

## UNCLASSIFIED

## EXHIBIT R-2, FY 2001 RDT&amp;E,N BUDGET ITEM JUSTIFICATION

DATE: FEB 2000

BUDGET ACTIVITY: 7

PROGRAM ELEMENT: 0303140N

PROGRAM ELEMENT TITLE: Information Systems Security Program

(U) COST: (Dollars in Thousands)

PROJECT NUMBER & TITLE	FY 1999	FY 2000	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	TO COMPLETE	TOTAL PROGRAM
X0734 Information Systems Security	20,218	22,854	21,530	22,560	22,908	27,012	27,165	CONT.	CONT.
TOTAL	20,218	22,854	21,530	22,560	22,908	27,012	27,165	CONT.	CONT.

(U) MISSION DESCRIPTION AND BUDGET ITEM JUSTIFICATION: The goal of the Navy Information Systems Security (INFOSEC) Program (ISSP) is to ensure the continued protection of Navy and Joint information and information systems from hostile exploitation and attack. With the advent of the information age, the network environment, and the evolving reliance on distributed information systems that communicate via computer networks, protecting these networks, the data flowing on the networks, and the attached information systems has become critical to the effective performance of the Navy mission. The fundamental nature of these distributed systems in modern Naval and Joint war fighting means that attacks against the systems are increasingly likely. 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, attacks involving malicious changes to critical information, changes to the functioning of critical systems, or the destruction of systems and networks have become much more feasible. Since many Navy information systems are based on commercially available technologies, an adversary often has access to the very technologies that are targeted for exploitation.

(U) The complexity of Navy distributed systems, and the rapid rate of change of the underlying commercial and government technologies; makes the provision of security an increasingly complex and ever changing problem. Technologies involved with providing security are a mix of computer security, network security, and cryptographic security which must be carefully developed and integrated into many parts of the Navy information infrastructure. The placement of technologies and the mix of technologies required must evolve quickly to meet the rapidly evolving threats and vulnerabilities. This is a departure from years past when protections were mostly associated with the eavesdropping threat and were primarily provided by cryptographic devices. In order to gain the requisite levels of protection, the various security technologies must be applied in a carefully architected manner. Information Assurance (IA) is the comprehensive management of both the information and the information system security disciplines. At the same time the IA problem is becoming more complex, demands to move information between security levels and to and from coalition partners are increasing.

R-1 Shopping List - Item No. 183 - 1 of 183 - 16

UNCLASSIFIED

Exhibit R-2, RDT&amp;E,N Budget Item Justification

UNCLASSIFIED

EXHIBIT R-2, FY 2001 RDT&E,N BUDGET ITEM JUSTIFICATION

DATE: FEB 2000

BUDGET ACTIVITY: 7

PROGRAM ELEMENT: 0303140N

PROGRAM ELEMENT TITLE: Information Systems Security Program

(U) The Navy ISSP RDT&E program is structured to stay abreast of the exploding information system security problem and ensure that Navy systems possess the requisite level of protection. To model the way DOD information systems are evolving (rather than being one-time developments), the ISSP RDT&E program is structured to continuously evaluate technical directions/options. The program develops frameworks and architectures based on mission threats, exploitation risks, integrated Joint information system efforts, etc. The program provides the resources to determine the proper security functions and placement of the functions; uses the frameworks and architectures to coordinate Navy work with DoD and National Security Agency (NSA) IA efforts. The program also examines commercial technologies to determine their fit within the architectures; provides feedback to vendors and standards bodies about what Navy requires in commercial products. It develops or tailors technologies, standards, and processes to Navy requirements if necessary; prototypes systems or portions of systems and examines their operational utility in operational Navy settings, and provides IA expertise and engineering to Navy and Joint information system developments. All technology development efforts are aimed at specific Navy and Joint IA problems and are designed to 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.

UNCLASSIFIED

EXHIBIT R-2, FY 2001 RDT&E,N BUDGET ITEM JUSTIFICATION

DATE: FEB 2000

BUDGET ACTIVITY: 7

PROGRAM ELEMENT: 0303140N

PROGRAM ELEMENT TITLE: Information Systems Security Program

(U) COST: (Dollars in Thousands)

PROJECT NUMBER & TITLE	FY 1999	FY 2000	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	TO COMPLETE	TOTAL PROGRAM
X0734 Information Systems Security	20,218	22,854	21,530	22,560	22,908	27,012	27,165	CONT.	CONT.

A. (U) MISSION DESCRIPTION AND BUDGET ITEM JUSTIFICATION: The Navy RDT&E program analyzes existing information assurance products and solutions, and develops improved, interoperable communications security equipment and methods, computer security technology and other high assurance techniques/solutions to protect voice, video and data communications from exploitation and provide IA for critical Navy information systems. This program element is a continuing effort to modernize obsolete computer security and cryptographic equipment and ancillaries with state-of-the-art replacements in order to counter evolving and increasingly sophisticated threats. Communication Security (COMSEC) replacements, in most cases, will use embedded modules incorporating (NSA approved crypto engines) and programmable cryptographic technology. The technical strategy and framework efforts are focused on the use of IA technology (e.g., COMSEC, COMPUSEC and NETSEC technology) to counter a wide variety of INFOSEC threats in a Navy environment. Processes and tools are being evaluated, developed and/or tested to design and evaluate the security of systems that integrate IA products. Technology base efforts include: developing new secure voice prototypes; developing or applying technology for a new family of programmable COMSEC modules; developing or applying network security products, (including technology to interconnect networks of dissimilar classification, and address the Multi-level Security (MLS) technology requirements for the DON); and developing or applying public key infrastructure and associated access control technologies (such as Smart Cards and similar security tokens). The resulting expertise is applied to a wide variety of Navy development programs that must integrate IA technology.

(U) The expertise in the DON RDT&E program is applied to the development of Navy INFOSEC products and systems, computer and other high assurance technology, development of missing technology (e.g., network security technology and certification methods), and the development of standards, processes and tools, etc). These efforts encompass the selective evaluation, integration and test of Commercial off-the-shelf (COTS)/Non-developmental Item (NDI) IA security products into prototype capabilities such as firewalls, guards, virtual private networks, and network monitoring systems to provide for monitoring, detecting,

UNCLASSIFIED

EXHIBIT R-2, FY 2001 RDT&E,N BUDGET ITEM JUSTIFICATION

DATE: FEB 2000

BUDGET ACTIVITY: 7

PROGRAM ELEMENT: 0303140N

PROGRAM ELEMENT TITLE: Information Systems Security Program

isolating and reacting to network intrusions throughout the DON. With the Navy now making profound changes in the way it approaches communications and computer security, the current operating environment has virtually eliminated the traditional distinction between telecommunications and information systems. The Navy RDT&E program analyzes existing INFOSEC and high assurance equipment and solutions, and develops improved, interoperable communications security equipment and methods to protect information from exploitation and provide IA for critical Navy systems. The project provides a continuing effort to modernize obsolete cryptographic and network security equipment and ancillaries with state-of-the-art replacements in order to meet the evolving threat on Navy communication networks. Because INFOSEC is a cradle-to-grave discipline, this program develops the technology and methodology to systems in development, production and operation, and develops the infra-structure needed to support and evaluate the security of deployed systems. These objectives are pursued by using equipment/systems focusing on information assurance technology and their use and impact on distributed information systems.

(U) Under the Navy Secure Voice program, technology to provide high grade, secure tactical and strategic voice connectivity shall be developed and assessed. Efforts shall focus on designing, demonstrating and integrating a secure voice capability for IT-21 and other Command, Control, Communications and Computers (C4I) programs and initiatives. Technology to support the secure integration and transport of voice, video, and data over Internet Protocol (IP) and Asynchronous Transfer Mode (ATM) networks will be prototyped and demonstrated to support Navy Marine Corps Internet (NMCI) and IT-21 applications. Additionally, the secure voice program will examine digital cellular and land mobile satellite secure voice technology. Under the Navy Security Management Infrastructure (SMI) program, new emerging technology and enhanced capabilities shall be developed, evaluated and applied to the Electronic Key Management System (EKMS) and other Navy Information Systems. Additional efforts shall focus on the architecture, design, and development of systems to manage the security parameters (for example, encryption 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. Under the Secure Data program, efforts focus on architectures, designing, acquiring, demonstrating and integrating the IA technologies into Navy distributed information systems (e.g., IT-21, NMCI). It involves the injection of security technologies and solutions in Navy C<sup>4</sup>I systems to maintain pace with the evolving infrastructure of the internet and expanding network capabilities of ashore and afloat users. Secure data RDT&E,N focuses primarily on designing and proving IA solutions for IT-21 and the NMCI (and the broad and complex underlying and interconnected metropolitan, base, and local area networks). 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

R-1 Shopping List - Item No. 183 - 4 of 183 - 16

UNCLASSIFIED

Exhibit R-2, RDT&E,N Budget Item Justification

UNCLASSIFIED

EXHIBIT R-2, FY 2001 RDT&E,N BUDGET ITEM JUSTIFICATION

DATE: FEB 2000

BUDGET ACTIVITY: 7

PROGRAM ELEMENT: 0303140N

PROGRAM ELEMENT TITLE: Information Systems Security Program

(BLII). It involves the design of standard network security suites for various layers of the Navy's network infrastructure, from wide area network boundary points to local area network and workstation protections. It also provides solutions to the coalition operations problem and to the Navy cryptographic equipment obsolescence problem.

1. (U) FY 1999 ACCOMPLISHMENTS:

- (U) (\$2,110) Continued development of the programmable embedded COMSEC prototype and began integration and system testing. The first targeted application is the Submarine LF/VLF VME Bus Receiver (SLVR) system for replacement of the KG-3X family of cryptos. Initiated efforts to address the use of programmable embedded COMSEC solutions and other cryptographic technology for replacement of aging and obsolete cryptos in Navy systems (e.g., Advanced Narrow-Band Digital Voice Terminal (ANDVT), VINSON, KG-84, KG-40 in support of Link-11, and the Thornton family in support of Link-16). Identified applications and technology for new ship construction and other platforms, as well as for new emerging communications backbones/circuits in support of Navy initiatives such as IT-21/NMCI.
- (U) (\$2,095) Continued development of EKMS Tier 1, including completion of all software builds and testing.
- (U) (\$4,660) Began the development of EKMS Phase IV. This included development of requirements for Data Transfer Device (DTD) 2000, and for addressing incorporation of key management solutions for IT-21/NMCI. Addressed the integration of PKI/CMI technology, integration of key management and net planning capabilities and functions, and support for the incorporation of the Key Systems Operation (KSO) exchange. Also developed a Navy Single Point Command, Control and Keying (NSPC<sup>2</sup>K) design as a solution for Navy platforms, embedded cryptographic technology and associated crypto replacement efforts. Continued the development, evaluation and application assessment of high assurance products, and provided system security and C&A engineering and testing for key management components and systems.
- (U) (\$475) Began the design, development, application and evaluation of PKI/CMI techniques (e.g., benign key), netted re-key technology, application of COTS key and certificate management technology, key/net management integration, key and certificate workstation integration, key fill device and delivery technology, new cryptographic algorithm developments, and new approaches to cryptographic technology (e.g., software and chaos theory based). Provided the design, development, application and evaluation of new key generation and distribution techniques and technology. Conducted laboratory assessments of the latest NSA and COTS key management technology and products, and demonstrated prototype key and certificate management systems.

UNCLASSIFIED

EXHIBIT R-2, FY 2001 RDT&E,N BUDGET ITEM JUSTIFICATION

DATE: FEB 2000

BUDGET ACTIVITY: 7

PROGRAM ELEMENT: 0303140N

PROGRAM ELEMENT TITLE: Information Systems Security Program

- (U) (\$900) Began development of the Navy Security Management Infrastructure (NSMI) architecture and design. This included the development of the concept, architecture, and requirements for the integration of PKI and CMI components and technology for Navy applications and sites. Evaluated and assessed the use and application of medium assurance commercial products for PKI/CMI public key and certificate applications through a prototype pilot initiative involving up to 5000 users focused on individual messaging and web server security. Assessed the feasibility of integrating PKI/CMI technology with key management products and initiatives.
- (U) (\$2,729) Continued the design, development and assessment of 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 COTS communications backbones, specifically addressing wireless applications and strategic and tactical communications. Supported the integration of secure voice services in support of IT-21/NMCI. Developed/assessed the requirements for integrated secure voice/data, and provided system security and Certification & Accreditation (C&A) engineering and testing for secure voice components and systems. Continued the development of voice algorithms and security techniques, and conducted assessments of COTS secure voice technology and products. This included development of secure voice technology to support Navy unique requirements/applications (e.g., point-to-multipoint) for new ship construction, existing ship platforms, and for shore sites.
- (U) (\$200) Continued to research secure voice and biometric access consortia. Performed research into new high assurance secure voice technology, including wireless cellular and satellite technology.
- (U) (\$620) Developed a security architecture for NMCI and for selected Navy distributed information system development programs. Ensured that developed architecture provides 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 IT-21, NMCI, and large development programs including (Global Command and Control System, Maritime (GCCS-M), Global Command and Control System (GCCS), DMS, JMCOMS and others. Included both defensive protections as well as intrusion detection system capabilities.
- (U) (\$2,692) Evaluated, tested and integrated distributed information system security technology solutions into Navy information systems. This included the examination and selection of various components, such as firewalls, intrusion detection systems, virtual private networking systems, public

UNCLASSIFIED

EXHIBIT R-2, FY 2001 RDT&E,N BUDGET ITEM JUSTIFICATION

DATE: FEB 2000

BUDGET ACTIVITY: 7

PROGRAM ELEMENT: 0303140N

PROGRAM ELEMENT TITLE: Information Systems Security Program

key based secure e-mail and web systems, and others as well as high assurance components for connection of Top Secret and SCI systems to lower level systems. Prototyped components at operational sites. Began examining alternatives for high speed network encryption (IP packet encryption at speeds of at least 100 Mbps) and scaleable boundary level security solutions.

- (U) (\$1,950) Provided developmental systems security engineering, C&A support to Navy information system developments such as GCCS-M, GCCS, DMS, JMCOMS, IT-21, NMCI, NSSN, LPD-17, SC-21, and others. Support focused on Information Technology Service Centers being designed in multiple repair regions, including San Diego, Norfolk and Hawaii. Focused on integration of the proper functions to ensure adherence to the common security architectures and to ensure that the security and performance of the tactical systems, including those operating at Top Secret and at SCI are consistent with Navy and DOD requirements.
- (U) (\$705) Continued developing and updating INFOSEC standards and engineering guidance documents to ensure they are consistent with the security architecture, rapidly changing technology, and the evolving threat. Included guidance for proper operational procedures for the use of the security protections at various levels of the NMCI architecture.
- (U) (\$550) Developed, prototyped, and tested solutions to the coalition interoperability problem including, development of a Multilevel Security (MLS) web server. Based on available security technologies as well as emerging architectural methods of providing interoperability across different security levels.
- (U) (\$532) Continue vulnerability/threat assessments and development and systems integration of network countermeasures tools (NVACM) efforts.

3. (U) FY 2000 PLAN:

- (U) (\$2,000) Continue development of programmable embedded COMSEC solutions for the KG-3X family of cryptos to satisfy requirements associated with SLVR for KG-3X replacement. Begin the development and implementation of benign keying technology for crypto replacement efforts. Initiate efforts to develop a flexible, digital modular cryptographic solution based on multi-channel, programmable technology (e.g., AIM, CORNFIELD) to replace a wide variety of aging and obsolete cryptos in existing and new navy communications systems/circuits (e.g., ANDVT, VINSON, KG-84, KG-40 in support of Link-11, and the

R-1 Shopping List - Item No. 183 - 7 of 183 - 16

UNCLASSIFIED

Exhibit R-2, RDT&E,N Budget Item Justification

UNCLASSIFIED

EXHIBIT R-2, FY 2001 RDT&E,N BUDGET ITEM JUSTIFICATION

DATE: FEB 2000

BUDGET ACTIVITY: 7

PROGRAM ELEMENT: 0303140N

PROGRAM ELEMENT TITLE: Information Systems Security Program

Thornton family in support of Link-16). This capability will yield significant benefits including simplified operation, improved interoperability, and reduced space and weight requirements. Identify and document performance parameters, form factors, and interface requirements for the digital modular cryptographic solution. These efforts will be fully coordinated with the NSA.

- (U) (\$4,025) Complete development of EKMS, and ensure compatibility with the Tier 0, Tier 2, and Tier 3 components and software.
- (U) (\$2,675) Continue the development of EKMS Phase IV for Tier 1, Tier 2 and Tier 3. This includes support for incorporation of enhanced key management capabilities/solutions for IT-21/NMCI. Address the development and inclusion of web-based technology and support for the incorporation of the KSO exchange. Begin the requirements definition for integration of certificate management and key management. Additional efforts focus on the development and prototyping of the NSPC<sup>2</sup>K design and solution for Navy platforms, supporting the development and prototyping of the DTD 2000, and key management support for embedded cryptographic technology and the Navy's crypto replacement efforts. Conduct laboratory assessments of the latest NSA and industry COTS key management technology and products, and demonstrations of prototype key management systems. Provide system security and C&A engineering and testing for key management components and systems.
- (U) (\$2,385) 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 IT-21/NMCI initiatives. Prototype and assess the use and application of medium and high assurance commercial products for PKI/CMI applications, including the assessment of these technologies over tactical communications paths. Continue 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. Evaluate, assess, and integrate multiple related technologies including security tokens, such as smart cards, and virtual private networks (VPNs). Support the definition of standards for smart cards and the evolution of computer workstation technology to support the widespread introduction of smart card technology.
- (\$860) Continue the design, development and assessment of security solutions/capabilities for next generation voice systems. Develop prototypes/demonstrations to illustrate secure voice, video, and data capabilities over IP and ATM networks, specifically addressing quality of service and reliability issues. Continue research into new secure voice technology, developing technology and techniques for secure voice

UNCLASSIFIED

EXHIBIT R-2, FY 2001 RDT&E,N BUDGET ITEM JUSTIFICATION

DATE: FEB 2000

BUDGET ACTIVITY: 7

PROGRAM ELEMENT: 0303140N

PROGRAM ELEMENT TITLE: Information Systems Security Program

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. Investigate the application of digital cellular and satellite secure voice technology.

- (U) (\$823) Initiate the design, development and assessment of the 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 SPC<sup>2</sup>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, the DDG-51 class, NSSN, and CVX class of ships by providing a secure voice solution for telephonic, tactical and secure voice problems, specifically addressing the IT-21 initiatives.
- (U) (\$250) Continue 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) Continue the evolutionary development of security architectures for IA that include virtually all Navy distributed information system development programs. Ensure the architecture evolves 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 IT-21, NMCI, the Joint Technical Architecture, and large development programs including GCCS-M, GCCS, DMS, ADNS, BLII and others. Include both defensive protections as well as intrusion monitoring in the architecture.
- (U) (\$3,736) Continue developing and testing distributed information system security solutions for Navy information systems. This includes 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 SCI systems to lower level systems. Examine and evaluate next generation network security components including scaleable security products, ATM firewalls and intrusion detection systems, and sophisticated malicious code monitors. Design and prototype standard security suites for delivery to Naval commands, bases, and afloat platforms. Support the design of situational awareness and visualization capabilities to support active computer network defense and

UNCLASSIFIED

EXHIBIT R-2, FY 2001 RDT&E,N BUDGET ITEM JUSTIFICATION

DATE: FEB 2000

BUDGET ACTIVITY: 7

PROGRAM ELEMENT: 0303140N

PROGRAM ELEMENT TITLE: Information Systems Security Program

the development of a sensor grid, with underlying data mining and correlation tools. Prototype components and standard security suites at selected operational sites.

- (U) (\$2,100) Provide systems security engineering, C&A support to Navy information system developments such as GCCS-M, GCCS, DMS, ADNS, IT-21, NMCI, 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 SCI are consistent with Navy and DOD requirements.
- (U) (\$825) 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 standard network security suites and tools.
- (U) (\$1,265) Develop, prototype, and test solutions to the coalition interoperability problem. Base the solutions on available multilevel security technologies as well as emerging architectural methods of providing interoperability across different security levels.
- (U) (\$1,260) Continue 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 (e.g., AIM, CORNFIELD). 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 NSA.

(U) (\$2,533) Complete the development of EKMS Phase IV for Tier 1, Tier 2 and Tier 3. 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.

R-1 Shopping List - Item No. 183 - 10 of 183 - 16

UNCLASSIFIED

Exhibit R-2, RDT&E,N Budget Item Justification

UNCLASSIFIED

EXHIBIT R-2, FY 2001 RDT&E,N BUDGET ITEM JUSTIFICATION

DATE: FEB 2000

BUDGET ACTIVITY: 7

PROGRAM ELEMENT: 0303140N

PROGRAM ELEMENT TITLE: Information Systems Security Program

Demonstrate prototype of the NSPC<sup>2</sup>K 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 industry COTS key management technology and products. Provide system security and C&A engineering and testing for key management components and systems.

(U) (\$3,036) 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 IT-21/NMCI initiatives. Continue to assess the use and application of medium and high assurance commercial products for 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) (\$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 IP and ATM networks. Demonstrate secure voice server 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 NSPC<sup>2</sup>K 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

UNCLASSIFIED

EXHIBIT R-2, FY 2001 RDT&E,N BUDGET ITEM JUSTIFICATION

DATE: FEB 2000

BUDGET ACTIVITY: 7

PROGRAM ELEMENT: 0303140N

PROGRAM ELEMENT TITLE: Information Systems Security Program

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 IT-21, NMCI, the Joint Technical Architecture, and large development programs including GCCS-M, GCCS, DMS, ADNS, BLII and others. Include both defensive protections as well as intrusion monitoring in the architecture.

(U) (\$4,500) 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 OC-12 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) (\$2,500) Provide systems security engineering, C&A support to Navy information system developments such as GCCS-M, GCCS, DMS, ADNS, IT-21, NMCI, 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 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.

UNCLASSIFIED

EXHIBIT R-2, FY 2001 RDT&E,N BUDGET ITEM JUSTIFICATION

DATE: FEB 2000

BUDGET ACTIVITY: 7

PROGRAM ELEMENT: 0303140N

PROGRAM ELEMENT TITLE: Information Systems Security Program

B. (U) CHANGE SUMMARY EXPLANATION:

(U) Funding:

(U) FY 1999: Inflation savings -\$100K. -\$288K transfer for SBIR and -\$401K department adjustment.

(U) FY 2000: -\$124K miscellaneous department adjustments. -\$312K, portion of extramural program is reserved for Small Business Innovation Research assessment in accordance with 15 USC 638.

FY 2001: -\$2,182K miscellaneous department adjustments.

(U) Schedule: Navy's 1<sup>st</sup> 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.

(U) Technical: N/A

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

	FY 1999	FY 2000	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	TO	TOTAL COMPLETE	PROGRAM
(U) OPN 3415 Information Systems Security Program (ISSP)	39,176	66,765	46,563	90,849	60,622	88,225	94,795	CONT.	CONT.	
(U) O&MN 4A6M	10,942	13,930	25,203	19,233	19,821	17,774	17,819	CONT.	CONT.	

(U) RELATED RDT&E:

(U) PE 0303140G (Cryptographic Equipments)

UNCLASSIFIED

EXHIBIT R-2, FY 2001 RDT&E,N BUDGET ITEM JUSTIFICATION

DATE: FEB 2000

BUDGET ACTIVITY: 7

PROGRAM ELEMENT: 0303140N

PROGRAM ELEMENT TITLE: Information Systems Security Program

D. ACQUISITION STRATEGY

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

UNCLASSIFIED

EXHIBIT R-3, FY 2001 RDT&E,N PROJECT COST ANALYSIS

DATE: FEB 2000  
PROJECT NUMBER: X0734

BUDGET ACTIVITY: 7

PROGRAM ELEMENT: 0303140N  
PROGRAM ELEMENT TITLE: Information Systems Security Program

Exhibit R-3 Cost Analysis (page 1)										Date: FEB 2000		
APPROPRIATION/BUDGET ACTIVITY: 7					PROGRAM ELEMENT: 0303140N					PROJECT NAME AND NUMBER: ISSP (X0734)		
Cost Categories	Contract Method & Type	Performing Activity & Location	Total PYs Cost	FY99 Cost	FY99 Award Date	FY00 Cost	FY00 Award Date	FY01 Cost	FY01 Award Date	Cost To Complete	Total Cost	Target Value of Contract
HARDWARE DEVELOPMENT	CPFF/	VIASAT	7,282	0		0				0	7,282	7,582
SOFTWARE DEVELOPMENT	CPAF	SAIC	23,366	1,781	12/98	4,450	11/99			0	29,597	37,621
HARDWARE DEVELOPMENT	VAR	MITRE	1,911	532	02/99	1,260	10/99	1,000	10/00	Cont.	Cont.	Cont.
HARDWARE DEVELOPMENT	VAR	VARIOUS	21,876	16,710	VAR	16,394	VAR	20,530	VAR	Cont.	Cont.	Cont.
Subtotal Product Development			54,435	19,023		22,104		21,530		Cont.	Co t.	Cont.
Remarks:												
SAIC target value of contract includes other services' funding.												
SYSTEMS ENGINEERING	VAR	VAR	2,976							0	2,976	2,976
Subtotal Support			2,976							0	2,976	2,976
Remarks												

(Exhibit R-3, page 1 of 2 )

UNCLASSIFIED

EXHIBIT R-3, FY 2001 RDT&E,N PROJECT COST ANALYSIS

DATE: FEB 2000  
PROJECT NUMBER: X0734

BUDGET ACTIVITY: 7

PROGRAM ELEMENT: 0303140N  
PROGRAM ELEMENT TITLE: Information Systems Security Program

Exhibit R-3 Cost Analysis (page 2)										Date: FEB 2000		
APPROPRIATION/BUDGET ACTIVITY: 7				PROGRAM ELEMENT: 0303140N				PROJECT NAME AND NUMBER: X0734				
Cost Categories	Contract Method & Type	Performing Activity & Location	Total Pys Cost	FY99 Cost	FY99 Award Date	FY00 Cost	FY00 Award Date	FY01 Cost	FY01 Award Date	Cost To Complete	Total Cost	Target Value of Contract
Subtotal T&E												
Remarks												
PROGRAM MGMT SUPPORT	VAR	VARIOUS	1,995	1,191	10/98	750	10/99	0		Cont.	Cont.	Cont.
Subtotal Management			1,995	1,191		750		0		Cont.	Cont.	Cont.
Remarks												
Total Cost			59,406	20,214		22,854		21,530		Cont.	Cont.	Cont.

(Exhibit R-3, page 2 of 2)