

CLASSIFICATION:

EXHIBIT R-2, RDT&E Budget Item Justification						DATE: February 2007		
APPROPRIATION/BUDGET ACTIVITY RESEARCH DEVELOPMENT TEST & EVALUATION, NAVY / BA-7				R-1 ITEM NOMENCLATURE 0303140N Information Systems Security Program (ISSP)				
COST (\$ in Millions)	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013
Total PE Cost	21.362	28.911	28.393	32.251	30.355	31.696	34.174	34.771
0734 Information Systems Security	18.007	20.943	26.249	30.090	28.141	29.452	31.890	32.448
0734 Communications Security (ONR)	2.075	1.991	2.144	2.161	2.214	2.244	2.284	2.323
9999 Congressional Increases	1.280	5.977						
Quantity of RDT&E Articles								
(U) A. MISSION DESCRIPTION AND BUDGET ITEM JUSTIFICATION:								
<p>(U) The goal of the Navy Information Systems Security Program (ISSP) is to ensure the continued protection of Navy and Joint telecommunications and information systems from hostile exploitation and attack. 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 Department of Defense 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.</p> <p>(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.</p> <p>(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.</p>								

CLASSIFICATION:

EXHIBIT R-2, RDT&E Budget Item Justification		DATE: February 2007
APPROPRIATION/BUDGET ACTIVITY RESEARCH DEVELOPMENT TEST & EVALUATION, NAVY BA-7	R-1 ITEM NOMENCLATURE 0303140N Information Systems Security Program (ISSP)	
<p>(U) The Navy ISSP RDT&E program works to provide the Navy with these essential Information Assurance (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 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.</p> <p>(U) All ISSP RDT&E efforts comply with the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113) as implemented through OMB 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 reflect this emphasis on interoperable standards.</p> <p>(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; prototype: 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.</p> <p>(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.</p>		

Exhibit R-2, RDTE Budget Item Justification

CLASSIFICATION:

EXHIBIT R-2, RDT&E Budget Item Justification		DATE: February 2007		
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME			
RESEARCH DEVELOPMENT TEST & EVALUATION, NAVY/BA-7	0303140N Information Systems Security Program (ISSP)			
(U) B. PROGRAM CHANGE SUMMARY:				
(U) Funding:	FY 2006	FY 2007	FY 2008	FY 2009
FY 07 President's Budget	21.569	23.037	28.535	33.100
FY 08/09 President's Budget	21.362	28.911	28.393	32.251
Total Adjustments	-0.207	5.874	-0.142	-0.849
Summary of Adjustments				
Sec. 8125: Revised Economic Assumptions	0.035			
Congressional Action	0.081			
Small Business Innovation Research (SBIR) Tax	-0.090			
Non-Enterprise related CIVPERS/CS Adjustments			-0.039	-0.039
FY 08 / FY 09 NWCF Rate Adjustments - Naval Research Laboratory			0.008	0.020
Sec. 8106: Revised Economic Assumptions		-0.110		
Congressional Interest: Tactical Key Loader		3.200		
Congressional Interest: SECUREKit		1.000		
Congressional Interest: Universal Decryption, Discovery and Integrate		1.800		
Sec. 8023: Federally Funded R&D Center		-0.016		
Non-Purchased Inflation Adj - Navy			-0.272	0.130
Program Adjustments	-0.233		-0.118	-1.213
FY08/FY09 NWCF Rate Adjustments - SPAWAR Systems Centers			0.279	0.253
Subtotal	-0.207	5.874	-0.142	-0.849
(U) Schedule:				
N/A.				
(U) Technical:				
N/A.				

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification						DATE: February 2007		
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 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013
Project Cost	18.007	20.943	26.249	30.090	28.141	29.452	31.890	32.448
RDT&E Articles Qty								
<p>(U) A. MISSION DESCRIPTION AND BUDGET ITEM JUSTIFICATION: The ISSP RDT&E provides Information Assurance (IA) solutions for the 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.</p> <p>(U) ISSP RDT&E must work closely within the Navy's Information Operations – Exploit (Signals Intelligence - SIGINT) and Information Operations – Attack (INFOWAR - information warfare) 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 Navy Information Operations Command (NIOC).</p> <p>(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 Global Information Grid (GIG) Capabilities Requirements Document (CRD) for the development of Content Based Encryption (CBE) continuing in FY 06-11.</p> <p>(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 Code of Federal Regulation (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.</p> <p>(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.</p> <p>(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-based efforts include developing or applying: (1) new secure voice prototypes; (2) technology for a new family of programmable Communication Security (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 Solutions (CDS); (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).</p> <p>(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.</p>								

Exhibit R-2a, RD TEN Budget Item Justification

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: February 2007
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
<p>(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 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/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).</p> <p>(U) The current operating environment has virtually eliminated the traditional distinction between telecommunications and information systems. Because Information Assurance (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:</p> <p>(U) Under the Navy Secure Voice (NSV) program, ISSP RDT&E assesses technology to provide high grade, secure tactical and strategic voice connectivity.</p> <p>(U) Under the Navy Cryptographic Modernization Program, ISSP RDT&E provides high assurance and other cryptographic technologies protecting information and telecommunication systems.</p> <p>(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 Public Key Infrastructure (PKI) and Certificate Management Infrastructure (CMI) technology, and the development of improved techniques for key and certificate management to support emerging, embedded cryptographic technology.</p> <p>(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, outside the continental United States (OCONUS) Navy Enterprise Network (ONE-NET), and the Integrated Shipboard Network Systems (ISNS), along with constituent systems such as Automated Digital Network System (ADNS), Global Command and Control System - Maritime (GCCS-M). It includes activities to:</p> <ul style="list-style-type: none"> • 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 2007
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
<ul style="list-style-type: none"> • 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. <p>(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.</p>		

EXHIBIT R-2a, RDT&E Project Justification		DATE: February 2007
---	--	----------------------------

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 06	FY 07	FY 08	FY 09
Computer Network Defense (CND)	4.956	5.567	9.089	9.213
RDT&E Articles Quantity				

FY 06: Continued to integrate security products and new technologies for resilient Computer Network Defense (CND) systems for both ship and shore installation. Provided Information Assurance (IA) engineering system design (+\$1.655M), evaluation, and testing techniques to maintain IA controls from system end-to-end and information source-to-sink. Integration of IA appliances, software, and implementation techniques for Intrusion Prevention, CND Virus Scanning of all network data exchange protocols, Vulnerability management, and initial Host Based Security requirement were assessed. Began development of a tiered management system (+\$2.0M) between Fleet Network Operations Centers (NOCs) and the Navy Cyber Defense Operation Center for real-time situation awareness and display of security risk as: Computer Network Threats, Vulnerabilities, and Critical System Security Performance. Began development of enhanced Security Management Tools (+\$1.301M) with new capabilities to support system configuration management and monitoring. Supported development of online engineering support to access subject matter security system experts; automate security system Information Assurance & Vulnerability Assessment (IAVA) distributions, web based information server, NOC site 'As Built' Configuration Data, and Emergency Restoration Files. Developed an IAVA verification assessment system to status Network Operation Center IAVA status for fielded security equipment.

FY 07: Plans include: Provide the broadest range of Information Assurance (IA) research and development support across Joint, Fleet, and ashore networks. Provide on-going security 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 technique to support a range of Sea Shield initiatives in Joint Command security solutions, Navy Sea Power tactical edge support to Global War on Terrorism, and Sea-Based cyber defense operations in coalition data sharing networks. Provide IA engineering to translate FORCEnet capabilities into CND solutions and conduct security design evaluations certification test results. Includes IA appliances, software, and implementation techniques for policies such as IAVA requirements, Information Operation Condition (INFOCON) response, and USN firewall policy. Provide continuous development of a Shipboard unit level tier situation information management system (+\$1.717M) as a means of hierarchically integrating Ship Security Monitors Network Operating Center security systems, and Navy Cyber Defense Operation Center for real-time display of security risk. Continue the development of using authenticated administrator access control techniques enhance fielded Security Management Tools (+\$0.945M) with new capabilities to support system configuration management and monitoring. Begin development of improved real-time computer network security, policy administration, and situation command control for Navy CND incremental program product acquisition 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. Evaluate combined system security effectiveness between each systems networking layer end-to-end, data link layer security through application exchange layer security.

FY 08: Integrate security situational awareness technologies (+\$7.316) for knowledge empowered Computer Network Defense (CND) operations for both ship and shore installation. Establish system management capabilities to enforce proactive unit level security policies across the Navy Network Enterprise to centrally manage security policies to controllable devices such as Firewalls, Intrusion Prevention Systems (IPS), and Filtering Routers at shore based Network Operation Centers. Includes IA appliances, software, and implementation techniques for automated response products such as vulnerability remediation, Information Operation Condition (INFOCON) response, and intrusion prevention policies.

Complete the development and integration of the patch management and host based security agents tools. Develop additional tools to determine accurate asset location and inventory information. Through the use of the data in the new tool, initiate the development of the process to assign asset criticality at the host and application level (+\$1.773M).

FY 09: Continue system integration efforts with analytical tools to identify asset criticality at the host and application level. Develop computer-network evaluation capabilities to perform real-time metrics of operational compliance with IA security controls, Mission Assurance Category, and data Confidentiality. Evolve system incremental capabilities to advance CND Protect, Monitor, Detect, Analyze, and Respond (+\$7.176M). Conduct Honey Net research to develop proactive Insider Threat Countermeasures and application layer Content Scanning. Develop User Defined Operational Pictures (UDOP) to enhance Security Information Manager (SIM) tools with active defense capabilities, improved incident correlation, and situation awareness reporting.

Complete the development of the process to assign asset criticality at the host and application level. Initiate the development of new capabilities to support the selective and automatic reactive settings of the network in accordance with INFOCON policies. Address the capabilities required to support the INFOCON management at both the Naval Cyber Defense Operation Center (NCDOC) and the Fleet NOC level (+\$2.037M).

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification			DATE: February 2007	
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 06	FY 07	FY 08	FY 09
Crypto	4.579	5.378	7.227	12.064
RDT&E Articles Quantity				
<p>FY 06: Provided for research, evaluation and prioritization of cryptographic products and KeyMat in modernizing the Naval Cryptographic inventory, including Type-1 US only, allied and coalition, and COTS. Provided support of development efforts in coordination with the Information Systems Security Office, Joint Services, and NSA. Provided (+\$1.641M) specific design, testing, and evaluation assistance for new USN platforms and assisted in defining embedded cryptographic product engineering requirements. Provided sustained IA engineering support for the development, acquisition, and installation of Crypto Modernization products including KG-3X, KG-40AR, Communication Security (COMSEC)/TRANSEC Integrated Circuit (CTIC)/Device Hybrid (CDH), Mode 5 Identify Friend or Foe (IFF), Link Encryption Family (LEF), Universal Crypto Device (UCD)/Expendable Crypto devices, and Next Generation COMSEC devices such as: Programmable Embedded Information Security product (PEIP) follow-on, Modern Legacy Crypto Solution (MLCS), KIV-7M/KIV-19M WALBURN and SAVILLE (+\$.808M), Thorton-KEESEEE (+\$2.130M) and KW-46, KG-45, KL-51, KG-68B (based on UCD development) sustainment/replacement. Additional efforts also focused on replacing NSA decertified products. Continued development of next generation network encryption devices, to include application and implementation of High Assurance Internet Protocol Encryptor (HAIPE) in transformational architectures such as FORCEnet and Joint Tactical Radio System (JTRS) Wideband Networking Waveform (WNW), and analysis of critical harmonization/development solutions between modernized In-line Network Encryptor (INE) devices and Key Management, Future Narrowband Digital Terminal (FNBDT) and Wireless standards to ensure net-centric capability.</p> <p>FY 07: 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 of Crypto Modernization (+\$2.353M) 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-KEESEEE-SAVILLE (+\$2.431M) and KW-46, KG-45, KL-51, KGV-68B (based on UCD development). Continue acquisition documentation mandated by Joint Capabilities Integration and Development System (JCIDS) for development of identified cryptographic devices for replacement in FY06. Continue research, evaluation and prioritization of KEESEE, SAVILLE and GOODSPEED cryptographic products and KeyMat in recommending replacement solution sets to provide cryptographic products, including type-1 US only, allied and coalition, and commercial-off-the-shelf devices to the war-fighter. Application and implementation of HAIPE in transformational architectures such as FORCEnet and Joint Tactical Radio System Wideband Networking Waveform (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. Establish solutions for DoN unique Crypto's including: IOC for KL-51; Solution identified for KG-45; and Solution identified for KWR-46. Establish first Air Force/DoN LPO. Publish Crypto Product Roadmap and complete UCD requirements specifications and source selection for first UCD product. Establish Industry Working Group charter. Validate Information Assurance Cryptographic Product (IACP) Management Tool. Complete KEESEE Integrated Product Team (IPT) (90% of Navy operational Crypto devices identified) and complete SAVILLE IPT (90% Crypto's identified).</p>				

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: February 2007
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
<p>FY 08: Provide development support efforts in coordination with the Information Systems Security Office, Joint Services, and the National Security Agency. Continue development efforts and acquisition documentation for identified and selected KEESEE Cryptographic products as IPT completes at 100%. Complete SAVILLE IPT (90% Crypto's identified). Begin major pre-acquisition and development of specification for KGR-68. Provide consistent IA engineering support for on-going development of Crypto Modernization devices including UCD, KG-45, KL-51 and KG-68B. Continue development and testing of Cryptographic Module (Engine) in a joint effort with other services. A next generation cryptographic device for replacing identified legacy devices providing for secure communication capabilities to the war fighter. Begin additional pre-acquisition and development of on-going Decertified Cryptographic Algorithms affecting legacy DoN Cryptographic Devices.</p> <p>FY 09: Continue to provide cryptographic products, including Type-1 US only, allied and coalition, and commercial-off-the-shelf to DoN. Continue research, evaluation, and prioritization of several other Decertified Cryptographic products. Provide consistent IA engineering support for the development and integration of Crypto Modernization products and begin major pre-acquisition and development specification for KGV-68. Complete development and testing of first UCD module in a joint effort with other services. Begin installation of identified first device groupings. Continue development and testing of on-going Decertified Cryptographic Algorithms affecting legacy DoN Cryptographic Devices and Communication Security (COMSEC). Continue pre-acquisition and development of on-going Decertified Cryptographic Algorithms affecting legacy DoN Cryptographic Devices.</p>		

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification	DATE: February 2007
---	-------------------------------

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 06	FY 07	FY 08	FY 09
Information Assurance Readiness	0.000	0.269	0.000	0.000
RDT&E Articles Quantity				

FY 06: N/A.

FY 07: Provide systems security engineering support to all USN organizations in the certification and accreditation of information systems. A primary responsibility is the Certification and Accreditation (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.

FY 08: N/A

FY 09: N/A

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification			DATE: February 2007	
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 06	FY 07	FY 08	FY 09
Secure Voice	0.617	0.697	1.149	1.184
RDT&E Articles Quantity				

FY 06: 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. Developed survey for collecting secure voice mission and operational requirements from users for a new COMSEC device that will replace various legacy voice devices. Developed and fielded 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 Secure Telephone Equipment (STE)/FNBDT devices as well as secure conference capabilities. The first TSG system was installed at Naval Computer and Telecommunications Area Master Station (NCTAMS) LANT. Developed the first draft version of Naval Advanced Secure Voice Architecture (NASVA) to establish a baseline for synchronized secure voice evolution in net-centric environment.

FY 07: Complete development and integration test of submarine SCIP Inter-working Function (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. Update the Naval Advanced 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) 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 - Universal Voice Terminal (UVT) and Personal Secure Telephone (PST). Research and develop a compression technique (SCIP IWF or gateway) to allow SCIP IWF signaling be transmitted off-ship for underway submarines.

FY 08: 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 (MSC) 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).

FY 09: Complete development and integration test of the SCIP IWF for MSC and Coast Guard ships. Continue the design and development of next generation Secure Voice capabilities/products.

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: February 2007
---	--	-------------------------------

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 06	FY 07	FY 08	FY 09
Cross Domain Solutions (CDS)	1.284	0.709	0.000	0.000
RDT&E Articles Quantity				

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

FY 06: Provided systems security engineering for the development, testing, and evaluation of complex multi-level security solutions, including complicated evaluations involving allied and coalition participation. Analyzed, evaluated and examined cross domain applications and technologies including databases, web browsers, routers/switches, etc. Developed and integrated Cross Domain Solutions (CDS) prototype architecture at Network Operation Center (NOC) facilities. Continued 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. Began coordination with the Cross Domain Management Office (CDMO) including development of the Navy's Cross Domain Solution Office.

FY 07: 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 Multiple Security Levels (MSL)/CDS prototype architecture at NOC facilities.

FY 08: N/A

FY 09: N/A

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: February 2007
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 06	FY 07	FY 08	FY 09
Key Management Infrastructure	3.820	4.713	5.690	5.235
RDT&E Articles Quantity				

FY 06: Began prototyping and certification/accreditation of the Navy's Key management system. Began Common User Application Software (CUAS), Data Mgmt Device (DMD), Simple Key Loader (SKL) and Electronic Key Management System (EKMS) Phase V development and integration. Completed Mode 5 Identify Friend or Foe (IFF) (Time of Day) design and development. Provided engineering design evolution for the supporting key management infrastructure, EKMS Phase IV for Tier 0,1,2,3. 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 (+\$2.278). Began security and functionality testing and evaluation of current Public Key Infrastructure (PKI) tokens and readers due to upgrades to middleware. Began research of solutions and tools to implement Cryptographic network logon specifically for Navy Enterprise Network (ONE-NET) and legacy networks in Continental United States (CONUS). Initiated testing of Navy Certificate Validation Infrastructure (NCVI) afloat to include testing of Integrated Shipboard Network Systems (ISNS) Common PC Operating System Environment (COMPOSE) with PKI components. Provided front-end analysis for role-based system administrator certificates on alternate token. Performed design, evaluation, integration, and test of key-related platforms, such as smart cards, authentication mechanisms and new contact-less interface smart cards (+\$1.542).

FY 07: Continue security and functionality testing and evaluation of current PKI tokens and readers to upgrade middleware, including Homeland Security Presidential Directive (HSPD-12) implementation. 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. Complete Defense Message System (DMS) migration to PKI. Continue research and development of solutions to resolve technical challenges and the tools required for deployment of Navy non-Navy/Marine Corps Intranet (NMCI) cryptographic network logon (CLO), CLO for non-Windows operating systems, and NCVI/Online Certificate Status Protocol (OCSP) both Ashore and Afloat. Research and evaluation of Microsoft VISTA integration, PKI with Internet Protocol Version 6 (IPv6), and Device (non-human) Certificates. Begin security and functionality testing and evaluation of OCSP architecture for the SIPRNet (+\$1.485).

Continue EKMS Phase V to include development and implementation of an extended, networked architecture (key distribution over Secret Internet Protocol Router Network (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 and Future fill devices. Begin Wireless Key Fill technology design and development. Complete the Key Loading and Initialization Facility design and development. Continue design and development of the Key Management Infrastructure (KMI) client workstation. Complete certification/accreditation of the Navy's Key Management System (NKMS). Conduct requirements definition for the IA Component (IAC) Encryption device. Continue KMI CI-3 Requirements development including Benign Fill and single point keying, and general development of CI-3 capabilities. Support and ensure coordinated developments for KMI/EKMS in the transition from IPv4 to IPv6 (+\$3.228).

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: February 2007
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
<p>FY 08: 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. Complete Wireless Key Fill technology design and development. Continue to develop Key Management Infrastructure (KMI) Capability Increment 2 (CI-2) client and Advanced Key Processor (AKP), including testing and Hub Management Interface (HMI) development. Continue KMI CI-3 capability development and design including Benign Fill and single point keying. Support and ensure coordinated developments for KMI/EKMS in the transition from Internet Protocol Version 4 (IPv4) to IPv6 (+\$4.191M). Complete security and functionality testing and evaluation of PKI tokens, readers and middleware for the SIPRNET. Continue security and functionality testing and evaluation of PKI tokens and readers to upgrades to middleware, in support of the HSPD-12 biometrics based smart cards. Continue research and development of solutions to resolve technical challenges and the tools required for deployment of Navy non-NMCI CLO, CLO for non-Windows operating systems, and NCVI/OCSP Afloat. Research and develop tools to support Microsoft VISTA implementation, PKI with IPv6, Device (non-human) Certificates, and signature applications/XML document signing. Complete development and integration of NCVI/OCSP ashore. Complete DMS migration to PKI. Support the development and testing of Tactical PKI (as part of DoD KMI) and its supporting architecture (+\$1.499M)</p> <p>FY 09: Continue KMI CI-2 client and Advanced KP security testing and certification and accreditation. Continue KMI CI-3 development support for Advanced Extremely High Frequency (AEHF), Transformational Satellite (TSAT), and Global Information Grid (GIG) requirements for Navy (+\$3.646M). Research and integrate PKI device certificates for mobile devices using 802.1x interfaces. Continue security and functionality testing and evaluation of PKI tokens and readers to support Tactical PKI and HSPD-12 implementation. Research and development of solutions to resolve technical challenges and the tools required for the deployment of MS Exchange 12, full implementation of IPv6, and additional Device (non-human) certificates. Complete development and integration of NCVI ashore, afloat NCVI, and shipboard CLO. Continue to research and develop solutions and tools for signature applications/XML document signing and Public Key Enabled (PKE) (+\$1.589M).</p>		

Exhibit R-2a, RDTEN Budget Item Justification

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification	DATE: February 2007
---	-------------------------------

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 06	FY 07	FY 08	FY 09
Emerging Technology	2.751	3.612	0.000	0.000
RDT&E Articles Quantity				

FY 06: Continued to provide security systems engineering (+\$1.087M) support for the developed of DoD and DoN Information Assurance architectures and the transition of new technologies to address Navy Information Assurance challenges. Supported the ongoing security design and integration of 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), and Secure Voice over Internet Protocol (SVoIP). Provided risk analysis and recommended risk mitigation strategies (+\$1.050M) for Navy critical networks and C4I systems. Coordinated with the Navy acquisition community to ensure IA requirements are identified and addressed within the development cycles for emerging Navy network and C4I capabilities. Continued development of open source authentication and authorization solution (+\$.450M) by incrementally adding new features/enhancements for federated identity, Public Key Infrastructure (PKI), Role Based Access Control (RBAC), and Common Access Card (CAC). Provided standardized security design and installation baselines to ensure enhancements of configuration management. Developed Next Generation Access Systems solutions (+\$0.164M) to provide improved security for access to computers, networks, and sensitive spaces or buildings. Seamless integration with CAC is necessary.

FY 07: Provide security systems engineering (+\$1.523M) support for the developed of DoD and DoN Information Assurance architectures and the transition of new technologies to address Navy Information Assurance challenges. Support the ongoing security design and integration of 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), and Secure Voice over Internet Protocol (SVoIP). Provide risk analysis and recommended risk mitigation strategies (+\$1.180M) for Navy critical networks and C4I systems. Coordinate with the Navy acquisition community to ensure IA requirements are identified and addressed within the development cycles for emerging Navy network and C4I capabilities. Initiate the development and integration (+\$.650M) of IA capabilities for integration into the Service Orientated Architecture being developed for deployment on Navy afloat networks. Provide IA engineering for development of Wireless Networks and Personal Digital Assistant (PDA) security (+\$0.259M) readiness of Naval wireless networks and mobile computing devices, continue to evaluate products for security issues and develop guidance and procedures.

FY08: N/A

FY09: N/A

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification			DATE: February 2007	
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 06	FY 07	FY 08	FY 09
Information Assurance Architectures	0.000	0.000	3.094	2.393
RDT&E Articles Quantity				
**Transitioned from Emerging Technology				
FY06: N/A				
FY07: N/A				
<p>FY 08: Provide security systems engineering (+\$1.5M) support for the development of DoD and DoN Information Assurance (IA) architectures and the transition of new technologies to address Navy Information Assurance challenges. Support the ongoing security design and integration of 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), and Secure Voice over Internet Protocol (SVoIP). Provide risk analysis and recommended risk mitigation strategies (+\$.678M) for Navy critical networks and C4I systems. Coordinate with the Navy acquisition community to ensure IA requirements are identified and addressed within the development cycles for emerging Navy network and C4I capabilities. Continue the development and integration (+\$.641M) of IA capabilities for integration into the Service Orientated Architecture being developed for deployment on Navy afloat networks. Provide IA engineering for development of Wireless Networks and PDA security (+\$.275M) readiness of Naval wireless networks and mobile computing devices, continue to evaluate products for security issues and develop guidance and procedures.</p>				
<p>FY 09: Provide security systems engineering (+\$1.510M) support for the development of DoD and DoN Information Assurance architectures and the transition of new technologies to address Navy Information Assurance challenges. Support the ongoing security design and integration of 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), and Secure Voice over Internet Protocol (SVoIP). Provide risk analysis and recommended risk mitigation strategies (+\$.553M) for Navy critical networks and C4I systems. Coordinate with the Navy acquisition community to ensure IA requirements are identified and addressed within the development cycles for emerging Navy network and C4I capabilities. Provide IA engineering for development of Wireless Networks and PDA security (+\$.330M) readiness of Naval wireless networks and mobile computing devices. Continue to evaluate products for security issues and develop guidance and procedures.</p>				

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Budget Item Justification						DATE: February 2007			
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:									
<u>Line Item No. & Name</u>	<u>FY 2006</u>	<u>FY 2007</u>	<u>FY 2008</u>	<u>FY 2009</u>	<u>FY 2010</u>	<u>FY 2011</u>	<u>FY 2012</u>	<u>FY 2013</u>	
OPN 3415 Info Sys Security Program (ISSP)	97.159	101.340	107.609	120.212	143.237	141.356	146.128	155.913	
(U) D. ACQUISITION STRATEGY:									
<p>EKMS Phase V - The Navy's ISSP Electronic Key Management System (EKMS) program is linked to the National Security Agency's (NSA) strategy in implementing EKMS in evolutionary phases and migrating to Key Management Infrastructure (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 Capability Increment 2 (CI-2). KMI is a 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/PMW 160 is collaborating with Naval Research Lab (NRL) to integrate commercial-off-the-shelf (COTS)/government-off-the-shelf (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. PMW 160 procures 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 Assistant Secretary of the Navy Research, Development & Acquisition (ASN/RDA) policies to reduced cost and streamline the integration, installation, logistics and training efforts.</p> <p>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 SECR ET. 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 Universal Crypto Device (UCD) effort. Navy is currently refining the requirement specs, preparing formal Analysis of Alternatives (AoA), Request For Information (RFI's), and Life Cycle Cost Estimates (LCCE's) to be completed in FY07 and the plan is to competitively award the development contract by 1Q FY08.</p> <p>Crypto Modernization (Universal Crypto Device) - Navy is currently refining the requirement specs, preparing formal AoA, RFI's, and LCCE'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 (Thornton-KEESE) cryptographic system will also necessitate preparation of formal AOA, RFI within FY06 & FY07.</p>									

Exhibit R-2a, RD TEN Budget Item Justification

CLASSIFICATION:

DATE: February 2007												
Exhibit R-3 Cost Analysis (page 1)			PROGRAM ELEMENT				PROJECT NUMBER AND NAME					
APPROPRIATION/BUDGET ACTIVITY			0303140N Information Systems Security Program (ISSP)				0734 Information Systems Security					
RDT&E, N / BA-7												
Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 07 Cost	FY 07 Award Date	FY 08 Cost	FY 08 Award Date	FY 09 Cost	FY 09 Award Date	Cost to Complete	Total Cost	Target Value of Contract
Primary Hardware Development	C/CPFF	VIASAT, Carlsbad, CA	7.282							7.282	7.282	7.282
Primary Hardware Development	C/MIPR	MITRE, San Diego, CA	5.522							5.522	5.522	5.522
Primary Hardware Development	C/VAR	Various	79.477	2.965	VAR	3.054	VAR	3.146	VAR	Continuing	Continuing	Continuing
Systems Engineering	C/VAR	Various	64.300	9.827	VAR	13.162	VAR	15.119	VAR	Continuing	Continuing	Continuing
Subtotal Product Development			156.581	12.792		16.216		18.265		Continuing	Continuing	Continuing
Remarks:												
Software Development	CPAF	SAIC, San Diego, CA	32.877							32.877	32.877	32.877
Software Development	C/WX	NRL, Washington, D.C.	1.798	0.165	11/06	0.180	11/07	0.200	11/08	Continuing	Continuing	Continuing
Software Development	C/VAR	Various		1.135	11/06	1.208	11/07	1.436	11/08	Continuing	Continuing	Continuing
Subtotal Support			34.675	1.300		1.388		1.636		Continuing	Continuing	Continuing
Remarks: SAIC target Value of contract includes other service's funding (ARMY RDT&E).												

CLASSIFICATION:

Exhibit R-3 Cost Analysis (page 2)										DATE: February 2007		
APPROPRIATION/BUDGET ACTIVITY			PROGRAM ELEMENT				PROJECT NUMBER AND NAME					
RDT&E, N / BA-7			0303140N Information Systems Security Program (ISSP)				0734 Information Systems Security					
Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 07 Cost	FY 07 Award Date	FY 08 Cost	FY 08 Award Date	FY 09 Cost	FY 09 Award Date	Cost to Complete	Total Cost	Target Value of Contract
Developmental Test & Evaluation	VAR	Various	23.231	3.000	VAR	3.785	VAR	4.462	VAR	Continuing	Continuing	Continuing
Subtotal T&E			23.231	3.000		3.785		4.462		Continuing	Continuing	Continuing
Remarks:												
Program Management Support	CPAF	Various	5.747	3.851	VAR	4.860	VAR	5.727	VAR	Continuing	Continuing	Continuing
Subtotal Management			5.747	3.851		4.860		5.727		Continuing	Continuing	Continuing
Remarks:												
Total Cost			220.234	20.943		26.249		30.090		Continuing	Continuing	Continuing
Remarks:												

CLASSIFICATION:

EXHIBIT R4, Schedule Profile																DATE: February 2007																			
APPROPRIATION/BUDGET ACTIVITY PROGRAM ELEMENT NUMBER AND NAME																PROJECT NUMBER AND NAME																			
RDT&E, N / BA-7																0734 Information Systems Security																			
0303140N Information Systems Security Program (ISSP)																																			
2006				2007				2008				2009				2010				2011				2012				2013							
1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Acquisition * Milestones																																			
Crypto Mod KW-46 Submarine Replacement/FSBS CDD																																			
Crypto Mod KG-45																																			
EKMS Phase V FOC																																			
CND AAP Designation																																			
CND Inc 1 CDD																																			
CND Inc 1 M/S B																																			
CND Inc 1 M/S C																																			
CDS-M Inc 1 M/S C																																			
CDS-M Inc 2 M/S B																																			
KG-3X Inc 1 M/S C																																			
KG-3X Inc 2 M/S C																																			
KMI M/S C																																			
KMI CI-2 IOC																																			
KMI CI-2 FOC																																			
Test & Evaluation Milestones																																			
Development Test																																			
EKMS Phase V Qual Test																																			
EKMS Phase V Qual Test																																			
KMI Pilots for CI-2 Spiral 1																																			
CND Inc 1 DT																																			
Crypto Mod KW-46 Assured IP																																			
KIV 7M Testing																																			
KG-40AR IV/V Test																																			
KG-40AR NSA Certification																																			
Operational Test																																			
CND Inc 1 OT																																			
EKMS Phase V Op Test																																			
Production Milestones																																			
KIV 7M Production																																			
KIV 7M Installs begin																																			
KG-40AR PM Prod Decision Rev/Award																																			
KG-3X Inc 1 First Articles																																			
KMI Client/AKP FRP																																			
CND Inc 1 LRIP Installs Begin																																			
KG-3X Inc 1 First Articles																																			
Deliveries																																			
EKMS Phase V S/W Delivery LCMS 5.1																																			
EKMS Phase V S/W LCMS 5.1 Delivery																																			
KW-46 LRIP Deliveries																																			
KW-46 LRIP Deliveries																																			
KG-45 LRIP Deliveries																																			
KG-45 LRIP Deliveries																																			

* Note: MLCS Deliveries support the MLCS Capability Certifications

CLASSIFICATION:

Exhibit R-4a, Schedule Detail					DATE: February 2007			
APPROPRIATION/BUDGET ACTIVITY RDT&E, N / BA-7				PROJECT NUMBER AND NAME 0734 Information Systems Security				
Schedule Profile	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013
EKMS Phase V FOC				1Q				
Crypto Modernization KW-46 FSBS CDD		4Q						
Crypto Modernization KCA5 AAP		3Q						
CND AAP		2Q						
CND Inc 1 CDD			1Q					
CND Inc 1 M/S B			2Q					
CND Inc 1 M/S C					2Q			
KG-3X Inc 1 M/S C		2Q						
KG-3X Inc 2 M/S C			4Q					
KMI M/S C				2Q				
KMI CI-2 IOC					3Q			
KMI CI-2 FOC						3Q		
Developmental Test								
EKMS Phase V Qualification Test		2Q						
KMI Pilots for CI-2 Spiral 1				2Q				
CND Inc DT					1Q			
KIV 7M Testing	2Q							
KG-40AR IV/V Test		3Q						
KG-40AR NSA Certification		3Q						
Operational Test								
EKMS Phase V Operational Test		4Q						
Crypto Modernization KW-46 FRP Operational Test (UCD)				4Q	Cont'd-Q4			
CND Inc OT					3Q			
Production Milestones								
KIV 7M Production	4Q							
KIV 7M Installs begin		4Q						
KG-40AR PM Prod Decision Rev/Award		4Q						
KG-3X Inc 1 First Articles		2Q						
KMI Client/AKP FRP				1Q				
CND Inc 1 LRIP Installs Begin					3Q			
Deliveries								
EKMS Phase V S/W Delivery LCMS 5.1		3Q						
Crypto Mod KW-46 LRIP Deliveries			4Q					
KG45 LRIP Deliveries			1Q					

Exhibit R-4, Schedule Detail

CLASSIFICATION:								
EXHIBIT R-2a, RDT&E Project Justification							DATE: February 2007	
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 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013
Project Cost	2.075	1.991	2.144	2.161	2.214	2.244	2.284	2.323
RDT&E Articles Qty								
<p>(U) A. MISSION DESCRIPTION AND BUDGET ITEM JUSTIFICATION:</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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 Information Assurance (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.</p> <p>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 (PMW 160) in pursuance of this effort.</p> <p>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.</p> <p>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.</p>								

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: February 2007
---	--	-------------------------------

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 2006	FY 2007	FY 2008	FY 2009
Software and Systems Research	2.075	1.991	2.144	2.161
RDT&E Articles Quantity				

FY06: Completed the prototype development of the security management common picture of the networked environment with respect to information assurance and security. Completed the addition of security enhancements to cross-domain solutions (CDS), such as stenography scrubbing and user/workstation authentication. Enhanced the multi-level chat capability. Continued to develop new infrastructure protection technologies in support of network centric architectures and warfare concepts. Continued to conceptualize new network centric warfare technology to protect our assets, such as secure network gateways and routers, components, and tools that improve the survivability of Navy networks. Initiated the definition of new network technology critical to the protection of mission assets. Continued systems security engineering, certification, and accreditation support for high-confidence naval information systems.

FY07: Initiate efforts on enhancing commercial wireless technology to meet high assurance requirements, critical for the global information grid (GIG). Initiate the development of an information sharing architecture to address data integrity, confidentiality and policy management throughout networks of varying classification levels. Examine multi-level aware applications and technologies including databases, web browsers, routers/switches, etc. Complete the development of the common operational assessment tool of the networked environment with respect to information assurance and security. This addresses the need for a common operational picture for Information Assurance (IA), as well as assessment of security technology critical to the success of the mission. Continue development and refinement of infrastructure protection and architectures for Navy network centric architectures and warfare concepts. Continue systems security engineering, certification and accreditation support for high-confidence naval information systems and ensure certification and accreditation approaches are consistent with Navy and DoD requirements.

FY08: Continue working with commercial wireless technology to meet high assurance requirements, with particular emphasis on Navy and Marine Corps network centric environments. Initiate the development of wireless technology to augment the security posture of the commercial wireless technology. Continue the development of an information sharing architecture that addresses data integrity, confidentiality and policy management throughout networks of varying classification levels. Within the architecture/infrastructure, enhance the framework to provide on demand security services that support confidentiality, integrity and authentication across security domains, as well as enforces the mission security policy. Continue development and refinement of infrastructure protection and architectures for Navy network centric architectures and warfare concepts. Ensure the architectures evolve to provide proper protection as technology, DoD missions, and the threat all evolve. Include improved defensive protections and response capabilities in the architecture, as well as provide support for traditional intrusion monitoring (sensors) and warning mechanisms. Develop technology and/or tools to ensure the unique security and performance requirements of tactical systems, including those operating at various security levels are addressed. Continue 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.

FY09: Complete the development of the wireless technology to meet high assurance requirements. Place the technology in selected Navy and Marine Corps sites for assessment. Use the feedback to improve the capabilities of the technology to better meet the mission requirements. Continue the development of an information sharing architecture that addresses data integrity, confidentiality and policy management throughout networks of varying classification levels. Evaluate the security services of the framework that support confidentiality, integrity and authentication across security domains, as well as enforces the mission security policy. Use the assessment and operational feedback to improve the framework and security services. Enhance the framework to address survivability and hardening. Develop technology that protects the framework from attacks, assesses the attack, and responds appropriately to enable the framework to reconstitute and provide the requisite capabilities/services. Ensure the architecture/framework evolves to provide proper protection as technology, DoD missions, and the threat all evolve. Initiate development of modernized attack sensing and warning mechanisms based on new algorithms and data mining concepts, and response capabilities for the architecture/framework. Continue the development of technology and tools to ensure the unique security and performance requirements of tactical systems, including those operating at various security levels are addressed. Begin assessing the tools and technology in representative operational environments. Use the feedback to improve the tools and technology. Continue 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 2007
---	----------------------------

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) C. OTHER PROGRAM FUNDING SUMMARY:

<u>Line Item No. & Name</u>	<u>FY 2006</u>	<u>FY 2007</u>	<u>FY 2008</u>	<u>FY 2009</u>	<u>FY 2010</u>	<u>FY 2011</u>	<u>FY 2012</u>	<u>FY 2013</u>
OPN 3415 Info Sys Security Program (ISSP)	97.159	101.340	107.609	120.212	143.237	141.356	146.128	155.913
RDT&E 0303140N Info Sys Security (ISSP)	18.007	20.943	26.249	30.090	28.141	29.452	31.890	32.448

(U) D. ACQUISITION STRATEGY:

N/A.

UNCLASSIFIED

CLASSIFICATION

Exhibit R-3, Code Analysis (page 1)				DATE: February 2007								
APPROPRIATION/BUDGET ACTIVITY RDT&E,N/ BA-7			PROGRAM ELEMENT 0303140N/ INFORMATION SYSTEMS SECURITY PROGRAM				PROJECT NUMBER AND NAME 0734 Communications Security					
Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 07 Cost	FY 07 Award Date	FY 08 Cost	FY 08 Award Date	FY 09 Cost	FY 09 Award Date	Cost to Complete	Total Cost	Target Value of Contract
Hardware Development												
Subtotal Product Development			0.000	0.000		0.000		0.000		0.000	0.000	
Remarks:												
Software Development	WX	NRL, Washington, D.C.	4.162	1.991	10/06	2.144	10/07	2.161	10/08	Continuing	Continuing	
Subtotal Support			4.162	1.991		2.144		2.161		Continuing	Continuing	
Remarks:												

UNCLASSIFIED

CLASSIFICATION

Exhibit R-3, Code Analysis (page 1)										DATE: February 2007		
APPROPRIATION/BUDGET ACTIVITY			PROGRAM ELEMENT				PROJECT NUMBER AND NAME					
RDT&E,N/ BA-7			0303140N/ INFORMATION SYSTEMS SECURITY PROGRAM				0734 Communications Security					
Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 07 Cost	FY 07 Award Date	FY 08 Cost	FY 08 Award Date	FY 09 Cost	FY 09 Award Date	Cost to Complete	Total Cost	Target Value of Contract
Developmental Test & Evaluation												
Subtotal T&E			0.000	0.000		0.000		0.000		0.000	0.000	
Remarks:												
Program Management Support												
Subtotal Management			0.000	0.000		0.000		0.000		0.000	0.000	
Remarks:												
Total Cost			4.162	1.991		2.144		2.161		Continuing	Continuing	
Remarks:												

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification			DATE: February 2007	
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 Increases		
(U) B. Accomplishments/Planned Program				
	FY 06	FY 07	FY 08	FY 09
9430 SECUREKit	1.280	0.996		
9A99 Tactical Key Loader		3.188		
RDT&E Articles Quantity				
<p>FY06: SECUREKit: Further refined design of authorization software to include integration with authentication service, Navy Enterprise Single Sign-On (NESSO) and Trusted Services Engine (TSE). Integrated the product within test networks and worked 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.</p> <p>FY07: SECUREKit: Continue further refinement of the administration interface to the underlying authorization engine. Begin to integrate the SECUREKit trusted authorization processing engine with the discovery application. Begin Certification and Accreditation (C&A) documentation required to achieve a type accreditation. Begin Authority to Operate (ATO) on Secret Internet Protocol Router Network (SIPRNET) and Non-Classified Internet Protocol Router Network (NIPRNET).</p> <p>Tactical Key Loader: Begin system engineering activities to include requirements analysis, investigation of new technologies, development of prototype and Engineering Development Models, as well as test and evaluation of these units in the lab and operational environments. Integrated logistic support and supportability of the device once fielded will also be ascertained. Initiate development, and investigation of National Security Agency assessment certification requirements. Software and hardware will need to be develop and tested to assure it meets the needs of the Special Forces/USMC warfighter. Tradeoffs must be made to address security concerns of the NSA and still meet the special needs of the warfighter. This device must also be developed so that it will transition to the modern keying environment brought by KMI.</p>				

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: February 2007
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 Increases

(U) B. Accomplishments/Planned Program

	FY 06	FY 07	FY 08	FY 09
9903 Universal Description, Discovery, and Integration		1.793		
RDT&E Articles Quantity				

FY07: Universal Description, Discovery, and Integration: Begin systems development that will allow users to discover and access valuable information at the right time based on the user's access clearance and need to know. A trusted discovery service will ensure that information accessed is at the appropriate level, provide the requisite information and prevent extraneous or unauthorized inputs and access. Over-riding the rule set with the trusted discovery service will be configurable based on the users role and the rules of engagement. 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, begin the development of a component-based architecture called Secure Universal Description, Discovery, and Integration (UDDI). Secure UDDI will provide the necessary components to meet the Naval warfighter requirements.

- (1) Secure and non-reputable repository of services and information base on current open standards such as UDDI V3.
- (2) Incorporation of NSA certified SECUREKit components for authentication and authorization.
- (3) Secure discovery of services and information.

The evolutionary component architecture of the Secure UDDI architecture is being accomplished through partnering efforts with the National Security Agency (NSA) and PEO(C4I).