EXHIBIT R-2, RDT&E Budget Item Justification				DATE: February 2008			
APPROPRIATION/BUDGET ACTIVITY RESEARCH DEVELOPMENT TEST & EVALUATION, NAVY / BA-7		R-1 ITEM NOMENCLATURE 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)					
COST ($ in Millions)	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013
Total PE Cost	**30.133**	**34.337**	**27.037**	**24.404**	**28.557**	**30.769**	**31.699**
0734 Information Systems Security	19.789	26.252	24.894	22.181	26.303	28.472	29.359
0734 Communications Security (ONR)	4.491	2.124	2.143	2.223	2.254	2.297	2.340
9999 Congressional Increases	5.853	5.961					
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 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.

(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.

Exhibit R-2, RDTEN Budget Item Justification

EXHIBIT R-2, RDT&E Budget Item Justification	DATE: February 2008
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 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.

(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.

(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.

EXHIBIT R-2, RDT&E Budget Item Justification	DATE: February 2008
APPROPRIATION/BUDGET ACTIVITY RESEARCH DEVELOPMENT TEST & EVALUATION, NAVY/BA-7	R-1 ITEM NOMENCLATURE 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)

(U) B. PROGRAM CHANGE SUMMARY:

(U) Funding:	FY 2007	FY 2008	FY 2009
FY08/09 President's Budget	28.911	28.393	32.251
FY 09 President's Submit	30.133	34.337	27.037
Total Adjustments	1.222	5.944	-5.214
Summary of Adjustments			
Small Business Innovation Research (SBIR) Tax	-0.357	-0.331	
Funds moved to project X2144 SEW Engineering for MDA	-0.921		
Information Assurance (IA)		0.500	
Tactical Key Loader		3.200	
"Universal Description"		2.800	
Sec. 8097: Contractor Efficiencies		-0.053	
Sec. 8104: Revised Economic Assumptions		-0.166	
Sec. 8025: FFRDC Reduction		-0.006	
Misc. Realignments			-2.833
Misc. Adjustments	2.500		-2.381
Subtotal	1.222	5.944	-5.214

(U) Schedule:

x0734: KG-3X Inc 1 schedule change reflects the delay in NSA Certification of the End Cryptographic Unit (ECU).
KMI schedule reflects a restructure that combined Spiral 2 and Spiral 3. Delay in approval of KMI MS C has resulted in a slip of the production contract award.
EKMS Phase 5, FOC is based upon receipt of EKMS Phase 5 Software (LCMS/CUAS 5.1) and its certification from NSA. The delay in NSA's certification has pushed FOC to the right.

(U) Technical:

N/A.

EXHIBIT R-2a, RDT&E Project Justification						DATE: February 2008	
APPROPRIATION/BUDGET ACTIVITY RDT&E, N / BA-7	PROGRAM ELEMENT NAME AND NUMBER 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)			PROJECT NUMBER AND NAME 0734 INFORMATION SYSTEMS SECURITY			
COST ($ in Millions)	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013
Project Cost	**19.789**	**26.252**	**24.894**	**22.181**	**26.303**	**28.472**	**29.359**
RDT&E Articles Qty							

(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.

(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).

(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.

(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.

(U) The ISSP today includes much more than legacy 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-based 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 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).

(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.

EXHIBIT R-2a, RDT&E Project Justification		DATE: February 2008
APPROPRIATION/BUDGET ACTIVITY	**PROGRAM ELEMENT NAME AND NUMBER**	**PROJECT NUMBER AND NAME**
RDT&E, N / BA-7	0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	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 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).

(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:

(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 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.

(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:

- 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.

EXHIBIT R-2a, RDT&E Project Justification		DATE: February 2008
APPROPRIATION/BUDGET ACTIVITY	**PROGRAM ELEMENT NAME AND NUMBER**	**PROJECT NUMBER AND NAME**
RDT&E, N / BA-7	0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	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.

Exhibit R-2a, RDTEN Budget Item Justification

EXHIBIT R-2a, RDT&E Project Justification		DATE: February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, N / BA-7	PROGRAM ELEMENT NAME AND NUMBER 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	PROJECT NUMBER AND NAME 0734 INFORMATION SYSTEMS SECURITY

(U) B. Accomplishments/Planned Program

	FY 07	FY 08	FY 09
Computer Network Defense (CND)	5.261	9.411	8.705
RDT&E Articles Quantity			

FY07: Provided the broadest range of Information Assurance (IA) research and development support across Joint, Fleet, and ashore networks. Provided on-going security of new ships, aircraft, and submarines to ensure reduced manning and greater operational dependency on networks. Provided IA engineering design, 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. Provided IA engineering to translate FORCEnet capabilities into CND solutions and conduct security design evaluations certification test results. Included IA appliances, software, and implementation techniques for policies such as IAVA requirements, Information Operation Condition (INFOCON) response, and USN firewall policy. Provided continuous development of a Shipboard unit level tier situation information management system 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. Continued the development of using authenticated administrator access control techniques enhance fielded Security Management Tools with new capabilities to support system configuration management and monitoring. Began 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. Established 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. Evaluated the combined system security effectiveness between each systems networking layer end-to-end, data link layer security through application exchange layer security.

FY08: Integrate security situational awareness technologies 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. Initiate the development of the process to assign asset criticality at the host and application level through the use of the data in the new tool.

Conduct a pilot to address data-at-rest protection on mobile and removable devices.

FY09: 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. 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.

EXHIBIT R-2a, RDT&E Project Justification		DATE: February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, N / BA-7	PROGRAM ELEMENT NAME AND NUMBER 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	PROJECT NUMBER AND NAME 0734 INFORMATION SYSTEMS SECURITY

	FY 07	FY 08	FY 09
Crypto	5.082	7.093	8.755
RDT&E Articles Quantity			

FY07: Continued to provide cryptographic products, including Type-1 US only, allied and coalition, and commercial-off-the-shelf. Provided consistent IA engineering support for the development 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, KIV-19, KIV 7M, KG-194 (Walburn), Thorton-KEESEE-SAVILLE and KW-46, KG-45, KL-51, KGV-68B (based on UCD development). Continued acquisition documentation mandated by Joint Capabilities Integration and Development System (JCIDS) for development of identified cryptographic devices for replacement in FY06. Continued 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. Applied and implemented HAIPE in transformational architectures such as FORCEnet and Joint Tactical Radio System Wideband Networking Waveform (JTRS WNW), and developed integration solutions for modernized INE devices and Key Management, FNBDT and Wireless capabilities. Continued to research and develop potential uses of type-2 & 3 for use in type-1 historical environments. Established solutions for DoN unique Crypto's including: IOC for KL-51; Solution identified for KG-45; and Solution identified for KWR-46. Established first Air Force/DoN LPO. Published Crypto Product Roadmap and complete UCD requirements specifications and source selection for first UCD product. Established Industry Working Group charter. Validated Information Assurance Cryptographic Product (IACP) Management Tool. Completed KEESEE Integrated Product Team (IPT) (90% of Navy operational Crypto devices identified) and completed SAVILLE IPT (90% Crypto's identified).

FY08: 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.

FY09: 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. Develop program documentation and way ahead crypto identified devices. Continue to support to the on-going Cryptographic Joint integrated product team. Continue pre-acquisition and development of LINK 16 Common Crypto Module, VINSON/ANDVT Crypto Mod (VACM), Programmable Objective Encryption Technologies (POET), KW-46 Fleet Submarine Broadcast System (FSBS), and Telemetry. The Crypto Modernization Program Office (CMPO) will be developing LINK 16, KW46 and VACM, increasing the funding requirement from FY08 to FY09. Modernizing these devices will provide replacements in accordance with the Joint Chief of Staff's modernization schedule and NSA's planned decertification.

EXHIBIT R-2a, RDT&E Project Justification		DATE: February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, N / BA-7	PROGRAM ELEMENT NAME AND NUMBER 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	PROJECT NUMBER AND NAME 0734 INFORMATION SYSTEMS SECURITY

	FY 07	FY 08	FY 09
Information Assurance Readiness	0.254	0.000	0.000
RDT&E Articles Quantity			

FY07: Provided 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. Provided continued Antivirus Tools support and capabilities for R&D support systems and software to meet Navy Anti-Virus requirements.

EXHIBIT R-2a, RDT&E Project Justification		DATE: February 2008
APPROPRIATION/BUDGET ACTIVITY	**PROGRAM ELEMENT NAME AND NUMBER**	**PROJECT NUMBER AND NAME**
RDT&E, N / BA-7	0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	0734 INFORMATION SYSTEMS SECURITY

	FY 07	FY 08	FY 09
Secure Voice	0.658	1.127	1.118
RDT&E Articles Quantity			

FY07: Completed development and integration test of submarine Secure Communication Interoperability Protocol (SCIP) Inter-working Function (IWF)/gateway providing off-ship secure communication capabilities while underway. Began development and tested SCIP IWF providing off-ship secure voice communications underway Military Sealift Command ships and Coast Guard ships. Updated the Naval Advanced Secure Voice Architecture (NASVA) providing a transition to bridge from channel-centric to net-centric Secure Voice capability, guiding the next generation of Secure Voice and facilitated decision making on systems to be refreshed, retired and/or replaced. Continued development of the variable data rate voice algorithm (a component of Secure Voice Core Technology) and its baseline interface software. Initiated generation of baseline functionality (derived from operational and mission requirements and new technologies) and designed of a functional model for development of next generation secure voice products - Universal Voice Terminal (UVT) and Personal Secure Telephone (PST). Researched and developed a compression technique (SCIP IWF or gateway) allowing SCIP IWF signaling be transmitted off-ship for underway submarines.

FY08: Complete development and integration test of submarine SCIP IWF/gateway to provide off-ship secure communication capabilities while underway. Continue development and test a SCIP IWF to provide off-ship secure voice communications to underway Military Sealift Command (MSC) ships and Coast Guard 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).

FY09: Complete development and integration test of the SCIP IWF for MSC and Coast Guard ships. Continue the design and development of next generation voice and Secure Voice capabilities for shipboard voice services modernization and consolidation. Continue Small Business Innovative Research phase II R&D efforts.

EXHIBIT R-2a, RDT&E Project Justification		DATE: February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, N / BA-7	PROGRAM ELEMENT NAME AND NUMBER 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	PROJECT NUMBER AND NAME 0734 INFORMATION SYSTEMS SECURITY

	FY 07	FY 08	FY 09
Cross Domain Solutions (CDS)	0.669	0.000	0.000
RDT&E Articles Quantity			

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

FY07: Continued providing systems security engineering development, testing, and evaluation for multi-level security solutions, including complicated evaluations involving allied and coalition participation. Examined and evaluated multi-level aware applications and technologies including databases, web browsers, routers/switches, etc. Developed and integrated Multiple Security Levels (MSL)/CDS prototype architecture at NOC facilities.

EXHIBIT R-2a, RDT&E Project Justification		DATE: February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, N / BA-7	PROGRAM ELEMENT NAME AND NUMBER 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	PROJECT NUMBER AND NAME 0734 INFORMATION SYSTEMS SECURITY

	FY 07	FY 08	FY 09
Key Management Infrastructure	4.453	5.585	4.056
RDT&E Articles Quantity			

FY07: Continued security and functionality testing and evaluation of current PKI tokens and readers upgrading middleware, including Homeland Security Presidential Directive (HSPD-12) implementation. Continued streamlining the method for development of effective secure symmetric and asymmetric cryptographic key and generation, distribution, management, and usage products and services by identification and prioritization of fleet requirements. Completed Defense Message System (DMS) migration to PKI. Continued 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. Researched and evaluated of Microsoft VISTA integration, PKI with Internet Protocol Version 6 (IPv6), and Device (non-human) Certificates. Began security and functionality testing and evaluation of OCSP architecture for the SIPRNet.

Continued EKMS Phase V to include development and implementation of an extended, networked architecture (key distribution over Secret Internet Protocol Router Network (SIPRNET)) improving distribution and reliability for deployed forces, modernized key processors, common user application software and data transfer devices. Continued to develop and integrate Online Certificate Status Protocol and Future fill devices. Began Wireless Key Fill technology design and development. Completed the Key Loading and Initialization Facility design and development. Continued design and development of the Key Management Infrastructure (KMI) client workstation. Completed certification/accreditation of the Navy's Key Management System (NKMS). Conducted requirements definition for the IA Component (IAC) Encryption device. Continued KMI CI-3 Requirements development including Benign Fill and single point keying, and general development of CI-3 capabilities. Supported and ensured coordinated developments for KMI/EKMS in the transition from IPv4 to IPv6.

FY08: 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. 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.

FY09: 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. 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. Continue to research and develop solutions and tools for signature applications/XML document signing and Public Key Enabled (PKE).

EXHIBIT R-2a, RDT&E Project Justification		DATE: February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, N / BA-7	PROGRAM ELEMENT NAME AND NUMBER 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	PROJECT NUMBER AND NAME 0734 INFORMATION SYSTEMS SECURITY

	FY 07	FY 08	FY 09
Emerging Technology	3.412	0.000	0.000
RDT&E Articles Quantity			

FY07: Provided security systems engineering support for the development of DoD and DoN Information Assurance architectures and the transition of new technologies addressing 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 for Navy critical networks and C4I systems. Coordinated with the Navy acquisition community ensuring IA requirements are identified and addressed within the development cycles for emerging Navy network and C4I capabilities. Initiated the development and integration of IA capabilities for integration into the Service Orientated Architecture being developed for deployment on Navy afloat networks. Provided IA engineering for development of Wireless Networks and Personal Digital Assistant (PDA) security readiness of Naval wireless networks and mobile computing devices, continued to evaluate products for security issues and develop guidance and procedures.

EXHIBIT R-2a, RDT&E Project Justification		DATE: February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, N / BA-7	PROGRAM ELEMENT NAME AND NUMBER 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	PROJECT NUMBER AND NAME 0734 INFORMATION SYSTEMS SECURITY

	FY 07	FY 08	FY 09
Information Assurance Architectures	0.000	3.036	2.260
RDT&E Articles Quantity			

****Transitioned from Emerging Technology**

FY08: Provide security systems engineering 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 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 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 readiness of Naval wireless networks and mobile computing devices, continue to evaluate products for security issues and develop guidance and procedures.

FY09: Provide security systems engineering 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 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 readiness of Naval wireless networks and mobile computing devices. Continue to evaluate products for security issues and develop guidance and procedures.

EXHIBIT R-2a, RDT&E Budget Item Justification		DATE: February 2008
APPROPRIATION/BUDGET ACTIVITY RDT&E, N / BA-7	PROGRAM ELEMENT NAME AND NUMBER 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 2007	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013
OPN 3415 Info Sys Security Program (ISSP)	101.310	121.131	101.153	130.983	139.741	146.407	155.552

(U) D. ACQUISITION STRATEGY:

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. NSA certified COTS/GOTS devices are procured 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.

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 has refined the requirement specs, preparing formal Analysis of Alternatives (AoA), Request For Information (RFIs), and Life Cycle Cost Estimates (LCCEs) in 1Q FY08 and the plan is to competitively award the development contract in 2Q FY08.

Crypto Modernization (Universal Crypto Device) - Navy has refined the requirement specs, preparing formal AoA, RFIs, and LCCEs, and was completed in FY07. Plan is to competitively award the development contract by 3Q FY08. The evaluation of requirements of Crypto Modernization (Thorton-KEESEE) cryptographic system will also necessitate preparation of formal AOA, RFI within FY08.

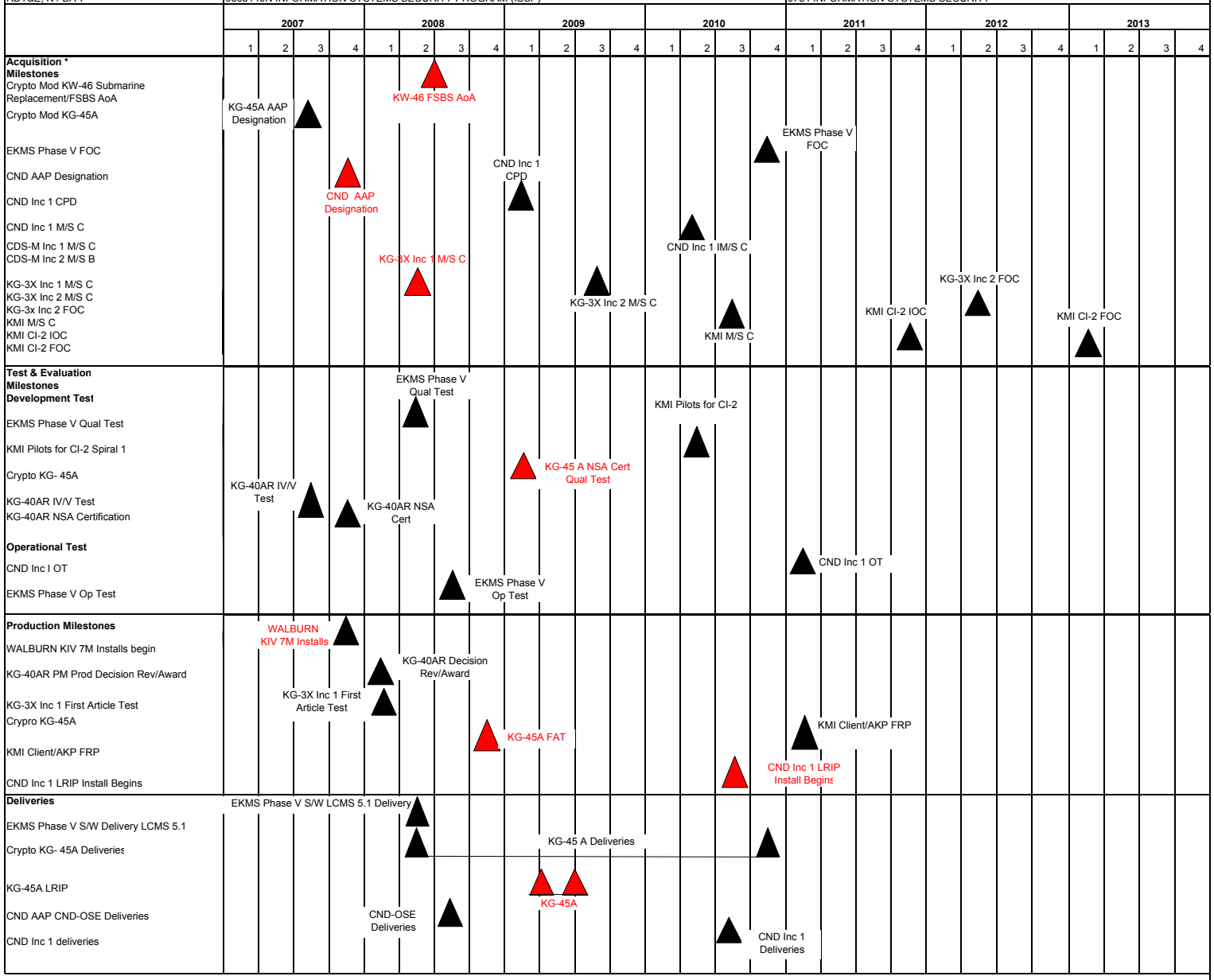
Exhibit R-3 Cost Analysis (page 1)												DATE: February 2008
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**			**PROGRAM ELEMENT** 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)				**PROJECT NUMBER AND NAME** 0734 INFORMATION SYSTEMS SECURITY					
Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 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	2.958	VAR	3.054	VAR	3.166	VAR	Continuing	Continuing	Continuing
Systems Engineering	C/VAR	Various	64.300	9.281	VAR	12.665	VAR	11.176	VAR	Continuing	Continuing	Continuing
Subtotal Product Development			156.581	12.239		15.719		14.342		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	0.975	11/06	0.180	11/07	0.200	11/08	Continuing	Continuing	Continuing
Software Development	C/VAR	Various		1.200	11/06	1.208	11/07	1.236	11/08	Continuing	Continuing	Continuing
Subtotal Support			34.675	2.175		1.388		1.436		Continuing	Continuing	Continuing
Remarks: SAIC target Value of contract includes other service's funding (ARMY RDT&E).												

Exhibit R-3, Project Cost Analysis

Exhibit R-3 Cost Analysis (page 2)									DATE: February 2008		
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 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	2.755	VAR	4.285	VAR	4.424	VAR	Continuing	Continuing	Continuing
Subtotal T&E			23.231	2.755		4.285		4.424		Continuing	Continuing	Continuing
Remarks:												
Program Management Support	CPAF	Various	5.747	2.620	VAR	4.860	VAR	4.692	VAR	Continuing	Continuing	Continuing
Subtotal Management			5.747	2.620		4.860		4.692		Continuing	Continuing	Continuing
Remarks:												
Total Cost			220.234	19.789		26.252		24.894		Continuing	Continuing	Continuing
Remarks:												

Exhibit R-3, Project Cost Analysis

EXHIBIT R4, Schedule Profile		DATE: February 2008
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



* Note: MLCS Deliveries support the MLCS Capability Certifications

Exhibit R-4a, Schedule Detail				DATE: February 2008			
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	**PROGRAM ELEMENT NUMBER AND NAME** 0303140N INFORMATION SYSTEMS SECURITY PR			PROJECT NUMBER AND NAME 0734 INFORMATION SYSTEMS SECURITY			
Schedule Profile	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013
EKMS Phase V FOC				4Q			
Crypto Modernization KW-46 FSBS AoA		3Q					
Crypto Modernization KG-45 AAP	3Q						
CND AAP	4Q						
CND Inc 1 CPD			1Q				
CND Inc 1 M/S C				2Q			
KG-3X Inc 1 M/S C		2Q					
KG-3X Inc 2 M/S C			3Q				
KG-3X Inc 2 FOC						2Q	
KMI M/S C				3Q			
KMI CI-2 IOC					4Q		
KMI CI-2 FOC							1Q
Developmental Test							
EKMS Phase V Qualification Test		2Q					
EKMS Phase V OP Test		3Q					
KMI Pilots for CI-2 Spiral 1				2Q			
Crypto KG-45A NSA Cert			1Q				
KG-40AR IV/V Test	3Q						
KG-40AR NSA Certification	4Q						
Operational Test							
EKMS Phase V Operational Test		3Q					
CND Inc OT					1Q		
Production Milestones							
WALBURN KIV 7M Production							
WALBURN KIV 7M Installs begin	4Q						
KG-40AR PM Prod Decision Rev/Award		1Q					
KG-45 FAT		4Q					
KG-3X Inc 1 First Articles		1Q					
KMI Client/AKP FRP					1Q		
CND Inc 1 LRIP Installs Begin				3Q			
CND Inc 1 First Articles				3Q			
Deliveries							
EKMS Phase V S/W Delivery LCMS 5.1		2Q					
KG45 LRIP Deliveries			2Q				
Crypto KG-45 Deliveries		2Q					
CND AAP CND-OSE Deliveries		3Q					
CND Inc 1 deliveries				3Q			

Exhibit R-4, Schedule Detail

EXHIBIT R-2a, RDT&E Project Justification							DATE: February 2008
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 2007	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013
Project Cost	**4.491**	**2.124**	**2.143**	**2.223**	**2.254**	**2.297**	**2.340**
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.

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.

EXHIBIT R-2a, RDT&E Project Justification		DATE: February 2008
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 2007	FY 2008	FY 2009
Software and Systems Research	4.491	2.124	2.143
RDT&E Articles Quantity			

FY07: Initiated efforts on enhancing commercial wireless technology to meet high assurance requirements, critical for the global information grid (GIG). Initiated the development of an information sharing architecture addressing data integrity, confidentiality and policy management throughout networks of varying classification levels. Examined multi-level aware applications and technologies including databases, web browsers, routers/switches, etc. Completed the development of the common operational assessment tool of the networked environment with respect to information assurance and security. This addressed 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. Continued development and refinement of infrastructure protection and architectures for Navy network centric architectures and warfare concepts. Continued systems security engineering, certification and accreditation support for high-confidence naval information systems and ensured certification and accreditation approaches were 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.

EXHIBIT R-2a, RDT&E Project Justification		DATE: February 2008
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:

Line Item No. & Name	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013
OPN 3415 Info Sys Security Program (ISSP)	101.310	121.131	101.153	130.983	139.741	146.407	155.552

(U) D. ACQUISITION STRATEGY:

N/A.

Exhibit R-2a, RDTEN Budget Item Justification

Exhibit R-3, Code Analysis (page 1)				DATE: February 2008								
APPROPRIATION/BUDGET ACTIVITY RDT&E,N / BA-7		PROGRAM ELEMENT 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)					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 Develop			0.000	0.000		0.000		0.000		0.000	0.000	
Remarks:												
Software Development	WX	NRL, Washington, D.C.	4.162	4.491	10/06	2.124	10/07	2.143	10/08	Continuing	Continuing	
Subtotal Support			4.162	4.491		2.124		2.143		Continuing	Continuing	
Remarks:												

Exhibit R-3, Project Cost Analysis

Exhibit R-3, Code Analysis (page 1)									DATE: February 2008			
APPROPRIATION/BUDGET ACTIVITY **RDT&E,N / BA-7**			PROGRAM ELEMENT 0303140N INFORMATION SYSTEMS SECURITY PR				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
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	4.491		2.124		2.143		Continuing	Continuing	
Remarks:												

Exhibit R-3, Project Cost Analysis

EXHIBIT R-2a, RDT&E Project Justification		DATE: February 2008
APPROPRIATION/BUDGET ACTIVITY	**PROGRAM ELEMENT NUMBER AND NAME**	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N INFORMATION SYSTEMS SECURITY PROG	9999 CONGRESSIONAL INCREASES

(U) B. Accomplishments/Planned Program

	FY 07	FY 08	FY 09
9430 SECUREKit	0.971		
9A99 Tactical Key Loader	3.128	3.180	
RDT&E Articles Quantity			

FY07: SECUREKit: Continued further refinement of the administration interface to the underlying authorization engine. Began integration of SECUREKit trusted authorization processing engine with the discovery application. Began 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).

Tactical Key Loader: Began 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. Initiated development, and investigation of National Security Agency assessment certification requirements. Software and hardware will continue to be developed and tested to assure it meets the needs of the Special Forces/USMC warfighter. Tradeoffs have been made to address security concerns of the NSA and still meet the special needs of the warfighter. This device will continue to be developed so that it will transition to the modern keying environment brought by KMI.

FY08: Tactical Key Loader: Establish the TKL as an Abbreviated Acquisition Program. 1) System specification and design, 2) Hardware specification, design, and development of hardware mockups and breadboards, 3) Software specification, design, and development, and 4) Security specification, design, and input into the hardware and software development efforts. 5) Build TKL test and evaluation laboratory with laboratory space provided by SPAWARSYSCEN San Diego (SSC-SD).

EXHIBIT R-2a, RDT&E Project Justification		DATE: February 2008
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	**PROGRAM ELEMENT NUMBER AND NAME** 0303140N INFORMATION SYSTEMS SECURITY PROG	**PROJECT NUMBER AND NAME** 9999 CONGRESSIONAL INCREASES

(U) B. Accomplishments/Planned Program

	FY 07	FY 08	FY 09
9903 Universal Description, Discovery, and Integration	1.754	2.781	
RDT&E Articles Quantity			

FY07: Universal Description, Discovery, and Integration: Began 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 allows 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, began 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.

FY08: Universal Description, Discovery, and Integration: Continue systems development of a demonstrable prototype 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. Efforts will also include support for Semantic services based on OWL-S and ebXML, Machine-to-Machine interfaces, and support to bridge OWL-S and WSDL based services. 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. The web architecture-based solution allows 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 Net-Centric Operations, continue 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 for both WSDL and OWL-S based services.

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