EXHIBIT R-2, FY 2002 RDT&E,N BUDGET ITEM JUSTIFICATION

DATE: JUNE 2001

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

(U) COST: (Dollars in Thousands)

PROJECT NUMBER & TITLE	FY 2000	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	FY2006	FY2007	TO COMPLETE
X0734 Information Systems Security	20,105	31,835	20,942						
TOTAL	20,105	31,835	20,942						

(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.

EXHIBIT R-2, FY 2002 RDT&E,N BUDGET ITEM JUSTIFICATION

DATE: JUNE 2001

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

(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.

EXHIBIT R-2, FY 2002 RDT&E,N BUDGET ITEM JUSTIFICATION

DATE: JUNE 2001

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

(U) COST: (Dollars in Thousands)

PROJECT NUMBER & TITLE	FY 2000	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	FY2006	FY2007	TO COMPLETE	TOTAL PROGRAM
X0734 Information Systems Security	20,105	31,835	20,942							

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.

(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 continuing 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 subchapter 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 that legacy Communications Security (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 Communications Security (COMSEC) and Transmission Security (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) a public key infrastructure (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 a public key

infrastructure (PKI) and directories. To ensure interoperability and commercial standards compliance, these efforts often encompass the research, selective evaluation, integration, and test of Commercial off-the-shelf (COTS)/Non-developmental Item (NDI) IA security products. For example, evaluation may include defensible network boundary capabilities such as firewalls, secure routers and switches, guards, virtual private networks (VPN), and network intrusion and misuse (IDS) detection systems.

(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 describe several major ISSP technology areas.

(U) Under the Navy Secure Voice (NSV) program, ISSP RDT&E develops and assesses technology to provide high grade, secure tactical and strategic voice connectivity. Efforts include designing, demonstrating and integrating a secure voice capability for shipboard networks (IT-21) and other Command, Control, Communications, Computers, and Intelligence (C4I) programs and initiatives. Secure voice capabilities must include switched, wired, routed, and wireless. ISSP RDT&E technologies support will prototype and demonstrate the secure integration and transport of voice, video, and data over Internet Protocol (IP) and Asynchronous Transfer Mode (ATM) networks. Specifically, the secure voice program will examine digital cellular and land mobile satellite secure voice technology.

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

EXHIBIT R-2, FY 2002 RDT&E,N BUDGET ITEM JUSTIFICATION

DATE: JUNE 2001

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

(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 2000 Accomplishments:

(U) ($2,000) Initiated efforts to develop a flexible, digital modular cryptographic solution based on multi-channel, programmable technology to replace a wide variety of aging and obsolete cryptos in existing and new navy communications systems/circuits (e.g., cryptographic equipments including the ANDVT, VINSON, KG-84, KG-40 in support of Link-11, and the Thornton family in support of Link-16). This capability will yield significant benefits including simplified operation, improved interoperability, and reduced space and weight requirements. Identified and documented performance parameters, form factors, and interface requirements for the digital modular cryptographic solution. These efforts were fully coordinated with the National Security Agency. Continued development of programmable embedded COMSEC solutions for the KG-3X family of cryptos to satisfy requirements associated with Submarine Low Frequency / Very Low Frequency VMEBUS Receiver (SLVR) for cryptographic equipment (KG-3X) replacement. Began the development and implementation of benign keying technology for crypto replacement efforts.

(U) ($4,025) Continued development of Electronic Key Management System (EKMS), and ensured compatibility with the Tier 0, Tier 2, and Tier 3 components and software.

(U) ($2,675) Continued the development of Electronic Key Management System (EKMS) Phase IV for Tier 1, Tier 2 and Tier 3. This included support for incorporation of enhanced key management capabilities/solutions for shipboard networks (IT-21) and the Navy Marine Corps Intranet (NMCI). Addressed the development and inclusion of web-based technology and support for the incorporation of the Key Systems Operations (KSO) exchange. Began the requirements definition for integration of certificate management and key management. Additional efforts focus on the development and prototyping of the Navy Single Point Command, Control, and Keying ($NSPC^2K$) design and solution for Navy platforms, supporting the development and prototyping of the Data Transfer Device (DTD) 2000, and key management support for embedded cryptographic technology and the Navy’s crypto replacement efforts. Conducted laboratory assessments of the latest National Security Agency (NSA) and industry commercial-off-the-shelf (COTS) key management technology and products, and demonstrations of prototype key management systems. Provided system security and Certification and Accreditation (C&A) engineering and testing for key management components and systems.

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

(U) ($750) Continued the design, development, evaluation and application of public key and certificate management infrastructure technologies and systems to support DoD and DON initiatives, including integration with IT-21 and N/MCI initiatives. Prototype and assessed the use and application of medium and high assurance commercial products for public key and certificate management infrastructures (PKI/CMI) applications, including the assessment of these technologies over tactical communications paths. Continued assessing the feasibility of integrating PKI/CMI technology with key management products and initiatives. Work closely with the commercial developers and vendors, infuse technology and requirements into the commercial products, and support efforts to PKI-enable applications. Evaluated, assessed, and integrated multiple related technologies including security tokens, such as SmartCards, and virtual private networks (VPNs). Supported the definition of standards for smart cards and the evolution of computer workstation technology to support the widespread introduction of smart card technology.

(U) ($708) Continued the design, development and assessment of security solutions/capabilities for next generation voice systems. Developed prototypes/demonstrations to illustrate secure voice, video, and data capabilities over Internet Protocol (IP) and Asynchronous Transfer Mode (ATM) networks, specifically addressing quality of service and reliability issues. Continued research into new secure voice technology, developing technology and techniques for secure voice over government and commercial communications backbones, specifically addressing wireline/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. Investigated the application of digital cellular and satellite secure voice technology.

(U) ($500) Initiated the analysis, design and assessment of the Secure Voice-21 (SV-21). This included the design and interfaces of the crypto gateways (i.e., network interface card, crypto interface card, and the voice processing card), crypto replacement technology, the SPC^{2}K technology to support the embedded crypto replacements, and new voice algorithms (e.g., Mixed Excitation Linear Prediction (MELP)). This suite of equipment/solutions is targeted to support the LPD-17 class ships, the DDG-51 class ships, NSSN (submarine), and CVX (carrier) class of ships by providing a secure voice solution for telephonic, tactical and secure voice problems, specifically addressing the IT-21 initiatives.

(U) ($250) Continued to support secure voice and biometric access consortia. Continued laboratory assessments of the latest NSA and industry INFOSEC technology and demonstrations of prototype voice systems. Continued research into new high assurance secure voice technology.

(U) ($650) Continued the evolutionary development of security architectures for IA that include virtually all Navy distributed information system development programs. Ensured the architecture evolves 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), Maritime Cryptologic Architecture, the Joint Technical 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. Included both defensive protections as well as intrusion monitoring in the architecture.

(U) ($3,187) Continued developing and testing distributed information system security solutions for Navy information systems. This included the examination and selection of various components required by the architectures that may include firewalls, intrusion detection 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. Examined and evaluated next generation network security components including scaleable security products, Asynchronous Transfer Mode (ATM) firewalls and intrusion detection systems, and sophisticated malicious code monitors. Designed and prototype standard security suites for delivery to Naval commands, bases, and afloat platforms. Supported 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. Prototype components and standard security suites at selected operational sites.

(U) ($2,010) Provided systems security engineering, C&A support to Navy information system developments such as 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), shipboard networks (IT-21), the Navy Marine Corps Intranet (NMCI), and new ship classes (e.g., LPD-17, DD-21, CVNX, NSSN,…), and others to ensure that security is integrated as early in the development process as possible. Worked with application and system developers across Navy system commands to implement security policies, architectures, and components during early stages of design. 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 sensitive compartmented information (SCI) are consistent with Navy and DOD requirements.

(U) ($825) Continued developing and updating INFOSEC standards and engineering guidance documents to ensure they are consistent with the security architecture, the rapidly changing technology, and the evolving threat. Focused on the development of security procedures associated with standard network security suites and tools.

(U) ($1,265) Developed, prototyped, and tested solutions to the coalition interoperability problem. Based the solutions on available multilevel security technologies as well as emerging architectural methods of providing interoperability across different security levels.

(U) ($1,260) Continued vulnerability/threat assessments and development and systems integration of network countermeasures tools (NVACM) efforts.

3. (U) FY 2001 PLAN:

(U) ($2,000) Continue development of the digital modular cryptographic solution based on multi-channel, programmable technology. Begin prototyping candidate cryptographic replacement solutions for evaluation and assessment in representative Navy platforms. Demonstrate digital modular crypto solution at selected operational locations and platforms to illustrate benefits and capabilities. Support the COMSEC certification process, including the conduct of analyses required and the development of associated documentation. These efforts will be fully coordinated with the National Security Agency.

(U) ($2,533) Continue 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 KSO 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 Data Transfer Device (DTD) 2000, and continue to provide key management support for embedded cryptographic technology and cryptographic replacement efforts. Conduct laboratory assessments of the latest National Security Agency and commercial-off-the-shelf key management technology and products. Provide system security, certification, and accreditation engineering and testing for key management components and systems.

(U) ($2,811) Continue the design, development, evaluation and application of public key and certificate management infrastructure 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. Continue to assess the use and application of medium and high assurance commercial products for public key infrastructure and certificate management infrastructure (PKI/CMI) applications, including integrating key management and certificate management infrastructures. 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). Assess the potential application of biometric access control tokens (fingerprint, voiceprint, iris) and the evaluation/development of electronic commerce applications to more efficiently perform Navy business functions using PKI technologies.

(U) ($8,600) This is a Congressional plus-up. Accelerate the design, development, evaluation and fielding of a public key and certificate management system and the supporting infrastructure. Develop PKI applications and concepts as they relate to afloat platforms to include evaluation of Medium Grade Services (MGS), Directory Services Testing (Single Sign On) and Hardware Cryptographic Modules (HCM). Conduct afloat demonstration of PKI on SIPRNET which will encompass use of Class 3 certificates, Local Registration Authority (LRA) support and will formalize the process for introduction of PKI into IT-21 Afloat (Government Off-The-Shelf (GOTS) Delta) deployment plan. Evaluate 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) ($2,000) Continue the design, development and assessment of security solutions/capabilities for next generation

voice systems. Continue to examine ways to integrate secure voice, video, and data capabilities over Internet Protocol (IP) and Asynchronous Transfer Mode (ATM) networks. Demonstrate secure voice server Internet Protocol (IP) conversion capabilities to interoperate with legacy equipment. Continue research into new secure voice technology, developing technology and techniques for secure voice over government and commercial communications backbones, specifically addressing wireline/wireless telephony and network applications applicable to strategic and tactical communications. Continue to develop and assess the technology for low data rate algorithms, voice compression technology in conjunction with cryptographic algorithm technology, and voice/speaker recognition. Continue to assess the application of digital cellular and satellite secure voice technology.

(U) ($1,000) Continue development of Secure Voice-21 (SV-21). This includes the development and integration of the crypto gateways (i.e., network interface card, crypto interface card, and the voice processing card), crypto replacement technology, the Navy Single Point Command, Control, and Keying ($NSPC^2K$) technology to support the embedded crypto replacements, and new voice algorithms (e.g., Mixed Excitation Linear Prediction (MELP). Demonstrate the SV-21 suite capability on a new ship operational platform for test and evaluation purposes.

(U) ($250) Continue to support secure voice and biometric access consortia. Continue laboratory assessments of the latest NSA and industry INFOSEC technology and demonstrations of prototype voice systems. Continue research into new high assurance secure voice technology.

(U) ($750) 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), 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. Include both defensive protections as well as intrusion monitoring in the architecture.

(U) ($4,430) Continue developing and testing distributed information system security solutions for Navy information systems. This includes 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. 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) ($2,000) This is a Congressional plus-up. Develop and evaluate 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. Define interfaces to existing Commercial Off-The-Shelf (COTS) products, collect and correlate data from these units and develop algorithms which will provide accurate, useful information to the System Administrator/Security Manager or Watch Officer. Design and develop a network defense visualization capability which displays data collected by the network IDS system and defines the level and severity of the attack, as well as options and responses.

(U) ($2,500) Provide systems security engineering, certification and accreditation (C&A) support to Navy information system developments such as shipboard networks (IT-21), Navy Marine Corps Intranet (NMCI), the Joint Technical Architecture (JTA), 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 new ship construction (e.g., NSSN, LPD-17, SCN-21,…) and others to ensure that security is integrated as early in the development process as possible. Work with application and system developers across Navy system commands to implement security policies, architectures, and components during early stages of design. 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) ($461) Continue developing and updating INFOSEC standards and engineering guidance documents to ensure they are

consistent with the security architecture, the rapidly changing technology, and the evolving threat. Focus on the development of security procedures associated with next generation network security suites and tools to facilitate rapid transition of these components and tools to the Fleet.

(U) ($1,500) 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) ($1,000) Continue vulnerability/threat assessments and development and systems integration of network countermeasures tools (NVACM) efforts.

3. (U) FY 2002 PLAN:

(U) ($600) 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) ($1,000) 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) ($640) 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) ($615) 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) ($300) 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) ($2,000) 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) ($1,615) 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. 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) ($1,200) 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) ($130) 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) ($1,178) 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) ($1,800) 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) ($1,000) 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) ($500) Continue vulnerability/threat assessments and development and systems integration of network countermeasures tools (NVACM) efforts.

(U) ($600) 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) ($450) 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) ($460) 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) ($500) 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) ($1,318) 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) ($400) 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) ($2,000) Complete the development of Electronic Key Management System (EKMS) Phase IV for Tier 1, Tier 2, Tier 3 and ensure compatibility with Tier 0. Continue to research and investigate new key management technologies. Demonstrate web-based technology and exchange capabilities. Demonstrate integration of certificate management and key management directory structures and workstation functions. Demonstrate prototype of the Navy Single Point Command, Control, and Keying ($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) ($786) 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) ($1,000) 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) ($250) 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) ($300) 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) ($300) Prepare protection profile and define key management architecture for secure wireless Ethernet local area network (LAN).

B. (U) CHANGE SUMMARY EXPLANATION:

(U) Funding:
(U) FY 2000: -$312K SBIR reduction; -$514K WINSAT; -$1,050K MUOS; -$100K NSS; -$448K ASN/RDA reduction; -$230K Miscellaneous Navy Adjustments; -$5K Federal Technology Transfer (FTT); -$90K Section 8055 Congressional Proportionate Rescission.

(U) FY 2001: +$8,600K Congressional Plus-Up for PKI (Public Key Infrastructure); +$2,000K Congressional Plus-Up for NIASM (Naval Intelligent Agent Secure Module); -$225K Section 8086 .7% Pro-Rata Reduction; -$70K Government-Wide Rescission: PL106-554, Section 14

(U) FY 2002: N/A

(U) Schedule: Navy's 1st Qtr IOC/GAT schedule was impacted due to the establishment of a master integrated EKMS schedule coordinated among NSA and Service representatives which synchronizes the individual EKMS efforts managed by the Navy and NSA. This master integrated schedule was briefed and approved by the Military Communications Electronics Board (MCEB) in October 1999 and again in June 2000. This replan adopted a system-oriented development approach and established a Final Operational Capability (FOC) date of August 2002. A medium degree of risk was associated with this date.

(U) Technical: N/A

EXHIBIT R-2, FY 2002 RDT&E,N BUDGET ITEM JUSTIFICATION

DATE: JUNE 2001

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

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

	FY 2000 ESTIMATE	FY 2001 ESTIMATE	FY 2002 ESTIMATE
COMPLETE PROGRAM:			
(U) OPN 3415 Information Systems Security Program (ISSP)	61,573	58,026	78,170
(U) O&MN 4A6M	11,874	27,419	18,304

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

EXHIBIT R-2, FY 2002 RDT&E,N BUDGET ITEM JUSTIFICATION

DATE: JUNE 2001

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

D. ACQUISITION STRATEGY

	FY 1999	FY 2000	FY 2001	FY 2002	To Complete
EKMS					
Program Milestones				1Q-Tier 1 IOC 4Q-Tier 1 FOC	
Engineering Milestones	1Q-Build Rev 3				
T&E Milestones	3Q-Tier 1 Test			1Q-Tier 1 Government Acceptance Test (GAT)	
Contract Milestones					

EXHIBIT R-3, FY 2002 RDT&E,N PROJECT COST ANALYSIS

DATE: JUNE 2001

BUDGET ACTIVITY: 7 PROGRAM ELEMENT: 0303140N PROJECT NUMBER: X0734

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

Exhibit R-3 Cost Analysis (page 1)												Date: MAY 2001
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	Cost	Award Date	Cost To Complete	Total Cost	Target Value of Contract
HARDWARE DEVELOPMENT	CPFF/	VIASAT	7,282	0		0				0	7,282	7,282
SOFTWARE DEVELOPMENT	CPAF	SAIC	29,597	233	03/01	0				0	29,830	42,590
HARDWARE DEVELOPMENT	VAR	MITRE	1,911	800	12/00	935	12/01			Cont.	Cont.	Cont.
HARDWARE DEVELOPMENT	VAR	VARIOUS	54,980	16,488	VAR	10,990	VAR			Cont.	Cont.	Cont.
Subtotal Product Development			93,770	17,521		11,925				Cont.	Cont.	Cont.
Remarks: SAIC target value of contract includes other services' funding (ARMY RDT&E).												
SYSTEMS ENGINEERING	VAR	VAR	2,976	11,446	VAR	6,148	VAR			CONT.	CONT.	CONT.

EXHIBIT R-3, FY 2002 RDT&E,N PROJECT COST ANALYSIS

DATE: JUNE 2001

BUDGET ACTIVITY: 7 PROGRAM ELEMENT: 0303140N PROJECT NUMBER: X0734

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

Subtotal Support			2,976	11,446		6,148				CONT.	CONT.	CONT.
Remarks												

EXHIBIT R-3, FY 2002 RDT&E,N PROJECT COST ANALYSIS

DATE: JUNE 2001

BUDGET ACTIVITY: 7 PROGRAM ELEMENT: 0303140N PROJECT NUMBER: X0734

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

Exhibit R-3 Cost Analysis (page 2)											Date: MAY 2001	
APPROPRIATION/BUDGET ACTIVITY: 7		PROGRAM ELEMENT: 0303140N									PROJECT NAME AND NUMBER: X0734	
Cost Categories	Contract Method & Type	Performing Activity & Location	Total Pys Cost	FY01Cost	FY01 Award Date	FY02 Cost	FY02 Award Date	Cost	Award Date	Cost To Complete	Total Cost	Target Value of Contract
TEST AND EVALUATION	VAR	VAR		2,868	VAR	2,869	VAR			CONT.	CONT	CONT.
Subtotal T&E				2,868		2,869				CONT.	CONT.	CONT.
Remarks												
PROGRAM MGMT SUPPORT	VAR	VARIOUS	3,936	0		0						
Subtotal Management			3,936	0		0				Cont.	Cont.	Cont.
Remarks												

EXHIBIT R-3, FY 2002 RDT&E,N PROJECT COST ANALYSIS

DATE: JUNE 2001

BUDGET ACTIVITY: 7 PROGRAM ELEMENT: 0303140N PROJECT NUMBER: X0734

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

Total Cost			100,682	31,835		20,942				Cont.	Cont.	Cont.