CLASSIFICATION:

EXHIBIT R-2, RDT&E Budget Item Justification						DATE: **February 2005**		
APPROPRIATION/BUDGET ACTIVITY **RESEARCH DEVELOPMENT TEST & EVALUATION, NAVY / BA-7**					R-1 ITEM NOMENCLATURE 0303140N Information Systems Security Program (ISSP)			
COST ($ in Millions)	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Total PE Cost	**25.769**	**26.511**	**28.660**	**33.490**	**34.071**	**34.299**	**33.052**	**34.363**
0734 Information Systems Security	**16.469**	**16.526**	**26.555**	**31.434**	**31.829**	**32.100**	**30.801**	**32.060**
0734 Communications Security	**2.271**	**1.973**	**2.105**	**2.056**	**2.242**	**2.199**	**2.251**	**2.303**
9281 Intelligent Agent Security Module	**5.300**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**
9430 SECURE Kit	**1.729**	**4.547**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**
9647 Collaborative Information Warfare Network	**0.000**	**3.465**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**
Quantity of RDT&E Articles								

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

(U) The goal of the Navy Information Systems Security Program (ISSP) is to ensure the continued protection of Navy and Joint information, telecommunications, and information systems from hostile exploitation and attack. The ISSP is the Navy's implementation of statutory and regulatory requirements specified in Presidential Decision Directive 63, the Computer Security Act of 1987 (Public Law 100 235), Appendix III of Office of Management and Budget (OMB) Circular A-130, and DOD Directive 8500.1. ISSP activities address the triad of Defensive Information Operations defined in Joint Publication 3-13; protection, detection, and reaction. Evolving detection and reaction responsibilities extend far beyond the traditional ISSP role in protection or Information Security (INFOSEC). Focused on FORCEnet supporting the highly mobile forward-deployed subscriber, the US Navy's implementation of Network-Centric Warfare (NCW) places demands upon the ISSP, as the number of users explodes 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, attachment to the public information infrastructure, and their use in modern Naval and Joint war fighting means that FORCEnet is an extremely high value and more easily attainable target for our enimies. 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 Navy 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, 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.

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2, RDT&E Budget Item Justification	DATE: **February 2005**
APPROPRIATION/BUDGET ACTIVITY **RESEARCH DEVELOPMENT TEST & EVALUATION, NAVY BA-7**	R-1 ITEM NOMENCLATURE 0303140N Information Systems Security Program (ISSP)

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

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

(U) The interconnection of FORCEnet into the DOD 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.

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification								DATE: **February 2005**	
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 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Project Cost		**16.469**	**16.526**	**26.555**	**31.434**	**31.829**	**32.100**	**30.801**	**32.060**
RDT&E Articles Qty									

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

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

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

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

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

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

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

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2005**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	0734 Information Systems Security

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

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

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

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

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

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

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

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2005**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	0734 Information Systems Security

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

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

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

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2005**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	0734 Information Systems Security

(U) B. Accomplishments/Planned Program

	FY 04	FY 05	FY 06	FY 07
Network Security Mission Capability Team (MCT)	2.635	2.965	7.195	8.295
RDT&E Articles Quantity				

FY04 Accomplishments include:
$2,635- Continue to integrate security products and new technologies for robust Computer-Network (CND) for both shore and afloat installation. Accomplished system product evaluations for improved boundary security to enhance computer-network systems with greater performance, critical asset vulnerability prevention, and ever increasing insider threat. Continued to integrate CND afloat components to include Information Assurance (IA) administration tools, network & host intrusion detectionsystems, and client distributed embedded firewalls. Conducted CND Shore based IA system security accreditation and developed improvements for enhanced intrusion prevention, vulnerability alert administration, and active threat reporting. Initiated online web based information server for engineering support to access subject matter on system security, Network Operating Center (NOC) site 'As Built' Configuration Data, support emergency restoration, automate security system, Information assurance Vulnerability assessment (IAVA) distribution. Began product evaluations for improved security measures against insider threats and malicious code exploit. Piloted site evaluations with email SPAM elimination applications and expanded virus scanning of application protocols such as: POP3, HTTP, and FTP. Evaluated options to develop Strike Group deployment of CND IA system management and situation awareness reporting; continue to evaluate system solutions for Surface Combatant Class ships to enforce CND security policies and counter evolving cyber attacks.

FY05 Plans include:
$2,965- Continue to integrate security products and new technologies for robust Computer-Network (CND) for both shore and afloat installation. Effort will be focused on CND system development to address recurring exploits against forward deployed units; to integrate CND management tools into a cohesive suite for unit level defense. Development to extend the security boundaries beyond the NOC's to enforce adaptive network security based on changing INFOCON policies, operator needs, and operational environments will be evaluated. Continue system security engineering design, modeling, technical evaluations, testing, and validation to formulate Commercial and Government product infusion for CND enhancement. Develop advanced IA tool kits to assist information system security managers to maintain computer network security posture and provide for vulnerability self assessment and remediation verification. Assess security systems to field capabilities to minimize the impact of the insider threat and to minimize the potential damage inflicted on information integrity or computer-network information systems. Enhance CND with leading technologies to block attacks with intrusion prevention management; to counter increasing threats posed by system vulnerabilities, malicious code, and malevolent insiders. Address user authorization and authentication techniques for system administration, remote user access, and enforce access controls on critical computer-network components. IA network components will be reviewed for application on UNCLASSIFIED through SECRET application networks and coordination with TOP SECRET host application requirements to provide the broadest support solution as possible.

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2005**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	0734 Information Systems Security

FY 06 Plans include:
$7,195- Continue to integrate security products and new technologies for robust Computer-Network (CND) for both shore and afloat installation. Provide IA engineering design (+$2.905M), evaluation, and testing techniques from end-to-end, through base-band networks, RF communications links, and information source-to-sink to satisfy the IA element of maintaining availability. Includes IA appliances, software, and implementation techniques for policies such as IAVA requirements, INFOCON response, and USN firewall policy. Begin development of a tier level management system (+$2M) between Unit Level Ships and Global Enterprise Management for real-time display of security risk as: Computer-Network Threats, Vulnerabilities, and Critical System Security Performance. Begin development of a Global Enterprise Management system to integrate a secure means of hierarchically managing Network Operating Center security systems, Ship Security Monitors, and other Network Security Monitoring products. Begin development of improved real-time computer-network security policy administration (+$0.925M) 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 Detection Systems (IDS), and Filtering Routers at unit level ships and fleet Network Operation Centers. Begin development of enhanced fielded Security Management Tools (+$1.365M) with new capabilities to support system configuration management and monitoring. Support development of online engineering support to access subject matter security system experts; automate security system IAVA distributions, web based information server, NOC site 'As Built' Configuration Data, and Emergency Restoration Files. Develop an IAVA verification assessment system to status Network Operation Center IAVA status for fielded security equipment.

FY 07 Plans include:
$8,295 - Continue to provide the broadest range of Information Assurance research across Joint, Fleet, and ashore networks. Continue to provide security design engineering of new ships, aircraft, and submarines to ensure that the reduced manning and greater operational dependency on networks. Continue to provide IA engineering design (+$3.497M), evaluation, and testing techniques from end-to-end, through base-band networks, RF communications links, and information source-to-sink to satisfy the IA element of maintaining availability. Continue development of a tier level management system (+$2.319M) between Unit Level Ships and Global Enterprise Management for real-time display of security risk. Continue development of improved real-time computer-network security policy administration (+$0.896M) with analytical tools to identify application or computer-network issues with operational compliance. Continue to develop management processes 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 (FW), IDS, and Filtering Routers at unit level ships and fleet NOCs. Continue development of enhance fielded Security Management Tools (+$1.583M) with new capabilities to support system configuration management and monitoring.

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification			DATE: **February 2005**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME	
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	0734 Information Systems Security	

	FY 04	FY 05	FY 06	FY 07
Crypto MCT	5.105	3.955	6.535	8.001
RDT&E Articles Quantity				

FY04 Accomplishments include:
$5,105- Continued to provide cryptographic products, including type-1 US only, allied and coalition, and commercial-off-the-shelf. Includes design, development, testing, and evaluation of link, network, session, data transfer devices, and associated equipments. Provided continuous development of Crypto Modernization products and components KG-3X, KG-40AR, CTIC/CDH, IFF Mode 5, Link Encryption Family, Advanced Weapons/Expendable Crypto devices, and Next Generation COMSEC devices such as PEIP follow-on, Modern Legacy Crypto Solution, HAIPE and KW-46. Provided the coordination with the Information Systems Security Office at the National Security Agency. Provided specific design, testing, and evaluation assistance for new USN platforms and assists in defining embedded cryptographic product engineering requirements. Included development, modeling, testing, and deployment evaluation of architectures supporting next-generation structures such as remote-keyed, gateways, "lights-out" facilities, and wireless devices. Included architecture modeling, end-to-end security analysis, and integration cryptographic products into USN platform specific architectures. Efforts included increased support for embedded cryptographic products in DD(X) and JTRS.

FY05 Plans Include:
$3,955 - Continue to provide security system engineering support for the development, evaluation and integration of emerging cryptographic products/components and devices, including type-1 US only, allied and coalition, and commercial-off-the-shelf. Includes design, development, testing, and evaluation of link, network, session, data transfer devices, and associated equipments. Continue to provide development of Crypto Modernization products and components KG-3X, KG-40AR, CTIC/CDH, IFF Mode 5, Link Encryption Family, Advanced Weapons/Expendable Crypto devices, and Next Generation COMSEC devices such as PEIP follow-on, Modern Legacy Crypto Solution, HAIPE and KW-46. Continue to provide the coordination of development efforts with the Information Systems Security Office at the National Security Agency. Continue to develop specific design, testing, and evaluation assistance for new USN platforms and assists in defining embedded cryptographic product engineering requirements. Continue development, modeling, testing, and deployment evaluation of architectures supporting next-generation structures such as remote-keyed, gateways, "lights-out" facilities, and wireless devices. Includes architecture modeling, end-to-end security analysis, and integration cryptographic products into USN platform specific architecture. Continue development and integration of embedded cryptographic products.

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2005**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	0734 Information Systems Security

FY06 Plans Include:
$6,535- Continue to provide cryptographic products, including type-1 US only, allied and coalition, and commercial-off-the-shelf. Provides continuous development coordination with the Information Systems Security Office at the National Security Agency. Provides (+$2.905M) specific design, testing, and evaluation assistance for new USN platforms and assists in defining embedded cryptographic product engineering requirements. Continue the development and integration of Crypto Modernization products including KG-3X, KG-40AR, CTIC/CDH, IFF Mode 5, Link Encryption Family, Advanced Weapons/Expendable Crypto devices, and Next Generation COMSEC devices such as: PEIP follow-on, Modern Legacy Crypto Solution, KIV-19 Walburn (+$1.130M), Thorton (+$2.5M) and KW-46. Continue development and integration on the next generation network encryption devices, to include application and implementation of HAIPE in transformational architectures such as FORCEnet and JTRS WNW, and analysis of critical harmonization/integration solutions between modernized INE devices and Key Management, FNBDT and Wireless standards to ensure net-centric capability. Research potential uses of type-2 & 3 for use in type-1 historical environments.

FY07 Plans Include:
$8,001 - Continue to provide cryptographic products, including type-1 US only, allied and coalition, and commercial-off-the-shelf. Continue the development and integration of Crypto Modernization (+$3.483M) products including KG-3X, KG-40AR, CTIC/CDH, IFF Mode 5, Link Encryption Family, Advanced Weapons/Expendable Crypto devices, and Next Generation COMSEC devices such as: PEIP follow-on, KIV-19 Walburn (+$.888M), Thorton (+$3.630M) and KW-46. Continue development and integration on the next generation network encryption devices, to include application and implementation of HAIPE in transformational architectures such as FORCEnet and JTRS WNW, and develop integration solutions for modernized INE devices and Key Management, FNBDT and Wireless capabilities. Continue to research and develop potential uses of type-2 & 3 for use in type-1 historical environments.

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification			DATE: **February 2005**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME	
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	0734 Information Systems Security	

	FY 04	FY 05	FY 06	FY 07
Information Assurance Readiness MCT	0.329	0.313	0.313	0.374
RDT&E Articles Quantity				

FY04 Accomplishment include:
$329- Continued to provide systems security engineering support to all USN organizations in the certification and accreditation (C&A) of information systems. Provided C&A for the Navy Marine Corps Intranet and various coalition networks, involved with all delivering USN systems to ensure secure networks before operational testing. C&A activities included networks, applications, sensors, and databases. Developed and integrated Perl-based custom sniffer script to monitor network traffic the following into the INFOSEC Web site. Upgraded the Snort IDS to Solaris 9 and faster hardware and completed development of Chat Server Supports the Fleet Information Warfare Center (FIWC), the Naval Security Group Activity Pensacola, and the CTF-NMCI for continuing Computer Network Vulnerability Assessment (CNVA) activities. Completed database development to identify unique users. Continued the development and maintenance of USN infrastructure security policy. Developed tools for automatic updating and incorporation of Electronic Key Management System (EKMS) certification and accreditation information. Provided analysis and research for TEMPEST threat and vulnerability to Navy wireless systems. Developed NIC Web single point-of-presence website for Programs of Record (POR) compliance reporting, fleet information and patch data, initially addressing PEO-C4I POR/CMS systems.

FY05 Plans include:
$313- Continue to provide systems security engineering support to all USN organizations in the certification and accreditation of emerging information systems. A primary responsibility is the C&A for the Navy Marine Corps Intranet and various coalition networks. Provide Antivirus Tools Support and Capabilities for R&D support systems and software to meet Navy Anti-Virus requirements. Complete the development and integration of tools for automatic updating and incorporation of EKMS certification and accreditation information. Complete integrations of Perl-based custom sniffer script to monitor network traffic the following into the INFOSEC Web site. Continue to update and maintain the USN infrastructure security policy. Continue follow-on development and integration of NIC Web single point-of-presence website for POR compliance reporting, fleet information and patch data, initially addressing PEO-C4I POR/CMS systems and adding other Navy SYSCOMs and PEOs.

FY06 Plans include:
$313 - Continue to provide systems security engineering support to all USN organizations in the certification and accreditation of emerging information systems. A primary responsibility is the C&A for the Navy Marine Corps Intranet and various coalition networks. Provide continued Antivirus Tools support and capabilities for IA R&D support systems and software to meet Navy Anti-Virus requirements. Continue follow-on development and integration of NIC Web single point-of-presence website for POR compliance reporting, fleet information and patch data, initially addressing PEO-C4I POR/CMS systems and adding other Navy SYSCOMs and PEOs.

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2005**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	0734 Information Systems Security

FY07 Plans include:
$374 - Continue to provide systems security engineering support to all USN organizations in the certification and accreditation of information systems. A primary responsibility is the C&A for the Navy Marine Corps Intranet and various coalition networks. Provide continued Antivirus Tools support and capabilities for R&D support systems and software to meet Navy Anti-Virus requirements.

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification			DATE: **February 2005**
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 04	FY 05	FY 06	FY 07
Secure Voice MCT	0.807	0.939	0.935	1.116
RDT&E Articles Quantity				

FY04 Plans Include:
$807- Continued design and development of the 21st Century Secure Voice Architecture including: Secure Voice over Internet Protocol (SVoIP) Data Networks, Secure Voice Gateways and Inter-Working Functions (IWF), Tactical Radio Communication Security, Telecommunication Security, and finalizing efforts for Secure Voice for the 21st Century (SV-21) architectures. Ensure information superiority through the use of encryption, authentication, and access control mechanisms over Navy mission essential voice circuits. Effort included: (1) continued fielding of state of the art secure voice capabilities enabling secure point-to-point, netted, and conference connectivity, (2) ensuring interoperability with legacy secure voice systems, as well as interoperability with other services, agencies and coalition partners, (3) planning for future secure voice capabilities, both ashore and afloat, over tactical radio, data networks and telecommunications networks. Specific programs for FY04 include Secure Voice over Internet Protocol (SVoIP) Data Networks, Secure Voice Gateways and Inter-Working Functions (IWF), Tactical Radio Communication Security, Telecommunication Security, and finalizing efforts for Secure Voice for the 21st Century (SV-21) architectures. IWF includes the development of future narrow band digital (FNBDT) signaling for the future Advanced Digital Network System (ADNS) over IP architecture to provide interoperability between shipboard STE and shore FNBDT devices (Tactical Secure Voice Over IP). Continued the development and integration of Secure Voice Data Terminal (SVDT) which incorporates the FNBDT. Completed test stages of the Tactical Shore Gateway (TSG). Finished development of TSG to provide tactical-to-strategic secure voice interoperability between land-based systems and mobile platforms (Ship/Aircraft/Ground Forces) as a replacement for the Radio Wireline (RWI). Completed testing stages of FNBDT IWF to provide secure FNBDT interoperability between afloat and shore platforms as well as Joint, NATO and Coalition interoperability. Completed the full range of data rates (from 2400 bits per second (the MELP compatible base rate) to 32,000 bits per second (bps)) for the Variable Data Rate (VDR) algorithm - providing dynamic voice encoding throughout the 2.4k to 32k bps range.

FY05 Plans Include:
$939-Continue development and integration efforts for Future Narrowband Digital Terminal (FNBDT) standard compression through Internet Protocol (IP) products. The FNBDT IP IWF will allow full utilization of STE capabilities and provides compression and protocol translation over an IP backbone. Begin the development and design of a functional model for development of the next generation secure voice/data crypto device. This effort will initiate development of baseline functionality (derived from operational/mission requirements and new technologies) for development of a RFP for production. This Secure Voice device shall incorporate the FNBDT algorithm and be able to support low bandwidth secure voice and data applications over High Frequency (HF), Ultra High Frequency (UHF), Extreme High Frequency (EHF), and Super High Frequency (SHF) designated Radio Frequency (RF) mediums. Conduct mission requirements definition of all secure voice equipment and their users to develop a new COMSEC device that will replace all legacy devices and incorporate the new voice technologies. Continue to develop a secure compression technique to support future narrow band digital (FNBDT) signaling for the future Advanced Digital Network System (ADNS) over IP architecture to provide interoperability between shipboard STE and shore FNBDT devices (Tactical Secure Voice Over IP). Begin development of Secure Voice Data Terminal (SVDT) which incorporates the FNBDT algorithm and supports low bandwidth secure voice and data applications over High Frequency (HF), Ultra High Frequency (UHF), Extreme High Frequency (EHF), and Super High Frequency (SHF) designated Radio Frequency (RF) mediums.

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2005**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	0734 Information Systems Security

FY06 Plans Include:
$935 - Continue development of secure voice modernization and continue prototype integration of 21st Century Secure Voice Architecture including Secure Voice over Internet Protocol (SVoIP) Data Networks, Secure Voice Gateways and Inter-Working Functions (IWF), Tactical Radio Communication Security, Telecommunication Security, and finalizing efforts for Secure Voice for the 21st Century (SV-21) architectures. This effort will pave the way for a tactical secure VoIP capability that is the first step towards integrating legacy secure voice systems and modern commercial telephony. The purpose of this effort is to begin this technology transition while completing some of the more essential features of a prototype radio gateway and the tactical VoIP application, e.g., the dynamic variable data rate processor that provides most efficient use of IP bandwidth (an FORCEnet goal) for voice traffic. Continue development and integration of Secure Voice Data Terminal (SVDT) which incorporates the FNBDT algorithm and supports low bandwidth secure voice and data applications over High Frequency (HF), Ultra High Frequency (UHF), Extreme High Frequency (EHF), and Super High Frequency (SHF) designated Radio Frequency (RF) mediums. Continue to develop a secure compression technique to support future narrow band digital (FNBDT).

FY07 Plans Include:
$1,116 - Complete development and begin integration of secure voice modernization prototype and transition Secure Voice Modernization Architecture including Secure Voice over Internet Protocol (SVoIP) Data Networks, Secure Voice Gateways and Inter-Working Functions (IWF), Tactical Radio Communication Security, Telecommunication Security, and finalizing efforts for Secure Voice for the 21st Century (SV-21) architectures. Continue to develop and integrate secure compression technique to support future narrow band digital (FNBDT) signaling for the future Advanced Digital Network System (ADNS) over IP architecture to provide interoperability between shipboard STE and shore FNBDT devices (Tactical Secure Voice Over IP). Complete development and continue integration of Secure Voice Data Terminal (SVDT) which incorporates the FNBDT.

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2005**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	0734 Information Systems Security

	FY 04	FY 05	FY 06	FY 07
Cross Domain Solutions (CDS)	0.840	0.950	0.936	1.128
RDT&E Articles Quantity				

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

FY04 Accomplishments include:
$840-Continued to provide systems security engineering development, testing, and evaluation for multi-level security solutions, including complicated evaluations involving allied and coalition participation to address emerging threats. Continued to develop multi-level security architecture for data transfer services (i.e. E-mail, file sharing , collaboration at SEA for Network Operating Centers (NOC) and US/Coalition afloat platforms. Began integration of initial Block Zero Multi-Security Level/Cross Domain Solution (MSL/CDS) prototype architecture at NOC facilities. Included integration of security requirements in the next generation Universal Mobile Telephone services, Generation 3.

FY05 Plans include:
$950- Continue to provide systems security engineering development, testing, and evaluation for multi-level security solutions, including complicated evaluations involving allied and coalition participation. Continue to examine multi-level aware applications and technologies including databases, web browsers, routers/switches, etc. Continue to develop and integrate MSL/CDS prototype architecture at NOC facilities. Continue development of Block One CDS solution as a follow-on to Block Zero. The Block One CDS solution focus on providing a robust coalition interoperability using Multi-Level Thin Client (MLTC), secure guarding devices and afloat coalition network systems.

FY06 Plans include:
$936- Continue to provide systems security engineering development, testing, and evaluation for multi-level security solutions, including complicated evaluations involving allied and coalition participation. Continue to examine multi-level aware applications and technologies including databases, web browsers, routers/switches, etc. Continue to develop and integrate MSL/CDS prototype architecture at NOC facilities. Continue development and integration of Block One CDS solutions to focus on providing a robust coalition interoperability using Multi-Level Thin Client (MLTC), secure guarding devices and afloat coalition network systems. Begin development of follow-on Block Two CDS upgrade to reduce footprint and provide reconfigurable, enabling IT network architecture for fleet combatants as well as ashore command centers that support data transfer service at multiple security levels.

FY07 Plans include:
$1,128- Continue to provide systems security engineering development, testing, and evaluation for multi-level security solutions, including complicated evaluations involving allied and coalition participation. Continue to examine multi-level aware applications and technologies including databases, web browsers, routers/switches, etc. Continue to develop and integrate MSL/CDS prototype architecture at NOC facilities. Continue to development of follow-on Block Two CDS upgrade to reduce footprint and provide reconfigurable, enabling IT network architecture for fleet combatants as well as ashore command centers that support data transfer service at multiple security levels.

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification			DATE: **February 2005**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME	
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	0734 Information Systems Security	

	FY 04	FY 05	FY 06	FY 07
Key Management Infrastructure MCT	5.106	5.547	5.753	7.125
RDT&E Articles Quantity				

FY04 Accomplishments include:
$5,106- Streamlined methods for secure symmetric and asymmetric cryptographic key and generation, distribution, management, and usage products, services and fleet requirements. Provided engineering design for key management infrastructure (KMI) , including the Electronic Key management System (EKMS Phase IV for Tier 0,1,2,3), Defense Messaging System (DMS) specific products, the DOD Public Key Infrastructure (DOD-PKI), and Certificate Management Infrastructures (CMI). Completed the design, development and performed the pilot of Navy's Key Management System. Provided the design and development of the Certificate Authorization Workstation (CAW) regionalization strategy to implement the Remote Key/Re-key capability that eliminates the requirement to install CAWs on ships where DMS messaging is to be fielded. Continued efforts in the design and develop of certificate validation infrastructure (On-line Certificate Status Protocol (OCSP)). Provided systems security engineering, test, evaluation, and development program support for organizations utilizing cryptographic equipments and associated keying systems. Specific projects include: Afloat and OCONUS DoD Class 3/4 PKI, Current Class 4 (X.509) PKI for Organizational Secure Messaging, EKMS Common Tier 1 (CT1), EKMS Tier 2/3, and KMI.

FY05 Plans include:
$5,547- Begin security and functionality testing and evaluation of PKI tokens, readers and middleware for the SIPRNET. Begin prototyping and certification/accreditation of the Navy's Key management system. Begin Common User Aplplication Software (CUAS), Data Mgmt Device (DMD) and Simple Key Loader (SKL) development and integration. Begin and complete Mode 5 Idenfiy Friend or Foe (IFF)(Time of Day) design and development. Begin deveoplemt and integration of Future fill device. Provide engineering design evolution for the supporting key management infrastructure, to include: Electronic Key management System (EKMS Phase IV for Tier 0,1,2,3), Defense Messaging System (DMS) specific products, DOD Public Key Infrastructure (DOD-PKI), and additional Certificate Management Infrastructures (CMI). Effort will Include design, evaluation, integration, and testing of key-related platforms, such as smart cards, authentication mechanisms and biometric devices. Provide systems security engineering, test, evaluation, and development program support for organizations utilizing cryptographic equipments and associated keying systems. Complete design and development of the Certificate Authorization Workstation (CAW) regionalization strategy and begin to implement and integrate the CAW Remote Key/Re-key capability.

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2005**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	0734 Information Systems Security

FY06 Plans include:
$5,753- Continue design and development of the KMI local management workstation. Continue EKMS Phase V to include development and implementation of an extended , networked architecture (key distribution over SIPRNET) to improve distribution and reliability for deployed forces, modernized key processors, common user application software and data transfer devices. Continue to develop and integrate Online Certificate Status Protocol. Continue deveoplemt and integration of Future fill device. Begin security and functionality testing and evaluation of (OCSP) architecture for the SIPRNet. Continue security and functionality testing and evaluation of PKI tokens, readers and middleware for the SIPRNET. Complete prototyping and certification/accreditation of the Navy's Key management system. Begin Common User Aplplication Software (CUAS), Data Mgmt Device (DMD) and Simple Key Loader (SKL) development and integration. Continue CUAS, DMD and SKL development and integration. Conduct requirements definition for the End IA Unit (EIAU) Encryption device. Begin Wireless Key Fill technology design and development. Begin the Key Loading and Initialization Facility (KLIF) design and development.

FY07 Plans include:
$7,125- Complete security and functionality testing and evaluation of PKI tokens, readers and middleware for the SIPRNET. Continue to streamline the method for developing effective secure symmetric and asymmetric cryptographic key and generation, distribution, management, and usage products and services by identifying and prioritizing fleet requirements. Continue EKMS Phase V to include development and implementation of an extended , networked architecture (key distribution over SIPRNET) to improve distribution and reliability for deployed forces, modernized key processors, common user application software and data transfer devices. Continue to develop and integrate Online Certificate Status Protocol. Complete Wireless Key Fill technology design and development . Complete development and integration of Online Certificate Status Protocol. Complete DMS migration to PKI. Complete the initial design for EIAU management. Complete the Key Loading and Initialization Facility design and development.

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification			DATE: **February 2005**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME	
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	0734 Information Systems Security	

	FY 04	FY 05	FY 06	FY 07
Emerging Technology MCT	1.647	1.857	4.888	5.395
RDT&E Articles Quantity				

FY04 Accomplishments include:
$1,647- Facilitated the transition and application of new technologies to Navy Information Assurance challenges. Specific areas focused on the following projects: (1) Secure Network Communications Including Coalition Applications, (2) Recognition and Prevention of Network Intrusions, (3) Convenient Wireless Applications with Adequate Security, (4) Synergistic Operation of IA and IO Functions, (5) Improved Access Control Using Biometrics, to include applications of commercially available biometrics technology to Navy logical and physical access problems, as well as applications considered for larger scale implementation, and (6) Rapid Transition of Technology to the Fleet, in support of Fleet Battle Experiments, Computer Network Defense in Depth (CNDID), Task Force WEB, Teleport, Ship Building and Construction, Navy (SCN) and other transition opportunities. Begin initial concept refinement for an Independent Host-based Intrusive Behavior Terminator (INHIBT) System that will proactively analyze transactions at the operating system level for normal behavior and initiate workstation and network survival systems for anomalous activity. Completed study to exploit recent strides in programmable cryptography to provide a "drop-in" Advanced Weapons Crypto (AWC) technology. Released v1.0 of Navy Enterprise Single Sign-On (NESSO) that contains an enhanced Java based Identity Server, initial implementations of Biometric Authentication, and implements the Liberty Alliance Federated Identity framework.

FY05 Plans include:
$1,857- Continue to support the transition and application of new technologies to Navy Information Assurance challenges. Continued emphasis will be placed on providing R&D support for programs that are identified by the product mission capability teams as their highest priorities, and on increasing the speed of delivery of useful information assurance capabilities to fleet users. Specific areas of continued focus will include the following projects: (1) Secure Network Communications Including Coalition Applications, (2) Recognition and Prevention of Network Intrusions, (3) Convenient Wireless Applications with Adequate Security, (4) Synergistic Operation of IA and IO Functions, (5) Improved Access Control Using Biometrics, to include applications of commercially available biometrics technology to Navy logical and physical access problems, as well as applications that are now considered ready for larger scale implementation, and (6) Rapid Transition of Technology to the Fleet, in support of Fleet Battle Experiments, CNDID, TF WEB, Teleport, SCN and other transition opportunities. Complete initial concept refinement for INHIBT System that will proactively analyze transactions at the operating system level for normal behavior and initiate workstation and network survival systems for anomalous activity. Continue AWC technology project with proof of concept demonstration and initial production development. Release v2.0 of NESSO which will be a full featured, open source, production quality product including an enhanced Java based Identity Server, complete implementation of Biometric Authentication, and the Liberty Alliance Federated Identity framework.

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2005**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	0734 Information Systems Security

FY 06 Plans include:
$4,888- Continue to provide security systems engineering (+$1.872M) support for the transition and application of new technologies to Navy Information Assurance challenges. Continue development of open source Single Sign-On solution (+$1.094M) by incrementally adding new features/enhancements for federated identity, Public Key Infrastructure (PKI), Role Based Access Control (RBAC), Common Access Card (CAC) and Next Generation Access Systems. Provide standardized security design and installation baselines to ensure enhancements of configuration management. Develop and integrate IA Components into programs such as FORCEnet, Computer Network Defense in Depth (CND-ID) Strategy, Transformational Communication (TC), Global Information Grid Enterprise Services (GIG-ES), Secure Voice over Internet Protocol (SVoIP), and Horizontal Fusion. Begin development of INHIBT system (+$1.199M) that will proactively analyze transactions at the operating system level for normal behavior and initiate workstation and network survival systems for anomalous activity. Develop Next Generation Access Systems solutions (+$0.240M) to provide improved security for access to computers, networks, and sensitive spaces or buildings. Seamless integration with CAC is necessary. Provide IA engineering (+$0.483M) for development of Wireless Networks and PDA security readiness of Naval wireless networks and mobile computing devices .

FY 07 Plans include:
$5,395- Continue to provide security systems engineering (+$2.245M) support for the transition and application of new technologies to Navy Information Assurance challenges. Continue to develop and begin transition of open source Single Sign-On solutions (+$0.930M) for federated identity, Public Key Infrastructure (PKI), Role Based Access Control (RBAC), Common Access Card (CAC) and Next Generation Access Systems across multiple trusted domains. Continue to provide standardized security design and installation baselines to ensure enhancements of configuration management. Continue to develop and integrate IA Components into programs such as FORCEnet, CND-ID Strategy, TC, GIG-ES, SVoIP and Horizontal Fusion. Continue to develop and begin integration of INHIBT system (+$1.469M) that will proactively analyze transactions at the operating system level for normal behavior and initiate workstation and network survival systems for anomalous activity. Continue to develop and begin integration of Next Generation Access Systems solutions (+$0.245M) to provide improved security for access to computers, networks, and sensitive spaces or buildings. Seamless integration with CAC is necessary. Provide IA engineering for development of Wireless Networks and PDA security (+$0.506M) readiness of Naval wireless networks and mobile computing devices, continue to evaluate products for security issues and develop guidance and procedures.

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2005**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	0734 Information Systems Security

(U) C. PROGRAM CHANGE SUMMARY:

(U) Funding:	FY 2004	FY 2005	FY 2006	FY 2007
FY 05 President's Budget:	15.876	16.539	15.535	18.624
FY 06 President's Budget:	16.469	16.526	26.555	31.434
Total Adjustments	0.593	-0.013	11.020	12.810
Summary of Adjustments				
Congressional Adjustments				
Congressional Recissions		-0.013		
Reprogrammings	0.811			
Programmatic Adjustments			10.930	12.457
Economic Assumptions			0.112	0.171
Pricing Adjustments			-0.022	0.182
SBIR/STTR Transfers	-0.218			
Subtotal	0.593	-0.013	11.020	12.810

(U) Schedule:

(U) Technical:

N/A.

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2005**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	0734 Information Systems Security

(U) D. OTHER PROGRAM FUNDING SUMMARY:

Line Item No. & Name	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
OPN 3415 Info Sys Security Program (ISSP)	81.582	90.364	96.201	126.363	131.772	132.409	157.227	159.731
OMN 4A6M Info Sys Security Program (ISSP)	18.819	12.167	24.970	26.954	31.189	28.420	28.391	28.960

(U) E. ACQUISITION STRATEGY: *

N/A.

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

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

Exhibit R-3 Cost Analysis (page 1)								DATE: **February 2005**				
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**		PROGRAM ELEMENT 0303140N Information Systems Security Program (ISSP)			PROJECT NUMBER AND NAME 0734 Information Systems Security							
Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 05 Cost	FY 05 Award Date	FY 06 Cost	FY 06 Award Date	FY 07 Cost	FY 07 Award Date	Cost to Complete	Total Cost	Target Value of Contract
Primary Hardware Development	C/CPFF	VIASAT, San Diego, CA	7.282							0.000	7.282	7.282
Primary Hardware Development	C/MIPR	MITRE, San Diego, CA	5.522	0.000		0.000		0.000		0.000	5.522	
Primary Hardware Development	C/CPAF	TBD	6.771	1.354	01/05	2.167	01/06	2.545	01/07	Continuing	Continuing	
Primary Hardware Development	C/VAR	Various	65.313	2.457	VAR	4.620	VAR	5.769	VAR	Continuing	Continuing	
Systems Engineering	C/VAR	Various	47.391	8.488	VAR	12.920	VAR	15.174	VAR	Continuing	Continuing	
Subtotal Product Development			132.279	12.299		19.707		23.488		Continuing	Continuing	

Remarks:

Software Development	CPAF	SAIC, San Diego, CA	32.877							0.000	32.877	42.590
Software Development	C/WX	NRL, Washington D.C.	0.145	0.640	10/04	0.794	10/05	0.933	10/06	Continuing	Continuing	
Subtotal Support			33.022	0.640		0.794		0.933		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 2005**				
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**		PROGRAM ELEMENT 0303140N Information Systems Security Program (ISSP)			PROJECT NUMBER AND NAME 0734 Information Systems Security							
Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 05 Cost	FY 05 Award Date	FY 06 Cost	FY 06 Award Date	FY 07 Cost	FY 07 Award Date	Cost to Complete	Total Cost	Target Value of Contract
Developmental Test & Evaluation	VAR	Various	16.337	3.386	Various	5.524	Various	6.390	Various	Continuing	Continuing	Continuing
Subtotal T&E			16.337	3.386		5.524		6.390		Continuing	Continuing	
Remarks:												
Program Management Support	VAR	Various	4.601	0.201	Various	0.530	Various	0.623	Various	Continuing	Continuing	Continuing
Subtotal Management			4.601	0.201		0.530		0.623		Continuing	Continuing	
Remarks:												
Total Cost			186.239	16.526		26.555		31.434		Continuing	Continuing	
Remarks:												

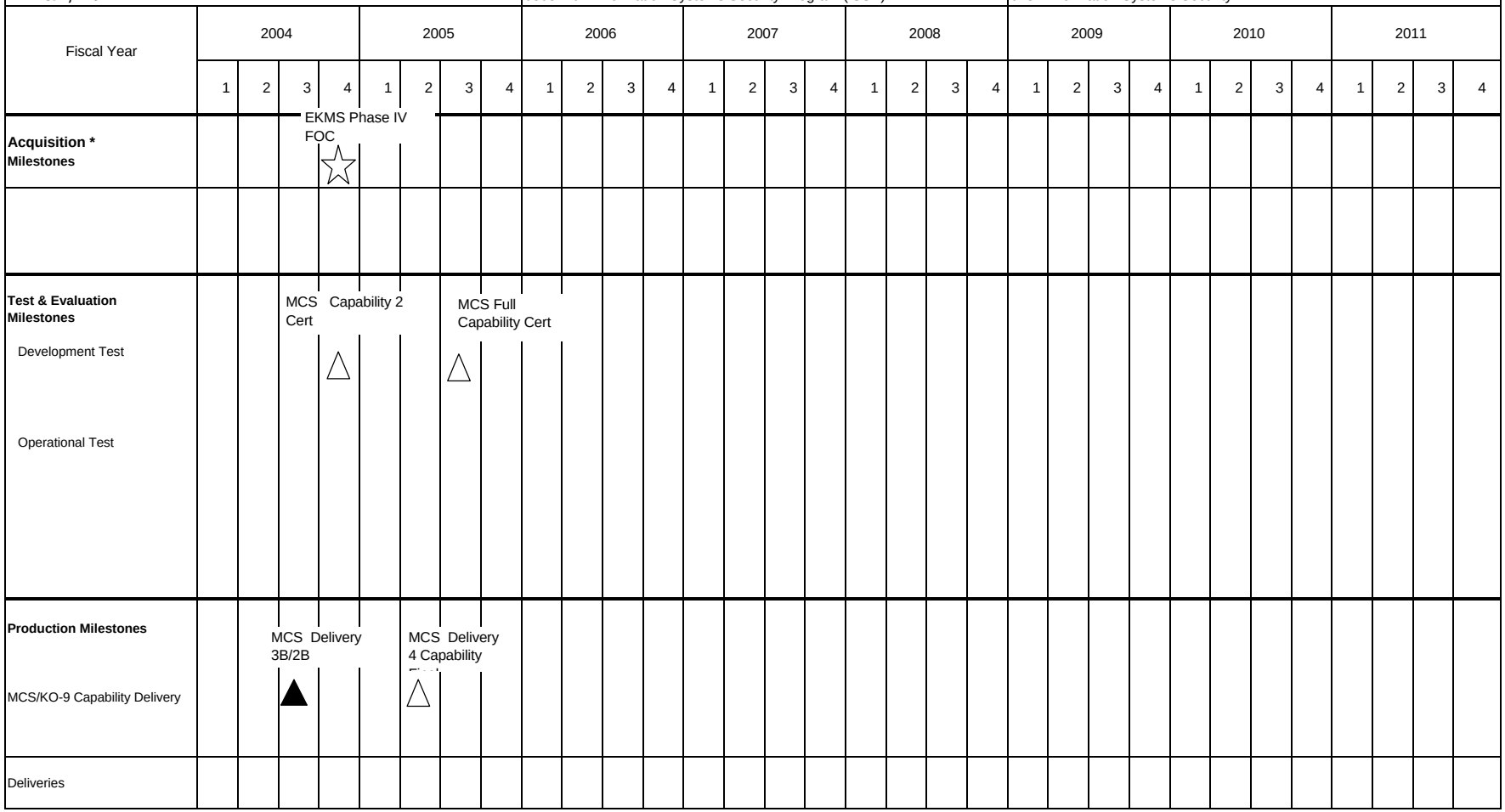
R-1 SHOPPING LIST - Item No. 194

EXHIBIT R4, Schedule Profile | DATE: February 2005

APPROPRIATION/BUDGET ACTIVITY: RDT&E, N / BA-7

PROGRAM ELEMENT NUMBER AND NAME: 0303140N Information Systems Security Program (ISSP)

PROJECT NUMBER AND NAME: 0734 Information Systems Security



R-1 SHOPPING LIST - Item No. 194

* Note: MCS Deliveries support the MCS Capability Certifications

CLASSIFICATION:

Exhibit R-4a, Schedule Detail						DATE: **February 2005**		
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT 0303140N Information Systems Security Program (ISSP)				PROJECT NUMBER AND NAME 0734 Information Systems Security			
Schedule Profile	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
EKMS Phase IV FOC	4Q							
Multifunctional Crypto System (MCS) Capability 2 Cert	4Q							
Multifunctional Crypto System (MCS) Full Capability Cert		3Q						
MCS Delivery 2B Capability	3Q							
MCS Delivery 3B Capability	3Q							
MCS Delivery 4 Capability		2Q						

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification								DATE: **February 2005**	
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 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Project Cost		**2.271**	**1.973**	**2.105**	**2.056**	**2.242**	**2.199**	**2.251**	**2.303**
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.

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.

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2005**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	0734 Communications Security

(U) B. Accomplishments/Planned Program

	FY 04	FY 05	FY 06	FY 07
Software and Systems Research	2.271	1.973	2.105	2.056
RDT&E Articles Quantity				

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

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **Frebruary 2005**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	0734 Communications Security

(U) C. PROGRAM CHANGE SUMMARY:

(U) Funding:	FY 2004	FY 2005	FY 2006	FY 2007
FY 05 President's Budget:	2.271	2.137	2.102	2.049
FY 06 President's Budget:	2.271	1.973	2.105	2.056
Total Adjustments	0.000	-0.164	0.003	0.007
Summary of Adjustments				
Congressional Recissions		-0.164		
Pricing Changes			0.003	0.007
Subtotal	0.000	-0.164	0.003	0.007

(U) Schedule:
N/A.

(U) Technical:
N/A

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 5005**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	0734 Communications Security

(U) D. OTHER PROGRAM FUNDING SUMMARY:

Line Item No. & Name	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
OPN 3415 Info Sys Security Program (ISSP)	81.582	90.364	96.201	126.363	131.772	132.409	157.227	159.731
OMN 4A6M Info Sys Security Program (ISSP)	18.819	12.167	24.970	26.954	31.189	28.420	28.391	28.960

(U) E. ACQUISITION STRATEGY: *

N/A.

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

CLASSIFICATION:

Exhibit R-3 Cost Analysis (page 1)								DATE: **February 2005**				
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 05 Cost	FY 05 Award Date	FY 06 Cost	FY 06 Award Date	FY 07 Cost	FY 07 Award Date	Cost to Complete	Total Cost	Target Value of Contract
Hardware Development											0.000	
Subtotal Product Development			0.000	0.000		0.000		0.000			0.000	
Remarks:												
Software Development	C/WX	NRL, Washington D.C.	6.361	1.973	10/04	2.105	10/05	2.056	10/06	Continuing	Continuing	
Subtotal Support			6.361	1.973		2.105		2.056		Continuing	Continuing	
Remarks:												

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

Exhibit R-3 Cost Analysis (page 2)								DATE: **February 2005**				
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 05 Cost	FY 05 Award Date	FY 06 Cost	FY 06 Award Date	FY 07 Cost	FY 07 Award Date	Cost to Complete	Total Cost	Target Value of Contract
Developmental Test & Evaluation											0.000	
Subtotal T&E			0.000	0.000		0.000		0.000			0.000	
Remarks:												
Program Management Support											0.000	
Subtotal Management			0.000	0.000		0.000		0.000			0.000	
Remarks:												
Total Cost			6.361	1.973		2.105		2.056		Continuing	Continuing	
Remarks:												

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification								DATE: **February 2005**	
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT NUMBER AND NAME 0303140N Information Systems Security Program (ISSP)					PROJECT NUMBER AND NAME 9281 Intelligent Agent Security Module (IASM)			
COST ($ in Millions)		FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Project Cost		**5.300**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**
RDT&E Articles Qty									

(U) A. MISSION DESCRIPTION AND BUDGET ITEM JUSTIFICATION: Congressional plus-up for Navy's Intelligent Agent Security Module (IASM). Continued research and development for Small Business Research Initiative (SBIR Phase 2) for a network wide Intrusion Detection System (IDS) (referred to as Naval Intelligent Agent Secure Module (NIASM)) which monitors existing sensors and devices to include Firewalls, Virtual Private Network (VPN) servers, and Information Decision Systems (IDS).The IASM is intended to enhance network security by correlating information from multiple security products and deriving a concise, accurate assessment of malicious actions and unauthorized use. In addition the IASM will provide network administrators with recommended response actions in order to terminate attacks. The IASM is intended for deployment at tactical Network Operation Centers, Shipboard, and at the Fleet Information Warfare Center.

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.

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2005**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	9281 Intelligent Agent Security Module (IASM)

(U) B. Accomplishments/Planned Program

	FY 04	FY 05	FY 06	FY 07
Intelligent Agent Security Module (IASM)	5.300	0.000	0.000	0.000
RDT&E Articles Quantity				

FY 04 Accomplishments include:
$5,300- Continued to develop network wide Intrusion Detection System (IDS) (referred to as Naval Intelligent Agent Secure Module (NIASM)). Continued to develop a hierarchal data monitoring and analysis system to support the design of a Global Navy, Base Level Information Infrastructure security assurance grid. Efforts will include independent operational and performance tests to verify the system hardness in a military ship-at-sea environment. Continued to resolve critical design issues to meet IASM Build 1.0 shore system integration readiness and certify shore Network Operating Center system security integration at Information Assurance test facilities.

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2005**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	9281 Intelligent Agent Security Module (IASM)

(U) C. PROGRAM CHANGE SUMMARY:

(U) Funding:	FY 2004	FY 2005	FY 2006	FY 2007
FY05 President's Budget:	5.439	0.000	0.000	0.000
FY06 President's Budget:	5.300	0.000	0.000	0.000
Total Adjustments	-0.139	0.000	0.000	0.000
Summary of Adjustments				
Economic Assumptions	-0.005	0.000	0.000	0.000
SBIR	-0.134			
Subtotal	-0.139	0.000	0.000	0.000

(U) Schedule:

N/A

(U) Technical:

N/A

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2005**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	9281 Intelligent Agent Security Module (IASM)

(U) D. OTHER PROGRAM FUNDING SUMMARY:

Line Item No. & Name	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
OPN 3415 Info Sys Security Program (ISSP)	81.582	90.364	96.201	126.363	131.772	132.409	157.227	159.731
OMN 4A6M Info Sys Security Program (ISSP)	18.819	12.167	24.970	26.954	31.189	28.420	28.391	28.960
RDT&E 0303140N Info Sys Security (ISSP)	16.469	16.526	26.555	31.434	31.829	32.100	30.801	32.060

(U) E. ACQUISITION STRATEGY: *

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

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

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

Exhibit R-3 Cost Analysis (page 1)								DATE: **February 2005**				
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**		PROGRAM ELEMENT 0303140N Information Systems Security Program (ISSP)			PROJECT NUMBER AND NAME 9281 Intelligent Agent Security Module (IASM)							
Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 05 Cost	FY 05 Award Date	FY 06 Cost	FY 06 Award Date	FY 07 Cost	FY 07 Award Date	Cost to Complete	Total Cost	Target Value of Contract
Primary Hardware Development											0.000	
Ancillary Hardware Development											0.000	
Aircraft Integration											0.000	
Ship Integration											0.000	
Ship Suitability											0.000	
Systems Engineering	C/CPAF	PROMIA, Inc.	4.500	0.000		0.000		0.000			4.500	
Training Development											0.000	
Licenses											0.000	
Tooling											0.000	
GFE											0.000	
Award Fees											0.000	
Subtotal Product Development			4.500	0.000		0.000		0.000		0.000	4.500	
Remarks:												
Development Support											0.000	
Software Development											0.000	
Integrated Logistics Support											0.000	
Configuration Management											0.000	
Technical Data											0.000	
Studies & Analyses											0.000	
GFE											0.000	
Award Fees											0.000	
Subtotal Support			0.000	0.000		0.000		0.000		0.000	0.000	
Remarks:												

CLASSIFICATION:

Exhibit R-3 Cost Analysis (page 2)								DATE: **February 2005**				
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**		PROGRAM ELEMENT 0303140N Information Systems Security Program (ISSP)			PROJECT NUMBER AND NAME 9281 Intelligent Agent Security Module (IASM)							
Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 05 Cost	FY 05 Award Date	FY 04 Cost	FY 04 Award Date	FY 05 Cost	FY 05 Award Date	Cost to Complete	Total Cost	Target Value of Contract
Developmental Test & Evaluation	WX	SSC Charleston, SC	0.400	0.000		0.000		0.000			0.400	
Developmental Test & Evaluation	WX	SSC San Diego, CA	0.400	0.000		0.000		0.000			0.400	
Live Fire Test & Evaluation											0.000	
Test Assets											0.000	
Tooling											0.000	
GFE											0.000	
Award Fees											0.000	
Subtotal T&E			0.800	0.000		0.000		0.000		0.000	0.800	
Remarks:												
Contractor Engineering Support											0.000	
Government Engineering Support											0.000	
Program Management Support											0.000	
Travel											0.000	
Transportation											0.000	
SBIR Assessment											0.000	
Subtotal Management			0.000	0.000		0.000		0.000		0.000	0.000	
Remarks:												
Total Cost			5.300	0.000		0.000		0.000		0.000	5.300	
Remarks:												

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification								DATE: **February 2005**	
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT NUMBER AND NAME 0303140N Information Systems Security Program (ISSP)					PROJECT NUMBER AND NAME 9430 SECURE Kit			
COST ($ in Millions)		FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Project Cost		**1.729**	**4.547**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**
RDT&E Articles Qty									

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

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.

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2005**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	9430 SECURE Kit

(U) B. Accomplishments/Planned Program

	FY 04	FY 05	FY 06	FY 07
SECUREKit	1.729	4.547	0.000	0.000
RDT&E Articles Quantity				

FY04 Accomplishment includes:
$1,729- Performed SECUREkit pathway feasibility demonstration of components to develop possible solution for MSL and CDS. Conducted research, development, and test and evaluation of this promising MSL technology to be applied to future phases of the MSL spiral development. Current MSL systems does not meet all fleet requirements, thus further R&D is required to fulfill the need. Specifically, the need that SECUREkit intends to satisfy is a fully multiple-level security Navy enterprise capability. The pathway components are the next elements of this capability requiring development.

FY05 Plans include:
$4,547 - FY05 efforts are directed to completing the design and development of Network access device that includes multi-factor identification, identity management process, and inline encryption engine. The design is currently still a work in progress but may be either internal PCI card or and external black box device. These components will be based on open architecture and designed for enabling web-based enterprise services in the Department of the Navy and coalition participants. These components will provide for a trusted path, or high assurance transactions, between servers, clients, and other resources in the FORCEnet enterprise.

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2005**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	9430 SECURE Kit

(U) C. PROGRAM CHANGE SUMMARY:

(U) Funding:	FY 2004	FY 2005	FY 2006	FY 2007
FY 05 President's Budget:	1.780	0.000	0.000	0.000
FY 06 President's Budget:	1.729	4.547	0.000	0.000
Total Adjustments	-0.051	4.547	0.000	0.000
Summary of Adjustments				
Congressional Adjustments		4.600		
Congressional Recissions		-0.053		
Reprogrammings				
Programmatic Adjustments				
Economic Assumptions	-0.002			
Pricing Adjustments				
SBIR/STTR Transfers	-0.049			
Subtotal	-0.051	4.547	0.000	0.000

(U) Schedule:

N/A

(U) Technical:

N/A

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2005**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	9430 SECURE Kit

(U) D. OTHER PROGRAM FUNDING SUMMARY:

Line Item No. & Name	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
OPN 3415 Info Sys Security Program (ISSP)	81.582	90.364	96.201	126.363	131.772	132.409	157.227	159.731
OMN 4A6M Info Sys Security Program (ISSP)	18.819	12.167	24.970	26.954	31.189	28.420	28.391	28.960
RDT&E 0303140N Info Sys Security (ISSP)	16.469	16.526	26.555	31.434	31.829	32.100	30.801	32.060

(U) E. ACQUISITION STRATEGY: *

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

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

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

Exhibit R-3 Cost Analysis (page 1)								DATE: **February 2005**				
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**		PROGRAM ELEMENT 0303140N Information Systems Security Program (ISSP)			PROJECT NUMBER AND NAME 9430 SECURE Kit							
Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 05 Cost	FY 05 Award Date	FY 06 Cost	FY 06 Award Date	FY 07 Cost	FY 07 Award Date	Cost to Complete	Total Cost	Target Value of Contract
Primary Hardware Development											0.000	
Ancillary Hardware Development											0.000	
Aircraft Integration											0.000	
Ship Integration											0.000	
Ship Suitability											0.000	
Systems Engineering	CPFF	PSI, Inc.	1.629	4.247	VAR	0.000		0.000			5.876	
Training Development											0.000	
Licenses											0.000	
Tooling											0.000	
GFE											0.000	
Award Fees											0.000	
Subtotal Product Development			1.629	4.247		0.000		0.000		0.000	5.876	
Remarks:												
Development Support											0.000	
Software Development											0.000	
Integrated Logistics Support											0.000	
Configuration Management											0.000	
Technical Data											0.000	
Studies & Analyses											0.000	
GFE											0.000	
Award Fees											0.000	
Subtotal Support			0.000	0.000		0.000		0.000		0.000	0.000	
Remarks:												

CLASSIFICATION:

Exhibit R-3 Cost Analysis (page 2)								DATE: **February 2005**				
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**		PROGRAM ELEMENT 0303140N Information Systems Security Program (ISSP)				PROJECT NUMBER AND NAME 9430 SECURE Kit						
Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 05 Cost	FY 05 Award Date	FY 06 Cost	FY 06 Award Date	FY 07 Cost	FY 07 Award Date	Cost to Complete	Total Cost	Target Value of Contract
Developmental Test & Evaluation	WX	SSC Charleston, SC	0.000	0.000		0.000		0.000			0.000	
Developmental Test & Evaluation	WX	SSC San Diego, CA	0.000	0.000		0.000		0.000			0.000	
Live Fire Test & Evaluation											0.000	
Test Assets											0.000	
Tooling											0.000	
GFE											0.000	
Award Fees											0.000	
Subtotal T&E			0.000	0.000		0.000		0.000		0.000	0.000	
Remarks:												
Contractor Engineering Support											0.000	
Government Engineering Support											0.000	
Program Management Support	CPFF	BAH, Inc.	0.100	0.300	VAR	0.000		0.000			0.400	
Travel											0.000	
Transportation											0.000	
SBIR Assessment											0.000	
Subtotal Management			0.100	0.300		0.000		0.000		0.000	0.400	
Remarks:												
Total Cost			1.729	4.547		0.000		0.000		0.000	6.276	
Remarks:												

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification								DATE: **February 2005**	
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT NUMBER AND NAME 0303140N Information Systems Security Program (ISSP)					PROJECT NUMBER AND NAME 9647 Collaborative Information Warfare Network (CIWN)			
COST ($ in Millions)		FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Project Cost		**0.000**	**3.465**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**
RDT&E Articles Qty									

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

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

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2005**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	9647 Collaborative Information Warfare Network (CIWN)

(U) B. Accomplishments/Planned Program

	FY 04	FY 05	FY 06	FY 07
CIWN	0.000	3.465	0.000	0.000
RDT&E Articles Quantity				

FY 05 Accomplishment includes:
N/A

FY05 Plans include:
$3.465- The FY 05 RDT&E Congressional increase will provide for the development of the Collaborative Information Warfare Network architecture and publish a guide that frames processes to both Federal and Military organizations for the monitoring, detection, protection and remediation of potential threats to the operation of the nations' critical infrastructure. The CIWN network architecture will establish a collaborative environment linking center's in four regional geographic areas and in Canada and Mexico.

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2005**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	9647 Collaborative Information Warfare Network (CIWN)

(U) C. PROGRAM CHANGE SUMMARY:

(U) Funding:	FY 2004	FY 2005	FY 2006	FY 2007
FY 05 President's Budget:	0.000	0.000	0.000	0.000
FY 06 President's Budget:	0.000	3.465	0.000	0.000
Total Adjustments	0.000	3.465	0.000	0.000

Summary of Adjustments	
Congressional Adjustments	3.500
Congressional Recissions	-0.035
Reprogrammings	
Programmatic Adjustments	
Economic Assumptions	
Pricing Adjustments	
SBIR/STTR Transfers	
Subtotal	3.465

(U) Schedule:

N/A

(U) Technical:

N/A

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2005**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	9647 Collaborative Information Warfare Network (CIWN)

(U) D. OTHER PROGRAM FUNDING SUMMARY:

Line Item No. & Name	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
OPN 3415 Info Sys Security Program (ISSP)	81.582	90.364	96.201	126.363	131.772	132.409	157.227	159.731
OMN 4A6M Info Sys Security Program (ISSP)	18.819	12.167	24.970	26.954	31.189	28.420	28.391	28.960
RDT&E 0303140N Info Sys Security (ISSP)	16.469	16.526	26.555	31.434	31.829	32.100	30.801	32.060

(U) E. ACQUISITION STRATEGY: *

+

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

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

Exhibit R-3 Cost Analysis (page 1)								DATE: **February 2005**				
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**		PROGRAM ELEMENT 0303140N Information Systems Security Program (ISSP)				PROJECT NUMBER AND NAME 9647 Collaborative Information Warfare Network (CIWN)						
Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 05 Cost	FY 05 Award Date	FY 06 Cost	FY 06 Award Date	FY 07 Cost	FY 07 Award Date	Cost to Complete	Total Cost	Target Value of Contract
Primary Hardware Development											0.000	
Ancillary Hardware Development											0.000	
Aircraft Integration											0.000	
Ship Integration											0.000	
Ship Suitability											0.000	
Systems Engineering											0.000	
Training Development											0.000	
Licenses											0.000	
Tooling											0.000	
GFE											0.000	
Award Fees											0.000	
Subtotal Product Development			0.000	0.000		0.000		0.000		0.000	0.000	
Remarks:												
Development Support	WX	SSC Charleston, SC	0.000	3.265	VAR						3.265	
Software Development											0.000	
Integrated Logistics Support											0.000	
Configuration Management											0.000	
Technical Data											0.000	
Studies & Analyses											0.000	
GFE											0.000	
Award Fees											0.000	
Subtotal Support			0.000	3.265		0.000		0.000		0.000	3.265	
Remarks:												

R-1 SHOPPING LIST - Item No. 194

CLASSIFICATION:

Exhibit R-3 Cost Analysis (page 2)								DATE: **February 2005**			
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**		PROGRAM ELEMENT 0303140N Information Systems Security Program (ISSP)			PROJECT NUMBER AND NAME 9647 Collaborative Information Warfare Network (CIWN)						
Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 05 Cost	FY 05 Award Date	FY 06 Cost	FY 06 Award Date	FY 07 Cost	FY 07 Award Date	Cost to Complete	Total Cost	Target Value of Contract
Developmental Test & Evaluation			0.000	0.000		0.000		0.000			0.000	
Developmental Test & Evaluation			0.000	0.000		0.000		0.000			0.000	
Live Fire Test & Evaluation											0.000	
Test Assets											0.000	
Tooling											0.000	
GFE											0.000	
Award Fees											0.000	
Subtotal T&E			0.000	0.000		0.000		0.000		0.000	0.000	
Remarks:												
Contractor Engineering Support											0.000	
Government Engineering Support											0.000	
Program Management Support		BAH, Inc.	0.000	0.200	VAR	0.000		0.000			0.200	
Travel											0.000	
Transportation											0.000	
SBIR Assessment											0.000	
Subtotal Management			0.000	0.200		0.000		0.000		0.000	0.200	
Remarks:												
Total Cost			0.000	3.465		0.000		0.000		0.000	3.465	
Remarks:												

R-1 SHOPPING LIST - Item No. 194