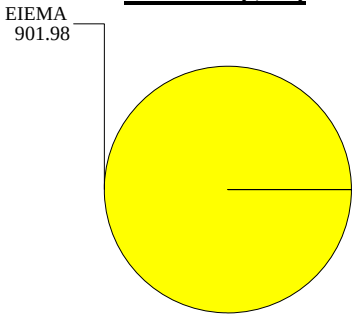
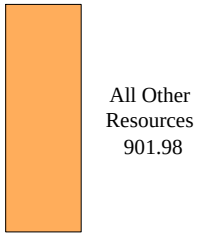
Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010

FY2011 ($M)



Mission Area



Defense Business Area Breakout

FY10/11PB Comparison ($M)

	FY2010	FY2011	Delta
PB FY2010:	$ 913.85	$ 899.66	-$ 14.20
PB FY2011:	$ 915.95	$ 901.98	-$ 13.97
Delta:	$ 2.10	$ 2.32	$ 0.22

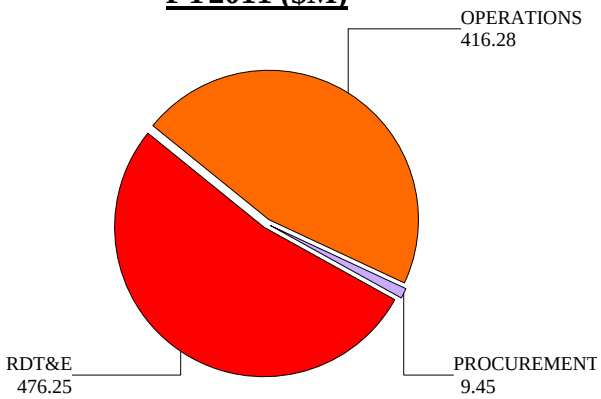
Explanation:
Refer to 'Significant Changes' section of the Overview

FY10 to FY11 Comparison ($M)

	FY2010	FY2011	Delta
PB FY2011:	$ 915.95	$ 901.98	$ -13.97

Explanation:
Refer to 'Significant Changes' section of the Overview

FY2011 ($M)



Appropriation

Page left intentionally blank

Executive Summary

(U) The primary focus of the National Security Agency (NSA) Information Systems Security Program (ISSP) is to provide the products, services, and capabilities that satisfy the Information Assurance (IA) needs of U.S. warfighters. The program specifically delivers capabilities for authentication, integrity, availability, confidentiality, and non-repudiation across the DoD information enterprise.

(U) Investments managed by the NSA's IA programs will enable the Department's ongoing efforts to transform to a net-centric force that can operate effectively in all warfighting domains—land, air, sea, space, and cyberspace. This transformation requires fundamental changes in processes, policies, and culture to accomplish the Department's four IA goals: organizing for unity of purpose and speed of action; enabling secure mission-driven access to information and services; anticipation and prevention of successful attacks on data and networks; and operational preparedness to overcome cyber degradation or attack. Beyond battlefield applications, IA capabilities increase efficiency and effectiveness across defensive operations, intelligence functions, and business processes. With information and its associated enabling technology (i.e., cyber) assets distributed worldwide and diverse domestic and international partners actively participating in DoD missions, the Department is moving to a joint global net-centric enterprise to accomplish requisite missions in increasingly more complex and hostile national security environments.

(U) The cyber domain is the most contested warfighting domain, and is the domain in which the Department relies most heavily on commercial products and services. The very nature of the cyber domain calls for an enterprise-wide IA approach, coupled with skilled users, defenders, and first responders and a close partnership with intelligence and homeland security communities and the private sector to provide for ready identification and response to cyber degradation or attacks while continuing to accomplish assigned objectives. The NSA ISSP directly supports the DoD Information Networks through its concept of operations, implementing architecture, and capabilities requirements documentation. The program invests in and evolves assured IA capabilities that afford secure information exchange, protect data and networks, and enable appropriate, active responses to cyber attacks and events. Selected investments recommended for resourcing comply with direction provided by the DoD Management Strategy, Guidance for Development of the Force (GDF), information enterprise strategies, and annual Component capability gap assessments. The Department's cyber investments for IA span the broad spectrum of Doctrine, Organization, Material, Leadership and Education, Personnel, and Facilities (DOTMLPF) and extend across all DoD entities, missions, and systems. NSA's FY2011 ISSP advances each of these goals.

(U) This program portfolio of managed investments is organized into nine interdependent investment categories:
• Computer Network Defense (CND)
• Cryptographic Systems
• Cyber Identity/Access Management
• Engineering and Deployment
• Cryptographic Key Production and Management
• Cross Domain
• Workforce Development
• IA Operational Resiliency
• Defense Industrial Base Cyber Security Task Force (DIBCSTF)

Significant Changes

(U) FY2010 to FY2011 Comparison Summary:

(U) The NSA ISSP top line decreased approximately $14.0M from FY2010 to FY2011. This augmentation reflects changes due to economic adjustments and other DoD-directed reductions.

(U) Changes in FY2011 between FY2010 PB submission and FY2011 PB submission:

(U) The NSA ISSP FY2011 total decreased approximately $34.0M due to the DoD-directed changes and economic adjustments made to the program.

(U) Changes in FY2010 between FY2010 PB submission and FY2011 PB submission:

(U) The NSA ISSP FY2010 total increased approximately $1.1M due to DoD adjustments for Overseas Contingency Operations.

(U) Changes in FY2009 between FY2010 PB submission and FY2011 PB submission:

(U) The NSA ISSP FY2009 total increased approximately $19.65M due to DoD adjustments for FY09 Omnibus Reprogramming.

Defense Business Systems

(U) A number of development activities will provide IA capabilities with applications for Defense Business Systems (DBS). However, no specific DBS are being developed with NSA ISSP funds.

Information Assurance Activities

(U) Summary of individual IA activities paid for by NSA ISSP dollars. These activities are organized according to the Department’s nine major investment categories:

(U) Computer Network Defense - Programs include: Mission Evolution, Software Engineering Services, NSA/CSS Threat Operations Center, Mission Enablers, Information Analysis, Technical and Technology Analysis, and Interactive On-Net Analysis.

(U) Cryptographic Systems - Programs include: National Cryptographic Solutions Management Office, Custom Solutions for Special Operations, Microelectronics, Advanced Computing Systems, Security for Critical Communications Networks, Space and Weapons Systems, and IA Center for Communications Research.

(U) Cyber Identity/Access Management - Programs include: DoD Public Key Infrastructure Program Management Office and Enterprise Security Management.

(U) Engineering and Deployment - Programs include: IA Information Technology Services, IA Installations and Logistics Services, IA Mission Support, Client Engagement and Community Outreach.

(U) Cryptographic Key Production & Management - Programs include: Key Management Infrastructure (KMI) and KMI Operations and Sustainment.

(U) Cross Domain - Programs include: Cross Domain Solutions; Mission and Network Systems, Net-centric Security Technologies, Ubiquitous Secure Collaboration, and Commercial Systems Solutions Engineering.

(U) Workforce Development includes Leadership and Workforce Development.

(U) IA Operational Resiliency - Programs include: Network Integration and Test, and National Information Assurance Partnership.

(U) Defense Industrial Base Cyber Security Task Force includes the Information Assurance Defense Industrial Base program.

(U) Each of these nine major investments categories fall into the framework of the Department's IA Strategic Plan, in which The National Security Agency's Information Assurance programs and initiatives support DoD's IA goals and objectives.

Major Accomplishments

FY09 Major Accomplishments:

(U) A Computer Network Defense Tool developed by NSA, USBDetect 3.0, is available to U.S. Government (USG) users free of charge. USBDetect gathers data (locally or on a network) from personal computers running Microsoft Windows 2000 or later operating systems, and reports unauthorized usage of Universal Serial Bus (USB) thumb (a.k.a. flash) drives, external hard drives, compact disk drives, and other storage devices. The USBDetect tool provides USG network administrators and system security officials with an automated capability to detect the introduction of USB storage devices into their networks. This tool closes potential security vulnerabilities; a definite success story in the pursuit of the DoD and NSA protect information technology system strategic goals.

(U) NSA prides itself on providing Information Assurance (IA) expertise and technology at reasonable cost to its national security clients when and where they need it to secure their critical information and mission operations. In recognition of NSA success in pursuing this DoD and NSA strategic goal of transforming IA solution deliver, NSA was presented with the DoD Chief Information Officer (CIO) Information Management and Information Technology Management Award. In announcing NSA's selection for this presitigious recognition, the DoD CIO cited the Agency's exemplary management performance in developing and delivering the Secure Mobile Environment – Portable Electronic Device (SME-PED) capability.

(U) The SME-PED is a smart phone converging secure wireless voice and data by combining the functionality of a wireless telephone and personal digital assistant. The SME-PED is certified by NSA to protect wireless voice communications classified up to Top Secret, as well as e-mail and website connectivity classified Secret and below. Compact and lightweight, its accommodates the needs of users in routine office environments and warfighters completing tactical operations – all in one easy to use handheld device. A senior

DoD official has said that “between 30,000 and 100,000 [SME-PED] smart phones can be delivered to the Defense, Homeland Security, and State departments and to every state governor as well.” By designing multiple functionalities into a single handheld device, NSA’s innovative IA management approach to the SME-PED development will mean significant savings for the federal government by eliminating the need for separate devices for classified and unclassified voice and data on-the-move communications.

(U) In pursuit of DoD and NSA strategic objectives to protect information, NSA oversees the development of next-generation Programmable Objective Encryption Technologies (POET). These cutting-edge technologies incorporate embeddable high-speed Type 1 cryptographic modules that provide NSA Suite A and Suite B cryptography and key management capabilities. POET enables highly secure, survivable communications and transmission security services at data transfer speeds up to two gigabits per second, and is capable of running multiple cryptographic algorithms simultaneously with varying security levels. Additionally, POET complies with Cryptographic Modernization Initiative requirements and is interoperable with NSA High Assurance Internet Protocol Encryptors. The POET goal is to ensure that strategic voice and data gets through to the warfighters securely and quickly, whatever the circumstances.

(U) In pursuit of its transformation strategic goal to, “lead an expanded supplier community by transforming information assurance delivery processes,” the National Security Agency transitioned the National Cryptographic Solutions Management Office (NCSMO) unclassified Internet web site to government control. At that point, the web site became the first live http://www.iad.gov unclassified Internet web site. This transition to government control results in a savings on web maintenance.

(U) POET’s light weight, reduced size and power needs, make it the ideal security device for Advanced Extremely High Frequency (AEHF) satellite and other advanced beyond line-of-sight communications applications. Increment 1 platforms with embedded POET have been fitted into U.S. Air Force (USAF) nuclear strike assets such as the B-2 Spirit and B-52 Stratofortress, USAF E-$B Nightwatch mobile command post for the National Command Authority (NCA), and the USAF RC-135 Stratolifter reconnaissance aircraft. POET devices also have been fitted into the communications suites in the U.S. Navy’s (USN) E-6B Mecury airborne command, control, and communications platform between the NCA and U.S. strategic and non-strategic forces. Subsequent increments will be fitted to Transformational Satellite constellations (needed science and technology work already is underway), RQ-4 Global Hawk unmanned aerial vehicles used by the USAF, USN, and some foreign national partners, as well as the USAF F-22 Raptor Homeland Defense fighters and the F-35 Lightning II multi-role aircraft to be operated by the USAF, USN, US Marine Corps, and many U.S. allies and coalition partners.

Major Planned Activities

FY11 Major Planned Activities:

(U) The Mission and Network Systems program will provide guidance and support for Certification, Test, and Evaluation (CT&E) efforts, as well as help with risk assessments and other information systems security engineering needs relating to Cross Domain Solutions (CDS). This activity includes sustainment of the Risk Decision Authority Criteria (RDAC), as well as CDS risk assessments for the Cross Domain Technical Advisory Board (CDTAB) and DISN Security Accreditation Working Group. Development, deployment, and sustainment of CASTER to support CT&E’s, Cross Domain Appendices, and Risk Decision Authority Criteria risk assessment activities will continue.

(U)The Net-centric Security Technologies program will provide Information Assurance (IA) consulting services and guidance on the implementation of commercial networking products. The program will provide security assessment reports on commercial products and investigate, analyze, and report on the IA technology trends for emerging commercial products/technologies. It will also develop recommended security standards and implementation guidance for commercial products supporting the collapse of coalition information sharing architectures, identify and develop solutions using existing technology, and support testing and deployment of those solutions in support of the Intelligence Community, the Department of Defense, and the Department of Homeland Security.

(U) NSA's Public Key Infrastructure (PKI) program will continue the development of Robust Certificate Validation Services (RCVS) nodes to include protocols such as Server Certificate Validation Protocol (SCVP). It will continue to develop an interoperability infrastructure to establish trust with external PKI's to include Federal Agencies, the Intelligence Community, and business partners. It will also continue to develop Second Source Certification Authority, Government developed PKI applets, Biometrics Integration, and distribute PKI root certificates. Development of a monitoring capability for Red Hat Certificate Management Systems and second phase monitoring system capabilities will continue.

(U) The National Cryptographic Solutions Management Office (NCSMO) will continue to support and oversee the entire Cryptographic Modernization (CM) Program, which includes the creation and modification of CM and Joint Staff policies and design guidance, as well as ensure that the individual NSA and Service CM program offices follow CM design specifications. It will also continue to support the development of IA for a variety of DoD Information Networks.

(U) The Cryptographic Products Engineering program will design and develop foreign releasable cryptographic products that provide interoperability between the U.S. and allies. It will continue to support the development of associated technologies that support foreign release, including protective techniques, electronic key distribution, embedded features, and public key exchanges.

(U) The Commercial Systems Solutions Engineering program will complete the implementation and operational deployment of the High Assurance Platform (HAP) Release 2. Release 2 deployments will be tested and validated at Special Operation Command, Pacific Command, and Fleet Numeric Meteorology and Oceanography Center. Begin development of the HAP Release 3 that fully leverages the commercial trusted computing technologies and capabilities implemented in HAP Release 2. It will continue work with industry to lead and influence trusted computing technology and solutions through participation in the Trusted Computing Group. It will also continue to enhance Secure Mobile Environment Portable Electronic Device. New capabilities to be developed under this program could include new radio frequency modules, satellite communications, and HAP technology.

(U) The Advanced Computing Research program will continue to promote ideation in the creation of new chip multiprocessor technologies that will benefit the missions of NSA in cryptology, digital signal processing, filtering and selection, intrusion detection, knowledge discovery, voice recognition, natural language machine translation, and event simulation. It will also continue to grow the capabilities of the interim Center for Exceptional Computing.

(U) The National Information Assurance Partnership (NIAP) will continue to maintain the NIAP Validated Products list. The NIAP Validated Products list is updated and maintained on an unclassified website by the NIAP office and is used by the entire U.S. Government community as a single U.S. government source for NIAP Common Criteria evaluated IA products. Per CNSS Acquisition Policy #11 (commonly referred to as NSTISSP 11), National Security Community customers must purchase IA products that have been Common Criteria evaluated, so this list is critical to Federal Government Acquisition agents to verify IA products that can be purchased for implementation on critical National Security Community networks.

(U) For national security reasons, some of the products and services that The National Security Agency (NSA) produces throughout the year are classified. To get additional and detailed descriptions of the major planned activities for NSA, please refer to the FY 2011 DoD IA Congressional Justification Book.

Global Information Grid (GIG) / Net-Centricity

(U) NSA's FY2011 IA Program provides for critical IA operations and development of IA capabilities to support the DoD Information Network and Net-centric operations, and the development of material and non-material capabilities across nine inter-dependent categories:

(U) Computer Network Defense – Department systems and networks are constantly under attack and must be continuously defended against adversaries that seek persistent insider presence to obtain access to critical mission-related data and communications, as well as being afforded opportunities to exploit, disrupt, and attack enterprise components and the resources of organizational and individual cyber network users. The Department is achieving its objectives by deploying a layered defensive that strengthens perimeter defenses, improves/strengthens operations within that perimeter, provides near real-time situational awareness, and increases capacities of network defenders to dynamically react. When determined adversaries do gain access to networks, improved internal defenses – provided by secure host and network configurations – can limit abilities to act or to penetrate with impunity. Provision of near real-time situational awareness ensures network defenders hold information necessary to mount responsive, effective, defensive operations. As these CND capabilities are emplaced, operational readiness must be resourced to ensure routine testing and continuous monitoring for operational-driven adequacy of security performance. Current NSA CND investments – upon which layered defense depends, include: Host/Network Configuration, IA Network Operations, and Situational Awareness.

(U) Cryptographic Systems – Cryptographic Systems provide significant enterprise infrastructure capabilities for protecting information by encrypting communication links or data into random formats that are extremely difficult to decipher (based on strength of the encrypting algorithm employed and length of its key). These systems provide confidentiality, authenticity, integrity, and non-repudiation services for crucial information being protected. Certified Cryptographic Systems are integrated into secure National Security Systems and defense information network communication links, by engineered employment of assured hardware or software applications. There are two main factors that assure superiority of these cryptographic products: research and development of new techniques/algorithms and modernization of legacy equipment. Current NSA Cryptographic System investments – upon which information protection is based, include: Combat Applications, Tactical Secure Voice, Secure Data, Space Cryptography, and Nuclear Command and Control (NC2).

(U) Cyber Identity/Access Management - Cyber Identity/Access Management is necessary to authenticate individual non-person/material entities (e.g., devices, application, platforms) to enable secure access services, data platforms, and facilities, based on mission necessity. NSA investments include: Public Key Infrastructure (PKI) and Privilege Management.

(U) Engineering and Deployment – Maintaining superiority and competitive edge over adversary exploitations demands deliberate continuation of initiatives to transform processes, procedures, and practices used to develop and deliver new and evolving cyber defense capabilities. These capabilities are crucial components for improving responsiveness to constantly changing needs and properly managing fundamental information sharing risks. The power of information sharing places great importance on harvesting and prioritizing validated needs for rapid research, development, and deployment of non-material concepts and material-based capabilities. Successes in these areas enable continuous preparation, shaping, and execution of Department responses to America’s operating environments. NSA investments include: Architecture, Systems Engineering, Compliance, Outreach, and Governance.

(U) Cryptographic Key Production and Management – Cryptographic Key Production and Management provides for generation, production, storage, protection, distribution, filling, use, control, tracking, and destruction for all key material the DoD employs to establish and sustain assured security of information transmissions across National Security System and DISN links. The Cryptographic Key Management System ensures on-demand availability of all key cryptographic devices. NSA investments include: Traditional Key and Key Management Infrastructure (KMI).

(U) Cross Domain – Cross Domain solutions provide abilities to securely access or transfer information between two or more enterprise network security domains. The goal for certified/accredited Cross Domain solutions is to securely and dynamically share information between authorized users or Communities of Interest (COI) within or between security domains. Such exchanges must assure those shared information exchanges are protected from modification; permit only authorized users to have access; share user access rights across the enterprise; and provide assured discovery and retrieval for sharing across domains. These capabilities are critical for enabling access to and exchanging information between the DoD and various U.S. Federal Agencies and Intelligence Community (IC) networks, operating at different classification levels in support of warfighter operational requirements. Cross Domain capabilities – upon which assured information sharing depends, include: Enterprise Cross Domains and Robust Platforms.

(U) Workforce Development - To ensure information crucial to mission execution and operational support is protected, the DoD recognizes the necessity to create and sustain a world-class IA professional cyber defense workforce that is capable of effectively deterring, preventing, and responding to threats against current and future DoD information, information systems, and infrastructures. Providing a continuum of learning activities (from basic IA literacy to certified skills for advanced security engineering specialties) is fundamental for recruitment and retention of highly qualified cyber warriors. Their essential work roles – with associated career paths – require ensuring effective development to perform proactively or in response to executed threats and to ensure accomplishment of operationally-assigned tasks. Cyber warriors must maintain their proficiencies, despite constant operational change and evolution; continuous learning is and skill development must be individual readiness norms. NSA resources include: Training.

(U) IA Operational Resiliency – National Security Systems and DISN provide the enterprise-wide DoD environment upon virtually all the Department’s missions depend. The nation’s adversaries would, if afforded opportunities, degrade, deny, and manipulate that environment of critical networks, core enterprise computing services, and information technology underpinnings. As the Department continues to evolve and mature cyberspace as a warfighting domain, its networks must be built to ensure operational resiliency necessary to: work when under fire, deflect attacks, recover quickly, and restore trust in transmitted information. Operational resiliency is the ability to be flexible, adaptable, and successful in the face of cyber degradation, transmission losses, or disruptive attacks. Continuity of information network operations under disconnected, intermittent, limited bandwidth conditions demands effective solutions for maintaining resiliency and minimizing disadvantages to clients, at all echelons. Of necessity, these network operations and defenses must be effectively staffed, equipped, and integrated in alignment with other cyber operations across the extended enterprise. NSA resources include: IA Integration and Test Networks, and Software Assurance.

(U) Defense Industrial Base Cyber Security Task Force (DIBCSTF) – IA support for the Defense Industrial Base (DIB) Cyber Security Task Force (CSTF) exists to invoke information protection for critical DoD programs and technologies employed to protect DoD unclassified national security information resident on and transiting DIB networks. These information protection measures support material development of DoD weapon platforms and focused technology improvements, as well as leading-edge design efforts, by commercial partners. Other security-related activities involve protecting design intellectual property and leveraging technical knowledge bases for improved cyber security. Resulting benefits include insight into and understanding network infrastructure issues, so industry best practices and processes can be leveraged. This activity is intended to effectively defend DIB systems and networks by employing a protected Collaborative Information Sharing Environment (CISE) information portal that expands information sharing and awareness. Investment for this effort supports development of three critical automated tools for vulnerability assessments, information-sharing portal implementation, and forensics.

Page left intentionally blank

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

	Dollars in Thousands		
	FY2009	*FY2010*	*FY2011*
NATIONAL SECURITY AGENCY RESOURCE SUMMARY:	**972,518**	**915,951**	**901,979**

0020 - SITUATIONAL AWARENESS/C2 - COMPUTER NETWORK DEFENSE (IA G3 CND) **Non-Major**

GIG Category: INFORMATION ASSURANCE ACTIVITIES - COMPUTER NETWORK DEFENSE

Operations

Appropriation	*Budget Activity*	*Budget Line Item*	Dollars in Thousands *FY2009*	*FY2010*	*FY2011*
O&M, DW	BA 00 N/A	N/A	1,618	3,281	5,018
O&M, DW	BA 04 ADMN & SRVWD ACT	CLASSIFIED AND INTELLIGENCE	132,559	104,482	116,887
		Sub Total:	**134,177**	**107,763**	**121,905**

Procurement

Appropriation	*Budget Activity*	*Budget Line Item*	Dollars in Thousands *FY2009*	*FY2010*	*FY2011*
Procurement, DW	BA 01 MAJOR EQUIPMENT	INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	1,843	2,151	1,351

RDT&E

Appropriation	*Budget Activity*	*Program Element*	Dollars in Thousands *FY2009*	*FY2010*	*FY2011*
RDT&E, DW	BA 00 N/A	0000000D N/A	4,500	5,507	3,405
RDT&E, DW	BA 07 OPER SYS DEV	0303140G INFORMATION SYSTEMS SECURITY PROGRAM	72,397	54,710	44,503
		Sub Total:	**76,897**	**60,217**	**47,908**
		Initiative Resource Summary:	**212,917**	**170,131**	**171,164**

0210 - TRANSFORM & ENABLE IA CAPABILITIES - CRYPTOGRAPHIC MODERNIZATION (IA G4 CM) **Non-Major**

GIG Category: INFORMATION ASSURANCE ACTIVITIES - CRYPTOGRAPHIC SYSTEMS

Operations

0210 - TRANSFORM & ENABLE IA CAPABILITIES - CRYPTOGRAPHIC MODERNIZATION (IA G4 CM) (Continued) **Non-Major**

GIG Category: INFORMATION ASSURANCE ACTIVITIES - CRYPTOGRAPHIC SYSTEMS

Operations (Continued)

			Dollars in Thousands		
Appropriation	*Budget Activity*	*Budget Line Item*	*FY2009*	*FY2010*	*FY2011*
O&M, DW	BA 04 ADMN & SRVWD ACT	CLASSIFIED AND INTELLIGENCE	21,319	20,588	19,310

RDT&E

			Dollars in Thousands		
Appropriation	*Budget Activity*	*Program Element*	*FY2009*	*FY2010*	*FY2011*
RDT&E, DW	BA 00 N/A	0000000D N/A	5,283	1,967	1,654
RDT&E, DW	BA 07 OPER SYS DEV	0303140G INFORMATION SYSTEMS SECURITY PROGRAM	93,437	93,522	91,289
		Sub Total:	**98,720**	**95,489**	**92,943**
		Initiative Resource Summary:	**120,039**	**116,077**	**112,253**

1030 - Key Management Infrastructure (KMI) **Major**

GIG Category: INFORMATION ASSURANCE ACTIVITIES - CRYPTOGRAPHIC KEY MANAGEMENT

Operations

			Dollars in Thousands		
Appropriation	*Budget Activity*	*Budget Line Item*	*FY2009*	*FY2010*	*FY2011*
O&M, DW	BA 00 N/A	N/A	0	0	0

RDT&E

			Dollars in Thousands		
Appropriation	*Budget Activity*	*Program Element*	*FY2009*	*FY2010*	*FY2011*
RDT&E, DW	BA 00 N/A	0000000D N/A	55,435	40,782	45,941
		Initiative Resource Summary:	**55,435**	**40,782**	**45,941**

3747 - Protect - Cyber Identity/Access Management (Protect Cyber) **Non-Major**

GIG Category: INFORMATION ASSURANCE ACTIVITIES - CYBER IDENTITY/ACCESS MANAGEMENT

Operations

			Dollars in Thousands		
Appropriation	*Budget Activity*	*Budget Line Item*	*FY2009*	*FY2010*	*FY2011*
O&M, DW	BA 00 N/A	N/A	300	0	0
O&M, DW	BA 04 ADMN & SRVWD ACT	CLASSIFIED AND INTELLIGENCE	851	1,089	727
		Sub Total:	**1,151**	**1,089**	**727**

Procurement

			Dollars in Thousands		
Appropriation	*Budget Activity*	*Budget Line Item*	*FY2009*	*FY2010*	*FY2011*
Procurement, DW	BA 00 N/A	N/A	2,792	0	0

RDT&E

			Dollars in Thousands		
Appropriation	*Budget Activity*	*Program Element*	*FY2009*	*FY2010*	*FY2011*
RDT&E, DW	BA 00 N/A	0000000D N/A	13,459	10,817	6,810
RDT&E, DW	BA 07 OPER SYS DEV	0303140G INFORMATION SYSTEMS SECURITY PROGRAM	6,744	7,641	8,197
		Sub Total:	**20,203**	**18,458**	**15,007**

Initiative Resource Summary:	**24,146**	**19,547**	**15,734**

3857 - Protect Cross Domain (Protect CD) **Non-Major**

GIG Category: INFORMATION ASSURANCE ACTIVITIES - CROSS DOMAIN

Operations

			Dollars in Thousands		
Appropriation	*Budget Activity*	*Budget Line Item*	*FY2009*	*FY2010*	*FY2011*
O&M, DW	BA 00 N/A	N/A	4,334	1,641	2,574
O&M, DW	BA 04 ADMN & SRVWD ACT	CLASSIFIED AND INTELLIGENCE	7,305	9,943	12,447

3857 - Protect Cross Domain (Protect CD) (Continued) **Non-Major**

GIG Category: INFORMATION ASSURANCE ACTIVITIES - CROSS DOMAIN

Operations (Continued)

Appropriation	Budget Activity	Budget Line Item	FY2009	FY2010	FY2011
			---------- Dollars in Thousands ----------		
		Sub Total:	**11,639**	**11,584**	**15,021**

Procurement

Appropriation	Budget Activity	Budget Line Item	FY2009	FY2010	FY2011
			---------- Dollars in Thousands ----------		
Procurement, DW	BA 00 N/A	N/A	10,768	0	0

RDT&E

Appropriation	Budget Activity	Program Element	FY2009	FY2010	FY2011
			---------- Dollars in Thousands ----------		
RDT&E, DW	BA 00 N/A	0000000D N/A	18,143	17,602	11,674
RDT&E, DW	BA 07 OPER SYS DEV	0303140G INFORMATION SYSTEMS SECURITY PROGRAM	105,303	107,937	101,471
		Sub Total:	**123,446**	**125,539**	**113,145**
		Initiative Resource Summary:	**145,853**	**137,123**	**128,166**

3915 - Protect - Defense Industrial Base (Protect DIB) **Non-Major**

GIG Category: INFORMATION ASSURANCE ACTIVITIES - DEFENSE INDUSTRIAL BASE

Operations

Appropriation	Budget Activity	Budget Line Item	FY2009	FY2010	FY2011
			---------- Dollars in Thousands ----------		
O&M, DW	BA 04 ADMN & SRVWD ACT	CLASSIFIED AND INTELLIGENCE	1,836	3,000	3,000
		Initiative Resource Summary:	**1,836**	**3,000**	**3,000**

3933 - Protect - IA Engineering and Deployment (Protect IA Eng) **Non-Major**

GIG Category: INFORMATION ASSURANCE ACTIVITIES - IA ENGINEERING AND DEPLOYMENT

Operations

			Dollars in Thousands		
Appropriation	*Budget Activity*	*Budget Line Item*	*FY2009*	*FY2010*	*FY2011*
O&M, DW	BA 00 N/A	N/A	2,537	4,547	6,077
O&M, DW	BA 04 ADMN & SRVWD ACT	CLASSIFIED AND INTELLIGENCE	70,505	77,416	88,212
		Sub Total:	**73,042**	**81,963**	**94,289**

Procurement

			Dollars in Thousands		
Appropriation	*Budget Activity*	*Budget Line Item*	*FY2009*	*FY2010*	*FY2011*
Procurement, DW	BA 01 MAJOR EQUIPMENT	INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	217	115	73

RDT&E

			Dollars in Thousands		
Appropriation	*Budget Activity*	*Program Element*	*FY2009*	*FY2010*	*FY2011*
RDT&E, DW	BA 00 N/A	0000000D N/A	3,588	3,638	3,600
RDT&E, DW	BA 07 OPER SYS DEV	0303140G INFORMATION SYSTEMS SECURITY PROGRAM	29,462	34,204	27,315
		Sub Total:	**33,050**	**37,842**	**30,915**
		Initiative Resource Summary:	**106,309**	**119,920**	**125,277**

3934 - Protect - Cryptographic Key Management (Crypto Key) **Non-Major**

GIG Category: INFORMATION ASSURANCE ACTIVITIES - CRYPTOGRAPHIC KEY MANAGEMENT

Operations

			Dollars in Thousands		
Appropriation	*Budget Activity*	*Budget Line Item*	*FY2009*	*FY2010*	*FY2011*

3934 - Protect - Cryptographic Key Management (Crypto Key) (Continued) **Non-Major**

GIG Category: INFORMATION ASSURANCE ACTIVITIES - CRYPTOGRAPHIC KEY MANAGEMENT

Operations (Continued)

			Dollars in Thousands		
Appropriation	*Budget Activity*	*Budget Line Item*	*FY2009*	*FY2010*	*FY2011*
O&M, DW	BA 04 ADMN & SRVWD ACT	CLASSIFIED AND INTELLIGENCE	89,960	76,183	81,376

Procurement

			Dollars in Thousands		
Appropriation	*Budget Activity*	*Budget Line Item*	*FY2009*	*FY2010*	*FY2011*
Procurement, DW	BA 01 MAJOR EQUIPMENT	INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	2,432	1,735	1,122

RDT&E

			Dollars in Thousands		
Appropriation	*Budget Activity*	*Program Element*	*FY2009*	*FY2010*	*FY2011*
RDT&E, DW	BA 07 OPER SYS DEV	0303140G INFORMATION SYSTEMS SECURITY PROGRAM	44,122	44,601	40,708
		Initiative Resource Summary:	**136,514**	**122,519**	**123,206**

3935 - Protect - Workforce Development (Workforce Dev) **Non-Major**

GIG Category: INFORMATION ASSURANCE ACTIVITIES - WORKFORCE DEVELOPMENT

Operations

			Dollars in Thousands		
Appropriation	*Budget Activity*	*Budget Line Item*	*FY2009*	*FY2010*	*FY2011*
O&M, DW	BA 04 ADMN & SRVWD ACT	CLASSIFIED AND INTELLIGENCE	15,259	17,200	18,358

RDT&E

			Dollars in Thousands		
Appropriation	*Budget Activity*	*Program Element*	*FY2009*	*FY2010*	*FY2011*

3935 - Protect - Workforce Development (Workforce Dev) (Continued) **Non-Major**

GIG Category: INFORMATION ASSURANCE ACTIVITIES - WORKFORCE DEVELOPMENT

RDT&E (Continued)

Appropriation	Budget Activity	Program Element	FY2009	FY2010	FY2011
			---------- Dollars in Thousands ----------		
RDT&E, DW	BA 07 OPER SYS DEV	0303140G INFORMATION SYSTEMS SECURITY PROGRAM	623	632	286
		Initiative Resource Summary:	**15,882**	**17,832**	**18,644**

3936 - Transform - Operational Resiliency (Trans GIG Res) **Non-Major**

GIG Category: INFORMATION ASSURANCE ACTIVITIES - OPERATIONAL RESILIENCY

Operations

Appropriation	Budget Activity	Budget Line Item	FY2009	FY2010	FY2011
			---------- Dollars in Thousands ----------		
O&M, DW	BA 04 ADMN & SRVWD ACT	CLASSIFIED AND INTELLIGENCE	936	931	524

RDT&E

Appropriation	Budget Activity	Program Element	FY2009	FY2010	FY2011
			---------- Dollars in Thousands ----------		
RDT&E, DW	BA 07 OPER SYS DEV	0303140G INFORMATION SYSTEMS SECURITY PROGRAM	9,089	8,780	7,177
		Initiative Resource Summary:	**10,025**	**9,711**	**7,701**

6404 - DEFEND SYSTEMS & NETWORKS - COMPUTER NETWORK DEFENSE (IA G2 CND) **Non-Major**

GIG Category: INFORMATION ASSURANCE ACTIVITIES - COMPUTER NETWORK DEFENSE

Operations

Appropriation	Budget Activity	Budget Line Item	FY2009	FY2010	FY2011
			---------- Dollars in Thousands ----------		

6404 - DEFEND SYSTEMS & NETWORKS - COMPUTER NETWORK DEFENSE (IA G2 CND) (Continued) **Non-Major**

GIG Category: INFORMATION ASSURANCE ACTIVITIES - COMPUTER NETWORK DEFENSE

Operations (Continued)

Appropriation	Budget Activity	Budget Line Item	FY2009	FY2010	FY2011
			---------- Dollars in Thousands ----------		
O&M, DW	BA 00 N/A	N/A	16,969	9,801	14,627
O&M, DW	BA 04 ADMN & SRVWD ACT	CLASSIFIED AND INTELLIGENCE	17,988	18,313	35,567
		Sub Total:	**34,957**	**28,114**	**50,194**

RDT&E

Appropriation	Budget Activity	Program Element	FY2009	FY2010	FY2011
			---------- Dollars in Thousands ----------		
RDT&E, DW	BA 07 OPER SYS DEV	0303140G INFORMATION SYSTEMS SECURITY PROGRAM	49,557	57,682	68,631
		Initiative Resource Summary:	**84,514**	**85,796**	**118,825**

6456 - PROTECT INFORMATION - PUBLIC KEY INFRASTRUCTURE (IA G1 PKI) **Major**

GIG Category: INFORMATION ASSURANCE ACTIVITIES - CYBER IDENTITY/ACCESS MANAGEMENT

Operations

Appropriation	Budget Activity	Budget Line Item	FY2009	FY2010	FY2011
			---------- Dollars in Thousands ----------		
O&M, DW	BA 00 N/A	N/A	9,619	13,576	11,574

Procurement

Appropriation	Budget Activity	Budget Line Item	FY2009	FY2010	FY2011
			---------- Dollars in Thousands ----------		
Procurement, DW	BA 00 N/A	N/A	17,946	33,199	6,902

RDT&E

6456 - PROTECT INFORMATION - PUBLIC KEY INFRASTRUCTURE (IA G1 PKI) (Continued) **Major**

GIG Category: INFORMATION ASSURANCE ACTIVITIES - CYBER IDENTITY/ACCESS MANAGEMENT

RDT&E (Continued)

			Dollars in Thousands		
Appropriation	*Budget Activity*	*Program Element*	*FY2009*	*FY2010*	*FY2011*
RDT&E, DW	BA 00 N/A	0000000D N/A	31,483	26,738	13,592
		Initiative Resource Summary:	**59,048**	**73,513**	**32,068**

Page left intentionally blank