (ECA). In FY15/16, DSS will continue to provide NCAISS services for DSS systems that support this NISP mission.

6. Enterprise Software Licensing through DoD: DSS currently employs, and will continue to implement, an acquisitions strategy that procures enterprise licensing across the department to reduce cost.

Core Network Infrastructure

In addition to the DSS operations and maintenance contracts in place for core network infrastructure support, the OCIO has focused on the effective delivery of SIPR access to its Field Offices (SIPR to the Field), and Multiprotocol Label Switching (MPLS) implementation.

The SIPR to the Field activity brings cost and time savings to the Agency through:
• Reduction in cost and maintenance by SIPRNet traversal on NIPRNet communication lines, which increases network speed on current NIPR and SIPR networks with the installation of DS3 network lines. Using this method of SIPRNet access cuts network operation and maintenance and its associated peripheral devices.
• Secret Open Storage allows for CounterIntelligence analysts to streamline storage and presentation of classified data, as well as allowing SIPR desktops to stay online 24/7. Reduction in operating costs and user downtime can be shown using historical Remedy data. The 3-5 day repair of a TALON laptop is now down to an over the phone fix for SIPR desktop computers.
• 24/7 connectivity allows for after-business hour patching, quick access to user drives, remote password resets, and increased security brought through Alarm system and Monitoring services for/of remote sites.
Furthermore, this solution gives the Field Offices a more stable operating environment, which has increased Field productivity as a whole. Moving forward, the Small Office Solution will allow OCIO to deploy systems quickly and with lower build out costs for smaller resident Field offices. Also, the Unified Communications project currently underway will continue to improve connectivity to all Field sites.

The DSS MPLS project is designed to bring voice, video and data services into a single network also known as Unified Communications. DSS is procuring new circuits that will allow for Quality of Service (QoS) and traffic priority that we do not have with our current infrastructure. The new circuits will be providing more bandwidth at a lower cost, it is expected to save upwards of $800,000 per year (roughly 28% in savings). At this time, DSS has deployed MPLS circuits at 7 of 48 field offices as well as at DSS

headquarters.

Joint Regional Security Stack (JRSS)

Not applicable for DSS at this time.

Data Center and Server Consolidation

DSS has accomplished the intent of this initiative by collapsing all data services and data centers into shared DoD facilities. As part of the Quantico/Russell Knox Facility, DSS is leveraging the third largest joint DoD Data Center for all mission operations. Additionally, for disaster recovery capabilities, DSS has partnered with the Defense Manpower Data Center (DMDC) to utilize their data center in a joint use environment. DSS expects to increase consolidation efforts with DMDC in the future and further maximize the return on investment in the shared facility.

Cloud Computing

DSS has not leveraged the cloud for the Business systems currently in production; however, DSS is evaluating cloud alternatives for the new development of the NISS by the end of the Fiscal Year 2015.

Defense Business Systems

DSS identifies business systems that meet criteria outlined in the 2005 National Defense Authorization Act (NDAA) and DoD IT Defense Business Systems Investment Review Process Guidance. Currently, five (5) DSS business systems undergo Investment Review Board (IRB) and the Defense Business Systems Management Committee (DBSMC) review. The DSS Business System portfolio is managed by the DSS Chief Information Officer (CIO) and currently consists of the following systems:

• The Industrial Security Facility Database (ISFD) provides a centralized, web-based platform for NISP personnel to manage the industrial security facility clearance process, from request to approval (or rejection) and store all investigative data associated with that process. ISFD provides a means for users to submit, update, search, and view facility verification requests. ISFD retains a list of cleared facilities and companies and provides users a nationwide perspective on NISP related facilities, as well as facilities under DSS oversight in the DoD conventional Arms, Ammunition, and Explosives (AA&E) program.

• The National Industrial Security System (NISS; formerly known as the Field Operations System (FOS)) is the next generation functional replacement for the ISFD system. NISS will provide a centralized web-based platform for NISP personnel to manage the industrial security facility clearance process, from request to approval (or rejection) and storage of all associated investigative data; and, to provide a means for users to submit, update, search, and view facility verification requests. NISS will contain a list of cleared facilities and companies to provide users with a nationwide perspective on NISP related facilities, as well as facilities under DSS oversight in the DoD AA&E program.

• The DSS ODAA Business Management System (OBMS) is the DSS system of record for the management of the information assurance accreditation of Contractor Information Systems under the NISP. The OBMS provides a centralized, flexible data management and reporting support system across the industry, allowing access from multiple sites. The information contained within OBMS will improve accreditation timeliness and accuracy and improved reporting capabilities to answer congressional staff inquiries.

• The NISP Contract Classification System (NCCS) is a robust, centralized repository mechanism with standardized procedures in managing the security classification specification data of all classified contracts for the Department of Defense (DoD) and Federal Agencies. NCCS is a web-based system that automates the DD Form 254 for contract security classification specification submission; provides submitter with intuitive form instructions, drop-down selections, and linkage to relevant contract information

for completing the form; and provides user access control, query/search, notification, tracking, and reporting capabilities for accountability of all contract security classification specifications.

• The Security Training, Education and Professionalization Portal (STEPP) system is a customized, Commercial Off-the-Shelf (COTS) Learning Management System (LMS) and Learning Content Management System (LCMS). Other components of STEPP include: Content Development Server (DLSTK), File and Course Hosting (CDSWS), exam application (Questionmark), flash content (Streaming Server).This system offers a web-based application accessible to DoD security professionals, DoD contractors, employees of other Federal agencies, and selected foreign governments. STEPP provides the DSS Academy with a means to grant security education and training curricula, access awareness products, and promote professional development services that are relevant and responsive to the needs of the security professionals, military personnel who perform security functions, and other DoD and contractor personnel requiring security training.

Consolidation of Software Purchases

DSS is leveraging the DoD Enterprise Software Initiative (ESI) for purchase/utilization of multiple products. In addition to the DoD-wide Antivirus and HBSS suite of tools, DSS uses the ESI for purchase of CAC middleware tools. At an agency specific level, DSS has pursued an enterprise agreement with select vendors to streamline purchases and lower costs for acquisition of desktop and server products. DSS is also consolidating existing contracts to reduce contract overhead and improve continuity of service, support, and maintenance contracts.

Consolidation of Hardware Purchases

DSS is leveraging a variety of hardware purchasing agreements available to DoD and other Federal agencies. Examples of Government Wide Acquisition Contracts (GWACs) and Indefinite Deliver Indefinite Quantities (IDIQs) used by DSS are General Services Administration (GSA) Schedule 70, Solutions for Enterprise Wide Procurement (SEWP), ENCORE II, NETWorx, and GSA Advantage. DSS expects to further leverage volume purchasing and enterprise buying solutions in the future and will reduce overhead in the area of contracting and service/support of existing IT assets by using consolidated purchasing vehicles. Additionally, internal DSS activities include collapsing hardware maintenance contracts into single contracts that leverage volume pricing and reduced complexity in coordinating service by hardware vendors. In the past year, DSS has reduced 13 network equipment support contracts into a single contract. Additional consolidation is underway on an estimated 30 hardware support agreements.

Information Technology Budget Exhibit Resource Summary by Investment (IT-1)

	---------- Dollars in Thousands ----------		
	FY2014	*FY2015*	*FY2016*
RESOURCE SUMMARY:	$33,638	$36,060	$40,095

007-000000595 - DEFENSE INFORMATION SYSTEM NETWORK (DISN) — Major

GIG Category: COMMUNICATIONS AND COMPUTING INFRASTRUCTURE

Operations

Appropriation	*Budget Activity*	*Budget Line Item*	*FY2014*	*FY2015*	*FY2016*
O&M, DW	BA 04 ADMIN & SRVWD ACTIVITIES	DEFENSE SECURITY SERVICE	0	1,954	2,022
		Investment Resource Summary:	0	1,954	2,022

007-000001513 - ODAA Business Management System (OBMS) — Non-Major

GIG Category: FUNCTIONAL AREA APPLICATIONS

Operations

Appropriation	*Budget Activity*	*Budget Line Item*	*FY2014*	*FY2015*	*FY2016*
O&M, DW	BA 04 ADMIN & SRVWD ACTIVITIES	DEFENSE SECURITY SERVICE	913	940	968

RDT&E

Appropriation	*Budget Activity*	*Program Element*	*FY2014*	*FY2015*	*FY2016*
RDT&E, DW	BA 07 OPERATIONAL SYSTEMS DEVELOPMENT	0604130V ENTERPRISE SECURITY SYSTEM (ESS)	1,854	320	0
		Investment Resource Summary:	2,767	1,260	968

007-000001794 - STANDARD PROCUREMENT SYSTEM (SPS) — Major

GIG Category: FUNCTIONAL AREA APPLICATIONS

Operations

Appropriation	*Budget Activity*	*Budget Line Item*	*FY2014*	*FY2015*	*FY2016*
O&M, DW	BA 04 ADMIN & SRVWD ACTIVITIES	DEFENSE SECURITY SERVICE	311	316	321
		Investment Resource Summary:	311	316	321

Information Technology Budget Exhibit Resource Summary by Investment (IT-1)

007-000002236 - Networks & Infrastructure (N&I)

Non-Major

GIG Category: COMMUNICATIONS AND COMPUTING INFRASTRUCTURE

Operations

Appropriation	Budget Activity	Budget Line Item	FY2014	FY2015	FY2016
			---------- Dollars in Thousands ----------		
O&M, DW	BA 04 ADMIN & SRVWD ACTIVITIES	DEFENSE SECURITY SERVICE	20,025	21,465	22,115
		Investment Resource Summary:	20,025	21,465	22,115

007-000002854 - Industrial Security Facility Database (ISFD)

Non-Major

GIG Category: FUNCTIONAL AREA APPLICATIONS

Operations

Appropriation	Budget Activity	Budget Line Item	FY2014	FY2015	FY2016
			---------- Dollars in Thousands ----------		
O&M, DW	BA 04 ADMIN & SRVWD ACTIVITIES	DEFENSE SECURITY SERVICE	2,790	1,413	640

RDT&E

Appropriation	Budget Activity	Program Element	FY2014	FY2015	FY2016
			---------- Dollars in Thousands ----------		
RDT&E, DW	BA 07 OPERATIONAL SYSTEMS DEVELOPMENT	0604130V ENTERPRISE SECURITY SYSTEM (ESS)	479	0	0
		Investment Resource Summary:	3,269	1,413	640

007-000002902 - DSS Enterprise Portal (Portal)

Non-Major

GIG Category: FUNCTIONAL AREA APPLICATIONS

Operations

Appropriation	Budget Activity	Budget Line Item	FY2014	FY2015	FY2016
			---------- Dollars in Thousands ----------		
O&M, DW	BA 04 ADMIN & SRVWD ACTIVITIES	DEFENSE SECURITY SERVICE	204	481	292
		Investment Resource Summary:	204	481	292

Information Technology Budget Exhibit Resource Summary by Investment (IT-1)

007-000002905 - Security Training, Education and Professionalization Portal (STEPP) — Non-Major

GIG Category: FUNCTIONAL AREA APPLICATIONS

Operations

Appropriation	Budget Activity	Budget Line Item	FY2014	FY2015	FY2016
			---------- Dollars in Thousands ----------		
O&M, DW	BA 04 ADMIN & SRVWD ACTIVITIES	DEFENSE SECURITY SERVICE	1,464	1,929	1,988
		Investment Resource Summary:	1,464	1,929	1,988

007-000004700 - National Industrial Security System (NISS) — Non-Major

GIG Category: FUNCTIONAL AREA APPLICATIONS

Operations

Appropriation	Budget Activity	Budget Line Item	FY2014	FY2015	FY2016
			---------- Dollars in Thousands ----------		
O&M, DW	BA 04 ADMIN & SRVWD ACTIVITIES	DEFENSE SECURITY SERVICE	1,728	1,972	3,366

RDT&E

Appropriation	Budget Activity	Program Element	FY2014	FY2015	FY2016
			---------- Dollars in Thousands ----------		
RDT&E, DW	BA 07 OPERATIONAL SYSTEMS DEVELOPMENT	0604130V ENTERPRISE SECURITY SYSTEM (ESS)	2,613	3,147	5,406
		Investment Resource Summary:	4,341	5,119	8,772

007-000004705 - Open Source Corporate Management Information System (OSCMIS) — Non-Major

GIG Category: FUNCTIONAL AREA APPLICATIONS

Operations

Appropriation	Budget Activity	Budget Line Item	FY2014	FY2015	FY2016
			---------- Dollars in Thousands ----------		
O&M, DW	BA 04 ADMIN & SRVWD ACTIVITIES	DEFENSE SECURITY SERVICE	1	0	0
		Investment Resource Summary:	1	0	0

Information Technology Budget Exhibit Resource Summary by Investment (IT-1)

007-000006312 - DEFENSE TRAVEL SYSTEM (DTS) — Major

GIG Category: FUNCTIONAL AREA APPLICATIONS

Operations

Appropriation	Budget Activity	Budget Line Item	FY2014	FY2015	FY2016
			---------- Dollars in Thousands ----------		
O&M, DW	BA 04 ADMIN & SRVWD ACTIVITIES	DEFENSE SECURITY SERVICE	0	41	42
		Investment Resource Summary:	0	41	42

007-000100066 - NISP Contract Classification System (NCCS) — Non-Major

GIG Category: FUNCTIONAL AREA APPLICATIONS

Operations

Appropriation	Budget Activity	Budget Line Item	FY2014	FY2015	FY2016
			---------- Dollars in Thousands ----------		
O&M, DW	BA 04 ADMIN & SRVWD ACTIVITIES	DEFENSE SECURITY SERVICE	0	1,160	1,350

RDT&E

Appropriation	Budget Activity	Program Element	FY2014	FY2015	FY2016
			---------- Dollars in Thousands ----------		
RDT&E, DW	BA 07 OPERATIONAL SYSTEMS DEVELOPMENT	0604130V ENTERPRISE SECURITY SYSTEM (ESS)	1,086	100	750
		Investment Resource Summary:	1,086	1,260	2,100

007-000100481 - Electronic Facility Clearance Services (eFCL) — Non-Major

GIG Category: FUNCTIONAL AREA APPLICATIONS

Operations

Appropriation	Budget Activity	Budget Line Item	FY2014	FY2015	FY2016
			---------- Dollars in Thousands ----------		
O&M, DW	BA 04 ADMIN & SRVWD ACTIVITIES	DEFENSE SECURITY SERVICE	0	651	662

RDT&E

Appropriation	Budget Activity	Program Element	FY2014	FY2015	FY2016
			---------- Dollars in Thousands ----------		
RDT&E, DW	BA 07 OPERATIONAL SYSTEMS DEVELOPMENT	0604130V ENTERPRISE SECURITY SYSTEM (ESS)	170	171	173
		Investment Resource Summary:	170	822	835