CLASSIFICATION:

EXHIBIT R-2, RDT&E Budget Item Justification	DATE: **February 2006**
APPROPRIATION/BUDGET ACTIVITY **RESEARCH DEVELOPMENT TEST & EVALUATION, NAVY / BA-7**	R-1 ITEM NOMENCLATURE 0303140N Information Systems Security Program (ISSP)

COST ($ in Millions)	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Total PE Cost	**25.696**	**21.569**	**23.037**	**28.535**	**33.100**	**31.316**	**32.601**
0734 Information Systems Security	**15.799**	**18.196**	**21.038**	**26.347**	**30.955**	**29.119**	**30.371**
0734 Communications Security	**2.089**	**2.073**	**1.999**	**2.188**	**2.145**	**2.197**	**2.230**
9999 Congressional Plus Up	**7.808**	**1.300**					
Quantity of RDT&E Articles							

(U) A. MISSION DESCRIPTION AND BUDGET ITEM JUSTIFICATION:

(U) The goal of the Navy Information Systems Security Program (ISSP) is to ensure the continued protection of Navy and Joint information, telecommunications, and information systems from hostile exploitation and attack. The ISSP is the Navy's implementation of statutory and regulatory requirements specified in Presidential Decision Directive 63, the Computer Security Act of 1987 (Public Law 100-235), Appendix III of Office of Management and Budget (OMB) Circular A-130, and DOD Directive 8500.1. ISSP activities address the triad of Defensive Information Operations defined in Joint Publication 3-13; protection, detection, and reaction. Evolving detection and reaction responsibilities extend far beyond the traditional ISSP role in protection or Information Security (INFOSEC). Focused on FORCEnet supporting the highly mobile forward-deployed subscriber, the US Navy's implementation of Network-Centric Warfare (NCW) places demands upon the ISSP, as the number of users dramatically increases and the criticality of their use escalates. Today, the ISSP protects an expanding core service critical to the effective performance of the Navy's mission, supported by Mission Assurance Category 1 systems.

(U) The interconnectivity of Naval networks, connections to the public information infrastructure, and their use in modern Naval and Joint warfighting means that FORCEnet is a more easily attainable and extremely high value target. An adversary has a much broader selection of attack types from which to choose than in the past. In addition to the traditional attacks that involve the theft or eavesdropping of information, United States Navy (USN) information and telecommunications systems face advanced attacks involving malicious changes to critical information, changes to the functioning of critical systems, denial of service (jamming), and the destruction of systems and networks. Since many Naval information systems are based on commercially available technologies, an adversary often has access to the very technologies they want to exploit.

(U) The rapid rate of change in the underlying commercial and government information infrastructures makes the provision of security an increasingly complex and dynamic problem. ISSP provides the Navy's war fighter the essential information trust characteristics of availability, confidentiality, integrity, authentication, privacy, and non-repudiation. Information Assurance (IA) technology mix and deployment strategies must evolve quickly to meet the rapidly evolving threats and vulnerabilities. No longer can information security divorce the information infrastructure.

CLASSIFICATION:

EXHIBIT R-2, RDT&E Budget Item Justification	DATE: **February 2006**
APPROPRIATION/BUDGET ACTIVITY **RESEARCH DEVELOPMENT TEST & EVALUATION, NAVY BA-7**	R-1 ITEM NOMENCLATURE 0303140N Information Systems Security Program (ISSP)

(U) The Navy ISSP RDT&E program works to provide the Navy with these essential IA elements: (1) Assured separation of information levels and user communities, including coalition partners; (2) Assurance of the telecommunications infrastructure; (3) Assurance of Joint user enclaves, using a Defense in Depth architecture; (4) Assurance of the computing base and information store; and, (5) Supporting assurance technologies, including a Public Key Infrastructure (PKI) and directories. The goal of all ISSP RDT&E activities is to produce the best USN operational system that can meet the certification and accreditation requirements outlined in Department of Defense (DOD) Instruction 5200.40 (new DODI 85xx series pending). Modeling DOD and commercial information and telecommunications systems evolution (rather than being one-time developments), the ISSP RDT&E program must be predictive, adaptive, and technology coupled. The program develops frameworks, architectures, and products based on mission threats, information criticality, exploitation risks, risk management, and integrated Joint information system efforts.

(U) All ISSP RDT&E efforts comply with the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113) as implemented through Office of Management and Budget Circular A-119 of February 10, 1998, DoD Instruction 4120.24, Defense Standardization Program (DSP), and DoD Instruction 4120.3-M, Defense Standardization Program Policies and Procedures. The predominant commercial standards bodies in ISSP-related matters include International Standards Organization (ISO), American National Standards Institute (ANSI), Institute of Electrical and Electronics Engineers (IEEE), Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C), and National Institute of Standards and Technologies (NIST). The Joint interoperability required in today’s telecommunications systems makes standards compliance a must, and the ISSP RDT&E program complies with the Joint Technical Architecture. The FORCEnet architecture and standards documents reflects this emphasis on interoperable standards.

(U) The interconnection of FORCEnet into the DoD Global Information Grid (GIG) requires all ISSP RDT&E activities to adopt a minimum standard of “best commercial IA practice.” The ISSP RDT&E program examines commercial technologies to determine their fit within the USN architectures, provides feedback to vendors about what the Navy requires, and participates in the standards bodies themselves. When necessary to protect mission critical systems specified in Clinger/Cohen Act, the ISSP RDT&E develops or tailors commercial and government technologies, standards, and processes to meet Navy-unique requirements; prototypes systems or portions of systems and examines their utility in operational Navy settings; and, provides IA expertise and engineering to Navy and Joint information system developments. All ISSP technology development efforts solve specific Navy and Joint IA problems using techniques that speed transition to procurement as soon as ready.

(U) JUSTIFICATION FOR BUDGET ACTIVITY: This program is funded under OPERATIONAL SYSTEMS DEVELOPMENT because it encompasses engineering and manufacturing development for upgrade and integration of existing, operational systems. This includes cryptographic systems required to protect information defined in 40 USC Chapter 25 Sec 1452, and the ISSP cryptographic RDT&E program is the implementation of requirements in Executive Orders 12333 and 12958 and National Security Decision Directive 145.

CLASSIFICATION:

EXHIBIT R-2, RDT&E Budget Item Justification	DATE: **February 2006**
APPROPRIATION/BUDGET ACTIVITY **RESEARCH DEVELOPMENT TEST & EVALUATION, NAVY/BA-7**	PROGRAM ELEMENT NUMBER AND NAME 0303140N Information Systems Security Program (ISSP)

(U) B. PROGRAM CHANGE SUMMARY:

(U) Funding:	FY 2005	FY 2006	FY 2007
FY 06 President's Budget:	26.511	28.660	33.490
FY 07 President's Budget Submit:	25.696	21.569	23.037
Total Adjustments	-0.815	-7.091	-10.453

Summary of Adjustments

FORCEnet Information Assurance (IA) Management Tools	0	0	-603
Contract Support Reduction	0	0	-1392
Information Systems Security Program (ISSP) Adjustment	0	0	-8400
NWCF Civpers Efficiencies	0	0	-211
Small Business Innovation Research (SBIR) Tax	-288	0	0
Nuclear Physical Security (OSD-09)	5	0	0
Inflation Adjustment	0	0	146
CIVPERS Pay Raise Rate Changes	0	0	7
Sec. 8125: Revised Economic Assumptions	0	-131	0
Congressional Reduction in base program	0	-7960	0
Congressional Add	0	1300	0
Congressional Action 1% Reduction	0	-300	0
Department of Energy Transfer	-21	0	0
Execution Realignments by Fund Holder	-511	0	0
Subtotal	-815	-7,091	-10,453

(U) Schedule:

(U) Technical:

N/A.

CLASSIFICATION:

EXHIBIT R-2, RDT&E Budget Item Justification	DATE: February 2006
APPROPRIATION/BUDGET ACTIVITY **RESEARCH DEVELOPMENT TEST & EVALUATION, NAVY/BA-7**	PROGRAM ELEMENT NUMBER AND NAME 0303140N Information Systems Security Program (ISSP)

(U) C. OTHER PROGRAM FUNDING SUMMARY:

Line Item No. & Name	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
OPN 3415 Info Sys Security Program (ISSP)	91.924	97.478	101.749	113.839	132.029	156.804	159.159

(U) D. ACQUISITION STRATEGY: *

EKMS Phase V- The Navy's ISSP EKMS program is linked to NSA’s strategy in implementing EKMS in evolutionary phases and migrating to Key Management Initiative (KMI). NSA is the lead for the joint EKMS effort and has been developing and certifying EKMS devices and capabilities in an evolutionary approach. EKMS Phase V is a major component evolving to KMI Common Increment 2 (CI-2). KMI is currently a Pre-Major Automated Information System (MAIS) program assigned to NSA. Therefore, it is crucial that the Research and Development efforts of EKMS coincide with those of KMI. Navy's EKMS requires Research, Development, Test and Evaluation (RDT&E) funding over the Future Years Defense Program (FYDP) to ensure the Navy infrastructure evolves with the EKMS phases, supports additional devices certified by NSA and supports the migration of EKMS to KMI CI-2. This will require the modification of the Navy EKMS Net Key Server.   PEO C4I & Space/PMW160 is collaborating with Naval Research Lab (NRL) to integrate COTS/GOTS devices into the Navy architecture to be compatible with Phase 5 and KMI architectures. These efforts require close work with NSA and the other services to ensure no impact on current operations and minimum impact on EKMS Phase 5 as it evolves to KMI CI-2. PMw160 procures National Security Agency (NSA) certified COTS/GOTS devices to support Navy requirements. The EKMS Phase V program will utilize existing competitively awarded NSA and SSC contracts for development and implementation of type 1 certified COTS/GOTS devices for initial production phases, with plans to initiate innovative contracting methods and types consistent with current ASN/RDA policies to reduced cost and the streamline the integration, installation, logistics and training efforts.

Crypto Modernization (KW-46 Replacement)-The KW-46 is a device that performs on-line decryption of digital messages, record, and data traffic over the broadcast system at data rates from 50 to 9,600 bits per second (BPS) that processes information up to and including TOP SECRET. The KWR-46 is used primarily on ships and submarines while the KWT-46 is located exclusively on shore sites, consisting of the KWT-46 transmitter and the KWR-46 receiver, **which are no longer in production**.   The PMW 160 is also evaluating acquisition development replacements of the KG-45, KL-51, KG-68B cryptographic devices per the UCD effort. Navy is currently refining the requirement specs, preparing formal Analysis of Alternatives, Request For Information (RFI’s), and LCEE's to be completed in FY 06 and the plan is to competitively award the development contract by 1Q FY07.

Crypto Modernization (Universal Crypto Device)- Navy is currently refining the requirement specs, preparing formal Analysis of Alternatives, Request For Information (RFI’s), and LCEE's to be completed in FY 06 and the plan is to competitively award the development contract by 1Q FY08. The evaluation of requirements of Crypto Modernization (Thorton-KEESEE) cryptographic system will also necessitate preparation of formal AOA, RFI within FY06 & FY07.

*** Not required for Budget Activities 1,2,3, and 6**

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification						DATE: **February 2006**	
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT NUMBER AND NAME 0303140N Information Systems Security Program (ISSP)			PROJECT NUMBER AND NAME 0734 Information Systems Security			
COST ($ in Millions)	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Project Cost	**15.799**	**18.196**	**21.038**	**26.347**	**30.955**	**29.119**	**30.371**
RDT&E Articles Qty							

(U) A. MISSION DESCRIPTION AND BUDGET ITEM JUSTIFICATION: The Navy Information Systems Security Program (ISSP), RDT&E provides Information Assurance (IA) solutions for the United States Navy (USN) forward deployed, highly mobile information subscriber. FORCEnet relies upon an assured information infrastructure, and the ISSP RDT&E program architects, engineers, and provides the Quality of Assurance (QoA) consistent with risks faced. The ISSP addresses engineering design, development, modeling, test, and evaluation for the unique IA challenges associated with the highly mobile, dispersed, bandwidth limited, and forward-tactical connected USN communications systems.

(U) ISSP RDT&E must work closely within the Navy's Information Operations – Exploit (Signals Intelligence - SIGINT) and Information Operations – Attack (INFOWAR) communities. ISSP RDT&E developed systems must dynamically change the Navy's current assurance vector, based upon operational indications and warnings. To ensure interoperability, ISSP RDT&E must integrate fully with the FORCEnet and Maritime Cryptologic Architectures. ISSP RDT&E developed systems can provide the trigger for offensive warfare activities, such as those developed by the Naval Information Warfare Activity (NIWA).

(U) This program element includes a rapidly evolving design and application engineering effort to modernize National-Security-grade (type-1) cryptographic equipment and ancillaries with state-of-the-art replacements in order to counter evolving and increasingly sophisticated threats. Communication Security (COMSEC) and Transmission Security (TRANSEC) evolution is from stand-alone dedicated devices to embedded modules incorporating National Security Agency (NSA) approved cryptographic engines, loaded with the certified algorithms and key, and interconnected via industry-defined interfaces. This includes the DoD GIG Capabilities Requirements Document (CRD) requirement for the development of Content Based Encryption (CBE) continuing in FY 06 -11.

(U) In addition to protecting National Security information, ISSP RDT&E must provide enterprise-wide assurance for statutorily protected information under the Privacy Act of 1974, Computer Matching and Privacy Protection Act of 1988, Medical Records Confidentiality Act of 1995, Model State Public Health Privacy Act, 45 CFR subtitle A sub-chapter C, parts 160- 164, 1999, and the Federal Education Records Privacy Act. ISSP RDT&E efforts must also provide assurance to the broad spectrum of Sensitive-but-Unclassified (SBU) information such as financial, personnel, contractor proprietary, and procurement sensitive.

(U) The ISSP today includes much more than legacy Computer Security (COMSEC) and Network Security (NETSEC) technology. IA, or Defensive Information Operations, exists to counter a wide variety of threats in a Navy environment. ISSP activities cover all telecommunications systems, and RDT&E projects must provide protection, detection, and reaction capabilities to the operational commander. ISSP RDT&E provides dynamic risk managed IA solutions to the Navy Information Infrastructure, not just security devices placed within a network.

(U) Few technology areas change as fast as telecommunications and computers, and IA must keep pace. This results in the continuing need to evaluate, develop, and/or test IA products and approaches. Technology base efforts include developing or applying: (1) new secure voice prototypes; (2) technology for a new family of programmable COMSEC and TRANSEC modules; (3) security appliances and software for switched and routed networks; (4) technology to interconnect networks of dissimilar classification, known as Cross Domain Security; (5) techniques for assuring code and data residing in and transiting the Navy's computing base and information store; and (6) PKI and associated access control technologies (such as SmartCards and similar security tokens).

(U) The resulting expertise applies to a wide variety of Navy development programs that must integrate IA technology. Unlike traditional single-product development programs, the ISSP RDT&E holds a unique Navy-enterprise responsibility outlined in SECNAVINST 5239.3 and OPNAVINST 5239.1B.

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2006**
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT NUMBER AND NAME 0303140N Information Systems Security Program (ISSP)	PROJECT NUMBER AND NAME 0734 Information Systems Security

(U) The ISSP RDT&E efforts must conclude with certified and accredited systems. This requires (1) Assured separation of information levels and user communities, including coalition partners; (2) Assurance of the telecommunications infrastructure; (3) Assurance of Joint user enclaves; (4) Assurance of the computing base and information store; and, (5) Supporting assurance technologies, including Public Key Infrastructure (PKI) and directories. To ensure interoperability and commercial standards compliance, these efforts often encompass the research, selective evaluation, integration, and test of Commercial off-the-shelf (COTS)/Non-developmental Item (NDI) IA security products. For example, evaluation may include defensible network boundary capabilities such as firewalls, secure routers and switches, guards, Virtual Private Networks (VPN), and network Intrusion Prevention Systems (IPS).

(U) The current operating environment has virtually eliminated the traditional distinction between telecommunications and information systems. Because IA is a cradle-to-grave enterprise-wide discipline, this program applies the technology and methodology to systems in development, production and operation, and develops the infrastructure needed to support and evaluate the security of deployed systems. The following describes several major ISSP technology areas:

(U) Under the Navy Secure Voice (NSV) program, ISSP RDT&E assesses technology to provide high grade, secure tactical and strategic voice connectivity.

(U) Under the Navy Cryptographic Modernization Program, ISSP RDT&E provides high assurance and other cryptographic technologies protecting information and telecommunication systems.

(U) Under the Navy Security Management Infrastructure (SMI) program, ISSP RDT&E develops, evaluates, and applies new emerging technology and enhanced capabilities to the Electronic Key Management System (EKMS) and other Navy Information Systems. Additional efforts will focus on the architecture, design, and development of systems to manage the security parameters (i.e., cryptographic keys) necessary to the operation of the systems developed by the Secure Data and Secure Voice portions of the ISSP. This includes the application of PKI and Certificate Management Infrastructure (CMI) technology, and the development of improved techniques for key and certificate management to support emerging, embedded cryptographic technology.

(U) Under the Secure Data program, efforts focus on architectures, designing, acquiring, demonstrating and integrating the IA technologies into FORCEnet and the Navy Marine Corp Intranet (NMCI). This portion of the ISSP supports delivery of network security engineering expertise needed to support the NMCI, OCONUS Navy Enterprise Network (ONEnet) , and the Integrated Shipboard Network Systems (ISNS), along with constituent systems such as Advanced Digital Network System (ADNS), Global Command and Control System - Maritime (GCCS-M). It includes activities to:

- Ensure that USN telecommunications and networks follow a consistent architecture and are protected against denial of service.
- Ensure that all data within the USN Enterprise is protected in accordance with its classification and mission criticality, as required by law.
- Provide the ability to protect from, react to, and restore operations after an intrusion or other catastrophic event.
- Support the USN Computer Network Defense (CND) Service Provider Enabler by providing IA response to Information Operation Conditions (INFOCONs).
- Defend against the unauthorized modification or disclosure of data sent outside enclave boundaries.
- Provide a risk-managed means of selectively allowing essential information to flow across the enclave boundary.
- Provide strong authentication of users sending or receiving information from outside their enclave.
- Defend against the unauthorized use of a host or application, particularly operating systems.
- Maintain configuration management of all hosts to track all patches and system configuration changes.
- Ensure adequate defenses against subversive acts of trusted people and systems, both internal and external.

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2006**
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT NUMBER AND NAME 0303140N Information Systems Security Program (ISSP)	PROJECT NUMBER AND NAME 0734 Information Systems Security

- Provide a cryptographic infrastructure that supports key, privilege and certificate management; and that enables positive identification of individuals utilizing network services.
- Provide an intrusion detection, reporting, analysis, assessment, and response infrastructure that enables rapid detection and reaction to intrusions and other anomalous events, and that enables operational situation awareness.

(U) JUSTIFICATION FOR BUDGET ACTIVITY: This program is funded under OPERATIONAL SYSTEMS DEVELOPMENT because it encompasses engineering and manufacturing development for upgrade of existing, operational systems.

(U) METRICS: Earned Value Management (EVM) is used for metrics reporting and risk management.

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2006**
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT NUMBER AND NAME 0303140N Information Systems Security Program (ISSP)	PROJECT NUMBER AND NAME 0734 Information Systems Security

(U) B. Accomplishments/Planned Program

	FY 05	FY 06	FY 07
Computer Network Defense (CND)	2.834	5.009	5.592
RDT&E Articles Quantity			

FY05 Plans include:
$2,834 - Integrated security products and new technologies for robust Computer Network Defense (CND) for both shore and afloat installation. Effort focused on CND system development to address recurring exploits against forward deployed units; to integrate CND management tools into a cohesive suite for unit level defense. Development effort to extend the security boundaries beyond the NOC's to enforce adaptive network security based on changing INFOCON policies, operator needs, and operational environments were evaluated. Provided system security engineering design, modeling, technical evaluations, testing, and validation to formulate Commercial and Government product infusion for CND enhancement. Developed advanced IA tool kits to assist information system security managers to maintain computer network security posture and provide for vulnerability self assessment and remediation verification. Assessed security systems to field capabilities to minimize the impact of the insider threat and to minimize the potential damage inflicted on information integrity or computer-network information systems. Enhanced CND with leading technologies to block attacks with intrusion prevention management; to counter increasing threats posed by system vulnerabilities, malicious code, and malevolent insiders. Addressed user authorization and authentication techniques for system administration, remote user access, and enforce access controls on critical computer-network components. IA network components were reviewed for application on UNCLASSIFIED through SECRET application networks and coordination with host application requirements to provide the broadest support solution as possible.

FY 06 Plans include:
$5,009 - Continue to integrate security products and new technologies for robust Computer Network Defense (CND) for both shore and afloat installation. Provide IA engineering design (+$1.644M), evaluation, and testing techniques from end-to-end and information source-to-sink to satisfy the IA element of maintaining availability. Includes IA appliances, software, and implementation techniques for policies such as IAVA requirements. Begin development of a tier level management system (+$2M) between Unit Level Ships and Global Enterprise Management for real-time display of security risk as: Computer-Network Threats, Vulnerabilities, and Critical System Security Performance. Begin development of a Global Enterprise Management system to integrate a secure means of hierarchically managing Network Operating Center security systems, Ship Security Monitors, and other Network Security Monitoring products. Begin development of enhanced fielded Security Management Tools (+$1.365M) with new capabilities to support system configuration management and monitoring. Support development of online engineering support to access subject matter security system experts; automate security system IAVA distributions, web based information server, NOC site ‘As Built’ Configuration Data, and Emergency Restoration Files. Develop an IAVA verification assessment system to status Network Operation Center IAVA status for fielded security equipment.

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification			DATE: **February 2006**
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT NUMBER AND NAME 0303140N Information Systems Security Program (ISSP)	PROJECT NUMBER AND NAME 0734 Information Systems Security	

FY 07 Plans include:
$5,592 - Provide the broadest range of Information Assurance (IA) research and development support across Joint, Fleet, and ashore networks. Provide on-going security design engineering of new ships, aircraft, and submarines to ensure reduced manning and greater operational dependency on networks. Provide IA engineering design (+$2.905M), evaluation, and testing techniques from end-to-end, through base-band networks, RF communications links, and information source-to-sink to satisfy the IA element of maintaining availability. Includes IA appliances, software, and implementation techniques for policies such as IAVA requirements, INFOCON response, and USN firewall policy. Provide continuous development of a tier level management system (+$1.202M) between Unit Level Ships and Global Enterprise Management for real-time display of security risk. Continue the development of enhance fielded Security Management Tools (+$0.970M) with new capabilities to support system configuration management and monitoring. Begin development of improved real-time computer-network security policy administration (+$0.515M) with analytical tools to identify application or computer-network issues with operational compliance. Establish a management process to enforce common unit level fleet firewall policies across the Navy Network Enterprise using products/techniques to centrally manage and push security policies to controllable devices such as Firewalls, Intrusion Prevention Systems (IPS), and Filtering Routers at unit level ships and fleet Network Operation Centers.

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification	DATE: **February 2006**

APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	0734 Information Systems Security

	FY 05	FY 06	FY 07
Crypto	3.780	4.627	5.402
RDT&E Articles Quantity			

FY05 Plans Include:
$3,780 - Provided sustained IA security system engineering support for the development, evaluation and integration of emerging cryptographic products/components and devices, including type-1 US only, allied and coalition, and commercial-off-the-shelf. Includes design, development, testing, and evaluation of link, network, session, data transfer devices, and associated equipments. Provided IA engineering support for the development of Crypto Modernization products and components KG-3X, KG-40AR, CTIC/CDH, IFF Mode 5, Link Encryption Family, Universal Crypto Device (UCD)/Expendable Crypto devices, and Next Generation COMSEC devices such as PEIP follow-on, Modern Legacy Crypto Solution, HAIPE and KW-46, KG-45, KL-51, KG-68B based on UCD development. Continued to provide the coordination of development efforts with the Information Systems Security Office at the National Security Agency. Continue to develop specific design, testing, and evaluation assistance for new USN platforms and assists in defining embedded cryptographic product engineering requirements. Continued to develop, model, test, and evaluated deployment of architectures supporting next-generation structures such as remote-keyed, gateways, "lights-out" facilities, and wireless devices. Includes architecture modeling, end-to-end security analysis, and integration cryptographic products into USN platform specific architecture. Provided continuous support for the development and integration of embedded cryptographic products.

FY06 Plans Include:
$4,627 - Provide for the integration of cryptographic products, including type-1 US only, allied and coalition, and commercial-off-the-shelf. Provide support of development efforts in coordination with the Information Systems Security Office, Joint Services, and the National Security Agency. Provide (+$1.700M) specific design, testing, and evaluation assistance for new USN platforms and assists in defining embedded cryptographic product engineering requirements. Provide sustained IA engineering support for the development, integration, and installation of Crypto Modernization products including KG-3X, KG-40AR, CTIC/CDH, IFF Mode 5, Link Encryption Family, Universal Crypto Device (UCD)/Expendable Crypto devices, and Next Generation COMSEC devices such as: PEIP follow-on, Modern Legacy Crypto Solution, KIV-7M/KIV-19M Walburn and SAVILLE (+$.797M), Thorton-KEESEE (+$2.130M) and KW-46, KG-45, KL-51, KG-68B (based on UCD development) sustainment/replacement. Additional efforts have to also focus on replacing NSA decertified products. Continue development and integration on the next generation network encryption devices, to include application and implementation of HAIPE in transformational architectures such as FORCEnet and JTRS WNW, and analysis of critical harmonization/integration solutions between modernized INE devices and Key Management, FNBDT and Wireless standards to ensure net-centric capability. Research potential uses of type-2 & 3 for use in type-1 historical environments.

FY07 Plans Include:
$5,402 - Continue to provide cryptographic products, including type-1 US only, allied and coalition, and commercial-off-the-shelf. Provide consistent IA engineering support for the development and integration of Crypto Modernization (+$2.377M) products including KG-3X, KG-40AR, CTIC/CDH, IFF Mode 5, Link Encryption Family, Universal Crypto Device (UCD)/Expendable Crypto devices, and Next Generation COMSEC devices such as: PEIP follow-on, KIV-19, KIV 7M, KG-194 (Walburn) (+$.594M), Thorton-KEESEE (+$2.431M) and KW-46, KG-45, KL-51, KGV-68B (based on UCD development). Continue development and integration on the next generation network encryption devices, to include application and implementation of HAIPE in transformational architectures such as FORCEnet and JTRS WNW, and develop integration solutions for modernized INE devices and Key Management, FNBDT and Wireless capabilities. Continue to research and develop potential uses of type-2 & 3 for use in type-1 historical environments.

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2006**
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT NUMBER AND NAME 0303140N Information Systems Security Program (ISSP)	PROJECT NUMBER AND NAME 0734 Information Systems Security

	FY 05	FY 06	FY 07
Information Assurance Readiness	0.298	0.000	0.270
RDT&E Articles Quantity			

FY05 Plans include:
$298 - Provided systems security engineering support to all USN organizations in the certification and accreditation of emerging information systems. Provided Antivirus Tools Support and Capabilities for R&D support systems and software to meet Navy Anti-Virus requirements. Completed the development and integration of tools for automatic updating and incorporation of EKMS certification and accreditation information. Completed integrations of Perl-based custom sniffer script to monitor network traffic the following into the INFOSEC Web site. Continue to update and maintain the USN infrastructure security policy. Continued follow-on development and integration of NIC Web single point-of-presence website for POR compliance reporting, fleet information and patch data, initially addressing PEO-C4I POR/CMS systems and adding other Navy SYSCOMs and PEOs.

FY06 N/A

FY07 Plans include:
$270 - Continue to provide systems security engineering support to all USN organizations in the certification and accreditation of information systems. A primary responsibility is the C&A for the Navy Marine Corps Intranet and various coalition networks. Provide continued Antivirus Tools support and capabilities for R&D support systems and software to meet Navy Anti-Virus requirements.

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2006**
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT NUMBER AND NAME 0303140N Information Systems Security Program (ISSP)	PROJECT NUMBER AND NAME 0734 Information Systems Security

	FY 05	FY 06	FY 07
Secure Voice	0.895	0.624	0.700
RDT&E Articles Quantity			

FY05 Plans Include:
$895 - Continued development and integration efforts of Secure Communication Interoperability Protocol (SCIP, formally Future Narrowband Digital Terminal (FNBDT)) standard compression to provide the Sea-Shore and Sea-Shore-Sea Secure Voice communications. Develop survey for collecting secure voice mission and operational requirements from users for a new COMSEC device that will replace various legacy voice devices. Develop and test the Tactical Shore Gateway (TSG) to provide interoperability between tactical secure voice equipment (i.e., KY-57 KY58, KY-68, KY99A, KY-100 and ANDVT) and STE/FNBDT devices as well as secure conference capabilities. Researching development of a Secure Voice/Data Terminal (e.g., Universal Voice Terminal (UVT) and Personal Secure Telephone (PST)) that uses new variable data rate encryption and voice algorithms (Secure Voice Core Technology) and supports low bandwidth secure voice and data applications over High Frequency (HF), Ultra High Frequency (UHF), Extreme High Frequency (EHF), and Super High Frequency (SHF) designated Radio Frequency (RF) mediums. Develop the first draft version of 21st Century Secure Voice Architecture (i.e., Naval Advanced Secure Voice Architecture, NASVA) to establish a baseline for synchronized secure voice evolution in net-centric environment.

FY06 Plans Include:
$624 - Continue development of the 21st Century Secure Voice Architecture (NASVA) to provide a transition to bridge from channel-centric to net-centric Secure Voice capability, guide the next generation of Secure Voice and facilitate decision making on systems to be refreshed, retired and/or replaced. Continue development of the variable data rate voice algorithm (a component of Secure Voice Core Technology). Research and develop a compression technique (SCIP IWF or gateway) to allow SCIP signaling be transmitted off-ship for underway submarines.

FY07 Plans Include:
$700 - Complete development and integration test of submarine SCIP IWF/gateway to provide off-ship secure communication capabilities while underway. Begin development and test a SCIP IWF to provide off-ship secure voice communications to underway Military Sealift Command ships and Coast Guards ships. Complete development of the Variable Data Rate Voice Encoder and its baseline interface software. Initiate generation of baseline functionality (derived from operational and mission requirements and new technologies) and design of a functional model for development of next generation secure voice products (UVT and PST).

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2006**
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT NUMBER AND NAME 0303140N Information Systems Security Program (ISSP)	PROJECT NUMBER AND NAME 0734 Information Systems Security

	FY 05	FY 06	FY 07
Cross Domain Solutions (CDS)	0.905	1.296	0.712
RDT&E Articles Quantity			

Note: Multiple Security Level (MSL) nomenclature changed to Cross Domain Solutions (CDS)

FY05 Plans include:
$905 - Continued to provide systems security engineering development, testing, and evaluation for multi-level security solutions, including complicated evaluations involving allied and coalition participation. Continued to examine, evaluate and analyze multi-level aware applications and technologies including databases, web browsers, routers/switches, etc. Continue to develop and integrate MSL/CDS prototype architecture at NOC facilities. Continued development of Block One CDS solution as a follow-on to Block Zero. The Block One CDS solution focused on providing a robust coalition interoperability using Multi-Level Thin Client (MLTC), secure guarding devices and afloat coalition network systems.

FY06 Plans include:
$1,296 - Provide systems security engineering for the development, testing, and evaluation of complex multi-level security solutions, including complicated evaluations involving allied and coalition participation. Analyze, evaluate and examine multi-level aware applications and technologies including databases, web browsers, routers/switches, etc. Develop and integrate MSL/CDS prototype architecture at NOC facilities. Continue development and integration of Block One CDS solutions to focus on providing a robust coalition interoperability using Multi-Level Thin Client (MLTC), secure guarding devices and afloat coalition network systems. Begin development of follow-on Block Two CDS upgrade to reduce footprint and provide reconfigurable, enabling IT network architecture for fleet combatants as well as ashore command centers that support data transfer service at multiple security levels.

FY07 Plans include:
$712 - Continue to provide systems security engineering development, testing, and evaluation for multi-level security solutions, including complicated evaluations involving allied and coalition participation. Examine and evaluate multi-level aware applications and technologies including databases, web browsers, routers/switches, etc. Develop and integrate MSL/CDS prototype architecture at NOC facilities.

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2006**
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT NUMBER AND NAME 0303140N Information Systems Security Program (ISSP)	PROJECT NUMBER AND NAME 0734 Information Systems Security

	FY 05	FY 06	FY 07
Key Management Infrastructure	5.310	3.869	4.734
RDT&E Articles Quantity			

FY05 Plans include:
$5,310 - Began security and functionality testing and evaluation of PKI tokens, readers and middleware for the SIPRNET. Began prototyping and certification/accreditation of the Navy's Key management system. Began Common User Application Software (CUAS), Data Mgmt Device (DMD) and Simple Key Loader (SKL) development and integration. Begin and complete Mode 5 Identify Friend or Foe (IFF) (Time of Day) design and development. Began development and integration of Future fill device. Provided engineering design evolution for the supporting key management infrastructure, to include: Electronic Key management System (EKMS Phase IV for Tier 0,1,2,3), Defense Messaging System (DMS) specific products, DOD Public Key Infrastructure (DOD-PKI), and additional Certificate Management Infrastructures (CMI). Performed design, evaluation, integration, and test of key-related platforms, such as smart cards, authentication mechanisms and biometric devices. Provided systems security engineering, test, evaluation, and development program support for organizations utilizing cryptographic equipments and associated keying systems. Completed design and development of the Certificate Authorization Workstation (CAW) regionalization strategy and begin to implement and integrate the CAW Remote Key/Re-key capability.

FY06 Plans include:
$3,869- Continue design and development of the KMI local management workstation. Begin EKMS Phase V to include development and implementation of an extended , networked architecture (key distribution over SIPRNET) to improve distribution and reliability for deployed forces, modernized key processors, common user application software and data transfer devices. Continue to develop and integrate Online Certificate Status Protocol. Continue development and integration of Future fill device. Begin security and functionality testing and evaluation of (OCSP) architecture for the SIPRNet. Continue security and functionality testing and evaluation of PKI tokens, readers and middleware for the SIPRNET. Complete prototyping and certification/accreditation of the Navy's Key management system. Begin Common User Application Software (CUAS), Data Mgmt Device (DMD) and Simple Key Loader (SKL) development and integration. Continue CUAS, DMD and SKL development and integration. Conduct requirements definition for the End IA Unit (EIAU) Encryption device. Begin Wireless Key Fill technology design and development. Begin the Key Loading and Initialization Facility (KLIF) design and development.

FY07 Plans include:
$4,734 - Complete security and functionality testing and evaluation of PKI tokens, readers and middleware for the SIPRNET. Continue to streamline the method for developing effective secure symmetric and asymmetric cryptographic key and generation, distribution, management, and usage products and services by identifying and prioritizing fleet requirements. Continue EKMS Phase V to include development and implementation of an extended , networked architecture (key distribution over SIPRNET) to improve distribution and reliability for deployed forces, modernized key processors, common user application software and data transfer devices. Continue to develop and integrate Online Certificate Status Protocol. Complete Wireless Key Fill technology design and development . Complete development and integration of Online Certificate Status Protocol. Complete DMS migration to PKI. Complete the initial design for EIAU management. Complete the Key Loading and Initialization Facility design and development.

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2006**
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT NUMBER AND NAME 0303140N Information Systems Security Program (ISSP)	PROJECT NUMBER AND NAME 0734 Information Systems Security

	FY 05	FY 06	FY 07
Emerging Technology	1.777	2.771	3.628
RDT&E Articles Quantity			

FY05 Plans include:
$1,777 - Provide sustained IA security engineering and technical expertise for the transition, application and integration of new technologies to Navy Information Assurance challenges. Provided IA R&D support for specific programs that included the following projects: (1) Secure Network Communications Including Coalition Applications, (2) Recognition and Prevention of Network Intrusions, (3) Convenient Wireless Applications with Adequate Security, (4) Synergistic Operation of IA and IO Functions, (5) Improved Access Control Using Biometrics, to include applications of commercially available biometrics technology to Navy logical and physical access problems, as well as applications that are now considered ready for larger scale implementation, and (6) Rapid Transition of Technology to the Fleet, in support of Fleet Battle Experiments, CNDID, TF WEB, Teleport, SCN and other transition opportunities. Completed initial concept refinement for INHIBT System that will proactively analyze transactions at the operating system level for normal behavior and initiate workstation and network survival systems for anomalous activity. Continued AWC technology project with proof of concept demonstration and initial production development. Released v2.0 of NESSO which will be a full featured, open source, production quality product including an enhanced Java based Identity Server, completed implementation of Biometric Authentication, and the Liberty Alliance Federated Identity framework.

FY 06 Plans include:
$2,771 - Continue to provide security systems engineering (+$1.053M) support for the transition and application of new technologies to Navy Information Assurance challenges. Continue development of open source Single Sign-On solution (+$.610M) by incrementally adding new features/enhancements for federated identity, Public Key Infrastructure (PKI), Role Based Access Control (RBAC), Common Access Card (CAC) and Next Generation Access Systems. Provide standardized security design and installation baselines to ensure enhancements of configuration management. Develop and integrate IA Components into programs such as FORCEnet, Computer Network Defense in Depth (CND-ID) Strategy, Transformational Communication (TC), Global Information Grid Enterprise Services (GIG-ES), Secure Voice over Internet Protocol (SVoIP), and Horizontal Fusion. Begin development of INHIBT system (+$.693M) that will proactively analyze transactions at the operating system level for normal behavior and initiate workstation and network survival systems for anomalous activity. Develop Next Generation Access Systems solutions (+$0.138M) to provide improved security for access to computers, networks, and sensitive spaces or buildings. Seamless integration with CAC is necessary. Provide IA engineering (+$0.277M) for development of Wireless Networks and PDA security readiness of Naval wireless networks and mobile computing devices .

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2006**
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT NUMBER AND NAME 0303140N Information Systems Security Program (ISSP)	PROJECT NUMBER AND NAME 0734 Information Systems Security

FY 07 Plans include:
$3,628 - Provide security systems engineering (+$1.524M) support for the transition and application of new technologies to Navy Information Assurance challenges. Continue technology development and begin transition of open source Single Sign-On solutions (+$.617M) for federated identity, Public Key Infrastructure (PKI), Role Based Access Control (RBAC), Common Access Card (CAC) and Next Generation Access Systems across multiple trusted domains. Provide standardized security design and installation baselines to ensure enhancements of configuration management.   Provide security systems engineering to develop and integrate IA Components, technologies and solutions into programs such as FORCEnet, CND-ID Strategy, TC, GIG-ES, SVoIP and Horizontal Fusion. Begin integration of INHIBT system (+$.980M) that will proactively analyze transactions at the operating system level for normal behavior and initiate workstation and network survival systems for anomalous activity. Continue to develop and begin integration of Next Generation Access Systems solutions (+$0.181M) to provide improved security for access to computers, networks, and sensitive spaces or buildings. Seamless integration with CAC is necessary. Provide IA engineering for development of Wireless Networks and PDA security (+$0.326M) readiness of Naval wireless networks and mobile computing devices, continue to evaluate products for security issues and develop guidance and procedures.

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2006**
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT NUMBER AND NAME 0303140N Information Systems Security Program (ISSP)	PROJECT NUMBER AND NAME 0734 Information Systems Security

(U) C. OTHER PROGRAM FUNDING SUMMARY:

Line Item No. & Name	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
OPN 3415 Info Sys Security Program (ISSP)	91.924	97.478	101.749	113.839	132.029	156.804	159.159

(U) D. ACQUISITION STRATEGY: *

EKMS Phase V- The Navy's ISSP EKMS program is linked to NSA’s strategy in implementing EKMS in evolutionary phases and migrating to Key Management Initiative (KMI). NSA is the lead for the joint EKMS effort and has been developing and certifying EKMS devices and capabilities in an evolutionary approach. EKMS Phase V is a major component evolving to KMI Common Increment 2 (CI-2). KMI is currently a Pre-Major Automated Information System (MAIS) program assigned to NSA. Therefore, it is crucial that the Research and Development efforts of EKMS coincide with those of KMI. Navy's EKMS requires Research, Development, Test and Evaluation (RDT&E) funding over the Future Years Defense Program (FYDP) to ensure the Navy infrastructure evolves with the EKMS phases, supports additional devices certified by NSA and supports the migration of EKMS to KMI CI-2. This will require the modification of the Navy EKMS Net Key Server.   PEO C4I & Space/PMW160 is collaborating with Naval Research Lab (NRL) to integrate COTS/GOTS devices into the Navy architecture to be compatible with Phase 5 and KMI architectures. These efforts require close work with NSA and the other services to ensure no impact on current operations and minimum impact on EKMS Phase 5 as it evolves to KMI CI-2. PMw160 procures National Security Agency (NSA) certified COTS/GOTS devices to support Navy requirements. The EKMS Phase V program will utilize existing competitively awarded NSA and SSC contracts for development and implementation of type 1 certified COTS/GOTS devices for initial production phases, with plans to initiate innovative contracting methods and types consistent with current ASN/RDA policies to reduced cost and the streamline the integration, installation, logistics and training efforts.

Crypto Modernization (KW-46 Replacement)-The KW-46 is a device that performs on-line decryption of digital messages, record, and data traffic over the broadcast system at data rates from 50 to 9,600 bits per second (BPS) that processes information up to and including TOP SECRET. The KWR-46 is used primarily on ships and submarines while the KWT-46 is located exclusively on shore sites, consisting of the KWT-46 transmitter and the KWR-46 receiver, **which are no longer in production**.   The PMW 160 is also evaluating acquisition development replacements of the KG-45, KL-51, KG-68B cryptographic devices per the UCD effort. Navy is currently refining the requirement specs, preparing formal Analysis of Alternatives, Request For Information (RFI’s), and LCEE's to be completed in FY 06 and the plan is to competitively award the development contract by 1Q FY07.

Crypto Modernization (Universal Crypto Device)- Navy is currently refining the requirement specs, preparing formal Analysis of Alternatives, Request For Information (RFI’s), and LCEE's to be completed in FY 06 and the plan is to competitively award the development contract by 1Q FY08. The evaluation of requirements of Crypto Modernization (Thorton-KEESEE) cryptographic system will also necessitate preparation of formal AOA, RFI within FY06 & FY07.

*** Not required for Budget Activities 1,2,3, and 6**

CLASSIFICATION:

Exhibit R-3 Cost Analysis (page 1)	DATE: **February 2006**

APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT 0303140N Information Systems Security Program (ISSP)	PROJECT NUMBER AND NAME 0734 Information Systems Security

Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 05 Cost	FY 05 Award Date	FY 06 Cost	FY 06 Award Date	FY 07 Cost	FY 07 Award Date	Cost to Complete	Total Cost	Target Value of Contract
Primary Hardware Development	C/CPFF	VIASAT, San Diego, CA	7.282								7.282	7.282
Primary Hardware Development	C/MIPR	MITRE, San Diego, CA	5.522								5.522	5.522
Primary Hardware Development	C/CPAF	TBD	6.771	1.354	01/05	1.027	01/06	1.291	01/07	Continuing	Continuing	
Primary Hardware Development	C/VAR	Various	65.313	2.457	VAR	2.555	VAR	2.965	VAR	Continuing	Continuing	
Systems Engineering	C/VAR	Various	47.391	7.787	VAR	9.122	VAR	10.539	VAR	Continuing	Continuing	
Subtotal Product Development			132.279	11.598		12.704		14.795		Continuing	Continuing	12.804

Remarks:

Software Development	CPAF	SAIC, San Diego, CA	32.877							0.000	32.877	42.590
Software Development	C/WX	NRL, Washington D.C.	0.145	0.640	10/04	1.013	10/05	1.233	10/06	Continuing	Continuing	
Subtotal Support			33.022	0.640		1.013		1.233		Continuing	Continuing	42.590

Remarks: SAIC target Value of contract includes other service's funding (ARMY RDT&E).

CLASSIFICATION:

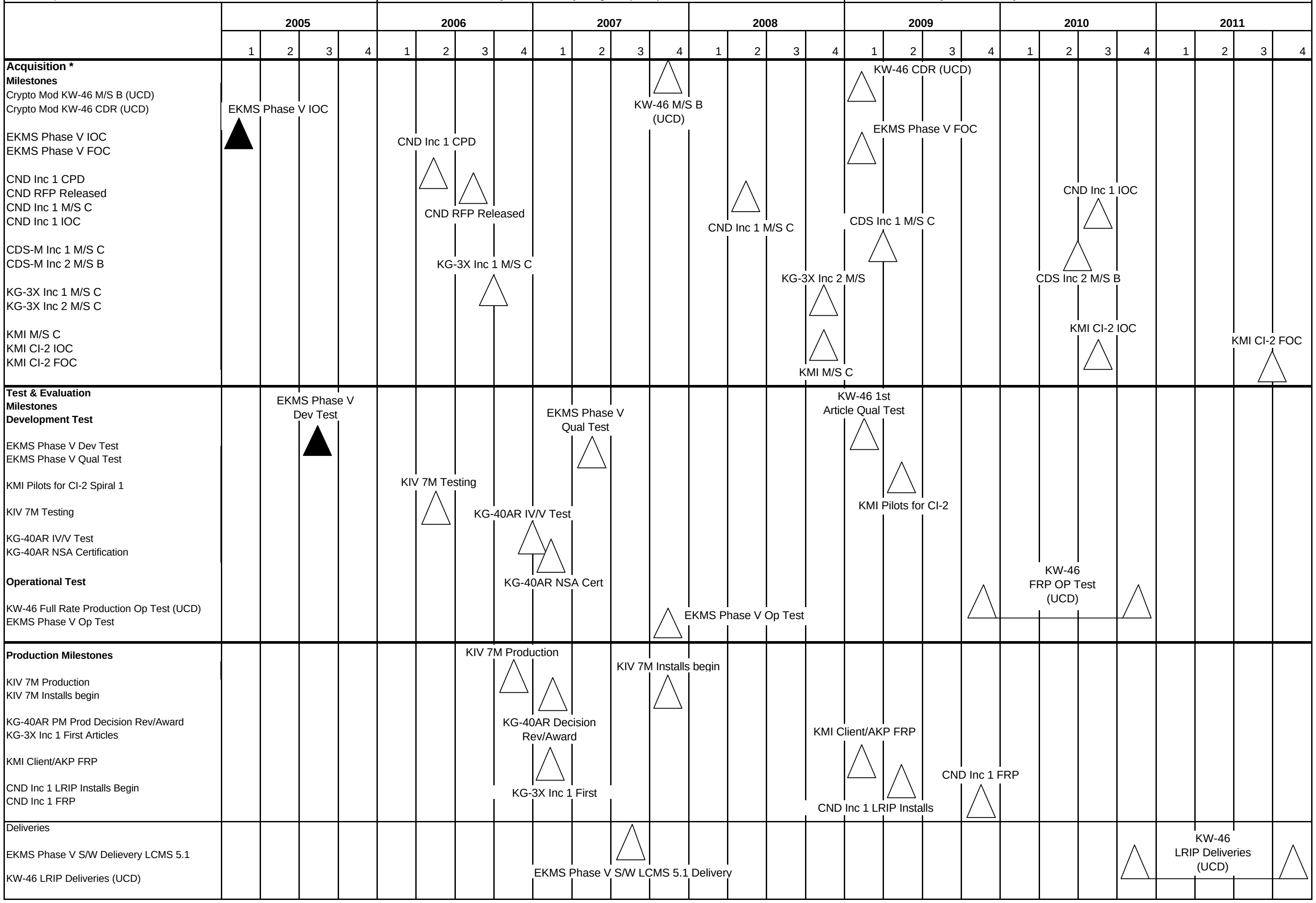
Exhibit R-3 Cost Analysis (page 2)	DATE: **February 2006**

APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT 0303140N Information Systems Security Program (ISSP)	PROJECT NUMBER AND NAME 0734 Information Systems Security

Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 05 Cost	FY 05 Award Date	FY 06 Cost	FY 06 Award Date	FY 07 Cost	FY 07 Award Date	Cost to Complete	Total Cost	Target Value of Contract
Developmental Test & Evaluation	VAR	Various	16.337	3.360	Various	3.534	Various	3.997	Various	Continuing	Continuing	Continuing
Subtotal T&E			16.337	3.360		3.534		3.997		Continuing	Continuing	
Remarks:												
Program Management Support	VAR	Various	4.601	0.201	Various	0.945	Various	1.013	Various	Continuing	Continuing	Continuing
Subtotal Management			4.601	0.201		0.945		1.013		Continuing	Continuing	
Remarks:												
Total Cost			186.239	15.799		18.196		21.038		Continuing	Continuing	
Remarks:												

CLASSIFICATION:

EXHIBIT R4, Schedule Profile		DATE: February 2006
APPROPRIATION/BUDGET ACTIVITY RDT&E, N / BA-7	PROGRAM ELEMENT NUMBER AND NAME 0303140N Information Systems Security Program (ISSP)	PROJECT NUMBER AND NAME 0734 Information Systems Security



R-1 SHOPPING LIST - Item No. 196

* Note: MLCS Deliveries support the MLCS Capability Certifications

Exhibit R-4, Schedule Profile

CLASSIFICATION:

Exhibit R-4a, Schedule Detail						DATE: **February 2006**	
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**					PROJECT NUMBER AND NAME 0734 Information Systems Security		
Schedule Profile	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
EKMS Phase V IOC	1Q						
EKMS Phase V FOC					1Q		
Crypto Modernization KW-46 M/S B (UCD)			4Q				
Crypto Modernization KW-46 CDR (UCD)					1Q		
CND Inc 1 CPD		2Q					
CND RFP Released		3Q					
CND Inc 1 M/S C				2Q			
CND Inc 1 IOC						3Q	
CDS-M Inc 1 M/S C					1Q		
CDS-M Inc 2 M/S B						2Q	
KG-3X Inc 1 M/S C		3Q					
KG-3X Inc 2 M/S C				4Q			
KMI M/S C				4Q			
KMI CI-2 IOC						3Q	
KMI CI-2 FOC							3Q
Developmental Test							
EKMS Phase V Developmental Test	3Q						
EKMS Phase V Qualification Test			2Q				
KMI Pilots for CI-2 Spiral 1					2Q		
KIV 7M Testing		2Q					
KG-40AR IV/V Test		4Q					
KG-40AR NSA Certification			1Q				
Operational Test							
EKMS Phase V Operational Test			4Q				
Crypto Modernization KW-46 FRP Operational Test (UCD)					4Q-	Cont'd-Q4	
Production Milestones							
KIV 7M Production		4Q					
KIV 7M Installs begin			4Q				
KG-40AR PM Prod Decision Rev/Award			1Q				
KG-3X Inc 1 First Articles			1Q				
KMI Client/AKP FRP					1Q		
CND Inc 1 LRIP Installs Begin					2Q		
CND Inc 1 FRP					4Q		
Deliveries							
EKMS Phase V S/W Delievery LCMS 5.1			3Q				
Crypto Mod KW-46 LRIP Deliveries (UCD)						4Q-	Cont'd-Q4

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification								DATE: **February 2006**	
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT NUMBER AND NAME 0303140N Information Systems Security Program (ISSP)				PROJECT NUMBER AND NAME 0734 Communications Security				
COST ($ in Millions)	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011		
Project Cost	**2.089**	**2.073**	**1.999**	**2.188**	**2.145**	**2.197**	**2.230**		
RDT&E Articles Qty									

(U) A. MISSION DESCRIPTION AND BUDGET ITEM JUSTIFICATION: The goal of the Navy Information Systems Security Program (ISSP) is to ensure the continued protection of navy and joint information and information systems from hostile exploitation and attack. ISSP activities address the triad of Defense Information Operations: protection ,detection, and reaction. Evolving attack sensing (detection), warning, and response (reaction) responsibilities extend far beyond the traditional ISSP role in protection or Information Systems Security (INFOSEC). Focused on the highly mobile forward-deployed subscriber, the US Navy's adoption of Network-Centric Warfare (NCW) places demands upon the ISSP, as the number of users explodes and the criticality of their use escalates. Today, the ISSP protects an expanding core of services critical to the effective performance of the Navy's mission.

The rapid rate of change in the underlying commercial and government information infrastructures makes the provision of security an increasingly complex and dynamic problem. Information Assurance (IA) technology mix and deployment strategies must evolve quickly to meet rapidly evolving threats and vulnerabilities. No longer can information security divorce the information infrastructure. The ISSP enables the Navy's war fighter to trust in the availability, integrity, authentication, privacy, and non-repudiation of information.

This project includes funds for advanced technology development, test and evaluation of naval information systems security based on leading edge technologies that will improve information assurance (e.g., situational awareness and information infrastructure protection) across all Command echelons to tactical units afloat and war fighters ashore. This effort will provide the research to develop a secure seamless interoperable, common operational environment of networked information systems in the battlespace and for monitoring and protecting the information infrastructure from malicious activities. This effort will provide Naval Forces a secure capability and basis in its achievement of protection from unauthorized access and misuse, and optimized IA resource allocations in the information battlespace. This program will also develop core technology to improve network infrastructure resistance and resiliency to attacks; enable the rapid development and certification of security-aware applications and information technologies in accordance with the Common Criteria for IA and IA-Enabled information technology products by the National Security Telecommunications and Information Systems Security Instructions; and measure the effectiveness and efficiency of IA defensive capabilities under Naval environments.

A Memorandum of Agreement (MOA) was signed in FY01 between the Office of Naval Research Department of Information, Electronics & Surveillance (ONR31) and Office of the Chief of Naval Operations, Directorate of Space, Information Warfare, Command and Control, Information Warfare Division (N64), and provides for interagency coordination with ONR, N71, and PEO C4I and Space (PMW160) in pursuance of this effort.

This Project under Program Element 0303140N is a restructuring with the transfer of responsibility from SPAWAR to ONR in FY 2003 for prototyping IA concepts.

JUSTIFICATION FOR BUDGET ACTIVITY: This program is funded under OPERATIONAL SYSTEMS DEVELOPMENT because it encompasses engineering and manufacturing development for upgrade of existing,

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2006**
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT NUMBER AND NAME 0303140N Information Systems Security Program (ISSP)	PROJECT NUMBER AND NAME 0734 Communications Security

(U) B. Accomplishments/Planned Program

	FY 05	FY 06	FY 07
Software and Systems Research	2.089	2.073	1.999
RDT&E Articles Quantity			

The program will develop common architectural frameworks that facilitate integration of network security capabilities, enable effective seamless interoperation, and contribute to a common consistent picture of the networked environment with respect to information assurance and security. This effort will address the need for a common operational picture for IA, as well as assessment of security technology critical to the success of the mission. Initiate requirements definition for situation awareness capabilities to support computer network defense in highly distributed, homogeneous, and heterogeneous networks including mobile and embedded networked devices. This effort also includes the architectural definition of situational awareness and visualization capabilities to support active computer network defense and support underlying data mining and correlation tools. This includes addressing the capability to remotely manage and securely control the configurations of network security components to implement changes in real time or near real time. Initiate requirements definition for secure coalition data exchange and interoperation among security levels and classifications. Ensure approaches address various security level technologies as well as emerging architectural methods of providing interoperability across different security levels. Examine multi-level aware applications and technologies including databases, web browsers, routers/switches, etc. Initiate infrastructure protection efforts as the Navy develops network centric architectures and warfare concepts, ensuring an evolutionary development of security architectures and products for IA that addresses Navy infrastructure requirements. Ensure the architectures evolve to provide proper protection as technology, DOD missions, and the threat all evolve. Include defensive protections as well as intrusion monitoring (sensors), warning mechanisms, and response capabilities in the architecture. Ensure the unique security and performance requirements of tactical systems, including those operating various security levels are addressed. Initiate the efforts to conceptualize new network centric warfare technology to protect our assets, such as secure network gateways and routers, and components and tools that improve the survivability of Navy networks. Provide systems security engineering, certification and accreditation support for high-confidence naval information system and ensure certification and accreditation approaches are consistent with Navy and DoD requirements.

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification	DATE: **February 2006**

APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	0734 Communications Security

(U) C. OTHER PROGRAM FUNDING SUMMARY:

Line Item No. & Name	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
OPN 3415 Info Sys Security Program (ISSP)	91.924	97.478	101.749	113.839	132.029	156.804	159.159

(U) D. ACQUISITION STRATEGY: *

N/A.

*** Not required for Budget Activities 1,2,3, and 6**

CLASSIFICATION

Exhibit R-3, Code Analysis (page 1)	DATE: **February 2006**

APPROPRIATION/BUDGET ACTIVITY **RDT&E,N / BA-7**	PROGRAM ELEMENT 0303140N/ INFORMATION SYSTEMS SECURITY PROGRAM	PROJECT NUMBER AND NAME R0734 COMMUNICATIONS SECURITY R&D (INFORMATION ASSURANCE)

Cost Categories	Contract Method & Type	Performing Activity & Location	Total PYs Cost	FY 05 Cost	FY 05 Award Date	FY 06 Cost	FY 06 Award Date	FY 07 Cost	FY 07 Award Date	Cost to Complete	Total Cost	Target Value of Contract
Hardware Development											0.000	
Subtotal Product Development			0.000	0.000		0.000		0.000			0.000	
Remarks:												
Software Development	C/WX	NRL, Washi NRL, Washing	0.000	2.089	10/05	2.073	10/06	1.999	10/07	Continuing	Continuing	
Subtotal Support			0.000	2.089		2.073		1.999		Continuing	Continuing	
Remarks:												

CLASSIFICATION

Exhibit R-3, Code Analysis (page 1)		DATE: **February 2006**
APPROPRIATION/BUDGET ACTIVITY **RDT&E,N / BA-7**	PROGRAM ELEMENT 0303140N/ INFORMATION SYSTEMS SECURITY PROGRAM	PROJECT NUMBER AND NAME R0734 COMMUNICATIONS SECURITY R&D (INFORMATION ASSURANCE)

Cost Categories	Contract Method & Type	Performing Activity & Location	Total PYs Cost	FY 05 Cost	FY 05 Award Date	FY 06 Cost	FY 06 Award Date	FY 07 Cost	FY 07 Award Date	Cost to Complete	Total Cost	Target Value of Contract
Subtotal T&E			0.000	0.000		0.000		0.000			0.000	
Remarks:												
Program Management Support											0.000	
Subtotal Management			0.000	0.000		0.000		0.000			0.000	
Remarks:												
Total Cost			0.000	2.089		2.073		1.999		Continuing	Continuing	
Remarks:												

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2006**
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT NUMBER AND NAME 0303140N Information Systems Security Program (ISSP)	PROJECT NUMBER AND NAME 9999 Congressional Plus Up

COST ($ in Millions)		FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	
Project Cost		**7.808**	**1.300**						
RDT&E Articles Qty									

(U) A. MISSION DESCRIPTION AND BUDGET ITEM JUSTIFICATION: Congressional plus-up for Navy's SECURE Kit . Develop systems that will allow a user at a single workstation seat to access multiple security networks based on the user's access clearance and need to know. The web architecture-based solution will allow the user to access this information at the Navy enterprise level and eliminates the need to reconfigure networks and hardware when accessing one domain or another. In order to implement a fully enabled end-to-end network enterprise environment envisioned by the FORCEnet vision document, we have developed a component-based architecture called SECUREkit. SECUREkit will provide the necessary components to meet the Naval warfighter needs, which can be summarized as three.
(1) Single points of entry anywhere on the network to any place on the network with complete transparency to the tiers of enterprise services.
(2) Access from that single point to all appropriate security domains.
(3) Provide the ability to dynamically, or on the fly, reconfigure the Multi-Level System (MLS) enterprise.
The evolutionary the component architecture of the SECUREkit architecture is being accomplished through partnering efforts with the National Security Agency (NSA) and the PEO(C4I&Space). This architecture is made up of trusted servers, trusted pathways, and trusted clients. The goal of SECUREkit will be to make available to warfighters in the Global Information Grid Enterprise Services (GIG ES) all components that are certified at Evaluated Assurance Level 6 (EAL6).

Congressional plus-up for the Collaborative Information Warfare Network (CIWN). The CIWN will provide an architecture by which other networks (Marine Corps (MC), Navy, Homeland Security (HLS), Health Services Department (HSD), National Guard Bureau (NGB), Federal Bureau of Investigation (FBI)), can be integrated and interoperate securely. The CIWN architecture provides the interfaces by which agencies with specific network requirements can maintain their networks in a distributed fashion and interoperate and share critical infrastructure data and information. This CIWN architecture enables a distributed network solution that reduces the risk of attack on a single national network. CIWN includes the network architecture by which the CIPCs and CIPC partners and subscribers interoperate and conduct information operations (to include data and information sharing, knowledge engineering, and data and infrastructure protections). Embedded within the CIWN architecture is the National Technology Assessment Network (NTAN). The NTAN is a virtual network designed to provide a virtual environment in which technologies can be assessed by CIPC partners for inclusion in their IT Infrastructures without the building the additional infrastructure required to support its assessment. In addition, the NTAN provides an environment in which Federal, State, Local, Industry and Academia can assess existing and future technologies for compatibility and interoperability within the CIWN.

U) JUSTIFICATION FOR BUDGET ACTIVITY: These programs are funded under OPERATIONAL SYSTEMS DEVELOPMENT because it encompasses engineering and manufacturing development for upgrade of existing, operational systems.

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2006**
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT NUMBER AND NAME 0303140N Information Systems Security Program (ISSP)	PROJECT NUMBER AND NAME 9999 Congressional Plus Up

(U) B. Accomplishments/Planned Program

	FY 05	FY 06	FY 07
(9430) SECUREKit	4.434	1.300	
RDT&E Articles Quantity			

FY05 Plans include:
$4,434 - Completed the initial design of network access device that includes multi-factor identification, identity management process, and inline encryption engine. The design is currently still a work in progress but may be either internal PCI card or and external black box device. These components are based on open architecture and designed for enabling web-based enterprise services in the Department of the Navy and coalition participants. These components provide for a trusted path, or high assurance transactions, between servers, clients, and other resources in the FORCEnet enterprise.

FY06 Plans include:
$1,300 - Further refine design of authorization software to include integration with authentication service, Navy Enterprise Single Sign-On (NESSO). This year the program will work to integrate the product within test networks and work with the user community for feedback using a well defined authorization language approach. The final design, still a work in progress, is based on open architecture and designed for enabling web-based enterprise services in the Department of the Navy and coalition participants. The software components provide authorization services for the Global Information Grid (GIG) and for the FORCEnet enterprise.

	FY 05	FY 06	FY 07
(9647 CIWN)	3.374		
RDT&E Articles Quantity			

FY05 Accomplishment include:
$3,374 - The FY 05 RDT&E Congressional increase provided for the development of the Collaborative Information Warfare Network architecture and publish a guide that frames processes to both Federal and Military organizations for the monitoring, detection, protection and remediation of potential threats to the operation of the nations' critical infrastructure.
The CIWN network architecture establishes a collaborative environment linking center's in four regional geographic areas and in Canada and Mexico.

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2006**
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT NUMBER AND NAME 0303140N Information Systems Security Program (ISSP)	PROJECT NUMBER AND NAME 9999 Congressional Plus Up

(U) C. OTHER PROGRAM FUNDING SUMMARY:

Line Item No. & Name	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
OPN 3415 Info Sys Security Program (ISSP)	91.924	97.478	101.749	113.839	132.029	156.804	159.159
RDT&E 0303140N Info Sys Security (ISSP)	15.799	18.196	21.038	26.347	30.955	29.119	30.371

(U) D. ACQUISITION STRATEGY: *

The Navy intends to continue SECUREKit development on existing RD contract with PSI, Inc.
The Navy intends to continue IASM development on existing RD contract with Promia, Inc.

*** Not required for Budget Activities 1,2,3, and 6**

CLASSIFICATION:

Exhibit R-3 Cost Analysis (page 1)		DATE: **February 2006**
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT 0303140N Information Systems Security Program (ISSP)	PROJECT NUMBER AND NAME 9999 Congressional Plus Up

Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 05 Cost	FY 05 Award Date	FY 06 Cost	FY 06 Award Date	FY 07 Cost	FY 07 Award Date	Cost to Complete	Total Cost	Target Value of Contract
Primary Hardware Development												
Ancillary Hardware Development												
Aircraft Integration												
Ship Integration												
Ship Suitability												
Systems Engineering	CPFF	PSI, Inc.	1.629	4.123		1.125					6.877	6.877
Training Development												
Licenses												
Tooling												
GFE												
Award Fees												
Subtotal Product Development			1.629	4.123		1.125					6.877	6.877
Remarks:												
Development Support	WX	SSC Charleston, SC		3.181								3.181
Software Development												
Integrated Logistics Support												
Configuration Management												
Technical Data												
Studies & Analyses												
GFE												
Award Fees												
Subtotal Support				3.181								3.181
Remarks:												

CLASSIFICATION:

Exhibit R-3 Cost Analysis (page 2)	DATE: **February 2006**

APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT 0303140N Information Systems Security Program (ISSP)	PROJECT NUMBER AND NAME 9999 Congressional Plus Up

Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 05 Cost	FY 05 Award Date	FY 06 Cost	FY 06 Award Date	FY 07 Cost	FY 07 Award Date	Cost to Complete	Total Cost	Target Value of Contract
Developmental Test & Evaluation	WX	SSC Charleston, SC										
Developmental Test & Evaluation	WX	SSC San Diego, CA										
Live Fire Test & Evaluation												
Test Assets												
Tooling												
GFE												
Award Fees												
Subtotal T&E												

Remarks:

Contractor Engineering Support												
Government Engineering Support												
Program Management Support	CPFF	BAH, Inc.	0.100	0.504		0.175					0.779	0.779
Travel												
Transportation												
SBIR Assessment												
Subtotal Management			0.100	0.504		0.175					0.779	0.779

Remarks:

Total Cost			1.729	7.808		1.300					10.837	10.837

Remarks: