

UNCLASSIFIED  
EXHIBIT R-2, FY 2000 PRESIDENT'S BUDGET ESTIMATES

DATE: February 1999

BUDGET ACTIVITY: 7

PROGRAM ELEMENT: 0303140N

PROGRAM ELEMENT TITLE: Information Systems Security Program

(U) COST: (Dollars in Thousands)

PROJECT NUMBER & TITLE	FY 1998	FY 1999	FY 2000	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	TO COMPLETE	TOTAL PROGRAM
X0734 Information Systems Security	17,287	21,003	22,978	23,712	24,436	24,962	27,151	27,951	CONT.	CONT.
TOTAL	17,287	21,003	22,978	23,712	24,436	24,962	27,151	27,951	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) Owing to the attack variety, the complexity of Navy distributed systems, and the rapid rate of change of the underlying commercial and government technologies; the provision of security is an increasingly complex and ever changing problem. Technologies involved with providing security are a mix of computer security, network security, and cryptographic security technologies 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.

UNCLASSIFIED

EXHIBIT R-2, FY 2000 PRESIDENT'S BUDGET ESTIMATES

DATE: February 1999

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 in Navy 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, and integrated Joint information system efforts, etc. The program provides the efforts and 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 with 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 aimed 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 2000 PRESIDENT'S BUDGET ESTIMATES

DATE: February 1999

BUDGET ACTIVITY: 7

PROGRAM ELEMENT: 0303140N

PROGRAM ELEMENT TITLE: Information Systems Security Program

(U) COST: (Dollars in Thousands)

PROJECT NUMBER & TITLE	FY 1998	FY 1999	FY 2000	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	TO COMPLETE	TOTAL PROGRAM
X0734 Information Systems Security	17,287	21,003	22,978	23,712	24,436	24,962	27,151	27,951	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 meet the evolving threat. Communication Security (COMSEC) replacements, in most cases, will use embedded modules (using 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 and COMPUSEC 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 information assurance products. Technology base efforts are: developing new secure voice algorithms and prototypes; developing technology for a new family of programmable COMSEC modules; development of network security products, which are designed to interconnect networks of dissimilar classification, and address the Multi-level Security (MLS) technology requirements for the DON, and assessing a variety of potentially high pay-off NSA and industry products. 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). Specific emphasis is being placed on evaluation, integration and test of Contractor off-the-shelf (COTS)/Non-developmental Item (NDI) IA security products into prototype capabilities such as firewalls, guards and monitoring systems to provide for monitoring, detecting, isolating and reacting MDIR 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

UNCLASSIFIED

EXHIBIT R-2, FY 2000 PRESIDENT'S BUDGET ESTIMATES

DATE: February 1999

BUDGET ACTIVITY: 7

PROGRAM ELEMENT: 0303140N

PROGRAM ELEMENT TITLE: Information Systems Security Program

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. Additional efforts shall focus on architectures, designing, demonstrating and integrating a secure voice capability for IT-21 and other Command, Control, Communications and Computers (C4I) programs and initiatives. Gateway technology to address Navy unique point-to-multipoint communications shall be developed in support of IT-21 and the Naval Virtual Intranet (NVI). This technology will comprise the secure voice communications suite of equipment for shipboard applications, as well as shore-based sites. 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 and Certificate Management Infrastructure (PKI/CMI) technology, and the development of a Single Point Command, Control and Keying (SPC<sup>2</sup>K) solution 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 (IT-21, NVI). 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, focuses primarily on designing and proving IA solutions for IT-21 and the NVI. This portion of the ISSP supports delivery of network security engineering expertise needed to stand-up the NVI and securely deploy IT-21 constituent systems such as Joint Maritime Communications (JMCOMS), Joint Maritime Command Information System (JMCIS), and Base Level information Infrastructure (BLII). It also provides solutions to the coalition operations problem and to the Navy cryptographic equipment obsolescence problem.

UNCLASSIFIED

EXHIBIT R-2, FY 2000 PRESIDENT'S BUDGET ESTIMATES

DATE: February 1999

BUDGET ACTIVITY: 7

PROGRAM ELEMENT: 0303140N

PROGRAM ELEMENT TITLE: Information Systems Security Program

(U) PROGRAM ACCOMPLISHMENTS AND PLANS:

1. (U) FY 1998 ACCOMPLISHMENT:

- (U) (\$300) Complete development of the Embeddable INFOSEC Product (EIP).
- (U) (\$250) Continue development of PEIP prototype.
- (U) (\$6,671) Perform development demonstrations, software design reviews, and development, integration and system testing for Tier 1 Phase 1.
- (U) (\$1,117) Continue development and begin testing of Tiers 2 and 3 components.
- (U) (\$1,810) Provide developmental systems security engineering, Certification, and Accreditation (C&A) support to Navy information systems such as Defense Messaging System (DMS) and Multi-Level Information System Security Initiative (MISSI). This will include systems security engineering support to Navy tactical and non-tactical systems, that are required to incorporate DMS and MISSI evolving technology. Particular emphasis will be directed to system engineering associated with implementation of DMS and MISSI technology into tactical systems, including those associated with Top Secret and Secure Compartmented Information (SCI) systems.
- (U) (\$1,030) Develop and test network security solutions for Navy information systems. This will include the high assurance components associated with Top Secret and SCI system solutions.
- (U) (\$1,033) Continue development of integrated security architectures for Naval INFOSEC systems, both for C4I systems and non-C4I systems. This will include refinements of interim, incremental security architectures that display how MISSI, Electronic Key Management System (EKMS), and Secure Terminal Equipment (STE) security technology will be integrated into Navy systems. The architectures will include analysis of all technical issues and related concepts of operations associated with the architectures. Develop requirements for mid-term INFOSEC products that may be required. Continue to analyze achieved INFOSEC performance in operational systems. Include latest operational requirements, technical opportunities and new threat information.
- (U) (\$405) Continue to participate in revising/refining INFOSEC standards to reflect evolving capabilities. Refine INFOSEC engineering guideline documents as directed by the CNO/Marine Corps co-chaired INFOSEC Steering Group. In coordination with NSA, continue refinements to automated tools to accomplish systems C&A.

UNCLASSIFIED

EXHIBIT R-2, FY 2000 PRESIDENT'S BUDGET ESTIMATES

DATE: February 1999

BUDGET ACTIVITY: 7

PROGRAM ELEMENT: 0303140N

PROGRAM ELEMENT TITLE: Information Systems Security Program

- (U) (\$879) Develop secure voice integrated shipboard architecture incorporating NSA STE products and integrating COTS assessments of the latest NSA and industry INFOSEC technology and demonstrations of prototype voice systems. Continue research into new INFOSEC voice technology.
  - (U) (\$386) Develop and update Naval Command, Control, Communications and Computers Information Surveillance and Reconnaissance (C4ISR) implementation guidance. Develop and update Naval C4ISR mission to incorporate an overarching systems, technical and information architectures. Conduct associated C4ISR analysis and studies.
  - (U) (\$906) Reflects realignment of Navy Vulnerability Assessment and Countermeasures (NVACM) under the INFOSEC Program. Continue vulnerability assessments and information warfare threat assessments in support of critical developing information systems. Continue development, evaluation, integration and prototype of COTS/NDI network countermeasures capabilities to MDIR unwanted intrusions into Navy information systems.
2. (U) FY 1999 PLAN:
- (U) (\$2,110) Continue development of the programmable embedded COMSEC prototype and begin 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. Initiate 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). Identify 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/NVI.
  - (U) (\$1,249) Continue development of EKMS Tier 1.
  - (U) (\$842) Complete development, integration and testing of the Tier 1 system with Tiers 0, 2 and 3 components and software.
  - (U) (\$4,802) Begin the development of EKMS Phase IV. This includes support for the support for the incorporation of the DMS in EKMS, development of requirements for Data Transfer Device (DTD) 2000, and for addressing incorporation of key management solutions for IT-21/NVI. Address the development and inclusion of web-based technology, 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

## UNCLASSIFIED

## EXHIBIT R-2, FY 2000 PRESIDENT'S BUDGET ESTIMATES

DATE: February 1999

BUDGET ACTIVITY: 7

PROGRAM ELEMENT: 0303140N

PROGRAM ELEMENT TITLE: Information Systems Security Program

(KSO) exchange. Additional efforts focus on the development of the Navy Single Point Command, Control and Keying (NSPC<sup>2</sup>K) design and solution for Navy platforms and support for embedded cryptographic technology and the Navy's crypto replacement efforts. Continue the development, evaluation and application assessment of high assurance products, and provide system security and C&A engineering and testing for key management components and systems.

- (U) (\$475) Begin the design, development, application and evaluation of PKI/CMI techniques (e.g., benign key), netted re-key technology, application of COTS key 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, quantum cryptography, and chaos theory based). Provide the design, development, application and evaluation of new key generation and distribution techniques and technology. Conduct laboratory assessments of the latest NSA and industry COTS key management technology and products, and demonstrations of prototype key management systems.
- (U) (\$900) Begin development of the Navy Security Management Infrastructure (NSMI) architecture and design. This includes the development of the concept, architecture, and requirements for the integration of PKI/CMI components and technology for Navy applications and sites. Evaluate and assess the use and application of medium (and other) assurance commercial products for PKI/CMI applications. Assess the feasibility of integrated PKI/CMI technology with key management products and initiatives. Additional NSMI efforts shall focus on incorporating technology and techniques in support of the IT-21/NVI initiatives.
- (U) (\$2,576) Continue the design, development and assessment of security solutions/capabilities for next generation voice systems. Continue research into new secure voice technology, developing technology and techniques for secure voice over government and COTS communications backbones, specifically addressing wireline and wireless telephony applications and strategic and tactical communications. Support the integration of secure voice services in support of IT-21/ NVI. Develop/assess the requirements for integrated secure voice/data, and provide system security and C&A engineering and testing for secure voice components and systems. Continue the development of voice algorithms and security techniques, and conduct laboratory assessments of the latest NSA and industry COTS secure voice technology and products, and demonstrations of prototype secure voice systems. This includes 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.

## UNCLASSIFIED

## EXHIBIT R-2, FY 2000 PRESIDENT'S BUDGET ESTIMATES

DATE: February 1999

BUDGET ACTIVITY: 7

PROGRAM ELEMENT: 0303140N

PROGRAM ELEMENT TITLE: Information Systems Security Program

- (U) (\$200) Continue to research secure voice and biometric access consortia. Continued 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) (\$620) Develop a security architecture for IA that includes 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, NVI, the Navy CIO Technology Infrastructure project, the Joint Technical Architecture, and large development programs including (Global Command and Control System, Maritime (GCCS-M), Global Command and Control System (GCCS), DMS, JMCOMS and others. Include both defensive protections as well as intrusion monitoring in the architecture.
- (U) (\$2,692) Evaluate, test and if necessary, develop distributed information system security technology solutions for Navy information systems. This includes the examination and selection of various components, such as firewalls, intrusion detection systems, virtual private networking systems, public 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. Prototype some of the components at operational sites. Begin examining alternatives for high speed network encryption (IP packet encryption at speeds of at least 100 Mbps).
- (U) (\$1,950) Provide developmental systems security engineering, C&A support to Navy information system developments such as GCCS-M, GCCS, DMS, JMCOMS, IT-21, NVI, NSSN, LPD-17, SC-21, and others. 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) (\$705) 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. Include guidance for proper operational procedures for the use of the security protections at various levels in the command hierarchy.
- (U) (\$550) 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.

UNCLASSIFIED

EXHIBIT R-2, FY 2000 PRESIDENT'S BUDGET ESTIMATES

DATE: February 1999

BUDGET ACTIVITY: 7

PROGRAM ELEMENT: 0303140N

PROGRAM ELEMENT TITLE: Information Systems Security Program

- (U) (\$1332) 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 remainder of the KG-3X family of cryptos, addressing specifically the ground based transmitter sites and TACAMO aircraft. Begin the development and implementation of benign keying technology for all crypto replacement efforts. Continue efforts to address the use of other cryptographic technology for replacement 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 Thornton family in support of Link-16). Continue to identify and target applications for cryptographic replacement 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/NVI. Begin prototyping candidate cryptographic replacement solutions for evaluation and assessment in Navy representative circuits and platforms. These efforts will be coordinated with the NSA.
  
  - (U) (\$825) 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 the incorporation of the DMS into EKMS, and for addressing incorporation of enhanced key management capabilities/solutions for IT-21/NVI. 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, development and prototyping of the DTD 2000, and key management support for embedded cryptographic technology and the Navy's crypto replacement efforts. Provide system security and C&A engineering and testing for key management components and systems.
  
  - (U) (\$1,260) Continue the design, development, application and evaluation of key management technology, key management techniques (e.g., benign key), netted re-key technology, application of COTS key 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, quantum cryptography, and chaos theory based). Initiate

## UNCLASSIFIED

## EXHIBIT R-2, FY 2000 PRESIDENT'S BUDGET ESTIMATES

DATE: February 1999

BUDGET ACTIVITY: 7

PROGRAM ELEMENT: 0303140N

PROGRAM ELEMENT TITLE: Information Systems Security Program

prototyping and demonstration of technology. Provide the design, development, application and evaluation of new key generation and distribution techniques and technology. Conduct laboratory assessments of the latest NSA and industry COTS key management technology and products, and demonstrations of prototype key management systems.

- (U) (\$1,125) Continue development of the NSMI architecture and design. Based on the Navy's architecture/concept and requirements, begin the evaluation, development and integration of PKI/CMI components and technology for Navy applications and sites. Additional NSMI efforts shall focus on incorporating SMI technology and techniques in support of the IT-21/NVI initiatives. Evaluate and assess the use and application of medium (and other) assurance commercial products for PKI/CMI applications. Continue assessing the feasibility of integrated 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, as required.
- (U) (\$2,110) Continue the design, development and assessment of security solutions/capabilities for next generation voice systems. Continue research into new secure voice technology, developing technology and techniques for secure voice over government and COTS communications backbones, specifically addressing wireline and wireless telephony applications and strategic and tactical communications. Support the integration of secure voice services in support of IT-21/NVI. Continue to develop and assess the technology for integrated secure voice/data, low data rate algorithms, voice compression technology in conjunction with cryptographic algorithm technology, and voice/speaker recognition. Continue the development of voice algorithms and security techniques, and conduct laboratory assessments of the latest NSA and industry COTS secure voice technology and products, and demonstrations of prototype secure voice systems. This includes 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, and for providing system security and C&A engineering and testing for secure voice components and systems.
- (U) (\$2,773) 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), the crypto replacement technology based on PEIP, 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.

UNCLASSIFIED

EXHIBIT R-2, FY 2000 PRESIDENT'S BUDGET ESTIMATES

DATE: February 1999

BUDGET ACTIVITY: 7

PROGRAM ELEMENT: 0303140N

PROGRAM ELEMENT TITLE: Information Systems Security Program

- (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, NVI, the Navy CIO Technology Infrastructure project, the Joint Technical Architecture, and large development programs including GCCS-M, GCCS, DMS, JMCOMS and others. Include both defensive protections as well as intrusion monitoring in the architecture.
- (U) (\$3,860) 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, and others as well as high assurance components for connection of Top Secret and SCI systems to lower level systems. Prototype some of the components at operational sites.
- (U) (\$2,100) Provide systems security engineering, C&A support to Navy information system developments such as GCCS-M, GCCS, DMS, JMCOMS, IT-21, NVI, NSSN, LPD-17, SC-21, and others. 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) (\$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.
- (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.

UNCLASSIFIED

EXHIBIT R-2, FY 2000 PRESIDENT'S BUDGET ESTIMATES

DATE: February 1999

BUDGET ACTIVITY: 7

PROGRAM ELEMENT: 0303140N

PROGRAM ELEMENT TITLE: Information Systems Security Program

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

B. (U) CHANGE SUMMARY EXPLANATION:

(U) Funding:

(U) FY 1998: -\$361K SBIR, \$2,120K is for pending below threshold reprogrammings, and -\$1,245K for DD1002: April 98 Update.

(U) FY 1999: -\$51K Revised Economic Assumption, -\$30K for Civilian Personnel Underexecution, and -\$1,040K CAAS adjustments and -\$77K for FFRDC Distribution.

(U) FY 2000: -\$1,660 reduction to finance other higher priority programs, \$300K for NWCF rates, -\$332K for Non-Pay Inflation, and \$92K for Civilian Pay Rates.

(U) Schedule: The schedule impact is directly related to the contractor's late start in portions of the software development effort and the additions of new requirements on the Tier 1 baseline contract.

(U) Technical: Tier 1 development contractor experienced unexpected delays in completing detail design or certain Tier 1 functions. New requirements were added to the present baseline Tier 1 Contract to maintain compatibility with NSA's Tier 0 design. These new requirements had a direct affect on the present software development resulting in re-work of current design and some new design work.

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

	FY 1998	FY 1999	FY 2000	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	TO COMPLETE	TOTAL PROGRAM
(U) OPN 3415 Information Systems Security Program (ISSP)	25,492	45,800	64,139	52,338	66,912	56,747	74,703	78,524	CONT.	CONT.

(U) O&MN 4A6M

UNCLASSIFIED  
EXHIBIT R-2, FY 2000 PRESIDENT'S BUDGET ESTIMATES

DATE: February 1999

BUDGET ACTIVITY: 7

PROGRAM ELEMENT: 0303140N

PROGRAM ELEMENT TITLE: Information Systems Security Program

13,213	14,767	14,247	14,847	15,356	15,862	18,362	18,862	CONT.	CONT.
--------	--------	--------	--------	--------	--------	--------	--------	-------	-------

(U) RELATED RDT&E:

(U) PE 0303140G (Cryptographic Equipments)

D. ACQUISITION STRATEGY

	<u>FY 1998</u>	<u>FY 1999</u>	<u>FY 2000</u>	<u>To Complete</u>
EKMS				
Program Milestones			1Q-Tier 1 IOC	
Engineering Milestones	2Q-Build Review 1 3Q-Build Rev 2 3Q-Initial Phase IV Development	1Q-Build Rev 3		
T&E Milestones		3Q-Tier 1 Test	1Q-Tier 1 Government Acceptance Test (GAT)	
Contract Milestones				
EIP				
Program Milestones				
Engineering Milestones				
T&E Milestones				

UNCLASSIFIED

EXHIBIT R-2, FY 2000 PRESIDENT'S BUDGET ESTIMATES

DATE: February 1999

BUDGET ACTIVITY: 7

PROGRAM ELEMENT: 0303140N

PROGRAM ELEMENT TITLE: Information Systems Security Program

Contract  
Milestones