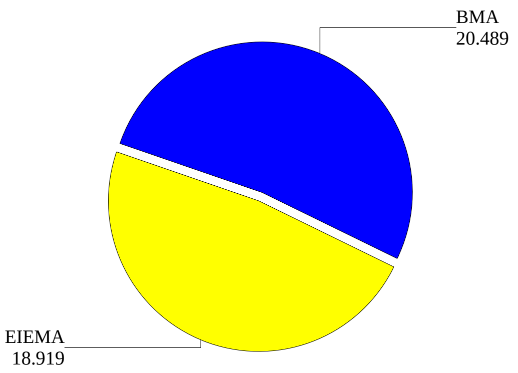
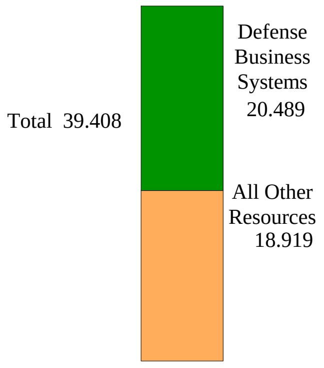
Department of Defense
Fiscal Year (FY) 2013 IT President's Budget Request
Defense Security Service Overview

Mission Area



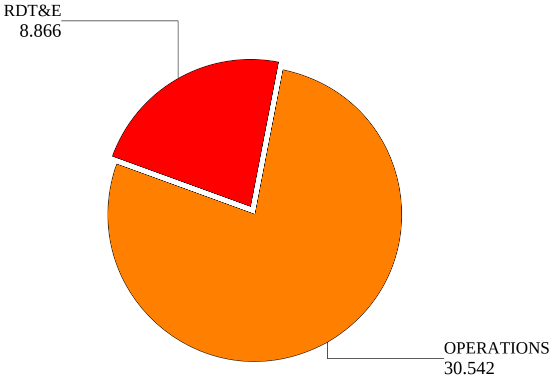
FY 2013 ($M)

Business System Breakout



FY 2013 ($M)

Appropriation



FY 2013 ($M)

FY12 to FY13 Comparision ($M)	FY2012	FY2013	Delta
PB FY2013:	32.205	39.408	7.203

Explanation:

The increase is to realign previously unreported O&M funding in support of the IT infrastructure to sustain and operate deployed applications, and to continue RDT&E system development activities.

FY12/FY13PB Comparision ($M)	FY2012	FY2013	Delta
PB FY2012:	29.369	28.772	-0.597
PB FY2013:	32.205	39.408	7.203
Delta:	2.836	10.636	

Explanation:

Increases due to realignment of previously unreported O&M funding, and funding adjustments directed in Fiscal Guidance. In addition, $ 0.708 M of Information Assurance Activities are detailed in the DoD IT Budget Classified Annex.

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.

DSS manages the Enterprise Security System (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.

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 ESS systems.

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 DSS Enterprise Portal, and the Security Training, Education and Professionalization Portal (STEPP) (formerly the Electronic Network Registration and Online Learning (ENROL) system).

ESS strengthens agency performance through enhanced automation and oversight of the industrial security facility clearance process and improvement of the DSS Office of the Designated Approving Authority (ODAA) Industrial Security accreditation process.

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.

Significant Changes

DSS has successfully completed relocation of its headquarters from Alexandria, Virginia to Quantico, Virginia as mandated by the Base Realignment and Closure (BRAC) initiative. This move was completed flawlessly, without impact to the greater DoD stakeholder.

Business Defense 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, seven (7) 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 Field Operations System (FOS) is the next generation functional replacement for the ISFD system. FOS 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. FOS 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 Open Source Corporate Management Information System (OSCMIS) is an automated, web-enabled, enterprise-wide management information system to streamline management of DSS Manpower, Human Resource, Security, Training, and Personnel Management processes and data. The most significant benefits of OSCMIS are: Executive reporting capability required for effective organizational decision-making; Increased accuracy and management of Continuity of Operations Planning (COOP) related data and notifications; Improved Employee Training and Staff Development Plan management; Enhanced badging and credentialing oversight capabilities; and, Streamlined control of Manpower and Billet management activities.

• DSS Identity and Access Management (IdM) service controls ESS User service-accessibility through single sign-on authentication. The web-based IdM enterprise portal is the Public Key Infrastructure (PKI) compliant point-of-entry to the suite of services offered by the ESS. Through sign-on authentication, user service-level permissions are verified and authorized services are offered to the ESS User accordingly.

• The DSS Enterprise Portal (Portal) provides one-stop access to the services, business applications, and information assets of the DSS enterprise. Individuals seeking knowledge of the DSS enterprise can globally access agency information through the internet at “www.dss.mil”. DoD customers, with proper account credentials, can use the portal as a central point of access to DSS business applications and services. Customer efficiency and productivity are increased by instant accessibility to DSS business applications, information, news, and scheduled system outage postings. Through the portal, advanced collaboration, process orchestration, user experience management, and composite application access is consolidated from multiple sources onto a single public-facing interface.

• 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.

Information Assurance Activities

DSS Information Assurance (IA) is currently realigning the goals and objectives of the network security into a holistic framework that supports the continuous assessment and defense of the DSS enclave. This process is based on a three pillar approach of People, Process and Technology. The pillars are link via people who perform defined processes using approved technology and tools.

People: IA is reviewing and updating the skills, training and certification levels of all IA personnel. Each position is being reviewed to identify the skills, training and certifications required to support the function. Funding is then being allocated to bring the individual in the position to a level of IA competency based on DoD 8570, Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), and DSS policies. Additionally, Continuous Education Credits are being maintained through the purchase of a library of required reading dealing with security, policy and compliance as well as other training courses that maintain or improve skills.

Process: The IA is broken down into three service areas: Policy and Training, Certification and Engineering, and Computer Network Defense. Each service area is subdivided into core services. Each core service is supported through IA's Security Policy Architecture (SPA) consisting of Regulations, Guidelines and Standard Operating Procedures. The SPA provides the process flow to achieve any core function in which include high level cost can be extrapolated for travel, equipment and specialized training. Programs such as :

- Identity and access management, Public Key Infrastructure/Key Management Infrastructure (PKI/KMI), and PKI-enabled applications which allows IA to support the Common Access Card (CAC) login, Alternate Tokens and SIPRNET token programs. IA is purchasing equipment and card stock to support this initiative.

- Certification an Accreditation handbook which is designed to provide a standard process used by DSS to Certify and Accredit network systems. It expands DSS compliance with DoD Instruction 8500.2, the Global Information Grid - Information Assurance (GIG-IA) Architecture and Secure Configuration Compliance Validation/Secure Configuration Remediation Initiatives (SCCVI/SCRI) programs. Funding is allocated for travel, equipment and tools used in the validation process to ensure compliance.

- Information Systems Security Engineering of Systems in the Systems Development Lifecycle process, Configuration and Asset Management and feeds the Certification and Accreditation (C&A) process. High level training in the Information Systems Security Engineering Professional (ISSEP) and Project Management Professional (PMP) certifications.

- Developing and deploying a technical Insider Threat and Detection process used to detect and deter insider threat activity. Funding is used to purchase tools and services the feed the technical process of insider threat detection.

- Forensics investigations including: Computer compromise, Insider Threat, Malicious Code Detection/Eradication, Auditing, and command level investigations. Funds are made available to purchase tools and training to achieve this vital service.

- Technology: Technology used by IA, is key to a successful, compliant, monitored and useable computer environment. IA is current conducting technical refresh on key

Network Security Monitoring tools, services and contracts. IA has also conducted gap analysis in areas such as forensics, wireless scanning, penetration testing and Network Security monitoring. Funding is being used to purchase technologies to automate, improve accuracy, increase monitoring range and develop a strong security monitoring and continuous monitoring program.

IA is also expending time in researching future technologies to use in the creation of a “Compliant Computer Environment” which leverages technology in compliance monitoring, penetration testing and network access control to ensure all systems are security compliant.

Major Accomplisments

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:

- Implemented the ISFD Metrics Release system enhancement, which provides additional metric reporting and processing capability to ISFD for the tracking and reporting of information pertaining to facilities under DSS auspices.

- Accomplished the Initial Operational Capability (IOC) for OBMS, necessary to support the DSS national security mission by providing security oversight and protection of classified information and technologies in the hands of the Defense Industrial Base (DIB) under the NISP.

- Initiated the Electronic Facility Clearance System (eFCL) system interface between ISFD and the Department of Energy (DoE) eFCL. DSS has adopted eFCL as the tool to collect and manage security information on facilities with Foreign Ownership, Control, or Influence (FOCI). eFCL provides the ability to collect and manage security information relating to a cleared facility, from the initial processing of the facility clearance, the record decision pertaining to facility clearance request, to include FOCI information, as well as decommissioning the facility clearance, and capturing the DSS oversight activities. eFCL provides a means for users to submit, update, search, and view facility verification requests.

- Entered the Business Capability Definition phase for FOS to modernize current ISFD capabilities in support of the growing DSS industrial security mission.

- Completed significant changes in the user interface of the ENROL Learning Management system version 8.2 release. In conjunction with these changes, the ENROL system has been rebranded to STEPP.

- Completed the Business Capability Definition phase for OSCMIS to develop an automated, web-enabled system to effectively manage the agency’s Manpower, Human Resource, and Training.

- Completed the Engineering Development phase, and entered the Limited Deployment phase of the IdM/Portal solution to provide centralized account management through DoD CAC and PKI for improved information security of all DSS IT mission systems.

- DSS has successfully completed relocation of its headquarters from Alexandria, Virginia to Quantico, Virginia as mandated by the BRAC initiative. This move was completed flawlessly, without impact to the greater DoD stakeholder.

Major Planned Activities

The DSS OCIO will focus on pre-planned product improvements (P3I) 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 Office of the Chief Information Officer (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 FY12 and FY13:

• OBMS: Continue the development of the system in FY12 to achieve Full Operational Capability (FOC) in FY13. Delivery of OBMS completely modernizes the manual DSS security oversight and protection mission by automating the submission and management of System Security Plans (SSP) and C&A documentation. This automation will allow DSS to more effectively oversee classified information in the hands of industry, improving mitigation and response to new and emerging threats to the DIB.

• OSCMIS: Implement and automate an enterprise web-based system to effectively manage the agency's Manpower, Human Resources, and Training. Deliver IOC at the end of FY12; with planned incremental development of Security and Support Services, to include COOP functionalities for FOC in FY13.

• DD 254: Research automation capabilities of the DoD Form 254 - Contract Security Classification Specification, which provides information on the classification requirements of contractors and contractor facilities that handle classified information in the performance of government contracts, in FY12. In FY13, deliver IOC toward full automation of the oversight and management of providing classified information access and guidance required for the performance on classified contracts. The DoD Form 254 - Contract Security Classification Specification; is required by DoD 5220.22-4, Industrial Security Regulation and the National Industrial Security Program Operating Manual (NISPOM). The DD Form 254, and underlying business processes, are critical to ensure access to our Nation’s classified information is properly safeguarded.

• Mobile Workforce Applications (MWA): Research technical capabilities to implement mobile technologies to improve the efficacy of the DSS mission. The global DSS industrial security and oversight mission requires field representatives to audit remote contract facilities and information systems that process classified information. By incorporating mobile technologies into daily operations, the workforce has access to relevant and timely information, critical in ensuring security oversight decision making.

• FOS: The next generation enterprise capability replacement for ISFD, which is nearing end of life and becoming too expensive to enhance and maintain. Additionally, FOS will provide seamless integration of other DSS systems and applications, such as eFCL, OBMS, DD 254, and MWA. FOS will provide DSS with a comprehensive enhanced capability to manage its entire mission portfolio. FOS will improve information sharing and collaboration, providing timely and accurate data for decision-making in the hands of field representatives. The system will provide agency-wide metrics to measure and improve agency performance in providing security oversight and the protection of national security. The system will be developed in an iterative fashion in accordance with the Business Transformation Agency (BTA) Business Capability Lifecycle (BCL). High-level program plan is to complete the functional and technical requirements in FY12, and deliver IOC that supports the core functionality of the system in FY13. Incremental planning and systems engineering development will focus on future integration activities with DSS mission support systems and applications.

• Continued development of IdM to achieve FOC; thus, delivering centralized account management through DoD CAC and PKI for improved information security of all DSS IT mission systems.

IT Enterprise Strategy & Roadmap (ITESR) Implementation Activities

Consolidate Security Infrastructure (NS1)

The DSS OCIO Networks & Infrastructure Division (CION) is working multiple avenues to accomplish this initiative. Step one is to leverage the multi-agency data center facility at Quantico, which reduces the total number of GiG connections and eliminates previous connections that were dedicated to DSS alone. Second, DSS has redesigned routing of agency networks to leverage a common security model that allows all agency traffic to be monitored via a single point of presence as opposed to deploying sensors at multiple sites. Lastly, DSS is working to collapse the Host Based Security System (HBSS) environment into a single management and technical architecture. This effort, with support of DISA, cuts the HBSS footprint in half, and leverages economies of scale and a simplified physical environment.

The DSS OCIO Cyber Security Division (CIOI) is working with CION to develop a C&A Validation process that aligns IA efforts to improve security configuration, validation and continuous assessment. Additionally, IA is working towards a three tier approach to define a security architecture that is capable of strong security compliance with the flexibility to meet changing demands of DSS.

Implement Cross-Domain Solution as an Enterprise Service (NS3)

CION is pursuing two approaches to this initiative. Option one includes leveraging a community service within the Intelligence Community (IC) known as IC Clear. This capability currently exists and is being used by DSS. Option two is pending further analysis of requirements, but may include installation of an approved cross domain solution available to government agencies. If DSS does not have further requirements for a cross domain capability, we will retain option one as the solution.

Joint Information Environment (JIE)/Joint Enterprise Network (JEN) (NS8)

DSS does not have equities or mission requirements in this mission area at this time. If DSS pursues and implements a permanent presence in the European Theater of Operations, DSS will leverage services available through DISA, the host installation or command, and the IC to maximize value and seamless integration with JIE/JEN.

Data Center and Server Consolidation (CS1)

DSS has largely 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.

Enterprise Messaging and Collaboration (including email) (ADS1)

DSS has taken steps to consolidate email servers and systems internally as part of the re-architected IT footprint used within the agency. Modernization of the mail server applications includes the ability to seamlessly integrate email tools and messaging services with partner agencies and in shared data centers. Additionally, DSS has leveraged a web environment to improve communications facilitated via a portal capability. DSS has also reduced travel costs and improved communications by fielding a 188 node Video Teleconferencing (VTC) solution that connects over 25 sites via existing IP networks. In the future, DSS will have the ability to interface with other DoD VTC solutions when DISA completes modernization of the Defense Information Systems Network (DISN) VTC presence.

Identity and Access Management (idAM) Services (ADS2)

DSS is engaged in leveraging an Identity Management solution that will seamlessly connect systems and allow single-sign-on services. This directory centric capability is not fully developed, but it is already providing VPN access to support telework and a mobile workforce in addition to general desktop network access. In the future, it is anticipated to support PKI-CAC services to applications that support DSS and our DIB partners.

DSS is engaged in leveraging an Identity Management solution that will securely connect users to DSS applications and allow single-sign-on services (where feasible). This solution is not fully developed. A complete fully functioning Identity Management solution consists of 3 components: 1) Liferay portal for providing a front end for accessing and requesting access to DSS applications; 2) Sun Identity Manager for managing user accounts and credential information; 3) Sun OpenSSO to support CAC/PKI based authentication.

In the next nine (9) months, DSS plans to integrate three enterprise information systems: OBMS, STEPP, and ISFD. To be compliant with Joint Task Force - Global Network Operations (JTF-GNO) Communications Tasking Order (CTO) 06-02, the solution will allow certificate based client authentication to the DSS web applications using authorized certificates.

Consolidate Software Purchasing (BP1)

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.

Consolidate Hardware Purchasing (BP2)

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.

Page left intentionally blank

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

	----------- Dollars in Thousands ----------- FY2011	FY2012	FY2013
RESOURCE SUMMARY:	24,713	32,205	39,408

1513 - ODAA Business Management System (OBMS)

Non-Major

GIG Category: FUNCTIONAL AREA APPLICATIONS - INFORMATION MANAGEMENT

Operations

Appropriation	Budget Activity	Budget Line Item	----------- Dollars in Thousands ----------- FY2011	FY2012	FY2013
OPR & MAINT	BA 04 ADMIN & SRVWD ACTIVITIES	DEFENSE SECURITY SERVICE	0	750	3,810

RDT&E

Appropriation	Budget Activity	Program Element	----------- Dollars in Thousands ----------- FY2011	FY2012	FY2013
RDT&E	BA 07 OPERATIONAL SYSTEMS DEVELOPMENT	0305133V INDUSTRIAL SECURITY ACTIVITIES	820	2,728	1,561

	FY2011	FY2012	FY2013
Investment Resource Summary:	820	3,478	5,371

1794 - STANDARD PROCUREMENT SYSTEM (SPS)

Major

GIG Category: FUNCTIONAL AREA APPLICATIONS - ACQUISITION

Operations

Appropriation	Budget Activity	Budget Line Item	----------- Dollars in Thousands ----------- FY2011	FY2012	FY2013
OPR & MAINT	BA 04 ADMIN & SRVWD ACTIVITIES	DEFENSE SECURITY SERVICE	325	330	336

	FY2011	FY2012	FY2013
Investment Resource Summary:	325	330	336

2236 - Networks & Infrastructure (N&I)

Non-Major

GIG Category: COMMUNICATIONS AND COMPUTING INFRASTRUCTURE - COMPUTING INFRAST

Operations

Appropriation	Budget Activity	Budget Line Item	----------- Dollars in Thousands ----------- FY2011	FY2012	FY2013
OPR & MAINT	BA 04 ADMIN & SRVWD ACTIVITIES	DEFENSE SECURITY SERVICE	10,746	17,639	18,919

	FY2011	FY2012	FY2013
Investment Resource Summary:	10,746	17,639	18,919

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

2854 - Industrial Security Facility Database (ISFD)

Non-Major

GIG Category: FUNCTIONAL AREA APPLICATIONS - SECURITY ACTIVITIES (NON IA)

Operations

			----------- Dollars in Thousands -----------		
Appropriation	*Budget Activity*	*Budget Line Item*	*FY2011*	*FY2012*	*FY2013*
OPR & MAINT	BA 04 ADMIN & SRVWD ACTIVITIES	DEFENSE SECURITY SERVICE	10,305	5,623	5,791

RDT&E

			----------- Dollars in Thousands -----------		
Appropriation	*Budget Activity*	*Program Element*	*FY2011*	*FY2012*	*FY2013*
RDT&E	BA 07 OPERATIONAL SYSTEMS DEVELOPMENT	0305133V INDUSTRIAL SECURITY ACTIVITIES	175	663	475

Investment Resource Summary:	10,480	6,286	6,266

2902 - DSS Enterprise Portal (Portal)

Non-Major

GIG Category: FUNCTIONAL AREA APPLICATIONS - INFORMATION MANAGEMENT

Operations

			----------- Dollars in Thousands -----------		
Appropriation	*Budget Activity*	*Budget Line Item*	*FY2011*	*FY2012*	*FY2013*
OPR & MAINT	BA 04 ADMIN & SRVWD ACTIVITIES	DEFENSE SECURITY SERVICE	950	242	246

Investment Resource Summary:	950	242	246

2905 - Security Training, Education and Professionalization Portal (STEPP)

Non-Major

GIG Category: FUNCTIONAL AREA APPLICATIONS - OTHER (NOT OTHERWISE SPECIFIED)

Operations

			----------- Dollars in Thousands -----------		
Appropriation	*Budget Activity*	*Budget Line Item*	*FY2011*	*FY2012*	*FY2013*
OPR & MAINT	BA 04 ADMIN & SRVWD ACTIVITIES	DEFENSE SECURITY SERVICE	1,392	1,415	1,440

Investment Resource Summary:	1,392	1,415	1,440

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

4700 - Field Operations System (FOS)

Non-Major

GIG Category: FUNCTIONAL AREA APPLICATIONS - INFORMATION MANAGEMENT

RDT&E

Appropriation	Budget Activity	Program Element	----------- Dollars in Thousands ----------- FY2011	FY2012	FY2013
RDT&E	BA 07 OPERATIONAL SYSTEMS DEVELOPMENT	0305133V INDUSTRIAL SECURITY ACTIVITIES	0	2,076	6,008
		Investment Resource Summary:	0	2,076	6,008

4705 - Open Source Corporate Management Information System (OSCMIS)

Non-Major

GIG Category: FUNCTIONAL AREA APPLICATIONS - INFORMATION MANAGEMENT

RDT&E

Appropriation	Budget Activity	Program Element	----------- Dollars in Thousands ----------- FY2011	FY2012	FY2013
RDT&E	BA 07 OPERATIONAL SYSTEMS DEVELOPMENT	00000000 N/A	0	739	822
		Investment Resource Summary:	0	739	822