CLASSIFICATION:

EXHIBIT R-2, RDT&E Budget Item Justification									DATE: February 2003		
APPROPRIATION/BUDGET ACTIVITY **RESEARCH DEVELOPMENT TEST & EVALUATION, NAVY / BA-7**						R-1 ITEM NOMENCLATURE 0303140N Information Systems Security Program (ISSP)					
COST ($ in Millions)	Prior Years Cost	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	Cost to Complete	Total Program
Total PE Cost	**130.541**	**26.447**	**23.665**	**18.404**	**19.190**	**18.203**	**21.849**	**22.248**	**22.656**	**Continuing**	**Continuing**
X0734 Information Systems Security	**130.541**	**24.037**	**15.035**	**16.107**	**16.642**	**15.591**	**18.692**	**19.045**	**19.404**	**Continuing**	**Continuing**
R0734 Information Assurance	**0.000**	**0.000**	**2.904**	**2.297**	**2.548**	**2.612**	**3.157**	**3.203**	**3.252**	**Continuing**	**Continuing**
X2987 Intelligent Agent Security Module	**0.000**	**2.410**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**2.410**
X9280 KG-40A Modernization Program	**0.000**	**0.000**	**1.283**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**1.283**
X9281 Intelligent Agent Security Module	**0.000**	**0.000**	**4.443**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**4.443**
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 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 5200.28. 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 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 service critical to the effective performance of the Navy's mission.

(U) The interconnectivity of Naval networks, attachment to the public information infrastructure, and their use in modern Naval and Joint war fighting means that the Naval Information Infrastructure (NII) is a higher value and more easily attainable target. An adversary has a much broader selection of attack types from which to choose than in the past. In addition to the traditional attacks that involve the theft or eavesdropping of information, United States Navy (USN) information systems face advanced attacks involving malicious changes to critical information, changes to the functioning of critical systems, denial of service, 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. 193

CLASSIFICATION:

EXHIBIT R-2, RDT&E Budget Item Justification	DATE: **February 2003**
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. Modeling DOD and commercial information 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. During meetings held with OPNAV N64 in March 2001, the ISSP established a revised goal and objective set that resulted in the creation of the Mission Capability Teams (MCT). This resulted in reorganization of the ISSP budget structure which facilitates the continuance of ISSP RDT&E efforts.

(U) The interconnection of USN and the NII 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 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 of existing, operational systems.

R-1 SHOPPING LIST - Item No. 193

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification								DATE: **February 2003**			
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT NUMBER AND NAME 0303140N Information Systems Security Program (ISSP)					PROJECT NUMBER AND NAME X0734 Information Systems Security					
COST ($ in Millions)	Prior Years Cost	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	Cost to Complete	Total Program
Project Cost	**130.541**	**24.037**	**15.035**	**16.107**	**16.642**	**15.591**	**18.692**	**19.045**	**19.404**	**Continuing**	**Continuing**
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. The Network-Centric afloat war fighter must rely 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 Maritime Cryptologic Architecture. 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.

(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, as either Multiple Security Level (MSL) or Multi-Level Security (MLS); (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.

R-1 SHOPPING LIST - Item No. 193

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2003**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	X0734 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 misuse 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 develops 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.

(U) 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 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 Navy distributed information systems (e.g., Information Technology for the 21st Century (IT-21), new total ship computing environments, and the Navy Marine Corp Intranet (NMCI). This portion of the ISSP supports delivery of network security engineering expertise needed to stand-up the NMCI and securely deploy IT-21 constituent systems such as Advanced Digital Network System (ADNS), Global Command and Control System - Maritime (GCCS-M) and Base Level Information Infrastructure (BLII). It includes activities to:

- Ensure that USN IA systems 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.
- Provide the ability to protect from, react to, and restore operations after an intrusion or other catastrophic event.
- Enable dynamic throttling of services due to change in risk posture resulting from changing 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.
- Maintain configuration management of all hosts to track all patches and system configuration changes.
- Ensure adequate defenses against subversive acts of trusted people and systems, both internal and external.

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2003**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	X0734 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.

R-1 SHOPPING LIST - Item No. 193

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2003**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	X0734 Information Systems Security

(U) B. Accomplishments/Planned Program

	FY 02	FY 03	FY 04	FY 05
Network Security Mission Capability Team (MCT)	8.069	6.292	2.613	2.963
RDT&E Articles Quantity				

FY02 Accomplishments include:
$1.562 - Continued developing and testing distributed IA solutions for Navy information systems. This included the examination and selection of next generation IA components required by the architectures which included firewalls, intrusion detection systems (including host-based systems), virtual private networking systems, public key based secure e-mail and web systems, operating systems and others as well as high assurance components for connection of Top Secret and Sensitive Compartmented Information (SCI) systems to lower level systems. Also examined, evaluated and demonstrated next generation network security appliances, specifically focusing on increasing performance rates to Optical Carrier Rate 12 (OC-12 = 622.08 Million Bits per Second (Mbps)) and greater. Continued to support the design of situational awareness and visualization capabilities to support active computer network defense and the development of a sensor grid with underlying data mining and correlation tools. Developed capability to remotely manage and securely control the configurations of network security components to implement changes in real time or near real time. Continued to prototype components at selected operational sites.

$1.160- Worked toward the Defense Advanced Research Projects Agency (DARPA) sponsored Common Intrusion Detection Framework (CIDF) object model. Conducted experiments and prepared protection profiles for Fleet Enclave boundary with Intrusion Detection System (IDS) driven auto-responding security policy. Continued integration of USN deployed afloat and ashore network security systems into the Joint (Commander-in-Chief Space Command (CINCSPACE), Joint Task Force – Computer Network Defense (JTF-CND)) IA common operating picture (IA-COP). Demonstrated the ability to share common IA enclave protection profiles definitions in response to Information Operations Condition (INFOCONs). Expanded activities of the Fleet Information Warfare Center (FIWC) IDS correlation process, Navy Component Task Force – Computer Network Defense, and the unification of the USN enterprise network operational status with the currently separate IA alarm status. Continued to explore IDS alternatives to existing USN deployed pattern-recognition-based intrusion detection systems. Other continuing tasks include: (1) expanding IDS requirements to address detection of both network misuse and intrusion, (2) market surveys of emerging agent and other sensor based IDS products focusing on CIDS Framework standards, (3) defining architectures that optimize IDS monitoring while minimizing sensor count, (4) mobile subscriber, forward deployed and shipboard IDS techniques and products, (5) native Asynchronous Transfer Mode (ATM), Signaling System Seven (SS7), sensors and alarm definitions, (6) workstation (personal) IDS techniques and products, and (7) build upon IDS capabilities included in existing commercial-off-the-shelf operating systems. Moreover, continued to work closely with the National Security Agency (NSA) and the Naval Information Warefare Activity (NIWA) to develop electronic infrastructure defense rules of engagement (ROE) that maximize the probability of protection mission success. Specific tasks included: (1) defining potential rules of engagement for automatic response to attack, (2) modeling and war gaming of auto-defend and manual-defend scenarios, (3) optimal selection of methods, (4) Command, Control, Computers, Communications, and Intelligence (C4I) support plan, (5) battle damage assessment plan, and (6) assessment modeling of impact to overall USN enterprise. Response capabilities included localized automatic and manual defensive and authorized active engagement to include the ability to quantitatively describe attack recovery (fratricide and hostile).

R-1 SHOPPING LIST - Item No. 193

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2003**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	X0734 Information Systems Security

$1.740 - Continued the evolutionary development of security architectures for IA that include virtually all Navy distributed information system development programs. Ensured the architectures evolve to provide proper protection as technology, DOD missions, and the threat all evolve. Provided inputs to the major Navy and joint initiatives that are defining and building distributed systems including shipboard networks (IT-21), Navy Marine Corps Intranet (NMCI), the Joint Technical Architecture (JTA), Global Command and Control System – Maritime (GCCS-M), Global Command and Control System (GCCS), Defense Messaging System (DMS), Automated Digital Network System (ADNS), Base Level Infrastructure Improvement (BLII), and others. Included both defensive protections as well as intrusion monitoring in the architecture.
Continued IA engineering, product selection assistance, and certification and accreditation support to Navy information system developments such as shipboard networks IT-21, NMCI), JTA, GCCS-M, GCCS, DMS, ADNS, BLII new ship construction (e.g. (NSSN, LPD-17, SCN-21…), Maritime Cryptologic System for the 21st Century (MCS-21), and others. Ensured IA integration at the earliest stage possible in the development process. Focused on integration of the proper functions to ensure adherence to the common security architectures. Ensured that the security and performance of the tactical systems, including those operating at Top Secret and at Sensitive Compartmented Information (SCI), were consistent with Navy and DOD requirements.

$0.967 - Prepared and tested lab model of a common criteria transition program that moved existing USN IA products and architectures to the newly required Common Criteria certified products and architectures, as published in March 2000 by the National Security Telecommunications and Information Systems Security Committee (NSTISSC), publication National Policy Governing the Acquisition of IA and IA-Enabled Information Technology Products" (NSTISSP No. 11).

$0.436- Conducted unclassified wireless local area network (LAN) products program testing and prepared protection profile for shipboard, office, and limited field use. Tasks included: (1) vulnerability testing of several common products (such as specifically within USN architectures), (2) security issues related to distributed antenna distribution within command centers and large offices, (3) configuration guidance for general use of the Wired Equivalent Privacy (WEP) protocol, and (4) completing a protection profile for "Wireless Network devices (access points and clients) used on Unclassified Networks."

$0.445 - Continued developing and updating IA standards and engineering guidance to ensure that they were consistent with the security architecture, the rapidly changing technology, and the evolving threat. Emphasized the paralleling of USN IA guidance to match the overall DoD Information Assurance Technical Framework (IATF). This included rapid guidance publication in response to Fleet-demanded new technologies which is usually several years prior to release of a CC protection profile. Worked closely with the Naval Postgraduate School to define a working set of IA metrics applicable to the USN enterprise. The goal was to work toward a Quality of IA value that is quantitative in nature, measurable, and optimizable. Tasks included: (1) defining current IA state vectors, (2) defining cost values, (3) defining reliability values, (4) defining availability values, and (5) defining the Quality of IA value as stochastic model, and enterprise implementation modeling and measurements.

$0.484 - Prepared protection profile for current Fleet enclave and shipboard security architectures for IA that included virtually all Navy distributed information system development programs. Continued refining an overall USN-wide enclave boundary policy, expanding upon the OPNAV N64 USN firewall policy into a comprehensive mobile subscriber enclave IA plan. Ensured the architectures evolved to provide proper protection as technology, DOD missions, and the threat all evolved. Provided inputs to the major Navy and joint initiatives that are defining and building distributed systems including shipboard networks (IT-21), the Navy Marine Corps Intranet (NMCI), the Joint Technical Architecture, Maritime Cryptologic Architecture, and large development programs including Global Command and Control System – Maritime (GCCS-M), Global Command and Control System (GCCS), Defense Messaging System (DMS), Automated Digital Network System (ADNS), Base Level Infrastructure Improvement (BLII)and others. Specific tasks included: (1) technical requirements development, (2) architecture and campaign plan preparation, (3) policy framework documentation, (4) application to surface, subsurface, air, and first-ashore forces maintaining connectivity to shipboard and ashore networks, and (5) coordination with Fleet components.

R-1 SHOPPING LIST - Item No. 193

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2003**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	X0734 Information Systems Security

$1.275 - Conducted a detect-respond experiment as part of a Fleet Battle Experiment in support of the Joint Task Force – Computer Network Defense (JTF-CND) and the Navy Component Task Force – Computer Network defense (NCTF-CND). Worked closely with the National Security Agency and the Naval Information Warfare Activity, fielded a test model of the electronic infrastructure that implemented defense rules of engagement (ROE) that maximized the probability of protection mission success. Tasks included: (1) defining potential rules of engagement for automatic response to attack, (2) modeling and war gaming of auto-defend and manual-defend scenarios, (3) optimal selection of methods, (4) Command, Control, Computers, Communications, and Intelligence (C4I) support plan, (5) battle damage assessment plan, and (6) assessment modeling of impact to overall USN enterprise. Capabilities included localized automatic and manual defensive and authorized active engagements. Included the ability to quantitatively describe attack recovery (fratricide and hostile).

FY03 Plans include:
$6.292- Continue to provide the broadest range of Information Assurance research across Joint, Fleet, and ashore networks. Applications include unclassified through TOP SECRET networks, while closely coordinating with TOP SECRET/SCI network requirements to ensure the broadest common solution. Provides robust design and evaluation for improved security product performance to accommodate higher speeds, more complicated architectures, and the ever-increasing threat. Focus becomes more and more on risk management approaches against state-sponsored network attack while preventing the nuisance disruption caused by the computer hacker community. Includes close work, design review, and operational testing with the Fleet CINCs to ensure that the IA infrastructure is available to enforce evolving critical infrastructure protection policies, including support for Fleet Battle Experiments and other short-reaction demonstrations.

Major emphasis includes early security design engineering of new ships, aircraft, and submarines to ensure that the reduced manning and greater operational dependency on networks. Provides for systems security engineering design, modeling, technical evaluations and designs, testing design and validation, and continuing COTS and GOTS evaluations and recommendations. Coordinates integration of secure design, testing, and products into new platforms and systems.

Design, modeling, and testing efforts are closely coordinated with the Joint Task Force – Computer Network Defense, the Defense Advanced Research Projects Agency, the new Commander, Naval Task Force – Navy Marine Corps Intranet, Commander, Naval Security Group Command, and the Fleet Information Warfare Center. Works design architectures and evaluation methods through the Information Assurance Technical Framework forum, the Internet Engineering Task Force, and other Information Assurance organizations.

For the first time, ISSP is applying IA engineering design, 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 Information Assurance appliances, software, and implementation techniques for policies such as IAVA requirements, INFOCON response, and USN firewall policy. This requires close engineering coordination with Information Operations activities, Exploit and Attack, to ensure coordination and fratricide prevention, network or RF path based. It includes engineering modeling and design of systems used in the isolation of network intrusion or attack from degradation caused by Electromagnetic Interference (EMI/RFI).

R-1 SHOPPING LIST - Item No. 193

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2003**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	X0734 Information Systems Security

FY04 Plans include:
$2.613- Continue to design, development and evaluation for improved security product performance to accommodate higher speeds, more complicated architectures, and the ever-increasing threat. Focusing on approaches and products against state-sponsored network attack while preventing the nuisance disruption caused by the computer hacker community. Includes product development and operational testing with the Fleet CINCs to ensure that the IA infrastructure is available to enforce evolving critical infrastructure protection policies, including support for Fleet Battle Experiments and other short-reaction demonstrations. Continue to provide security & test design, modeling, validation and integration engineering of network security COTS and GOTS into new ships, aircraft, submarines and systems.

FY05 Plans include:
$2.963- Continue to provide the broadest range of Information Assurance research across Joint, Fleet, and ashore networks. Applications include unclassified through TOP SECRET networks, while closely coordinating with TOP SECRET/SCI network requirements to ensure the broadest common solution. Provides design and evaluation for improved security product performance to accommodate higher speeds, more complicated architectures, and the ever-increasing threat. Continue to provide security design engineering of new ships, aircraft, and submarines to ensure that the reduced manning and greater operational dependency on networks. Provides for systems security engineering design, modeling, technical evaluations and designs, testing design and validation, and continuing COTS and GOTS evaluations and recommendations. Coordinates integration of secure design, testing, and products into new platforms and systems. Continue to provide IA engineering design, 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 Information Assurance appliances, software, and implementation techniques for policies such as IAVA requirements, INFOCON response, and USN firewall policy.

R-1 SHOPPING LIST - Item No. 193

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2003**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	X0734 Information Systems Security

	FY 02	FY 03	FY 04	FY 05
Crypto MCT	10.983	3.837	4.996	4.060
RDT&E Articles Quantity				

FY02 Accomplishments include:
$3.417- Continued development of a digital modular cryptographic design solution based on multi-channel, programmable technology. Entered certification and accreditation (C&A) cycle with the National Security Agency (NSA) for first item Multipurpose Cryptographic Unit (MCU) that will replace aging cryptographic equipment where the USN is either the sole or lead user. Expanded algorithm capability to Joint common legacy systems. Fully defined the first 4 interface specifications, and prepared specification and an RFP for release. Supported the Communications Security (COMSEC) equipment certification process, including the conduct of analyses required and the development of associated documentation. Also performed analysis and documentation required for software algorithm certification. These efforts were fully coordinated with the National Security Agency.

$5.307 - Continued the development of Electronic Key Management System (EKMS) Phase IV for Tier 1, Tier 2, Tier 3 and to ensure compatibility with Tier 0. Continued to research and investigate new key management technologies. Demonstrated web-based technology and exchange capabilities. Demonstrated integration of certificate management and key management directory structures and workstation functions. Demonstrated prototype of the Navy Single Point Command, Control, and Keying (NSPC2K) design and solution for Navy platforms. Continued to support development of the DTD 2000, and continue to provide key management support for embedded cryptographic technology and cryptographic replacement efforts. Conducted laboratory assessments of the latest NSA and commercial-off-the-shelf key management technology and products. Provided systems security, Certification and Accreditation (C&A), engineering, and testing for key management components and systems.

$0.760 - Conducted analysis for Data Transfer Device (KOV-21), Single Point Keying, Netted Re-keying and Modular KOK-22 development. Conducted Security Testing, engineering and integration analysis for EKMS.

$0.967 - Continued the design, development, evaluation and application of class 4 and 5 public key and certificate management infrastructure technologies and systems to support DoD and DON initiatives, including integration with IT-21 and other new ship initiatives. Continued to work closely with the commercial developers and vendors, infused technology and requirements into the commercial products, and supported efforts to PKI-enable specific applications. Continued to evaluate, assess, integrate and demonstrate related technologies including smart card security tokens and Virtual Private Networks (VPNs).

$0.242 - Began key management architecture for forward-deployed tactical and shipboard “lights-out” or minimal crew communications centers. The effort included architectures for platforms such as DD-21 and VA-Class submarines. The architectures and interfaces of systems such as Electronic Key Management System (EKMS), Public Key Management (PKI), and Certificate Management Infrastructure (CMI) were analyzed to determine how isolated automated systems could be used to handle electronic keying, authentication, and code confirmation tasks.

$0.290 - Prepared protection profile and define key management architecture for secure wireless Ethernet Local Area Network (LAN).

R-1 SHOPPING LIST - Item No. 193

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2003**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	X0734 Information Systems Security

FY03 Plans include:
$3.837-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. Includes design, integration, and testing of new cryptographic modules, USN-unique and USN-lead-service high-assurance algorithm software development, module hotel support, and protocol and control interface functions. Provides engineering design evolution for the supporting key management infrastructure, 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 additional Certificate Management Infrastructures (CMI). Includes design, evaluation, integration, and testing of key-related platforms, such as smart cards, and authentication mechanisms, such as biometric devices. Provides systems security engineering, test, evaluation, and development program support for organizations utilizing cryptographic equipments and associated keying systems. Provides continuous development coordination with the DoD PKI program office, the DON Smart Card office, the US Army biometrics program office, and the Information Systems Security Office at the National Security Agency. Provides specific design, testing, and evaluation assistance for new USN platforms and assists in defining embedded cryptographic product engineering requirements. Includes 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 architectures. This year's efforts expand to cover increased support for embedded cryptographic products in DD(X) and JTRS.

FY04 Plans include:
$4.996- Continue 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. Includes design, integration, and testing of new cryptographic modules, USN-unique and USN-lead-service high-assurance algorithm software development, module hotel support, and protocol and control interface functions. Provides continuous development coordination with the Information Systems Security Office at the National Security Agency. Provides specific design, testing, and evaluation assistance for new USN platforms and assists in defining embedded cryptographic product engineering requirements. Includes 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 architectures. This year's efforts expanded to cover increased support for embedded cryptographic products in DD(X) and JTRS.

FY05 Plans Include:
$4.060- Continue 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. Includes design, integration, and testing of new cryptographic modules, USN-unique and USN-lead-service high-assurance algorithm software development, module hotel support, and protocol and control interface functions. Provides continuous development coordination with the Information Systems Security Office at the National Security Agency. Provides specific design, testing, and evaluation assistance for new USN platforms and assists in defining embedded cryptographic product engineering requirements. Includes 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 architectures. This year's efforts expanded to cover increased support for embedded cryptographic products in DD(X) and JTRS.

R-1 SHOPPING LIST - Item No. 193

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification			DATE: **February 2003**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME	
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	X0734 Information Systems Security	

	FY 02	FY 03	FY 04	FY 05
Information Assurance Readiness MCT	1.451	2.222	0.276	0.313
RDT&E Articles Quantity				

FY02 Accomplishments include:
$0.484 - Continued vulnerability/threat assessments and development and systems integration of network countermeasures tools (NVACM) efforts.

$0.580 - Began consolidating computing base and data store vulnerabilities program. Focused this year activities on securing delivery of tactical/command mobile code. Included the common DoD used forms of computer operating systems and mobile code. Tasks included: (1) expansion of techniques to other operating systems, including public and private operating systems, (2) trusted code delivery, (3) enclave mobile code repository, (4) database entry assurance, and (5) other emerging uses and users. Built configuration guidance for server-to-server trust relationships.

$0.387 - Updated the methods and tools for the afloat Certification and Accreditation (C&A) red-team. Revised experimental model and analyzed network performance impacts. Formalized the experimental model based upon OPNAV red-team goals. Established firm statistical model for team data gathering. Tasks included: (1) experimental model, including statistical estimation moment minimum values, (2) defining statistical methods, including random selection regime, (3) population definition, (4) data collection method and common worksheet, and (5) statistical analysis framework.

FY03 Plans include:
$2.222- 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. Involves work with all delivering USN systems to ensure secure networks before operational testing. C&A activities include networks, applications, sensors, and databases. Supports the Fleet Information Warfare Center (FIWC), the Naval Security Group Activity Pensacola, and the CTF-NMCI for continuing CNVA activities. Includes the development and maintenance of USN infrastructure security policy. Includes systems security engineering, testing, and evaluation supporting other organizations during development of the Systems Security Accreditation Agreement (SSAA) and supporting activities of the Certification Authorities and Designated Accreditation Authorities during the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). Includes development of network countermeasures tools (NVACM), in close coordination with the Naval Information Warfare Activity. Supports development of validation methods, including tools provided to the USN RED TEAMs and NMCI contract SLA validation teams.

FY04 Plans include:
$0.276- 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. Involves work with all delivering USN systems to ensure secure networks before operational testing. C&A activities include networks, applications, sensors, and databases. Supports the Fleet Information Warfare Center (FIWC), the Naval Security Group Activity Pensacola, and the CTF-NMCI for continuing CNVA activities. Includes the development and maintenance of USN infrastructure security policy.

FY05 Plans include:
$0.313- 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.

R-1 SHOPPING LIST - Item No. 193

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification			DATE: **February 2003**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME	
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	X0734 Information Systems Security	

	FY 02	FY 03	FY 04	FY 05
Secure Voice MCT	2.268	1.946	0.828	0.939
RDT&E Articles Quantity				

FY02 Accomplishments include:

$0.385 - Secure Telecommunication – Internet Protocol (IP) Gateway/Inter-Working Function (IWF). Finalized development efforts for the production release of a secure voice IWF capability between Telecommunication and IP systems. Conducted demonstrations of the Secure Telecommunication – IP Gateway IWF capabilities over operational commercial and Navy communication systems for test and evaluation purposes. Supported production readiness evaluation and environmental testing for new ship construction delivery. Finalized open system design requirements for the initial production specification release of SV-21 architecture.

$0.479 - Tactical Secure Voice Internet Protocol Server IWF. Released Request for Proposal (RFP) for an Engineering Development Model (EDM) to support the design and integration of tactical shipboard secure voice systems into the SV-21 architecture. Conducted laboratory demonstrations of secure voice interoperation between tactical crypto equipment and Voice over IP (VoIP) conversion capability. Evaluated VoIP technologies within fleet battle experiments over Non-classified IP Routed Network (NIPRNET) and Secret IP Routed Network (SIPRNET) to determine mission critical throughput reliability and impacts on tactical enclave network configurations.

$0.326 - Secure Voice over Wireless Technologies. From next generation secure voice studies conducted in FY 01, demonstrated and evaluate VoIP using the IEEE 802.11 standard for Wireless Ethernet Protocol (WEP). Conducted operational assessments on the applicability of digital cellular and hand-held satellite secure voice products within the Navy strategic and tactical communication environments.

$0.498 - Advanced Secure Voice System Development. Continued the design, development and assessment of security solutions/capabilities for SV-21 architecture applicable to strategic and tactical communication integration. Conducted research on developing secure voice technologies and techniques for secure voice over government and commercial communications backbones, specifically addressing Asynchronous Transfer Mode (ATM) technology and voice over data network applications.

$0.290 - Voice Processing and Biometric Access Consortia. Conducted exploratory research on digital voice processors and voice/speaker recognition technologies. Continued laboratory research on digital voice processing techniques to evaluate voice command and control communication suitability in tactical Navy operational environments. Developed and assessed digital voice-processing techniques for low data rate, multi-rate, and variable rate voice processing algorithms. Supported development of government and industry standards for digital voice processing technologies (e.g., Mixed Excitation Linear Prediction (MELP), in conjunction with joint cryptographic developments.

$0.290 - Prepared protection profile and specifications for gateway to Secure Terminal Equipment (STE)/Secure Telephone Unit Third Generation (STU-III) Public Switched Telephone Network (PSTN) and Integrated Services Digital Network (ISDN) gateway keying system requirements. Established architecture for user keying and access.

R-1 SHOPPING LIST - Item No. 193

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2003**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	X0734 Information Systems Security

FY03 Plans include:
$1.946- Ensure information superiority through the use of encryption, authentication, and access control mechanisms over Navy mission essential voice circuits. This includes: (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 FY03 include Secure Voice over Internet Protocal (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 Centurty (SV-21) architectures.

FY 04 Plans Include:
$0.828- Continue to design, develop 21st Century Secure Voice Architecture including Secure Voice over Internet Protocal (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 Centurty (SV-21) architectures.

FY05 Plans Include:
$0.939- Continue development and begin prototype integration of 21st Century Secure Voice Architecture including Secure Voice over Internet Protocal (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 Centurty (SV-21) architectures

	FY 02	FY 03	FY 04	FY 05
Multiple Security Level MCT	1.266	0.738	0.845	0.959
RDT&E Articles Quantity				

FY02 Accomplishments include:
$0.129 - Used current Navy INFOSEC/IA problems (including network security, multi-level security (MLS), public key infrastructure (PKI), tokens, biometrics, intrusion detection and reaction) as the basis for case studies, laboratory work and student thesis research efforts. Acted as a focal point within DoN for advanced education in INFOSEC/IA by creating new and innovative course materials addressing foundational issues in IA, INFOSEC and Computer Security (COMPUSEC). This effort reflects the cumulative and most recent developments from IA theory and practice.
$1.137 - Continued to design, develop, and prototype coalition interoperability and multi-level security solutions. Based the solutions on available multilevel security technologies as well as emerging architectural methods of providing interoperability across different security levels. Continued to examine multi-level aware applications and technologies.

FY03 Plans include:
$0.738- Continue to provides systems security engineering development, testing, and evaluation for multi-level security solutions, including complicated evaluations involving allied and coalition participation. Solutions developed will address operator interface, computing and storage, peripherals, access control and credentials, local area networks appliances, wide area networks appliances, and unique IA sensors. Involves substantial efforts ensuring interoperability across commercial and government standards. Includes engineering of voice encoding standards ensuring interoperability between US and allied/coalition voice products. Includes integration of security requirements in the next generation Universal Mobile Telephone services, Generation 3.

R-1 SHOPPING LIST - Item No. 193

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2003**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	X0734 Information Systems Security

FY04 Plans include:
$0.845-Continue to provides systems security engineering development, testing, and evaluation for multi-level security solutions, including complicated evaluations involving allied and coalition participation to address emerging threats. Includes engineering of voice encoding standards ensuring interoperability between US and allied/coalition voice products. Continue 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. Begin integration of MSL prototype architecture at NOC facilities. Includes integration of security requirements in the next generation Universal Mobile Telephone services, Generation 3.

FY05 Plans include:
$.959- Continue to provides systems security engineering development, testing, and evaluation for multi-level security solutions, including complicated evaluations involving allied and coalition participation. Continued to examine multi-level aware applications and technologies including databases, web browsers, routers/switches, etc. Continue to develop and integrate MSL prototype architecture at NOC facilities.

	FY 02	FY 03	FY 04	FY 05
Key Management Infrastructure MCT			4.912	5.551
RDT&E Articles Quantity				

FY04 Plans include:
$4.912- Serves 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. Provides engineering design evolution for the supporting key management infrastructure, 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 additional Certificate Management Infrastructures (CMI). Includes design, evaluation, integration, and testing of key-related platforms, such as smart cards, and authentication mechanisms, such as biometric devices. Provides systems security engineering, test, evaluation, and development program support for organizations utilizing cryptographic equipments and associated keying systems. Specific projects include: (1) Afloat and OCONUS DoD Class 3/4 PKI, (2) Current Class 4 (X.509) PKI for Organizational Secure Messaging, (3) EKMS Common Tier 1 (CT1), (4) EKMS Tier 2/3, and (5) Key Management Infrastructure (KMI).

FY05 Plans include:
$5.551- 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. Provides engineering design evolution for the supporting key management infrastructure, 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 additional Certificate Management Infrastructures (CMI). Includes design, evaluation, integration, and testing of key-related platforms, such as smart cards, and authentication mechanisms, such as biometric devices. Provides systems security engineering, test, evaluation, and development program support for organizations utilizing cryptographic equipments and associated keying systems. Specific projects include: (1) Afloat and OCONUS DoD Class 3/4 PKI, (2) Current Class 4 (X.509) PKI for Organizational Secure Messaging, (3) EKMS Common Tier 1 (CT1), (4) EKMS Tier 2/3, and (5) Key Management Infrastructure (KMI).

R-1 SHOPPING LIST - Item No. 193

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2003**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	X0734 Information Systems Security

	FY 02	FY 03	FY 04	FY 05
Emerging Technology MCT			1.637	1.857
RDT&E Articles Quantity				

FY04 Plans include:
$1.637- Facilitates the transition and application of new technologies to Navy Information Assurance challenges. 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 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, EC5G, TF WEB, Teleport, SCN and other transition opportunities.

FY05 Plans include:
$1.857- Continue to support the transition and application of new technologies to Navy Information Assurance challenges. 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 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, EC5G, TF WEB, Teleport, SCN and other transition opportunities.

R-1 SHOPPING LIST - Item No. 193

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2003**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	X0734 Information Systems Security

(U) C. PROGRAM CHANGE SUMMARY:

(U) Funding:	FY 2002	FY 2003	FY 2004	FY 2005
President's Budget:	20.942	15.453	0.000	0.000
Current BES/President's Budget	24.037	15.035	16.107	16.642
Total Adjustments	3.095	-0.418	16.107	16.642
Summary of Adjustments				
EKMS Tier 1	3.486			
Section 8123: Management Reform Initiative	-0.216			
PBD-630 FFRDC	-0.022			
SBIR Assessment	-0.384			
Multi Functional Cryptologic System	2.600			
TFWeb BTR #02-15	-1.371			
JMPS and JC1 Program BTR #02-29	-0.425			
Re-test JFK Battle Group BFIT BTR #02-47	-0.002			
Sec. 313, PL 107-206: Revised Economic Assumptions	-0.049			
Section 8100: Business Process Reform		-0.062		
Section 8135: Economic Assumptions	-0.068	-0.112		
Section 8109: IT Cost Growth	0	-0.028		
FY02 Federal Technology Transfer	-0.012	0		
Section 8029, P.L. 107-248: FY03 FFRDC Reduction	0	-0.021		
Miscellaneous Navy Adjustments	-0.442	0		
Miscellaneous Department Adjustments		-0.195		
Subtotal	3.095	-0.418	0.000	0.000

(U) Schedule:

EKMS Tier 1 IOC has been delayed 3 months until 1st quarter FY03 and FOC until 4th quarter FY03.

(U) Technical:

N/A.

R-1 SHOPPING LIST - Item No. 193

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2003**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	X0734 Information Systems Security

(U) D. OTHER PROGRAM FUNDING SUMMARY:

Line Item No. & Name	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	To Complete	Total Cost
OPN 3415 Info Sys Security Program (ISSP)	97.267	86.517	81.938	90.816	114.940	123.850	119.337	118.336	Continued	Continued
OPN DERF	15.115									

(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 2003**

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

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

PROJECT NUMBER AND NAME: X0734 Information Systems Security

Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 03 Cost	FY 03 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
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	3.660	0.916	12/02	0.946	12/03	0.973	12/04	Continuing	Continuing	
Primary Hardware Development	C/CPAF	Motorola, Scottsdale, AZ	2.782	1.274	12/02	1.315	12/03	1.354	12/04	Continuing	Continuing	
Primary Hardware Development	C/VAR	Various	60.936	2.313	VAR	2.386	VAR	2.457	VAR	Continuing	Continuing	
Systems Engineering	C/VAR	Various	33.045	7.064	VAR	7.883	VAR	8.175	VAR	Continuing	Continuing	
Subtotal Product Development			107.705	11.567		12.530		12.959		Continuing	Continuing	

Remarks:

Software Development	CPAF	SAIC, San Diego, CA	32.877							0.000	32.877	42.590
Software Development	C/WX	NRL, Washjngton D.C.		0.067	10/02	0.078	10/03	0.083	10/04	Continuing	Continuing	
Subtotal Support			32.877	0.067		0.078		0.083		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 2003**			
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**		PROGRAM ELEMENT 0303140N Information Systems Security Program (ISSP)			PROJECT NUMBER AND NAME X0734 Information Systems Security						
Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 03 Cost	FY 03 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	VAR	Various	9.793	3.200	Various	3.302	Various	3.399	Various	Continuing	Continuing	Continuing
Subtotal T&E			9.793	3.200		3.302		3.399		Continuing	Continuing	
Remarks:												
Program Management Support	VAR	Various	4.203	0.201	Various	0.197	Various	0.201	Various	Continuing	Continuing	Continuing
Subtotal Management			4.203	0.201		0.197		0.201		Continuing	Continuing	
Remarks:												
Total Cost			154.578	15.035		16.107		16.642		Continuing	Continuing	
Remarks:												

R-1 SHOPPING LIST - Item No. 193

CLASSIFICATION:

EXHIBIT R4, Schedule Profile																													DATE: **February 2003**
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**									PROGRAM ELEMENT NUMBER AND NAME 0303140N Information Systems Security Program (ISSP)														PROJECT NUMBER AND NAME X0734 Information Systems Security											
Fiscal Year	2002				2003				2004				2005				2006				2007				2008				2009			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Acquisition * Milestones					EKMS Tier 1 IOC ☆				EKMS Tier 1 FOC ☆																									
Test & Evaluation Milestones Development Test Operational Test	△ EKMS Tier 1 GAT				△ EKMS Tier 1 19 Aug - 31 Oct 02																											
Production Milestones																																
Deliveries																																

* Note: EKMS Tier 1 IOC and FOC schedule slipped by 3 months.

CLASSIFICATION:

Exhibit R-4a, Schedule Detail					DATE: **February 2003**			
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT 0303140N Information Systems Security Program (ISSP)				PROJECT NUMBER AND NAME X0734 Information Systems Security			
Schedule Profile	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009
EKMS Tier 1 Developmental Testing (GAT)	1Q							
EKMS Tier 1 Operational Testing	4Q	1Q						
EKMS Tier 1 IOC		1Q						
EKMS Tier 1 FOC		4Q						

R-1 SHOPPING LIST - Item No. 193

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification								DATE: **February 2003**			
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT NUMBER AND NAME 0303140N Information Systems Security Program (ISSP)					PROJECT NUMBER AND NAME R0734 Information Assurance					
COST ($ in Millions)	Prior Years Cost	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	Cost to Complete	Total Program
Project Cost	**0.000**	**0.000**	**2.904**	**2.297**	**2.548**	**2.612**	**3.157**	**3.203**	**3.252**	**Continuing**	**Continuing**
RDT&E Articles Qty											

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

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

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

A Memorandum of Agreement (MOA) was signed in FY01 between the Office of Naval Research Department of Information, Electronics & Surveillance (ONR31) and Office of the Chief of Naval Operations, Directorate of Space, Information Warfare, Command and Control, Information Warfare Division (N64), and provides for interagency coordination with ONR, N64, and SPAWAR (PMW161) in pursuance of this effort.

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

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

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2003**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	R0734 Information Assurance

(U) B. Accomplishments/Planned Program

	FY 02	FY 03	FY 04	FY 05
Software and Systems Research	0.000	2.904	2.297	2.548
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. 193

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2003**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	R0734 Information Assurance

(U) C. PROGRAM CHANGE SUMMARY:

(U) Funding:	FY 2002	FY 2003	FY 2004	FY 2005
President's Budget:	0.000	2.983	0.000	0.000
Current BES/President's Budget	0.000	2.904	2.297	2.548
Total Adjustments	0.000	-0.079	2.297	2.548
Summary of Adjustments				
Section 8100: Business Process Reform		-0.012		
Section 8135: Economic Assumptions		-0.024		
Section 8109: IT Cost Growth		-0.005		
Miscellaneous Department Adjustment		-0.038		
Subtotal	0.000	-0.079	0.000	0.000

(U) Schedule:

N/A.

(U) Technical:

N/A

R-1 SHOPPING LIST - Item No. 193

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2003**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	R0734 Information Assurance

(U) D. OTHER PROGRAM FUNDING SUMMARY:

Line Item No. & Name	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	To Complete	Total Cost
OPN 3415 Info Sys Security Program (ISSP)	97.267	86.517	81.938	90.816	114.940	123.850	119.337	118.336	Continued	Continued
OPN DERF	15.115									

(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 2003**				
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**		PROGRAM ELEMENT 0303140N Information Systems Security Program (ISSP)			PROJECT NUMBER AND NAME R0734 Information Assurance							
Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 03 Cost	FY 03 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
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.	0.000	2.904	10/02	2.297	10/03	2.548	10/04	Continuing	Continuing	
Subtotal Support			0.000	2.904		2.297		2.548		Continuing	Continuing	
Remarks:												

R-1 SHOPPING LIST - Item No. 193

CLASSIFICATION:

Exhibit R-3 Cost Analysis (page 2)										DATE: **February 2003**		
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**		PROGRAM ELEMENT 0303140N Information Systems Security Program (ISSP)				PROJECT NUMBER AND NAME R0734 Information Assurance						
Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 03 Cost	FY 03 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											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			0.000	2.904		2.297		2.548		Continuing	Continuing	
Remarks:												

R-1 SHOPPING LIST - Item No. 193

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification								DATE: **February 2003**			
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT NUMBER AND NAME 0303140N Information Systems Security Program (ISSP)					PROJECT NUMBER AND NAME X2987 Intelligent Agent Security Module					
COST ($ in Millions)	Prior Years Cost	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	Cost to Complete	Total Program
Project Cost	**0.000**	**2.410**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**2.410**
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).

(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. 193

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2003**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	X2987 Intelligent Agent Security Module

(U) B. Accomplishments/Planned Program

	FY 02	FY 03	FY 04	FY 05
Intelligent Agent Security Module (IASM)	2.410			
RDT&E Articles Quantity				

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).

R-1 SHOPPING LIST - Item No. 193

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2003**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	X2987 Intelligent Agent Security Module

(U) C. PROGRAM CHANGE SUMMARY:

(U) Funding:	FY 2002	FY 2003	FY 2004	FY 2005
President's Budget:	2.478			
Current BES/President's Budget	2.410			
Total Adjustments	-0.068	0.000	0.000	0.000
Summary of Adjustments				
Section 8135: Economic Assumptions	-0.007			
Miscellaneous Navy Adjustments	-0.061			
Subtotal	-0.068	0.000	0.000	0.000

(U) Schedule:

N/A.

(U) Technical:

N/A.

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2003**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	X2987 Intelligent Agent Security Module

(U) D. OTHER PROGRAM FUNDING SUMMARY:

Line Item No. & Name	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	To Complete	Total Cost
OPN 3415 Info Sys Security Program (ISSP)	97.267	86.517	81.938	90.816	114.940	123.850	119.337	118.336	Continued	Continued
OPN DERF	15.115									

(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 2003**				
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**		PROGRAM ELEMENT 0303140N Information Systems Security Program (ISSP)				PROJECT NUMBER AND NAME X2987 Intelligent Agent Security Module						
Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 03 Cost	FY 03 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
Systems Engineering	C/CPAF	Promia, San Francisco, CA	2.309							Continuing	Continuing	2.316
Subtotal Product Development			2.309	0.000		0.000		0.000		Continuing	Continuing	
Remarks:												
Subtotal Support			0.000	0.000		0.000		0.000			0.000	
Remarks:												

R-1 SHOPPING LIST - Item No. 193

CLASSIFICATION:

Exhibit R-3 Cost Analysis (page 2)								DATE: **February 2003**				
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**		PROGRAM ELEMENT 0303140N Information Systems Security Program (ISSP)				PROJECT NUMBER AND NAME X2987 Intelligent Agent Security Module						
Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 03 Cost	FY 03 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											0.000	
Subtotal T&E			0.000	0.000		0.000		0.000			0.000	
Remarks:												
Program Management Support	C/WX	SSC-San Diego, CA	0.101								0.101	
Subtotal Management			0.101	0.000		0.000		0.000			0.101	
Remarks:												
Total Cost			2.410	0.000		0.000		0.000		Continuing	Continuing	
Remarks:												

R-1 SHOPPING LIST - Item No. 193

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification								DATE: **February 2003**			
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT NUMBER AND NAME 0303140N Information Systems Security Program (ISSP)					PROJECT NUMBER AND NAME X9280 KG-40A Modernization Program					
COST ($ in Millions)	Prior Years Cost	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	Cost to Complete	Total Program
Project Cost	**0.000**	**1.283**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**1.283**
RDT&E Articles Qty											**0**

(U) A. MISSION DESCRIPTION AND BUDGET ITEM JUSTIFICATION: Congressional plus-up for Navy's Cryptographic KG-40A Modernization/Replacement Program. Provides for the design and development of a integrated solution for Navy's KG-40A crypto device replacement. The Department of the Navy (DON) cryptographic equipment inventory system does not have sufficient quantities of KG-40A crypto devices to satisfy the current and future requirements for Navy, Marine Corps, Army, and Air Force programs, and Allied Interoperability initiatives. Because of obsolete parts, the existing components are no longer manufactured or supported by industry. There are insufficient assets available in inventory to support the unfulfilled requirements to provide for Crypto sustainment. The Congressional plus up will provide for the design and development of the best low cost solutions for replacing existing crypto devices. In addition, the proposed add will facilitate the development of next generation cryptos to replace aging legacy equipment and support the network centric communications architecture.

(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. 193

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2003**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	X9280 KG-40A Modernization Program

(U) B. Accomplishments/Planned Program

	FY 02	FY 03	FY 04	FY 05
Cryptographic KG-40A Modernization	0.000	1.283	0.000	0.000
RDT&E Articles Quantity				

Congressional plus-up for Navy's Cryptographic KG-40A Modernization/Replacement Program. Provides for the design and development of a integrated solution for Navy's KG-40A crypto device replacement. The Department of the Navy (DON) cryptographic equipment inventory system does not have sufficient quantities of KG-40A crypto devices to satisfy the current and future requirements for Navy, Marine Corps, Army, and Air Force programs, and Allied Interoperability initiatives. Because of obsolete parts, the existing components are no longer manufactured or supported by industry. There are insufficient assets available in inventory to support the unfulfilled requirements to provide for Crypto sustainment. The Congressional plus up will provide for the design and development of the best low cost solutions for replacing existing crypto devices. In addition, the proposed add will facilitate the development of next generation cryptos to replace aging legacy equipment and support the network centric communications architecture.

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2003**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	X9280 KG-40A Modernization Program

(U) C. PROGRAM CHANGE SUMMARY:

(U) Funding:	FY 2002	FY 2003	FY 2004	FY 2005
Previous President's Budget:	0.000	0.000	0.000	0.000
Current BES/President's Budget	0.000	1.283	0.000	0.000
Total Adjustments	0.000	1.283	0.000	0.000
Summary of Adjustments				
Congressional Add KG-40 Modernization		1.300		
Miscellaneous Departmental Adjustment	0.000	-0.017		
Subtotal	0.000	1.283	0.000	0.000

(U) Schedule:

N/A

(U) Technical:

N/A

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification			DATE: **February 2003**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME	
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	X9280 KG-40A Modernization Program	

(U) D. OTHER PROGRAM FUNDING SUMMARY:

Line Item No. & Name	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	To Complete	Total Cost
OPN 3415 Info Sys Security Program (ISSP)	97.267	86.517	81.938	90.816	114.940	123.850	119.337	118.336	Continued	Continued
OPN DERF	15.115									

(U) E. ACQUISITION STRATEGY: *

The Navy intends to hold an open competition and award of an RD contract to provided an integrated solution for the KG-40A replacement at the best value to the government (lowest development/per unit/risk) that can be obtained.

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

CLASSIFICATION:

Exhibit R-3 Cost Analysis (page 1)								DATE: **February 2003**				
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**			PROGRAM ELEMENT 0303140N Information Systems Security Progran			PROJECT NUMBER AND NAME X9280 KG-40A Modernization Program						
Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 03 Cost	FY 03 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
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	TBD		1.100	09/03						1.100	
Training Development											0.000	
Licenses											0.000	
Tooling											0.000	
GFE											0.000	
Award Fees											0.000	
Subtotal Product Development			0.000	1.100		0.000		0.000		0.000	1.100	
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 2003**				
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**			PROGRAM ELEMENT 0303140N Information Systems Security Progran			PROJECT NUMBER AND NAME X9280 KG-40A Modernization Program						
Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 03 Cost	FY 03 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											0.000	
Operational Test & Evaluation											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	C/WX	SSC San Diego, CA		0.183	02/03						0.183	
Government Engineering Support											0.000	
Program Management Support											0.000	
Travel											0.000	
Transportation											0.000	
SBIR Assessment											0.000	
Subtotal Management			0.000	0.183		0.000		0.000		0.000	0.183	
Remarks:												
Total Cost			0.000	1.283		0.000		0.000		0.000	1.283	
Remarks:												

R-1 SHOPPING LIST - Item No. 193

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification								DATE: **February 2003**			
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	PROGRAM ELEMENT NUMBER AND NAME 0303140N Information Systems Security Program (ISSP)					PROJECT NUMBER AND NAME X9281 Intelligent Agent Security Module (IASM)					
COST ($ in Millions)	Prior Years Cost	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	Cost to Complete	Total Program
Project Cost	**0.000**	**0.000**	**4.443**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**4.443**
RDT&E Articles Qty											**0**

(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. 193

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2003**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	X9281 Intelligent Agent Security Module (IASM)

(U) B. Accomplishments/Planned Program

	FY 02	FY 03	FY 04	FY 05
Intelligent Agent Security Module (IASM)	0.000	4.443	0.000	0.000
RDT&E Articles Quantity				

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.

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2003**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	X9281 Intelligent Agent Security Module (IASM)

(U) C. PROGRAM CHANGE SUMMARY:

(U) Funding:	FY 2002	FY 2003	FY 2004	FY 2005
Previous President's Budget:	0.000	0.000	0.000	0.000
Current BES/President's Budget	0.000	4.443	0.000	0.000
Total Adjustments	0.000	4.443	0.000	0.000
Summary of Adjustments				
Congressional Add IASM		4.500		
Miscellaneous Departmental Adjustment	0.000	-0.057		
Subtotal	0.000	4.443	0.000	0.000

(U) Schedule:

N/A

(U) Technical:

N/A

CLASSIFICATION:

EXHIBIT R-2a, RDT&E Project Justification		DATE: **February 2003**
APPROPRIATION/BUDGET ACTIVITY	PROGRAM ELEMENT NUMBER AND NAME	PROJECT NUMBER AND NAME
RDT&E, N / BA-7	0303140N Information Systems Security Program (ISSP)	X9281 Intelligent Agent Security Module (IASM)

(U) D. OTHER PROGRAM FUNDING SUMMARY:

Line Item No. & Name	2002	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	To Complete	Total Cost
OPN 3415 Info Sys Security Program (ISSP)	97.267	86.517	81.938	90.816	114.940	123.850	119.337	118.336	Continued	Continued
OPN DERF	15.115									

(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**

CLASSIFICATION:

Exhibit R-3 Cost Analysis (page 1)								DATE: **February 2003**				
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**			PROGRAM ELEMENT 0303140N Information Systems Security Program (ISSP)			PROJECT NUMBER AND NAME X9281 Intelligent Agent Security Module (IASM)						
Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 03 Cost	FY 03 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
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.	0.000	3.943	09/03						3.943	
Training Development											0.000	
Licenses											0.000	
Tooling											0.000	
GFE											0.000	
Award Fees											0.000	
Subtotal Product Development			0.000	3.943		0.000		0.000		0.000	3.943	
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 2003**				
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**		PROGRAM ELEMENT 0303140N Information Systems Security Program (ISSP)			PROJECT NUMBER AND NAME X9281 Intelligent Agent Security Module (IASM)							
Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 03 Cost	FY 03 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	0.000	0.250	01/03						0.250	
Developmental Test & Evaluation	WX	SSC San Diego, CA	0.000	0.250	01/03						0.250	
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	0.500		0.000		0.000		0.000	0.500	
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			0.000	4.443		0.000		0.000		0.000	4.443	
Remarks:												

R-1 SHOPPING LIST - Item No. 193