EXHIBIT R-2, FY 2003 RDT&E,N BUDGET ITEM JUSTIFICATION

DATE: February 2002

BUDGET ACTIVITY: 7 PROGRAM ELEMENT: 0303140N
PROGRAM ELEMENT TITLE: Information Systems Security Program (ISSP)

(U) COST: (Dollars in Thousands)

PROJECT NUMBER & TITLE	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	FY2006	FY2007	TOTAL COMPLETE	TOTAL PROGRAM
X0734 Information Systems Security	30,277	24,190	15,453	19,476	20,571	20,351	20,611	CONT.	CONT.
R0734* Information Assurance			2,983	3,059	3,128	3,202	3,277	CONT.	CONT.
X2987**Intelligent Agent Security Module		2,478						CONT.	CONT.
TOTAL	30,277	26,668	18,436	22,535	23,699	23,553	23,888	CONT.	CONT.

*** Project Unit starting in FY03 for Office of Naval Research (ONR)**
**** FY02 Congressional Plus-up for Intelligent Agent.**

A. (U) 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. 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, 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.

(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 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 National Information Infrastructure (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.

B. (U) CHANGE SUMMARY EXPLANATION:

(U) FY 2001: +$8,600K Congressional Plus-up for PKI; +$2,000K Congressional Plus-up for NIASM; -$225K Section 8086 .7% ProRata Reduction; -$70K .22% Rescission; -$392K SBIR assessment; -$712 June 2001 BTR; and -$454K Navy miscellaneous adjustments.

(U) FY 2002: +$3,486K Adjustment for EKMS Tier 1; -$216K Section 8123 Management Reform Initiative; -$22K Section 8032 FFRDC.

(U) FY 2003: N/A

(U) Schedule: The EKMS schedule has slipped 6 months due to complex interoperability issues encountered during integration testing. Revised EKMS IOC date is 15 Jun 02, with Final Operational Capability (FOC) 22 Oct 02.

(U) Technical: N/A

EXHIBIT R-2a, FY 2003 RDT&E,N PROJECT JUSTIFICATION

DATE: FEBRUARY 2002

BUDGET ACTIVITY: 7 PROGRAM ELEMENT: 0303140N PROJECT NAME: ISSP
PROGRAM ELEMENT TITLE: Information Systems Security Program (ISSP) PROJECT NUMBER: X0734

(U) COST: (Dollars in Thousands)

PROJECT NUMBER & TITLE	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	FY2006	FY2007	TO COMPLETE	TOTAL PROGRAM
X0734 Information Systems Security	30,277	24,190	15,453	19,476	20,571	20,351	20,611	CONT.	CONT.

A. (U) MISSION DESCRIPTION AND BUDGET ITEM JUSTIFICATION: The Navy ISSP RDT&E program provides IA solutions for 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 COMSEC, Computer Security (COMPUSEC), 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.

(U) The ISSP RDT&E efforts must conclude with certified and accredited systems. This requires (1) Assured separation of information levels and user communities, including coalition partners; (2) Assurance of the telecommunications infrastructure; (3) Assurance of Joint user enclaves; (4) Assurance of the computing base and information store; and, (5) Supporting assurance technologies, including PKI and directories. To ensure interoperability and commercial standards compliance, these efforts often encompass the research, selective evaluation, integration, and test of Commercial off-the-shelf (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 (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.
•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.

1. (U) FY 2001 ACCOMPLISHMENTS:

(U) ($2,081) Completed initial development of architecture and preliminary design specifications for the digital modular cryptographic solution based on multi-channel, programmable technology. Validated candidate cryptographic replacement solutions (Blue sky/grey sky) for evaluation and assessment in representative Navy platforms, specifically VA class submarine. Continued support for the COMSEC certification process, including the conduct of analyses required and the development of associated documentation. These activities were coordinated with the National Security Agency.

(U) ($2,606) Continued the development of Electronic Key Management System (EKMS) Phase IV for Tier 1, Tier 2, Tier 3 and ensure compatibility with Tier 0. Completed the research and evaluation of several new key management technologies. Demonstrated prototype of the Navy Single Point Command, Control, and Keying ($NSPC^2K$) design and solution for Navy platforms. Completed several key design steps development of the Data Transfer Device (DTD) 2000, and provided key management support for embedded cryptographic technology and cryptographic replacement efforts.

(U) ($2,520) Completed US prototypes and quick-look evaluations related to the design, development, evaluation and application of PKI and CMI technologies and systems to support DoD and DON initiatives, including integration with shipboard network systems (IT-21) and the Navy Marine Corps Intranet (NMCI) initiatives. Established a new liaison office and promoted several demonstrations, working closely with the commercial developers and vendors. Demonstrated expansion of certificated based Virtual Private Networks (VPNs) security associations, specifically with Cisco VP gateways. Provided assessment of USN unique design requirements for application of biometric access control tokens (fingerprint, voiceprint and iris).

($8,600) This was a Congressional plus-up. Accelerated the design, development, evaluation and fielding of a PKI and CMI and the supporting infrastructure. Developed PKI applications and concepts as they related to afloat platforms to include evaluation of Medium Grade Services (MGS), Directory Services Testing (Single Sign On) and Hardware Cryptographic Modules (HCM). Conducted afloat demonstration of PKI on SIPRNET which encompassed use of Class 3 certificates, Local Registration Authority (LRA) support and formalized the process for introduction of PKI into IT-21 Afloat (Government Off-The-Shelf

(GOTS) Delta) deployment plan. Evaluated current PKI enabled applications to determine compatibility with DOD PKI certificates and investigate DOD policy and procedures required for enabling for PKI object signing certificates.

(U) ($1,971) Completed evaluations of several voice-sealed IP applications including assessment of several security solutions/capabilities for next generation voice systems. Continued research into new secure voice technology, developing technology and techniques for secure voice over government and commercial communications backbones, specifically addressing wire-line/wireless telephony and network applications applicable to strategic and tactical communications. Continued to develop and assess the technology for low data rate algorithms, voice compression technology in conjunction with cryptographic algorithm technology, and voice/speaker recognition.

(U) ($985) Continued development of Secure Voice-21 (SV-21). This included the development and integration of the crypto gateways (i.e., network interface card, crypto interface card, and the voice processing card), crypto replacement technology, the Navy Single Point Command, Control, and Keying ($NSPC^2K$) technology to support the embedded crypto replacements, and new voice algorithms (e.g., Mixed Excitation Linear Prediction (MELP). Demonstrated the SV-21 suite capability on a new ship operational platform for test and evaluation purposes.

(U) ($246) Continued USN representation to secure voice and biometric access consortia.

(U) ($739) Completed the first of several phases in the evolutionary development of security architectures for IA that include virtually all Navy distributed information system development programs. Completed support to Information Assurance demonstrations in Fleet Battle Experiments. Provided security engineering design and development assistance to other USN program offices, including major Navy and joint initiatives that are defining and building distributed systems including shipboard networks (IT-21), NMCI, the Joint Technical Architecture (JTA), and large development programs including GCCS-M, GCCS, DMS, ADNS, BLII, and others.

(U) ($3,272) Completed rollout and first technology refresh associated with major USN enclave security enclaves, such as at the Fleet Network Operating Centers. This included the examination and selection of next generation networking components required by the architectures that may include 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 SCI systems to lower level systems. Completed initial architecture and initiated policy discussions supporting 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.

(U) ($2,000) This was a Congressional plus-up. Completed Small Business Research Initiative (SBIR) Phase 1 and awarded 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 IDS's.

(U) ($2,464) Completed initial security engineering, Certification and Accreditation (C&A) support to Navy information system developments such as shipboard networks (IT-21) NMCI, JTA, and large development programs including GCCS-M, GCCS, DMS, ADNS, BLII and new ship construction (e.g., NSSN, LPD-17, and SCN-21).

(U) ($454) Provided INFOSEC standards and engineering guidance documents to several program offices. This ensured compliance with statutory requirements, including the FY01 Federal Information Security Act, ensuring that they are consistent with the security architecture, the rapidly changing technology, and the evolving threat.

(U) ($1,478) Completed evaluation of several prototype coalition interoperability and multi-level security solutions. Initiated security engineering support for the coalition cryptographic systems which are associated with battle Force E-mail 66. Conducted the US Navy's workshop on multi-level aware applications and technologies, including databases, web browsers, routers/switches, and workstations.

(U) ($811) Continued vulnerability/threat assessments and development and systems integration of network countermeasures tools (NVACM) efforts. Results of this effort are classified.

2. (U) FY 2002 PLAN:

(U) **SECURE VOICE ($594)** Secure Telecommunication – Internet Protocol (IP) Gateway/Inter-Working Function (IWF). Finalize development efforts for the production release of a secure voice IWF capability between Telecommunication and IP systems. Conduct demonstrations of the Secure Telecommunication – IP Gateway IWF capabilities over operational commercial and Navy communication systems for test and evaluation purposes. Support production readiness evaluation and environmental testing for new ship construction delivery. Finalize open system design requirements for the initial production specification release of Secure Voice 21 (SV-21) architecture.

(U) **SECURE VOICE ($990)** Tactical Secure Voice Internet Protocol Server IWF. Release Request for Proposal (RFP) for an Engineering Development Model (EDM) to support design and integration of tactical shipboard secure voice systems into the Secure Voice 21 (SV-21) architecture. Conduct laboratory demonstrations of secure voice interoperation between tactical crypto equipment and Voice over IP (VoIP) conversion capability. Evaluate 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.

(U) **SECURE VOICE ($634)** Secure Voice over Wireless Technologies. From next generation secure voice studies conducted in FY 01, demonstrate and evaluate VoIP using the IEEE 802.11 standard for Wireless Ethernet Protocol (WEP). Conduct operational assessments on the applicability of digital cellular and hand-held satellite secure voice products within the Navy strategic and tactical communication environments.

(U) **SECURE VOICE ($609)** Advanced Secure Voice System Development. Continue the design, development and assessment of security solutions/capabilities for SV-21 architecture applicable to strategic and tactical communication integration. Conduct 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.

(U) **SECURE VOICE ($297)** Voice Processing and Biometric Access Consortia. Conduct exploratory research on digital voice processors and voice/speaker recognition technologies. Continue laboratory research on digital voice processing techniques to evaluate voice command and control communication suitability in tactical Navy operational environments. Develop and assess digital voice-processing techniques for low data rate, multi-rate, and variable rate voice processing algorithms. Support development of government and industry standards for digital voice processing technologies (e.g., Mixed Excitation Linear Prediction (MELP), in conjunction with joint cryptographic developments.

(U) **CRYPTO ($1,981)** Continue development of a digital modular cryptographic design solution based on multi-channel, programmable technology. Enter 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. Expand algorithm capability to Joint common legacy systems. Fully define the first 4 interface specifications, and prepare specification and request-for-proposal (RFP) for release. Support the Communications Security (COMSEC) equipment certification process, including the conduct of analyses required and the development of associated documentation. A new effort will be analysis and documentation required for software algorithm certification. These efforts will be fully coordinated with the National Security Agency.

(U) **NSS (Network Security Systems) ($1,599)** Continue developing and testing distributed IA solutions for Navy information systems. This includes the examination and selection of next generation IA components required by the architectures that may include 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.

EXHIBIT R-2a, FY 2003 RDT&E,N PROJECT JUSTIFICATION

DATE: FEBRUARY 2002

BUDGET ACTIVITY: 7 PROGRAM ELEMENT: 0303140N PROJECT NAME: ISSP
PROGRAM ELEMENT TITLE: Information Systems Security Program (ISSP) PROJECT NUMBER: X0734

Examine, evaluate, and demonstrate 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. Continue 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. Develop capability to remotely manage and securely control the configurations of network security components to implement changes in real time or near real time. Continue to prototype components at selected operational sites.

(U) **NSS ($1,188)** Work toward the Defense Advanced Research Projects Agency (DARPA) sponsored Common Intrusion Detection framework (CIDF) object model. Conduct experiment and prepare protection profile for Fleet Enclave boundary with intrusion detection system (IDS) driven auto-responding security policy. Continue 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). Demonstrate the ability to share common IA enclave protection profiles definitions in response to Information Operations Condition (INFOCONs). Expand 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. Continue to explore IDS alternatives to existing USN deployed pattern-recognition-based intrusion detection systems. Continuing tasks include: (1) expanding IDS requirements, to address detection of both network misuse and intrusion, (2) market survey 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. Working closely with the National Security Agency (NSA) and the Naval Information Warefare Activity (NIWA), develop electronic infrastructure defense rules of engagement (ROE) that maximize the probability of protection mission success. Tasks include: (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 include localized automatic and manual defensive and authorized active engagement. Includes the ability to quantitatively describe attack recovery (fratricide and hostile).

(U) **MSL (Multiple Security Level) ($129)** Use current Navy INFOSEC/IA problems (to include 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. Based on continuing research, act 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 should reflect the cumulative, and most recent, developments from IA theory and practice.

(U) **MSL ($1,167)** Continue to design, develop, and prototype coalition interoperability and multi-level security solutions. Base the solutions on available multilevel security technologies as well as emerging architectural methods of providing interoperability across different security levels. Continue to examine multi-level aware applications and technologies including databases, web browsers, routers/switches, etc.

(U) **NSS ($1,782)** Continue the evolutionary development of security architectures for IA that include virtually all Navy distributed information system development programs. Ensure the architectures evolve to provide proper protection as technology, DOD missions, and the threat all evolve. Provide 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. Include both defensive protections as well as intrusion monitoring in the architecture. Continue 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. Ensure IA integration as early in the development process as possible. Focus on integration of the proper functions to ensure adherence to the common security architectures. Ensure that the security and performance of the tactical systems, including those operating at Top Secret and at sensitive compartmented information (SCI) are consistent with Navy and DOD requirements.

(U) **NSS ($990)** Prepare and test lab model of a common criteria transition program that moves 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).

(U) **CA (Certification and Accreditation) ($495)** Continue vulnerability/threat assessments and development and systems integration of network countermeasures tools (NVACM) efforts.

(U) **CA ($594)** Begin a consolidated computing base and data store vulnerabilities program. Focus this year activities to secure delivery of tactical/command mobile code. Include the common DoD used forms of computer operating systems and mobile code. Tasks include (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. Build configuration guidance for server-to-server trust relationships.

(U) **NSS ($446)** Conduct unclassified wireless local area network (LAN) products program testing and prepare protection profile for shipboard, office, and limited field use. Tasks include: (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) complete a protection profile for "Wireless Network devices (access points and clients) used on Unclassified Networks."

(U) **NSS ($456)** Continue developing and updating IA standards and engineering guidance to ensure they are consistent with the security architecture, the rapidly changing technology, and the evolving threat. Emphasis is on the paralleling of USN IA guidance to match the overall DoD Information Assurance Technical Framework (IATF). This includes rapid guidance publication in response to Fleet-demanded new technologies, usually several years prior to release of a CC protection profile. Work closely with Naval Postgraduate School to define a working set of IA metrics applicable to the USN enterprise. Goal is to work toward a Quality of IA value that is quantitative in nature, measurable, and optimizable. Tasks include: (1) defining current IA state vectors, (2) defining cost values, (3) defining reliability values, (4) defining availability values, (5) defining the Quality of IA value as stochastic model, and enterprise implementation modeling and measurements.

(U) **NSS ($495)** Prepare protection profile for current Fleet enclave and shipboard security architectures for IA that include virtually all Navy distributed information system development programs. Continue refining an overall USN-wide enclave boundary policy - expanding upon OPNAV N64 USN firewall policy into a comprehensive mobile subscriber enclave IA plan. Ensure the architectures evolve to provide proper protection as technology, DOD missions, and the threat all evolve. Provide 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 include: (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.

(U) **NSS ($1,305)** Conduct 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). Working closely with the National Security Agency and the Naval Information Warfare Activity, field a test model of the electronic infrastructure that implement defense rules of engagement (ROE) that maximize the probability of protection mission success. Tasks include: (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 include localized automatic and manual defensive and authorized active engagement. Includes the ability to quantitatively describe attack recovery (fratricide and hostile).

(U) **CA ($396)** Update the methods and tools for the afloat certification and accreditation (C&A) red-team. Revise experimental model, and understand network performance impacts. Formalizes the experimental model based upon OPNAV red-team goals. Establishes firm statistical model for team data gathering. Tasks include: (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.

(U) **CRYPTO ($5,433)** Complete the development of Electronic Key Management System (EKMS) Phase IV for Tier 1, Tier 2, Tier 3 and ensure compatibility with Tier 0. Continue to research and investigate new key management technologies. Demonstrate web-based technology and exchange capabilities. Demonstrate integration of certificate management and key management directory structures and workstation functions. Demonstrate prototype of the Navy Single Point Command, Control, and Keying ($NSPC^2K$) design and solution for Navy platforms. Continue to support development of the DTD 2000, and continue to provide key management support for embedded cryptographic technology and cryptographic replacement efforts. Conduct laboratory assessments of the latest NSA and commercial-off-the-shelf key management technology and products. Provide system security, certification, and accreditation (C&A) engineering and testing for key management components and systems.

(U) **CRYPTO ($778)** Conduct analysis for Data Transfer Device (KOV-21), Single Point Keying, Netted Re-keying and Modular KOK-22 development. Conduct Security Testing, engineering and integration analysis for EKMS.

(U) **CRYPTO ($990)** Continue 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. Continue to work closely with the commercial developers and vendors, infuse technology and requirements into the commercial products, and support efforts to PKI-enable specific applications. Continue to evaluate, assess, integrate and demonstrate related technologies including smart card security tokens and virtual private networks (VPNs).

(U) **CRYPTO ($248)** Begin key management architecture for forward-deployed tactical and shipboard "lights-out" or minimal crew communications centers. This includes 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) must be analyzed to determine how isolated automated systems can be used to handle electronic keying, authentication, and code confirmation tasks.

(U) **SECURE VOICE ($297)** Prepare 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. Establish architecture for user keying and access.

(U) **CRYPTO ($297)** Prepare protection profile and define key management architecture for secure wireless Ethernet local area network (LAN).

3. (U) FY 2003 PLAN:

U) **SECURE VOICE Communication Mission Capability Team**

(U) Crypto Mission Capability Team - Cryptographic Equipments and Security Management Infrastructure -

(U) $4,517) 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 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.

EXHIBIT R-2a, FY 2003 RDT&E,N PROJECT JUSTIFICATION

DATE: FEBRUARY 2002

BUDGET ACTIVITY: 7 PROGRAM ELEMENT: 0303140N PROJECT NAME: ISSP
PROGRAM ELEMENT TITLE: Information Systems Security Program (ISSP) PROJECT NUMBER: X0734

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), JCCX, and JTRS.

(U) Network Security Mission Capability Team -

(U) $7,427) 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. 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.

(U) 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.

(U) 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).

(U) Multiple Security Level Mission Capability Team -

(U) ($880) This is a major Fleet and Unified Command interest area. Involves application of all ISSP R&D toward the solution of shared networks, shared computing base, and information release to US allies and coalition partners, including Partners for Peace. Includes design engineering and application of new technologies that ensure rapid collaboration and strike execution. Includes security applications associated with shared RF paths, such as Battle Force E-mail 66, and support for multinational networks. Provides systems security engineering development, testing, and evaluation, 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.

(U) Information Assurance Readiness-Certification and Accreditation Mission Capability Team -

(U) ($2,629) 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.

B. (U) OTHER PROGRAM FUNDING SUMMARY: (Dollars in thousands)

FY 2001 ESTIMATE	FY 2002 ESTIMATE	FY 2003 ESTIMATE	FY 2004 ESTIMATE	FY 2005 ESTIMATE	FY 2006 ESTIMATE	FY 2007 ESTIMATE	TO COMPLETE	TOTAL PROGRAM

EXHIBIT R-2a, FY 2003 RDT&E,N PROJECT JUSTIFICATION

DATE: FEBRUARY 2002

BUDGET ACTIVITY: 7 PROGRAM ELEMENT: 0303140N PROJECT NAME: ISSP
PROGRAM ELEMENT TITLE: Information Systems Security Program (ISSP) PROJECT NUMBER: X0734

COMPLETE PROGRAM:

(U) OPN 3415 Information Systems Security Program (ISSP)								
64,216	86,822	78,473	61,800	34,637	50,992	49,466	CONT.	CONT.
(U) O&MN 4A6M								
17,534	19,983	20,344	19,287	14,895	13,940	14,302	CONT.	CONT.

(U) RELATED RDT&E:
(U) PE 0303140G
(Cryptographic Equipments)

C. ACQUISITION STRATEGY

	FY 2001	FY 2002	FY2003	To Complete
EKMS				
Program Milestones		3Q-Tier 1 IOC	1Q-Tier 1 FOC	
Engineering Milestones				
T&E Milestones		1Q-Tier 1 Government Acceptance Test (GAT)		
Contract Milestones				

EXHIBIT R-3, FY 2003 RDT&E,N COST ANALYSIS

DATE: FEBRUARY 2002

BUDGET ACTIVITY: 7 PROGRAM ELEMENT: 0303140N PROJECT NAME: ISSP
PROGRAM ELEMENT TITLE: Information Systems Security Program (ISSP) PROJECT NUMBER: X0734

Exhibit R-3 Cost Analysis (page 1)												Date: FEBRUARY 2002
APPROPRIATION/BUDGET ACTIVITY: 7			PROGRAM ELEMENT: 0303140N									PROJECT NAME AND NUMBER: ISSP (X0734)
Cost Categories	Contract Method & Type	Performing Activity & Location	Total PYs Cost	FY01 Cost	FY01 Award Date	FY02 Cost	FY02 Award Date	FY03 Cost	FY03 Award Date	Cost To Complete	Total Cost	Target Value of Contract
SOFTWARE DEVELOPMENT	CPAF	SAIC	29,597	233	03/01	3,047	12/01			0	32,877	42,590
SOFTWARE DEVELOPMENT	WX	NRL-DC	0	0	N/A	0	N/A	67	10/02	Cont.	Cont.	Cont.
HARDWARE DEVELOPMENT	CPFF/	VIASAT	7,282	0		0				0	7,282	7,282
HARDWARE DEVELOPMENT	MIPR	MITRE	1,911	823	12/00	926	12/01	916	12/02	Cont.	Cont.	Cont.
HARDWARE DEVELOPMENT	CPAF	MOTOROLA	0	1,000	06/01	1,782	12/01	1,274	12/02	Cont.	Cont.	Cont.
HARDWARE DEVELOPMENT	VAR	VARIOUS	54,980	3,620	VAR	2,336	VAR	2,313	VAR	Cont.	Cont.	Cont.
Subtotal Product Development			93,770	5,676		8,091		4,570		Cont.	Cont.	Cont.
Remarks: SAIC target value of contract includes other services' funding (ARMY RDT&E).												
SYSTEMS ENGINEERING	VAR	VAR	2,976	17,474	VAR	12,484	VAR	7,482	VAR	CONT.	CONT.	CONT.
Subtotal Support			2,976	17,474		12,484		7,482		CONT.	CONT.	CONT.
Remarks												

EXHIBIT R-3, FY 2003 RDT&E,N COST ANALYSIS

DATE: FEBRUARY 2002

BUDGET ACTIVITY: 7 PROGRAM ELEMENT: 0303140N PROJECT NAME: ISSP
PROGRAM ELEMENT TITLE: Information Systems Security Program (ISSP) PROJECT NUMBER: X0734

Exhibit R-3 Cost Analysis (page 2)										Date: February 2002		
APPROPRIATION/BUDGET ACTIVITY: 7			PROGRAM ELEMENT: 0303140N							PROJECT NAME AND NUMBER: X0734		
Cost Categories	Contract Method & Type	Performing Activity & Location	Total PYs Cost	FY01 Cost	FY01 Award Date	FY02 Cost	FY02 Award Date	FY03 Cost	FY03 Award Date	Cost To Complete	Total Cost	Target Value of Contract
TEST AND EVALUATION	VAR	VAR		6,561	VAR	3,232	VAR	3,200	VAR	CONT.	CONT	CONT.
Subtotal T&E				6,561		3,232		3,200		CONT.	CONT.	CONT.
Remarks												
PROGRAM MGMT SUPPORT	VAR	VARIOUS	3,936	566		383		201				
Subtotal Management			3,936	566		383		201		Cont.	Cont.	Cont.
Remarks												
Total Cost			100,682	30,277		24,190		15,453		Cont.	Cont.	Cont.

EXHIBIT R-3, FY 2003 RDT&E,N COST ANALYSIS

DATE: FEBRUARY 2002

BUDGET ACTIVITY: 7 PROGRAM ELEMENT: 0303140N PROJECT NAME: ISSP
PROGRAM ELEMENT TITLE: Information Systems Security Program (ISSP) PROJECT NUMBER: R0734

(U) COST: (Dollars in Thousands)

PROJECT NUMBER & TITLE	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	FY2006	FY2007	TO COMPLETE	TOTAL PROGRAM
R0734* Information Assurance	0	0	2,983	3,059	3,128	3,202	3,277	CONT.	CONT.
Total	0	0	2,983	3,059	3,128	3,202	3,277	CONT.	CONT.

* Project Unit starting in FY03 for Office of Naval Research (ONR)

A. (U) MISSION DESCRIPTION AND BUDGET ITEM JUSTIFICATION: This PE includes funds for advanced technology development, test and evaluation of naval information systems security based on leading edge technologies that will improve information assurance (IA) situational awareness and information infrastructure protection across all Command echelons from the Commander in Chief (CINC) to tactical units afloat and warfighters ashore. This effort will demonstrate a secure capability for building, maintaining, and administering a seamlessly 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 thereby provide Naval Forces a secure capability and basis in its achievement of reliable self-synchronization, protection from unauthorized access and mis-use, and optimized IA resource allocations in the information battlespace. The Naval Information Systems Security Program (ISSP) is supportive of the Future Naval Capabilities (FNCs) including the Knowledge Superiority and Assurance (KSA) FNC. Advanced technologies to be developed, tested, evaluated, integrated, and demonstrated include multi-level security-aware applications and technologies, and automated tools for expediting the IA certification process of software, embedded software, and architectures.

(U) 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.

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

EXHIBIT R-3, FY 2003 RDT&E,N COST ANALYSIS

DATE: FEBRUARY 2002

BUDGET ACTIVITY: 7 PROGRAM ELEMENT: 0303140N PROJECT NAME: ISSP
PROGRAM ELEMENT TITLE: Information Systems Security Program (ISSP) PROJECT NUMBER: R0734

(U) FY 2001 ACCOMPLISHMENT: N/A

(U) FY 2002 PLANS: N/A

(U) FY 2003 PLAN:

(U) 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.

(U) ($2,983) Continue to develop an Information Assurance (IA) common operating picture framework to enable integration of network security systems and providing IA situational awareness. Continue to develop distributed software prototypes for information assurance (IA) capable of remotely managing and securely controlling the configurations of network security components in real time or near real time. This includes firewall based technology, virtual private networking systems, operating systems, and others as well as high assurance components for connection of Top Secret to lower level systems. Continue to prototype IA coalition interoperability and multi-level security systems components, and to evaluate new technology for applicability towards other multiple security levels (MSL) and interoperability problems for distributed databases, web browsers, routers/switches, etc. Continue to develop, test, and assess concepts for certifying legacy and COTS technologies for Information Assurance (IA) according 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).

B. (U) CHANGE SUMMARY EXPLANATION:
(U) FY 2003: N/A

C. (U) OTHER PROGRAM FUNDING SUMMARY: The Navy’s 6.1 program contributes to this effort.
(U) NAVY RELATED RDT&E:
(U) PE 0601153N (Defense Research Science)
(U) PE 0602235N (Common Picture Applied Research)
(U) PE 0602114N (Power Projection Applied Research)
(U) PE 0603235N (Common Picture Advanced Technology)
(U) NON-NAVY RELATED RDT&E:

D. ACQUISITION STRATEGY

EXHIBIT R-3, FY 2003 RDT&E,N COST ANALYSIS

DATE: FEBRUARY 2002

BUDGET ACTIVITY: 7 PROGRAM ELEMENT: 0303140N PROJECT NAME: ISSP
PROGRAM ELEMENT TITLE: Information Systems Security Program (ISSP) PROJECT NUMBER: R0734

E. SCHEDULE PROFILE: Not Applicable.

Exhibit R-3 Cost Analysis (page 1)												
APPROPRIATION/BUDGET ACTIVITY: 7		PROGRAM ELEMENT: 0303140N							Date: FEBRUARY 2002			
									PROJECT NAME AND NUMBER: ISSP R0734			
Cost Categories	Contract Method & Type	Performing Activity & Location	Total PYs Cost	FY01 Cost	FY01 Award Date	FY02 Cost	FY02 Award Date	FY03 Cost	FY03 Award Date	Cost To Complete	Total Cost	Target Value of Contract
SOFTWARE DEVELOPMENT	WX	NRL-DC						2,983	10/02	CONT.	CONT.	CONT.
HARDWARE DEVELOPMENT	N/A	N/A										
Subtotal Product Development								2,983		CONT.	CONT.	CONT.
Remarks:												
SYSTEMS ENGINEERING												
Subtotal Support												
Remarks												

EXHIBIT R-3, FY 2003 RDT&E,N COST ANALYSIS

DATE: FEBRUARY 2002

BUDGET ACTIVITY: 7 PROGRAM ELEMENT: 0303140N PROJECT NAME: ISSP
PROGRAM ELEMENT TITLE: Information Systems Security Program (ISSP) PROJECT NUMBER: R0734

Exhibit R-3 Cost Analysis (page 2)													Date: February 2002
APPROPRIATION/BUDGET ACTIVITY: 7			PROGRAM ELEMENT: 0303140N										PROJECT NAME AND NUMBER:ISSP R0734
Cost Categories	Contract Method & Type	Performing Activity & Location	Total PYs Cost	FY01 Cost	FY01 Award Date	FY02 Cost	FY02 Award Date	FY03 Cost	FY03 Award Date	Cost To Complete	Total Cost	Target Value of Contract	
TEST AND EVALUATION													
Subtotal T&E													
Remarks													
PROGRAM MGMT SUPPORT													
Subtotal Management													
Remarks													
Total Cost								2,983		CONT.	CONT.	CONT.	

EXHIBIT R-2a, FY 2003 RDT&E,N PROJECT JUSTIFICATION

DATE: February 2002

BUDGET ACTIVITY: 7 PROGRAM ELEMENT: 0303140N PROJECT NAME: ISSP

PROGRAM ELEMENT TITLE: Information Systems Security Program (ISSP) PROJECT NUMBER: 2987

(U) COST: (Dollars in Thousands)

PROJECT NUMBER & TITLE	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	FY2006	FY2007	TO COMPLETE	TOTAL PROGRAM
X2987 Intelligent Agent Security Module		2,478						CONT.	CONT.
Total		2,478						CONT.	CONT.

A. (U) MISSION DESCRIPTION AND BUDGET ITEM JUSTIFICATION: This PE includes funds for advanced technology development, test and evaluation of naval information systems security based on leading edge technologies that will improve information assurance (IA) situational awareness and information infrastructure protection across all Command echelons from the Commander in Chief (CINC) to tactical units afloat and warfighters ashore. This effort will demonstrate a secure capability for building, maintaining, and administering a seamlessly 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 thereby provide Naval Forces a secure capability and basis in its achievement of reliable self-synchronization, protection from unauthorized access and mis-use, and optimized IA resource allocations in the information battlespace. The Naval Information Systems Security Program (ISSP) is supportive of the Future Naval Capabilities (FNCs) including the Knowledge Superiority and Assurance (KSA) FNC. Advanced technologies to be developed, tested, evaluated, integrated, and demonstrated include multi-level security-aware applications and technologies, and automated tools for expediting the IA certification process of software, embedded software, and architectures.

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

EXHIBIT R-2a, FY 2003 RDT&E,N PROJECT JUSTIFICATION

DATE: February 2002

BUDGET ACTIVITY: 7 PROGRAM ELEMENT: 0303140N PROJECT NAME: ISSP
PROGRAM ELEMENT TITLE: Information Systems Security Program (ISSP) PROJECT NUMBER: 2987

(U) FY 2001 ACCOMPLISHMENT: N/A

(U) FY 2002 PLAN:

(U) ($2,478) Congressional plus-up for Navy's Intelligent Agent Security Module (IASM). Continue 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 IDSs.

(U) FY 2003 PLAN: N/A

B. (U) CHANGE SUMMARY EXPLANATION:

(U) FY 2002: +$2,500K Congressional Plus-up for Navy Intelligent Agent Security Module (NIASM), -$22K Non-Pay Inflation.

C. (U) OTHER PROGRAM FUNDING SUMMARY: (Dollars in thousands)

FY 2001 ESTIMATE	FY 2002 ESTIMATE	FY 2003 ESTIMATE	FY 2004 ESTIMATE	FY 2005 ESTIMATE	FY 2006 ESTIMATE	FY 2007 ESTIMATE	TO COMPLETE	TOTAL PROGRAM
COMPLETE PROGRAM:								
(U) OPN 3415 Information Systems Security Program (ISSP)								
64,216	86,822	78,473	61,800	34,637	50,992	49,466	CONT.	CONT.
(U) O&MN 4A6M								
17,534	19,983	20,344	19,287	14,895	13,940	14,302	CONT.	CONT.

(U) RELATED RDT&E:
(U) PE 0303140G
(Cryptographic Equipments)

D. ACQUISITION STRATEGY: N/A
E. SCHEDULE PROFILE: N/A

EXHIBIT R-2a, FY 2003 RDT&E,N PROJECT JUSTIFICATION

DATE: February 2002

BUDGET ACTIVITY: 7 PROGRAM ELEMENT: 0303140N PROJECT NAME: ISSP

PROGRAM ELEMENT TITLE: Information Systems Security Program (ISSP) PROJECT NUMBER: 2987

Exhibit R-3 Cost Analysis (page 1)												Date: FEBRUARY 2002
APPROPRIATION/BUDGET ACTIVITY: 7			PROGRAM ELEMENT: 0303140N									PROJECT NAME AND NUMBER: ISSP (X2987)
Cost Categories	Contract Method & Type	Performing Activity & Location	Total PYs Cost	FY01 Cost	FY01 Award Date	FY02 Cost	FY02 Award Date	FY03 Cost	FY03 Award Date	Cost To Complete	Total Cost	Target Value of Contract
SOFTWARE DEVELOPMENT												
SOFTWARE DEVELOPMENT												
HARDWARE DEVELOPMENT												
HARDWARE DEVELOPMENT												
HARDWARE DEVELOPMENT												
HARDWARE DEVELOPMENT												
Subtotal Product Development												
Remarks:												
SYSTEMS ENGINEERING	CPAF	PROMIA				2,368	02/02			CONT.	CONT.	CONT.
Subtotal Support						2,368				CONT.	CONT.	CONT.
Remarks												

EXHIBIT R-2a, FY 2003 RDT&E,N PROJECT JUSTIFICATION

DATE: February 2002

BUDGET ACTIVITY: 7 PROGRAM ELEMENT: 0303140N PROJECT NAME: ISSP

PROGRAM ELEMENT TITLE: Information Systems Security Program (ISSP) PROJECT NUMBER: 2987

Exhibit R-3 Cost Analysis (page 2)													Date: February 2002
APPROPRIATION/BUDGET ACTIVITY: 7			PROGRAM ELEMENT: 0303140N										PROJECT NAME AND NUMBER: ISSP (X2987)
Cost Categories	Contract Method & Type	Performing Activity & Location	Total PYs Cost	FY01 Cost	FY01 Award Date	FY02 Cost	FY02 Award Date	FY03 Cost	FY03 Award Date	Cost To Complete	Total Cost	Target Value of Contract
TEST AND EVALUATION												
Subtotal T&E												
Remarks												
PROGRAM MGMT SUPPORT	WX	SSC-CH				110	02/02					
Subtotal Management						110				CONT.	CONT.	CONT.
Remarks												
Total Cost						2,478				CONT.	CONT.	CONT.