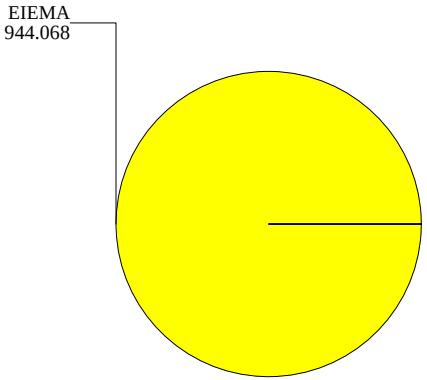
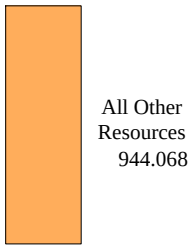
Department of Defense
Fiscal Year (FY) 2012 IT President's Budget Request
March 2011

FY2012 ($M)



Mission Area



Defense Business Area Breakout

FY11/12PB Comparison ($M)

	FY2011	FY2012	Delta
PB FY2011:	$ 901.979	$ 913.584	$ 11.605
PB FY2012:	$ 895.229	$ 944.068	$ 48.839
Delta:	$ -6.750	$ 30.484	

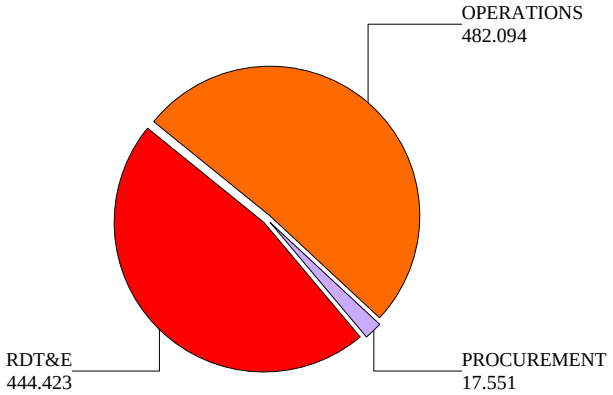
Explanation:
Refer to 'Significant Changes' section of the Overview

FY11 to FY12 Comparison ($M)

	FY2011	FY2012	Delta
PB FY2012:	$ 895.229	$ 944.068	$ 48.839

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

FY2012 ($M)



Appropriation

Page left intentionally blank

Executive Summary

The National Security Agency's (NSA) Information Assurance (IA) program provides products, services and capabilities to meet the information assurance needs of U.S warfighters and the Department of Defense Global Information Grid (GIG). It shares its IA expertise and knowledge with the rest of the Federal government to help ensure civil classified and sensitive information and systems also remain secure.

Investments managed by the NSA's IA programs support the Department's ongoing efforts to transform into net-centric force that can operate effectively in all warfighting domains: land; air; sea; space; and cyberspace. The Department's four IA goals set out the strategy for driving the fundamental changes in processes, policies, and culture needed to underpin transformation and ensure that the Department's information assets provide a trustworthy platform from which to launch today's dynamic mission. These four thrusts organize for unity of purpose and speed of action, enable secure mission-driven access to information and services, anticipate and prevent successful attacks on data and networks, operationally prepare to overcome cyber attack and degradation, and increase the DoD information advantage on and beyond the battlefield across defensive operations, intelligence functions and business processes.

NSA's investment strategy specifically addresses the challenge of providing security solutions that keep pace with a fast-moving technology sector, agile adversaries and rapidly-changing mission demands. NSA has identified three particular areas for growth, and initial implementation experience has confirmed the soundness of this approach for supporting DoD's emerging Information Technology (IT) and IA needs:

• Commercial-Off-The-Shelf (COTS) Imperative: Devising ways to use commercially available components securely to provide fast, affordable, state-of-the-market and sufficiently trustworthy solutions. We call this methodology trust engineering.

• Real-Time Security: Developing capabilities to characterize and continuously improve the posture of operational systems against real adversarial capabilities, as well as factoring all components of risk (threat and consequences as well as vulnerabilities) into decisions on how to harden assets.

• Operational Network Defense: Partnering with customers to make their networks as trusted as we have made their communications by complementing and refreshing pre-set defenses with active hunting and intrusion analysis.

Significant Changes

FY2011 to FY2012 Comparison Summary

The NSA ISSP top line increased approximately $42.1 M from FY2011 to FY2012. This change is reflected due to the addition of funding for operational network defense activities. Programs receiving funding include: Advanced Network Operations and Intrusion Analysis. Change is also reflected in the request for Overseas Contingency Operations funding.

Changes in 2010, 2011, 2012 between FY2011 PB submission and FY2012 PB submission.

FY2010 total decreased approximately $2.02M in PB12 due to pass thru reductions and economic adjustments.

FY2011 – no changes.

FY2012 total increased approximately $30.48M due to the addition of funding for operational network defense activities and adjustments made due to economic assumptions. Programs receiving funding include: Advanced Network Operations and Intrusion Analysis. Change is also reflected in the request for Overseas Contingency Operations funding.

Defense Business Systems

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

Information Assurance Activities

Summary of individual IA activities funded by NSA IA resources. These activities are organized according to the Department's nine major investment categories:

Computer Network Defense - Programs include: Information Environment Operations, Software Engineering Services, NSA/CSS Threat Operations Center, Mission Enablers, Information Analysis, Technical and Technology Analysis, Interactive On-Net Analysis, Advanced Network Operations, QDR Persistent Monitoring, and NSA/CSS Red Team.

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

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

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

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

Assured Information Sharing - Programs include: Cross Domain Solutions; Mission and Network Systems, Net-centric Security Technologies, Assured Information Sharing Technologies, Enduring Security Framework, Ubiquitous Secure Collaboration, and Commercial Systems Solutions Engineering.

Workforce Development includes Leadership and Workforce Development.

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

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

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

FY10 Major Accomplishments

NSA provided Information Assurance solutions and technical assistance to warfighters in both active theaters. NSA deployed security architecture experts and analysts to the conflict areas and supplied the equipment and software needed to shore-up defenses.

NSA developed and published security guidelines for several mobile devices popular with DoD customers including iPod, Droid, and Blackberry, and developed briefing materials and instructed Federal mobile device users on ways to maintain the security of their devices. NSA developed a software tool to quickly assess website compliance with recommended security configurations and settings and scanned hundreds of military service and DoD web sites, identifying and assisting in the repair of many vulnerabilities. NSA also provided guidance and technical advice to the Federal Chief Information Officer (CIO) Council on how all government websites could do the same, along with recommendations on how these sites could greatly increase their ability to resist and repel many types of intrusions.

NSA accomplished several successful tests and reviews leading toward the next major milestone in the Public Key Infrastructure (PKI) acquisition program and began discussing identity management interoperability with our partners in international defense activities. NSA continued to maintain and improve high assurance systems such as Nuclear Command and Control.

Major Planned Activities

FY12 Major Planned Activities

NSA will continue to support the warfighter, solving emerging problems, and developing strategic information assurance solutions for the battlefield environment. NSA will begin to develop tools the owners of the U.S.'s critical control systems can use to protect that infrastructure against intrusion and co-option. NSA's research program will continue to seek out new and better solutions to the perennially difficult problems associated with three emphasis areas outlined above.

NSA will continue to ensure maintenance of the highest possible cryptographic, and production and dissemination standards for the US's Nuclear Command and Control systems. NSA will advance the state of the art in cryptography through a multi-dimensional research program and by funding research at several centers of excellence. NSA will continue to develop, deploy and enhance the DoD Public Key Infrastructure to ensure secure, dependable identification, and authentication of all users on DoD networks at

all security levels.

In furtherance of the COTS Imperative, NSA will develop innovative partnerships with the information and communications sector to create secure solutions and accelerate DoD access to them. Focus areas for these sorts of partnerships include mobile applications and cloud computing security.

Global Information Grid (GIG) / Net-Centricity

NSA's FY2012 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:

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.

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).

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.

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: IA Systems

Engineering/Architecture and IA Governance, Management, and Administrative Support.

Cryptographic Key Production and Management – Cryptographic Key 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).

Assured Information Sharing – Assured Information Sharing 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.

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: IA Workforce Training.

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.

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.

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

	Dollars in Thousands		
	FY2010	*FY2011*	*FY2012*
NATIONAL SECURITY AGENCY RESOURCE SUMMARY:	**914,934**	**895,229**	**944,068**

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*	*FY2010*	*FY2011*	*FY2012*
			Dollars in Thousands		
O&M, DW	BA 00 N/A		11,573	19,645	14,694
O&M, DW	BA 04 ADMN & SRVWD ACT	CLASSIFIED AND INTELLIGENCE	144,320	146,454	214,248

Procurement

Appropriation	*Budget Activity*	*Budget Line Item*	*FY2010*	*FY2011*	*FY2012*
			Dollars in Thousands		
Procurement, DW	BA 01 MAJOR EQUIPMENT	INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	1,958	1,351	4,406

RDT&E

Appropriation	*Budget Activity*	*Program Element*	*FY2010*	*FY2011*	*FY2012*
			Dollars in Thousands		
RDT&E, DW	BA 00 N/A		5,507	3,405	2,896
RDT&E, DW	BA 07 OPER SYS DEV	0303140G INFORMATION SYSTEMS SECURITY PROGRAM	99,634	112,384	102,120

Initiative Resource Summary:	**262,992**	**283,239**	**338,364**

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

GIG Category: INFORMATION ASSURANCE ACTIVITIES - CRYPTOGRAPHIC SYSTEMS

Operations

Appropriation	*Budget Activity*	*Budget Line Item*	*FY2010*	*FY2011*	*FY2012*
			Dollars in Thousands		
O&M, DW	BA 04 ADMN & SRVWD ACT	CLASSIFIED AND INTELLIGENCE	22,527	19,310	19,927

RDT&E

Appropriation	*Budget Activity*	*Program Element*	*FY2010*	*FY2011*	*FY2012*
			Dollars in Thousands		
RDT&E, DW	BA 00 N/A		700	1,654	0
RDT&E, DW	BA 07 OPER SYS DEV	0303140G INFORMATION SYSTEMS SECURITY PROGRAM	95,368	91,289	97,972

Initiative Resource Summary:	**118,595**	**112,253**	**117,899**

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

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

GIG Category: INFORMATION ASSURANCE ACTIVITIES - CRYPTOGRAPHIC KEY PRODUCTION & MANAGEMENT

Operations

Appropriation	Budget Activity	Budget Line Item	FY2010	FY2011	FY2012
			Dollars in Thousands		
O&M, DW	BA 00 N/A		0	0	2,933

RDT&E

Appropriation	Budget Activity	Program Element	FY2010	FY2011	FY2012
			Dollars in Thousands		
RDT&E, DW	BA 00 N/A		40,782	45,941	33,751
		Initiative Resource Summary:	**40,782**	**45,941**	**36,684**

1204 - PROTECT INFORMATION - PUBLIC KEY INFRASTRUCTURE - INCREMENT TWO (IA G1 PKI) **Major**

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

Operations

Appropriation	Budget Activity	Budget Line Item	FY2010	FY2011	FY2012
			Dollars in Thousands		
O&M, DW	BA 00 N/A		5,257	3,637	47

Procurement

Appropriation	Budget Activity	Budget Line Item	FY2010	FY2011	FY2012
			Dollars in Thousands		
Procurement, DW	BA 00 N/A		33,199	6,902	8,764

RDT&E

Appropriation	Budget Activity	Program Element	FY2010	FY2011	FY2012
			Dollars in Thousands		
RDT&E, DW	BA 00 N/A		8,665	4,711	0
		Initiative Resource Summary:	**47,121**	**15,250**	**8,811**

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

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

Operations

Appropriation	Budget Activity	Budget Line Item	FY2010	FY2011	FY2012
			Dollars in Thousands		
O&M, DW	BA 00 N/A		600	0	0
O&M, DW	BA 04 ADMN & SRVWD ACT	CLASSIFIED AND INTELLIGENCE	2,021	727	666

RDT&E

		Dollars in Thousands	

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

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

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

RDT&E (Continued)

Appropriation	Budget Activity	Program Element	FY2010	FY2011	FY2012
			Dollars in Thousands		
RDT&E, DW	BA 00 N/A		11,780	6,810	4,538
RDT&E, DW	BA 07 OPER SYS DEV	0303140G INFORMATION SYSTEMS SECURITY PROGRAM	7,115	8,197	4,566
		Initiative Resource Summary:	**21,516**	**15,734**	**9,770**

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

GIG Category: INFORMATION ASSURANCE ACTIVITIES - ASSURED INFORMATION SHARING (AIS)

Operations

Appropriation	Budget Activity	Budget Line Item	FY2010	FY2011	FY2012
			Dollars in Thousands		
O&M, DW	BA 00 N/A		965	2,574	3,322
O&M, DW	BA 04 ADMN & SRVWD ACT	CLASSIFIED AND INTELLIGENCE	10,150	12,447	14,732

RDT&E

Appropriation	Budget Activity	Program Element	FY2010	FY2011	FY2012
			Dollars in Thousands		
RDT&E, DW	BA 00 N/A		17,602	11,674	11,581
RDT&E, DW	BA 07 OPER SYS DEV	0303140G INFORMATION SYSTEMS SECURITY PROGRAM	88,456	101,471	103,709
		Initiative Resource Summary:	**117,173**	**128,166**	**133,344**

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

GIG Category: INFORMATION ASSURANCE ACTIVITIES - DEFENSE INDUSTRIAL BASE CYBER SECURITY/IA

Operations

Appropriation	Budget Activity	Budget Line Item	FY2010	FY2011	FY2012
			Dollars in Thousands		
O&M, DW	BA 04 ADMN & SRVWD ACT	CLASSIFIED AND INTELLIGENCE	3,000	3,000	4,865
		Initiative Resource Summary:	**3,000**	**3,000**	**4,865**

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

GIG Category: INFORMATION ASSURANCE ACTIVITIES - ENGINEERING AND DEPLOYMENT

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

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

GIG Category: INFORMATION ASSURANCE ACTIVITIES - ENGINEERING AND DEPLOYMENT

Operations

Appropriation	Budget Activity	Budget Line Item	FY2010	FY2011	FY2012
			Dollars in Thousands		
O&M, DW	BA 00 N/A		6,096	6,077	7,324
O&M, DW	BA 04 ADMN & SRVWD ACT	CLASSIFIED AND INTELLIGENCE	77,280	88,212	94,063

Procurement

Appropriation	Budget Activity	Budget Line Item	FY2010	FY2011	FY2012
			Dollars in Thousands		
Procurement, DW	BA 01 MAJOR EQUIPMENT	INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	114	73	174

RDT&E

Appropriation	Budget Activity	Program Element	FY2010	FY2011	FY2012
			Dollars in Thousands		
RDT&E, DW	BA 00 N/A		3,638	3,600	3,666
RDT&E, DW	BA 07 OPER SYS DEV	0303140G INFORMATION SYSTEMS SECURITY PROGRAM	34,437	27,315	27,465

Initiative Resource Summary:	**121,565**	**125,277**	**132,692**

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

GIG Category: INFORMATION ASSURANCE ACTIVITIES - CRYPTOGRAPHIC KEY PRODUCTION & MANAGEMENT

Operations

Appropriation	Budget Activity	Budget Line Item	FY2010	FY2011	FY2012
			Dollars in Thousands		
O&M, DW	BA 04 ADMN & SRVWD ACT	CLASSIFIED AND INTELLIGENCE	80,855	81,376	86,717

Procurement

Appropriation	Budget Activity	Budget Line Item	FY2010	FY2011	FY2012
			Dollars in Thousands		
Procurement, DW	BA 01 MAJOR EQUIPMENT	INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	1,929	1,122	1,856

RDT&E

Appropriation	Budget Activity	Program Element	FY2010	FY2011	FY2012
			Dollars in Thousands		
RDT&E, DW	BA 00 N/A		10,304	0	0
RDT&E, DW	BA 07 OPER SYS DEV	0303140G INFORMATION SYSTEMS SECURITY PROGRAM	43,391	40,708	35,816

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

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

GIG Category: INFORMATION ASSURANCE ACTIVITIES - CRYPTOGRAPHIC KEY PRODUCTION & MANAGEMENT

	FY2010	FY2011	FY2012
Initiative Resource Summary:	**136,479**	**123,206**	**124,389**

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	FY2010	FY2011	FY2012
O&M, DW	BA 04 ADMN & SRVWD ACT	CLASSIFIED AND INTELLIGENCE	18,112	18,358	17,890

RDT&E

Dollars in Thousands

Appropriation	Budget Activity	Program Element	FY2010	FY2011	FY2012
RDT&E, DW	BA 07 OPER SYS DEV	0303140G INFORMATION SYSTEMS SECURITY PROGRAM	697	286	312
		Initiative Resource Summary:	**18,809**	**18,644**	**18,202**

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

GIG Category: INFORMATION ASSURANCE ACTIVITIES - IA OPERATIONAL RESILIENCY

Operations

Dollars in Thousands

Appropriation	Budget Activity	Budget Line Item	FY2010	FY2011	FY2012
O&M, DW	BA 04 ADMN & SRVWD ACT	CLASSIFIED AND INTELLIGENCE	893	524	666

RDT&E

Dollars in Thousands

Appropriation	Budget Activity	Program Element	FY2010	FY2011	FY2012
RDT&E, DW	BA 07 OPER SYS DEV	0303140G INFORMATION SYSTEMS SECURITY PROGRAM	9,611	7,177	9,483
		Initiative Resource Summary:	**10,504**	**7,701**	**10,149**

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

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

Operations

Dollars in Thousands

Appropriation	Budget Activity	Budget Line Item	FY2010	FY2011	FY2012
O&M, DW	BA 00 N/A		8,325	7,937	0

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

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

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

Procurement

			Dollars in Thousands		
Appropriation	*Budget Activity*	*Budget Line Item*	*FY2010*	*FY2011*	*FY2012*
Procurement, DW	BA 00 N/A		0	0	2,351

RDT&E

			Dollars in Thousands		
Appropriation	*Budget Activity*	*Program Element*	*FY2010*	*FY2011*	*FY2012*
RDT&E, DW	BA 00 N/A		8,073	8,881	6,548
		Initiative Resource Summary:	**16,398**	**16,818**	**8,899**