Exhibit R-2, RDT&E Budget Item Justification: PB 2011 Navy										DATE: February 2010	
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*				R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*							
COST ($ in Millions)	**FY 2009 Actual**	**FY 2010 Estimate**	**FY 2011 Base Estimate**	**FY 2011 OCO Estimate**	**FY 2011 Total Estimate**	**FY 2012 Estimate**	**FY 2013 Estimate**	**FY 2014 Estimate**	**FY 2015 Estimate**	**Cost To Complete**	**Total Cost**
Total Program Element	31.828	29.049	25.934	0.000	25.934	27.660	28.858	29.809	30.095	Continuing	Continuing
0734: *Communications Security R&D*	25.146	21.879	22.921	0.000	22.921	24.637	25.760	26.630	26.876	Continuing	Continuing
3230: *Information Assurance*	0.000	2.191	3.013	0.000	3.013	3.023	3.098	3.179	3.219	Continuing	Continuing
9999: *Congressional Adds*	6.682	4.979	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	24.598

A. Mission Description and Budget Item Justification

Information Systems Security Program (ISSP) ensures the protection of Navy and joint telecommunications and information systems from exploitation and attack. 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 Department of Defense Directive 8500.1. ISSP activities address the triad of defensive information operations defined in Joint Publication 3-13; protection, detection, and reaction. Focused on FORCEnet supporting the mobile forward-deployed subscriber, the Navy's implementation of Network-Centric Warfare places demands upon the ISSP as the number of users dramatically increases 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, supported by Mission Assurance Category 1 systems and crypto modernization requirements with Chairman Joint Chiefs of Staff Instruction 6510.

The interconnectivity of naval networks, connections to the public information infrastructure, and their use in naval and joint war fighting means that FORCEnet is a easier attacked and higher value target. The types of possible attacks continues to grow. In addition to the traditional attacks that involve the theft or eavesdropping of information, Navy information and telecommunications systems face advanced attacks involving malicious changes to critical information, changes to the functioning of critical systems, denial of service (jamming), and the destruction of systems and networks. Since many naval information systems are based on commercially available technologies, an adversary often has access to the very technologies they want to exploit.

The rapid change in the underlying commercial and government information infrastructures makes the security an increasingly complex and dynamic problem. ISSP provides the Navy's war fighter the essential information trust characteristics of availability, confidentiality, 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.

The ISSP Research Development Test & Evaluation (RDT&E) program provides the Navy with these essential Information Assurance (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

Exhibit R-2, RDT&E Budget Item Justification: PB 2011 Navy	DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*

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). ISSP RDT&E program is predictive, adaptive, and coupled to technology by modeling Department of Defense (DoD) and commercial information and telecommunications systems evolution (rather than being one-time developments). The program develops frameworks, architectures, and products based on mission threats, information criticality, exploitation risks, risk management, and integrated joint information system efforts.

All ISSP RDT&E efforts comply with the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113) as implemented through OMB 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 Organization for Standardization (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 and the ISSP RDT&E program complies with the joint technical architecture. The FORCEnet architecture and standards documents reflect this emphasis on interoperable standards.

The interconnection of FORCEnet into the DoD Global Information Grid (GIG) 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 Navy 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 and government 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.

JUSTIFICATION FOR BUDGET ACTIVITY: This program is funded under OPERATIONAL SYSTEMS DEVELOPMENT because it encompasses engineering and manufacturing development for upgrade and integration of existing, operational systems. This includes cryptographic systems required to protect information defined in Title 40 United States Code (USC) Chapter 25 Sec 1452, and the ISSP cryptographic RDT&E program is the implementation of requirements in Executive Orders 12333 and 12958 and National Security Decision Directive 145.

Major focus areas in FY11:
Computer Network Defense (CND) - Continue to develop and integrate CND capabilities in support of Common Computing Environment (CCE) and Afloat Core Services (ACS).

Cryptographic (Crypto)/Crypto Modernization (CM) - Continue the Link-22 Modernized Link Level Communications Security, VHF/UHF Wideband Tactical Secure Voice Cryptologic Equipment (VINSON)/Advanced Narrowband Digital Voice Terminal Cryptographic Modernization, and Link-16 CM development efforts, and start the Portable Repair Program, Cooperative Engagement Capability, Digital Modular Radio, Demand Assigned Multiple Access, Secure Voice Over Internet Protocol and

Exhibit R-2, RDT&E Budget Item Justification: PB 2011 Navy	DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	**R-1 ITEM NOMENCLATURE** PE 0303140N: *Information Sys Security Program*

Common Data Link development efforts. Coordinate a CM Plan for Range and Weapons Telemetry as well as Transmission Security with National Security Agency (NSA) and other services.

Electronic Key Management System (EKMS)/Key Management Infrastructure (KMI) - Continue EKMS to KMI transition planning; conduct Navy KMI Initial Operational Test and Evaluation to support NSA Milestone C and Low Rate Initial Production schedule. Begin transition strategy and define requirements for incorporation of other KMI roles into Navy architecture (e.g., Controlling Authority, Command Authority).

B. Program Change Summary ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
Previous President's Budget	33.639	24.226	0.000	0.000	0.000
Current President's Budget	31.828	29.049	25.934	0.000	25.934
Total Adjustments	-1.811	4.823	25.934	0.000	25.934
• Congressional General Reductions		-0.121			
• Congressional Directed Reductions		0.000			
• Congressional Rescissions	0.000	-0.056			
• Congressional Adds		5.000			
• Congressional Directed Transfers		0.000			
• Reprogrammings	-1.693	0.000			
• SBIR/STTR Transfer	-0.118	0.000			
• Program Adjustments	0.000	0.000	25.934	0.000	25.934

Congressional Add Details ($ in Millions, and Includes General Reductions)	FY 2009	FY 2010
Project: 9999: *Congressional Adds*		
Congressional Add: *Universal Description, Discovery and Integration*	4.288	4.979
Congressional Add: *TSG technology accreditation*	2.394	0.000
Congressional Add Subtotals for Project: 9999	6.682	4.979
Congressional Add Totals for all Projects	6.682	4.979

Change Summary Explanation

Schedule:

Exhibit R-2, RDT&E Budget Item Justification: PB 2011 Navy	DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	**R-1 ITEM NOMENCLATURE** PE 0303140N: *Information Sys Security Program*

Computer Network Defense (CND) - Schedule slip for Capability Production Document (CPD) approval, resulting in delay of Inc 2 Milestone C from 3rd Qtr FY10 to 3rd Qtr FY11.

Key Management Infrastructure (KMI) - NSA's KMI Capability Increment 2 (CI-2) MS C schedule delay from 4th Qtr FY10 to 2nd Qtr FY11.

Crypto Modernization - Link-22 MLLC Prototype Award delay from 4th Qtr FY09 to 3rd Qtr FY10. KW-46 Integration testing delay from 4th Qtr FY09 to 2nd Qtr FY11. AN-PYQ-20 (v) (c) (formerly KL-51M) testing and evaluation delayed from 4th Qtr FY09 to 2nd Qtr FY10.

Technical: N/A

FY11 from previous President's Budget is shown as zero because no FY11-15 data was presented in President's Budget 2010.

Exhibit R-2A, RDT&E Project Justification: PB 2011 Navy			DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 0734: *Communications Security R&D*	

COST ($ in Millions)	FY 2009 Actual	FY 2010 Estimate	FY 2011 Base Estimate	FY 2011 OCO Estimate	FY 2011 Total Estimate	FY 2012 Estimate	FY 2013 Estimate	FY 2014 Estimate	FY 2015 Estimate	Cost To Complete	Total Cost
0734: *Communications Security R&D*	25.146	21.879	22.921	0.000	22.921	24.637	25.760	26.630	26.876	Continuing	Continuing
Quantity of RDT&E Articles	0	0	0	0	0	0	0	0	0		

A. Mission Description and Budget Item Justification

The Information Systems Security Program (ISSP) Research Development Test & Evaluation (RDTE) program provides Information Assurance (IA) solutions for the Navy forward deployed, highly mobile information subscriber. FORCEnet relies upon an assured information infrastructure, and the ISSP RDT&E program architects, engineers, and provides the level of robustness consistent with risks faced. The ISSP addresses engineering design, development, modeling, test, and evaluation for the unique IA challenges associated with the highly mobile, dispersed, bandwidth limited, and forward-tactical connected US Navy communications systems.

ISSP RDT&E works closely with the Navy's Information Operations - Exploit (signals intelligence) and Information Operations - Attack (information warfare) communities. ISSP RDT&E developed systems dynamically change the Navy's current information assurance posture, based upon operational indications and warnings. To ensure interoperability, ISSP RDT&E integrates fully with the FORCEnet and maritime cryptologic architectures. ISSP RDT&E developed systems can provide the trigger for offensive warfare activities.

This project includes a rapidly evolving design and application engineering effort to modernize national security-grade (Type-1) cryptographic equipment and ancillaries with state-of-the-art replacements in order to counter evolving and increasingly sophisticated threats. Communication Security (COMSEC) and Transmission Security evolution is from stand-alone dedicated devices to embedded modules incorporating National Security Agency approved cryptographic engines, loaded with the certified algorithms and key, and interconnected via industry-defined interfaces. This includes the DoD Global Information Grid capability requirements document for the development of Content Based Encryption continuing through FY2011.

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 Code of Federal Regulation (CFR) subtitle A sub-chapter C, parts 160- 164, 1999, and the Federal Education Records Privacy Act. ISSP RDT&E efforts must also provide assurance to the broad spectrum of Sensitive-but-Unclassified (SBU) information such as financial, personnel, contractor proprietary, and procurement sensitive.

Exhibit R-2A, RDT&E Project Justification: PB 2011 Navy		DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 0734: *Communications Security R&D*

The ISSP today includes more than legacy COMSEC and network security technology. IA or defensive information operations exist to counter a wide variety of threats. 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.

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-based efforts include developing or applying: (1) new secure voice prototypes; (2) technology for a new family of programmable COMSEC and transmission security modules; (3) security appliances and software for switched and routed networks; (4) technology to interconnect networks of dissimilar classification, known as cross domain solutions; (5) techniques for assuring code and data residing in and transiting the Navy's computing base and information store; and (6) Public Key Infrastructure (PKI) and associated access control technologies (such as smart cards and similar security tokens).

The resulting expertise applies to a wide variety of Navy development programs that integrate IA technology. Unlike traditional single-product development programs, the ISSP RDT&E holds a unique Navy-enterprise responsibility.

The ISSP Research Development Test & Evaluation (RDTE) efforts conclude with certified and accredited systems. This requires (1) assured separation of information levels and user communities, including coalition partners; (2) assurance of the telecommunications infrastructure; (3) assurance of joint user enclaves; (4) assurance of the computing base and information store; and, (5) supporting assurance technologies, including PKI and directories. To ensure interoperability and commercial standards compliance, these efforts often encompass the research, selective evaluation, integration, and test of commercial-off-the-shelf/non-developmental item IA security products. For example, evaluation may include defensible network boundary capabilities such as firewalls, secure routers and switches, guards, virtual private networks, and network intrusion prevention systems.

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 applies 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. The following describes several major ISSP technology areas:

The Navy Secure Voice program assesses technology to provide high grade, secure tactical and strategic voice connectivity.

The Cryptographic Modernization Program provides high assurance and other cryptographic technologies protecting information and telecommunication systems.

The Security Management Infrastructure program develops, evaluates, and applies new emerging technology and enhanced capabilities to the Electronic Key Management System/Key Management Infrastructure 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

Exhibit R-2A, RDT&E Project Justification: PB 2011 Navy		DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 0734: *Communications Security R&D*

portions of the ISSP. This includes the application of PKI and Certificate Management Infrastructure technology, and the development of improved techniques for key and certificate management to support emerging, embedded cryptographic technology.

The Secure Data program focus on architectures, designing, acquiring, demonstrating and integrating the IA technologies into FORCEnet and the Navy Marine Corps Intranet (NMCI). This portion of the ISSP supports delivery of network security engineering expertise needed to support the NMCI, overseas networks, and the Integrated Shipboard Network Systems, along with constituent systems such as Automated Digital Network System, Global Command and Control System - Maritime. These efforts continue to transition to an open architecture in support of the Consolidated Afloat Networks and Enterprise Services Common Computing Environment (CCE) and Afloat Core Services (ACS). It includes activities to:

* Ensure that Navy telecommunications and networks follow a consistent architecture and are protected against denial of service.
* Ensure that all data within Navy Enterprise is protected in accordance with its classification and mission criticality, as required by law.
* Provide the ability to protect from, react to, and restore operations after an intrusion or other catastrophic event.
* Support the Navy Computer Network Defense (CND) Service Provider Enabler by providing IA response to information operation conditions.
* 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, particularly operating systems.
* 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.
* Transition to CCE.
* Transition to ACS.
* Provide a cryptographic (Crypto) 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.

FY 11 Highlights for ISSP and Computer Network Defense:

CND - Continue to develop and integrate CND capabilities in support of CCE and ACS. Continue the development of User Defined Operational Pictures to enhance Security Information Manager tools with adaptive reactive-defense capabilities, improve incident correlation and situation awareness reporting.

Exhibit R-2A, RDT&E Project Justification: PB 2011 Navy		DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 0734: *Communications Security R&D*

Crypto and Crypto Modernization (CM) - Continue development for the Link 22 Modernized Link Level COMSEC, Link 16 CM, Integrated Broadcast Service Multi-Mission Advanced Tactical Terminal, and Cooperative Engagement Capability. Continue Secure Voice (SV) RDTE&E efforts such as Small Business Innovative Research (SBIR) oversight, and research into SV emerging technologies and related technical products, and support to Air Force, lead for VINSON/Advanced Narrowband Digital Voice Terminal Cryptographic Modernization program.

Key Management Infrastructure (KMI) - Provide technical support to National Security Agency for operational assessment, Initial Operational Testing and Evaluation and Full Rate Production decision for KMI.

PKI - Research and develop tools to support Device Certificates. Design and develop PKI expansion to support Global Information Grid identity management and protection requirements onto the Secret Internet Protocol Router Network (SIPRNet).

IA Services (formerly IA Architecture) - Continue to provide security systems engineering support for the development of DoD and Navy IA architectures and the transition of new technologies to address Navy IA challenges. Provide IA risk analysis and recommended risk mitigation strategies for Navy networks and C4I systems.

B. Accomplishments/Planned Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
Computer Network Defense (CND)	8.681	8.055	8.010	0.000	8.010
FY 2009 Accomplishments: Developed computer-network evaluation capabilities to perform real-time metrics of operational compliance with Information Assurance (IA) security controls, Mission Assurance Category, and Data Confidentiality. Evolved system incremental capabilities to advance CND Protect, Monitor, Detect, Analyze, and Respond. Conducted malware research to develop proactive Insider Threat Countermeasures and Application Layer Content Scanning. Began developing User Defined Operational Pictures (UDOP) to enhance Security Information Manager (SIM) tools with active defense capabilities, improved incident correlation and situation awareness reporting. Completed the development of the process to assign asset criticality at the host and application level. Initiated the development of new capabilities to support the selective and automatic reactive settings of the network in accordance with Department of Defense (DoD) Information Operations Condition (INFOCON)					

Exhibit R-2A, RDT&E Project Justification: PB 2011 Navy		DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 0734: *Communications Security R&D*

B. Accomplishments/Planned Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
policies. Addressed the capabilities required to support the INFOCON management at both the Naval Cyber Defense Operation Center (NCDOC) and the Fleet Network Operation Center (NOC) level. *FY 2010 Plans:* Begin the development of the process to assign asset criticality at the host and application level. Advance development of proactive insider threat countermeasures and application layer security risk monitoring. Continue to develop UDOP to enhance SIM tools. Continue research to analyze Information Assurance capabilities to support Early Adopters (EA) systems with selective and autonomic settings on the CND posture as a proactive response to threat attack sensors and vulnerability indications. Address the capabilities required to support CND management of EA platforms from a tiered enclave organizational level, network operations intermediate level, and global enterprise management level. Begin transition to Consolidated Afloat Network Enterprise Services (CANES) with CND capabilities in support of Common Computing Environment (CCE) and Afloat Core Services (ACS). Complete DoD 5000 requirements to achieve Milestone (MS) C. Support developmental testing and determine joint interoperability test requirements for CND Increment 2. *FY 2011 Base Plans:* Continue the development of UDOP to enhance SIM tools with adaptive reactive-defense capabilities, improve incident correlation and situation awareness reporting. Continues the development of CND capabilities in support of Common Computing Environment (CCE) and Afloat Core Services (ACS). Address CND capabilities required to support IA management of virtual machine - virtual network environments from a tiered enclave organizational level, network operations intermediate level, and global enterprise management level. Develop dynamic security defense capabilities, based on the CND posture as an active response to threat attack sensors and vulnerability indications. Complete DoD 5000 requirements to achieve Milestone (MS) C. Support operational assessment (OA) for CND Increment 2.					
Crypto/Crypto Modernization	6.918	7.293	8.658	0.000	8.658

Exhibit R-2A, RDT&E Project Justification: PB 2011 Navy		DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 0734: *Communications Security R&D*

B. Accomplishments/Planned Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
FY 2009 Accomplishments: Provided continued research, evaluation, and prioritization of legacy cryptographic (crypto) products requiring modernization due to parts and algorithm obsolescence as well as the supported system modernization. Continued to support the on-going Department of Defense (DoD) Cryptographic Modernization (Crypto Mod (CM)) efforts and working groups. Continued pre-acquisition, program documentation, and development of CM ways ahead to include Link 22 Modernized Link Level COMSEC (MLLC), LINK 16 CM, KG-3X Increment 2, VINSON/Advanced Narrowband Digital Voice Terminal (ANDVT) Cryptographic Modernization (VACM) and Telemetry (Range and Weapons). Initiated the development of KW-46M in support of the Fleet Submarine Broadcast System (FSBS) and the KL-51M in support of the Submarine Off-line Encryption requirement. Modernization of these crypto devices will provide replacements in accordance with the Joint Chiefs of Staff CM schedule and National Security Agency (NSA) planned decertification, which improves the security of the Navy's data in transit. *FY 2010 Plans:* Continue research, evaluation, and prioritization of cryptographic products such as Demand Assigned Multiple Access (DAMA), portable tactical radios, Single Channel Ground and Airborne Radio System (SINCGARS), Integrated Broadcast Service Multi Mission Advanced Tactical Terminal (IBS MATT), Telemetry, and various embedded devices. Continue coordination with the Information Systems Security Office, Joint Services, and the NSA, including representing the Navy at the Joint Service Crypto Mod Working Group (JSCMWG). Continue identifying strategies to reduce the overall crypto inventory within the Navy to realize long term cost savings. Continue providing consistent Information Assurance (IA) engineering support for the development and integration of CM products. Continue to support the on-going Cryptographic Joint Algorithm Integrated Product Team (IPT). Transition Secure Voice (SV) RDT&E efforts under Crypto Mod Program Office (CMPO), including SV Small Business Innovative Research (SBIR) oversight, Naval Research Laboratory's (NRL) research into SV emerging technologies and related technical products, and the Navy's participation in the Air Force led VACM program (providing documentation review, as well as SV technical, acquisition, logistic, test and					

Exhibit R-2A, RDT&E Project Justification: PB 2011 Navy		DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 0734: *Communications Security R&D*

B. Accomplishments/Planned Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
evaluation support). Continue development of Link 22 MLLC, Link 16 CM, KW- 46M, KG-3X Inc 2 and VACM, while finalizing the development of KL-51M efforts. Continue Crypto voice standardization based on the Variable Data Rate (VDR), Voice Compression Algorithm (VCA). Support Nuclear Command Control and Communications (NC3) Crypto Modernization. *FY 2011 Base Plans:* Continue research, evaluation, and prioritization of cryptographic products. Continue coordination with the Information Systems Security Office, joint services, and the NSA, including representing the Navy at the JSCMWG. Continue identifying strategies to reduce the overall crypto inventory within the Navy to realize long term cost savings. Continue to support the on-going Cryptographic Joint Algorithm IPT. Provide consistent IA engineering support for the development and integration of CM products. Continue development for the Link 16 CM and Link 22 MLLC, IBS MATT, KW-46M, and Cooperative Engagement Capability (CEC). Continue Secure Voice RDT&E efforts such as SBIR oversight, and NRL's research into SV emerging technologies and related technical products, support to Air Force lead VACM program and continue supporting ASD (NII) NC3 CM. Initiate major pre-acquisition and development efforts for Digital Modular Radio (DMR), Demand Assigned Multiple Access (DAMA), Secure Voice Over Internet Protocol (SVoIP) Test & Evaluation (T&E), and Common Data Link (CDL) CM. Coordinate a CM plan for Portable Range and Weapons Telemetry as well as Transmission Security (TRANSEC) with NSA and other services.					
Secure Voice *FY 2009 Accomplishments:* Completed development and integration test of the Secure Communication Interoperability Protocol Inter-working Function (SCIP IWF) for Military Sealift Command (MSC) and Coast Guard ships. Continue the design and development of next generation voice and Secure Voice capabilities for shipboard voice services modernization and consolidation. Continued Small Business Innovative Research (SBIR) phase II R&D efforts.	0.995	0.000	0.000	0.000	0.000

Exhibit R-2A, RDT&E Project Justification: PB 2011 Navy		DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 0734: *Communications Security R&D*

B. Accomplishments/Planned Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
In FY 2010 and out, transition from Secure Voice to the Crypto Modernization Program for VHF/UHF Wideband Tactical Secure Voice Cryptologic Equipment (VINSON)/Advanced Narrowband Digital Voice Terminal (ANDVT) Crypto Mod (VACM) and R&D technology efforts.					
Key Management Infrastructure (KMI/EKMS/PKI) *FY 2009 Accomplishments:* Continued KMI Increment 2 client manager and advanced Key Processor (KP) security testing and certification and accreditation. Continued KMI development support for Advanced Extremely High Frequency (AEHF), Transformational Satellite (TSAT), and Global Information Grid (GIG) requirements for Navy. Researched and integrated Public Key Infrastructure (PKI) device certificates for mobile devices using 802.1x interfaces. Continued security and functionality testing and evaluation of PKI tokens and readers to support Tactical PKI and Homeland Security Presidential Directive (HSPD-12) implementation. Continued to research and develop solutions and tools for signature applications/XML document signing and Public Key Enabled (PKE). In FY 2010 and out, transition overarching KMI efforts to define Electronic Key Management System (EKMS), PKI, and KMI technology areas.	4.043	0.000	0.000	0.000	0.000
Key Management Infrastructure (KMI) *FY 2010 Plans:* Transitioned from Key Management Infrastructure (KMI) to define Electronic Key Management System (EKMS), Public Key Infrastructure (PKI), and KMI technology areas.Begin finalizing the Department of the Navy (DoN) KMI architecture and roll out strategy for deployment. Install KMI Manager Client/ Advanced Key Processors (MGC/AKPs) at selected pilot sites in support of operational assessment and initial operational test and evaluation. Identify any issues pertaining to transition from EKMS to KMI. Provide supporting information to Navy Acquisition Decision Memorandum (ADM) for full rate production/fielding within the Navy for Increment (Inc) 2. Support engineering and development efforts	0.000	2.477	2.549	0.000	2.549

Exhibit R-2A, RDT&E Project Justification: PB 2011 Navy		DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 0734: *Communications Security R&D*

B. Accomplishments/Planned Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
for Inc 2. Continue engineering efforts for Navy transition and test planning for KMI Inc 2 client and Advanced Key Processor (KP). Develop Navy implementation plan for KMI for Inc 2 to support Navy Programs of Record. Complete development of Tactical Key Loader (TKL), complete First Article testing and National Security Agency (NSA) Certification testing. Transition to production. Provide engineering support to EKMS software versions for possible incorporation prior to the delivery of KMI. *FY 2011 Base Plans:* Provide technical support to National Security Agency (NSA) for Operational Assessment (OA), Initial Operational Testing and Evaluation (IOT&E) and Full Rate Production (FRP) decision. Continue to support engineering and development efforts for KMI Inc 2 or incorporation into Navy architectures and networks. Support Navy input to KMI Increment 3 Capability Development Document (CDD) requirements. Begin transition strategy/define requirements for incorporation of other KMI roles into Navy architecture (Controlling Authority (CONAUTH), Command Authority (CMDAUTH), etc.).					
Public Key Infrastructure (PKI) *FY 2010 Plans:* Transitioned from overarching Key Management Infrastructure (KMI) to define Electronic Key Management System (EKMS), Public Key Infrastructure (PKI) and KMI technology areas. Initiate security and functionality testing and evaluation of multi-domain tokens, readers and middleware for the Non-Classified Internet Protocol Router (NIPR), Secret Internet Protocol Router (SIPR), and Tactical PKI. Continue research and development of solutions to resolve technical challenges and the tools required for continued deployment of Navy, non-Navy, Marine Corps Internet (NMCI)/ Cryptographic Log On (CLO) and Navy Certificate Validation Infrastructure/Online Certificate Status Protocol (NCVI/OCSP) Afloat. Research and develop tools to support Device (non-human) Certificates. Continue security and functionality testing and evaluation of PKI tokens and readers to support Tactical PKI and Homeland Security Presidential Directive-12 (HSPD-12) implementation. Support systems engineering during the integration process and the analysis/evaluation of new application updates including new Operating Systems (OSs) (Windows and non-Windows) into Navy	0.000	0.736	0.769	0.000	0.769

Exhibit R-2A, RDT&E Project Justification: PB 2011 Navy		DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 0734: *Communications Security R&D*

B. Accomplishments/Planned Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
PKI environments. Provide for evaluation of Commercial-Off-The-Shelf (COTS) products that can support coalition information sharing. Initiate test and evaluation of HSPD-12 token and middleware as part of the transition to stronger algorithms. Research and develop tools to support PKI with Internet Protocol Version 6 (IPv6) and Suite B implementation. *FY 2011 Base Plans:* Continue security and functionality testing and evaluation of PKI tokens, readers and middleware for SIPR and Tactical PKI. Research and develop tools to support Device (non-human) Certificates. Support systems engineering during the integration process and the analysis/evaluation of new application updates including new OS (Windows and non-Windows) into Navy PKI environments. Provide for evaluation of COTS products that can support coalition information sharing. Design and develop PKI expansion to support Global Information Grid (GIG) Identity management and protection requirements onto the Secret Internet Protocol Router Network (SIPRNet). Evaluate Automated on-line network device (eg., workstations, routers, switches etc.) certificate issuance infrastructure. Complete Department of Defense (DoD) 5000 requirements to achieve Milestone C.					
Electronic Key Management System (EKMS) *FY 2010 Plans:* Transitioned from overarching Key Management Infrastructure (KMI) to define EKMS, Public Key Infrastructure (PKI) and KMI technology areas. Continue to define EKMS technology gaps in preparation to the transition to KMI. Identify technical solutions for EKMS sustainment until KMI CI-2. Begin Tactical Key Loader (TKL) capability increment refinement. *FY 2011 Base Plans:* Continue EKMS systems engineering to support technology issues as a result of the introduction of KMI into the dual mode environment.	0.000	0.427	0.183	0.000	0.183
Information Assurance (IA) Services (formerly IA Architecture)	2.252	2.891	2.752	0.000	2.752

Exhibit R-2A, RDT&E Project Justification: PB 2011 Navy		DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 0734: *Communications Security R&D*

B. Accomplishments/Planned Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
FY 2009 Accomplishments: Continued to provide security systems engineering support for the development of DoD and Navy IA architectures and the transition of new technologies to address Navy IA challenges. Supported the ongoing security design and integration of IA Components into initiatives such as FORCEnet via a coordinated and Computer Network Defense in Depth (CNDiD) strategy. Provided risk analysis and recommended risk mitigation strategies for Navy critical networks and C4I systems. Coordinated with the Navy acquisition community to ensure IA requirements are identified and addressed within the development cycles for emerging Navy network and C4I capabilities. Provided IA engineering for development of Wireless Networks and Personal Digital Assistant (PDA) security readiness of Naval wireless networks and mobile computing devices. Continued to evaluate products for security issues and develop guidance and procedures. *FY 2010 Plans:* Continue to provide security systems engineering support for the development of DoD and DoN IA architectures and the transition of new technologies to address Navy IA challenges. Support the ongoing development of the Navy IA Master Plan and coordinate IA activities across the virtual System Command (SYSCOM) via the IA Technical Authority (TA) to ensure the security design and integration of CNDiD products and services is consistent across the Navy for major initiatives such as the future afloat, ashore, and Outside the Continental United States (OCONUS) networks. Provide IA risk analysis and recommended risk mitigation strategies for Navy critical networks and C4I systems. Coordinate with the Navy acquisition community to ensure IA requirements are identified and addressed within the development cycles for emerging Navy network and C4I capabilities. Provide IA engineering for development of Wireless Networks and PDA security readiness of Naval wireless networks and mobile computing devices. Continue to evaluate products for security issues and develop guidance and procedures for the design and integration of risk mitigation strategies via appropriate IA controls.					

Exhibit R-2A, RDT&E Project Justification: PB 2011 Navy		DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 0734: *Communications Security R&D*

B. Accomplishments/Planned Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
FY 2011 Base Plans: Continue to provide security systems engineering support for the development of DoD and DoN IA architectures and the transition of new technologies to address Navy IA challenges. Provide updates to the Navy IA Master Plan that reflect emerging priorities and address Navy specific threats. Coordinate IA activities across the virtual SYSCOM via the IA Technical Authority (TA) to ensure the security design and integration of CNDiD products and services is consistent across the Navy for major initiatives such as the future afloat, ashore, and OCONUS networks. Provide IA risk analysis and recommended risk mitigation strategies for Navy critical networks and C4I systems. Coordinate with the Navy acquisition community to ensure IA requirements are identified and addressed within the development cycles for emerging Navy network and C4I capabilities. Continue to evaluate products for security issues and develop guidance and procedures for the design and integration of risk mitigation strategies via appropriate IA controls.					
Software and Systems Research *FY 2009 Accomplishments:* Completed the development of the wireless technology to meet high assurance requirements. Placed technology in selected Navy and Marine Corps sites for assessment. Used feedback to improve the capabilities of the technology to better meet the mission requirements. Continued development of an information sharing architecture that addresses data integrity, confidentiality and policy management throughout networks of varying classification levels. Evaluated security services of the framework that support confidentiality, integrity and authentication across security domains, as well as enforces the mission security policy. Used assessment and operational feedback to improve the framework and security services. Enhanced framework to address survivability and hardening. Developed technology that protects the framework from attacks, assesses the attack, and responds appropriately to enable the framework to reconstitute and provide the requisite capabilities/services. Ensured architecture/framework evolves to provide proper protection as technology, Department of Defense (DoD) missions, and the threat all evolve. Initiated development of modernized attack sensing and	2.127	0.000	0.000	0.000	0.000

Exhibit R-2A, RDT&E Project Justification: PB 2011 Navy		DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 0734: *Communications Security R&D*

B. Accomplishments/Planned Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
warning mechanisms based on new algorithms and data mining concepts, and response capabilities for the architecture/framework. Continued development of technology and tools to ensure the unique security and performance requirements of tactical systems, including those operating at various security levels are addressed. Began assessing the tools and technology in representative operational environments. Used feedback to improve the tools and technology. Continued systems security engineering, certification and accreditation support for high-confidence naval information system and ensure certification and accreditation approaches are consistent with Navy and DoD requirements. Beginning in FY10, funding was realigned to project 3230.					
Acquisition Workforce Fund *FY 2009 Accomplishments:* Funded Acquisition Workforce Fund.	0.130	0.000	0.000	0.000	0.000
Accomplishments/Planned Programs Subtotals	25.146	21.879	22.921	0.000	22.921

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total	FY 2012	FY 2013	FY 2014	FY 2015	Cost To Complete	Total Cost
• OPN/3415: *Info Sys Security Program (ISSP)*	100.725	110.214	120.529	0.000	120.529	125.713	129.595	137.727	150.491	0.000	874.994

D. Acquisition Strategy

EKMS Phase V - ISSP Electronic Key Management System (EKMS) program is linked to the National Security Agency's (NSA's) strategy in implementing EKMS in evolutionary phases and migrating to Key Management Infrastructure (KMI). NSA is the lead for the joint EKMS effort and has been developing and certifying EKMS devices and capabilities in an evolutionary approach. EKMS Phase V is a major component evolving to KMI Capability Increment (CI-2). KMI is a Major Automated Information System (MAIS) program assigned to NSA. Therefore, it is crucial that the Research and Development efforts of EKMS coincide with those of KMI. Navy's EKMS requires Research, Development, Test and Evaluation (RDT&E) funding over the Future Years Defense Program (FYDP) to ensure the Navy infrastructure

Exhibit R-2A, RDT&E Project Justification: PB 2011 Navy		DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 0734: *Communications Security R&D*

evolves with the EKMS phases, supports additional devices certified by NSA and supports the migration of EKMS to KMI CI-2. This will require modifications to the Navy EKMS architecture including the Local Management Device and associated software. These efforts require close work with NSA and the other services to ensure no impact on current operations and minimum impact on EKMS Phase 5 as it evolves to KMI CI-2. NSA certified Commercial-Off-The-Shelf/Government-Off-The-Shelf (COTS/GOTS) devices are procured to support Navy requirements. The EKMS Phase V program will utilize existing competitively awarded NSA and Navy contracts for development and implementation of type 1 certified COTS/GOTS devices for initial production phases, with plans to initiate innovative contracting methods and types consistent with current policies to reduce cost and streamline the integration, installation, logistics and training efforts.

Key Management Infrastructure (KMI) - KMI is the next generation EKMS system that is net centric in nature, providing the infrastructure for management, ordering and distribution of key material as well as directly supporting the key requirements of all Crypto modernization efforts. Navy will continue to provide and refine Navy unique requirements into the NSA KMI CI-2 Capability Development Documents (CDD). In parallel, continue to define Navy operational architecture and requirements for roll out of this new capability in the Fiscal Year 2011.

Cryptographic Modernization (CM) - The procurement and fielding the Modernized Crypto devices, such as the KG-3X Increment 2, KG-45A, AN-PYQ-20(v)(c) (formerly KL-51M), KW-46M, VHF/UHF Wideband Tactical Secure Voice Cryptologic Equipment (VINSON)/Advanced Narrowband Digital Voice Terminal (ANDVT) Cryptographic Modernization (VACM), and Telemetry will provide replacements of legacy crypto in accordance with the Chairman of the Joint Chiefs of Staff (CJCS) mandate (CJCS Instruction 6510) as well as the NSA's planned decertification, which improves the security of the Navy's data in transit.

E. Performance Metrics

(KMI):
~ Install 100% of KMI Manager Client/Advanced Key Processor (MGC/AKPs) at selected pilot sites in support of operational assessment.
~ Conduct Navy testing across 100% of relevant network (i.e., NMCI/NGEN, ISNS/CANES, BLII ONEnet).
* Complete 100% of engineering efforts for Navy transition and test planning for the KMI CI-2 Inc 2 clients and Advanced Key Processor (KP) to ensure successful Navy transition to KMI in accordance with EKMS end of life priorities and objectives.
* Complete development and transition to production of the Tactical Key Loader (TKL) to achieve assuring 100% acceptance of First Article and NSA Certification testing and determination of suitability for production.

Cryptographic Modernization (CM):
* Meet 100% of TOP SECRET (TS) and SECRET Chairman of Joint Chiefs of Staff Instruction (CJCSI 6510) cryptographic modernization requirements within the current Future Years Defense Plan (FYDP) by conducting a gap analysis and building a CM Roadmap and Implementation Plan to allow the Navy NETWAR FORCEnet Enterprise to establish operational priorities based on risk assessments.
* Meet 100% of TS and SECRET CJCSI 6510 by fielding modern cryptographic devices or request "recertification" via the Joint Staff Military Communications-Electronics Board (MCEB).

Exhibit R-2A, RDT&E Project Justification: PB 2011 Navy		DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 0734: *Communications Security R&D*

* Increase the functionality cryptographic devices by replacing 2 legacy cryptographic devices with 1 modern device where possible and identify and implement modern small form factor, multi channel cryptos. (e.g., KIV-7M replacing KIV-7HS, KIV-7HSB, KG94, KWR-46, KL-51, etc.)

Computer Network Defense (CND):
* Provide the ability to protect from, react to, and restore operations after an intrusion or other catastrophic event through validated Contingency Plans (CPs) for 100% of CND systems, and validation of a Continuity of Operations Plan (COOP) solution for the Navy CND Service Provider.
* Develop dynamic security defense capabilities, based on the CND posture as an active response to threat attack sensors and vulnerability indications to provide adequate defenses against subversive acts of trusted people and systems, both internal and external, by integration of anomaly-based detection solutions into the design solutions for 100% of authorized Navy enclave types.
* Defend against the unauthorized use of a host or application, particularly operating systems, by development and/of integration of host-based intrusion prevention system design solutions for 100% of authorized Navy enclave types.

Information Assurance (IA) Services (formerly IA Architecture):
* Ensure 100% interoperability and application of commercial standards compliance for ISSP products by researching and conducting selective evaluations, to integrate and test of commercial-off-the-shelf/Non-Developmental Item (NDI) Information Assurance (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 Prevention Systems (IPS).
* Provide 100% of the services delineated in OPNAVINST 5239.1C by serving as the Navy's IA technical lead by developing IA risk analysis and recommended risk mitigation strategies for critical Navy networks and C4I systems.
* Coordinate IA activities across the Navy Enterprise via the IA Technical Authority (TA) to measure effectiveness of Navy networks and ensure the security design and integration of Computer Network Defense in Depth (CNDiD) products and services is 100% interoperable and operationally acceptable across the Navy for major initiatives such as the future afloat, ashore, and Outside Continental United States (OCONUS) networks.

Exhibit R-3, RDT&E Project Cost Analysis: PB 2011 Navy		DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 0734: *Communications Security R&D*

Product Development ($ in Millions)

				FY 2010		FY 2011 Base		FY 2011 OCO		FY 2011 Total			
Cost Category Item	Contract Method & Type	Performing Activity & Location	Total Prior Years Cost	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Cost To Complete	Total Cost	Target Value of Contract
Primary Hardware Development	C/CPFF	VIASAT Carlsbad, CA	7.282	0.000		0.000		0.000		0.000	0.000	7.282	Continuing
Primary Hardware Development	MIPR	MITRE San Diego, CA	5.522	0.000		0.000		0.000		0.000	0.000	5.522	Continuing
Primary Hardware Development (PY)	WR	Various Various	88.607	0.000		0.000		0.000		0.000	0.000	88.607	Continuing
Systems Engineering	WR	NUWC Newport, RI	0.000	0.608	Feb 2010	0.000	Oct 2010	0.000		0.000	0.000	0.608	Continuing
Systems Engineering	WR	SSC PAC/LANT San Diego, CA/ Charleston, SC	0.000	11.105	Nov 2009	11.605	Oct 2010	0.000		11.605	0.000	22.710	Continuing
Systems Engineering	WR	NRL Washington DC	0.000	0.300	Feb 2010	0.300	Oct 2010	0.000		0.300	0.000	0.600	Continuing
Systems Engineering	WR	FNMOC Monterey, CA	0.000	0.240	Feb 2010	0.240	Oct 2010	0.000		0.240	0.000	0.480	Continuing
Primary Hardware Development	WR	SSC PAC San Diego	0.000	1.264	Feb 2010	1.290	Oct 2010	0.000		1.290	0.000	2.554	Continuing
Primary Hardware Development	WR	NRL Washington DC	0.000	0.480	Feb 2010	0.490	Oct 2010	0.000		0.490	0.000	0.970	Continuing
Primary Hardware Development	WR	Various Various	0.000	0.725	Feb 2010	0.000		0.000		0.000	0.000	0.725	Continuing
		Subtotal	101.411	14.722		13.925		0.000		13.925	0.000	130.058	

Remarks

Exhibit R-3, RDT&E Project Cost Analysis: PB 2011 Navy			DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 0734: *Communications Security R&D*	

Support ($ in Millions)

				FY 2010		FY 2011 Base		FY 2011 OCO		FY 2011 Total			
Cost Category Item	Contract Method & Type	Performing Activity & Location	Total Prior Years Cost	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Cost To Complete	Total Cost	Target Value of Contract
Software Development	C/CPAF	SAIC San Diego, CA	32.877	0.000		0.000		0.000		0.000	0.000	32.877	Continuing
Software Development	WR	NRL Washington, D.C.	3.150	1.437	Jan 2010	1.705	Nov 2010	0.000		1.705	0.000	6.292	Continuing
Software Development	WR	SSC PAC/LANT San Diego, CA and Charleston, SC	3.625	3.094	Jan 2010	4.310	Nov 2010	0.000		4.310	0.000	11.029	Continuing
Software Development (Note 1)	WR	NRL Washington, D.C.	12.904	0.000		0.000		0.000		0.000	0.000	12.904	Continuing
Software	C/FP	Not Specified Not Specified	0.000	0.000		0.000		0.000		0.000	0.000	0.000	Continuing
		Subtotal	52.556	4.531		6.015		0.000		6.015	0.000	63.102	

Remarks

Note 1: Funding realigned to Project 3230 beginning FY10

Test and Evaluation ($ in Millions)

				FY 2010		FY 2011 Base		FY 2011 OCO		FY 2011 Total			
Cost Category Item	Contract Method & Type	Performing Activity & Location	Total Prior Years Cost	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Cost To Complete	Total Cost	Target Value of Contract
Developmental Test	WR	SSC PAC San Diego, CA	34.628	0.095	Dec 2009	0.055	Oct 2010	0.000		0.055	0.000	34.778	Continuing

Exhibit R-3, RDT&E Project Cost Analysis: PB 2011 Navy		DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 0734: *Communications Security R&D*

Test and Evaluation ($ in Millions)

				FY 2010		FY 2011 Base		FY 2011 OCO		FY 2011 Total			
Cost Category Item	Contract Method & Type	Performing Activity & Location	Total Prior Years Cost	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Cost To Complete	Total Cost	Target Value of Contract
Developmental Test	WR	NUWC Newport, RI	0.000	0.263	Feb 2010	0.360	Oct 2010	0.000		0.360	0.000	0.623	Continuing
Operational Test	WR	OPTEVFOR Norfolk, VA	0.000	0.080	Feb 2010	0.045	Oct 2010	0.000		0.045	0.000	0.125	Continuing
		Subtotal	34.628	0.438		0.460		0.000		0.460	0.000	35.526	

Remarks

Management Services ($ in Millions)

				FY 2010		FY 2011 Base		FY 2011 OCO		FY 2011 Total			
Cost Category Item	Contract Method & Type	Performing Activity & Location	Total Prior Years Cost	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Cost To Complete	Total Cost	Target Value of Contract
Program Management	C/CPFF	Various Various	15.579	1.685	Oct 2009	1.941	Oct 2010	0.000		1.941	0.000	19.205	Continuing
Program Management	WR	SSC PAC San Diego, CA	0.130	0.503	Nov 2009	0.580	Nov 2010	0.000		0.580	0.000	1.213	Continuing
		Subtotal	15.709	2.188		2.521		0.000		2.521	0.000	20.418	

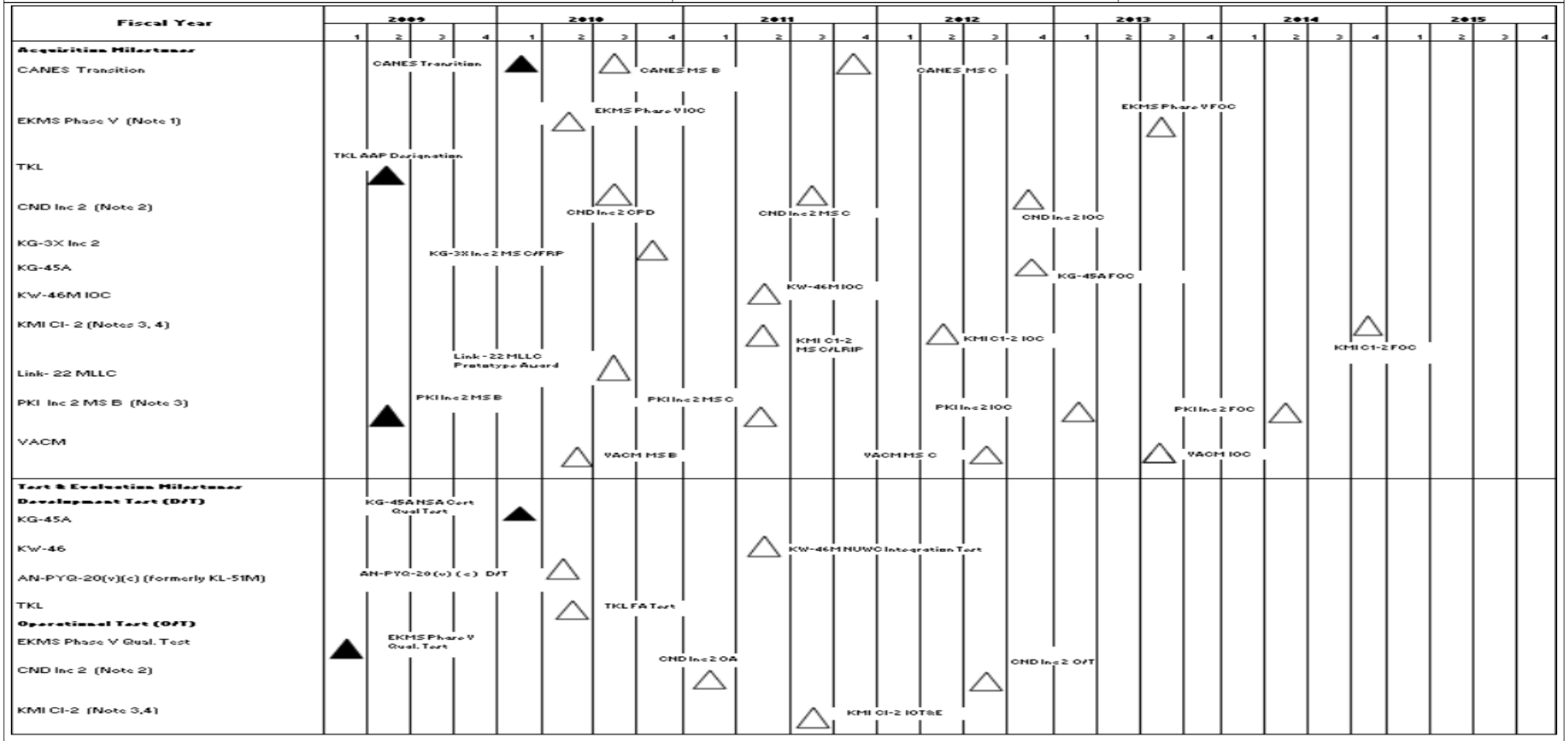
Remarks

Exhibit R-3, RDT&E Project Cost Analysis: PB 2011 Navy			DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 0734: *Communications Security R&D*	

	Total Prior Years Cost	FY 2010		FY 2011 Base		FY 2011 OCO		FY 2011 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	204.304	21.879		22.921		0.000		22.921	0.000	249.104	

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2011 Navy		DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	**R-1 ITEM NOMENCLATURE** PE 0303140N: *Information Sys Security Program*	**PROJECT** 0734: *Communications Security R&D*



Note 1: EKMS V FOC slip due to NSA software release delay.
Note 2: CND Inc 2 Delay due to Capability Production Decision (CPD) comment adjudication and review process.
Note 3: KMI C1-2 & PKI milestones reflect NSA Schedule.
Note 4: KMI CI-2 slip due to NSA development delay.

Exhibit R-4, RDT&E Schedule Profile: PB 2011 Navy		DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 0734: *Communications Security R&D*

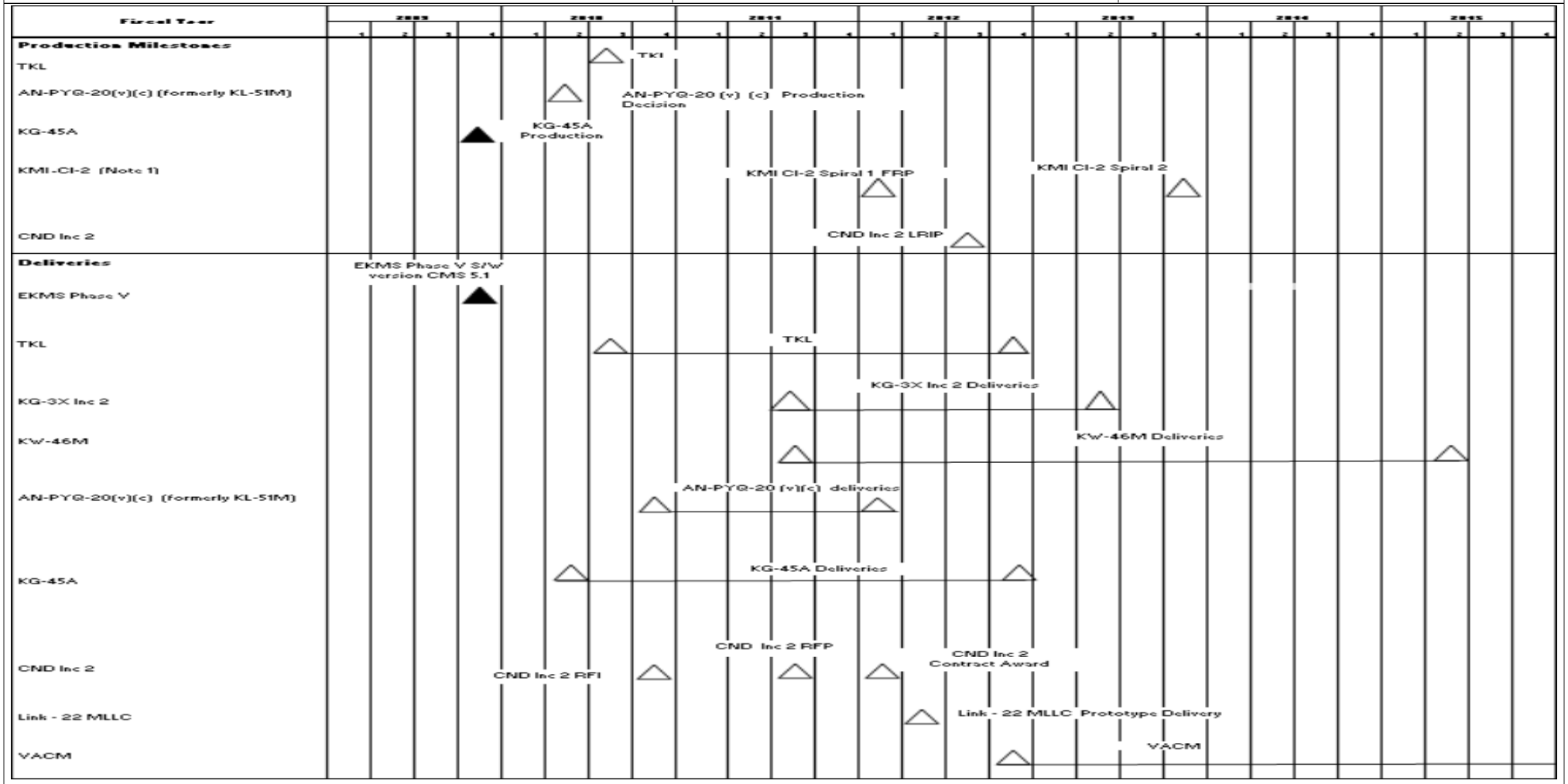


Exhibit R-4A, RDT&E Schedule Details: PB 2011 Navy		DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	**R-1 ITEM NOMENCLATURE** PE 0303140N: *Information Sys Security Program*	**PROJECT** 0734: *Communications Security R&D*

Schedule Details

	Start		End	
Event	**Quarter**	**Year**	**Quarter**	**Year**
CANES Transition	1	2010	1	2010
CANES MS B	3	2010	3	2010
CANES MS C	4	2011	4	2011
EKMS Phase V IOC	2	2010	2	2010
EKMS Phase V FOC	3	2013	3	2013
TKL AAP Designation	2	2009	2	2009
CND Inc 2 CPD	3	2010	3	2010
CND Inc 2 MS C	3	2011	3	2011
CND Inc 2 IOC	4	2012	4	2012
KG-3X Inc 2 MS C/FRP	4	2010	4	2010
KG-45A FOC	4	2012	4	2012
KW-46M IOC	2	2011	2	2011
KMI CI-2 MS C/LRIP	2	2011	2	2011
KMI CI-2 IOC	2	2012	2	2012
KMI CI-2 FOC	4	2014	4	2014
Link 22 MLLC Prototype Award	3	2010	3	2010
PKI Inc 2 MS B	2	2009	2	2009
PKI Inc 2 MS C	2	2011	2	2011

Exhibit R-4A, RDT&E Schedule Details: PB 2011 Navy		DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 0734: *Communications Security R&D*

	Start		End	
Event	Quarter	Year	Quarter	Year
PKI Inc 2 IOC	1	2013	1	2013
PKI Inc 2 FOC	2	2014	2	2014
VACM MS B	2	2010	2	2010
VACM MS C	3	2012	3	2012
VACM IOC	3	2013	3	2013
KG-45A NSA Cert Qual test	1	2010	1	2010
KW-46 NUWC Integration Testing	2	2011	2	2011
AN-PYQ-20(v) (c) (formerly KL-51M) Development Test	2	2010	2	2010
TKL FA Test	2	2010	2	2010
EKMS Phase V Qualification Test	1	2009	1	2009
CND Inc 2 O/A	1	2011	1	2011
CND Inc 2 O/T	3	2012	3	2012
KMI CI-2 IOT&E	3	2011	3	2011
TKL FRP	3	2010	3	2010
AN-PYQ-20(v) (c) formerly KL-51M Production Decision	2	2010	2	2010
KG-45A Production Decision	4	2009	4	2009
KMI CI-2 Spiral 1 FRP	1	2012	1	2012
KMI CI-2 Spiral 2 FRP	4	2013	4	2013
CND Inc 2 LRIP	3	2012	3	2012
EKMS Phase V S/W Delivery LCMS 5.1	4	2009	4	2009

Exhibit R-4A, RDT&E Schedule Details: PB 2011 Navy		DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 0734: *Communications Security R&D*

	Start		End	
Event	Quarter	Year	Quarter	Year
TKL Deliveries	3	2010	4	2012
KG-3X Inc 2 Deliveries	3	2011	2	2013
KW-46M Deliveries	3	2011	2	2015
AN-PYQ-20(v) (c) (formerly KL-51M) Deliveries	4	2010	1	2012
KG-45A Deliveries	2	2010	4	2012
CND Inc 2 RFI	4	2010	4	2010
CND Inc 2 RFP	3	2011	3	2011
CND Inc 2 Contract Award	1	2012	1	2012
Link 22 MLLC Prototype Delivery	2	2012	2	2012
VACM	4	2012	4	2015

Exhibit R-2A, RDT&E Project Justification: PB 2011 Navy			DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 3230: *Information Assurance*	

COST ($ in Millions)	FY 2009 Actual	FY 2010 Estimate	FY 2011 Base Estimate	FY 2011 OCO Estimate	FY 2011 Total Estimate	FY 2012 Estimate	FY 2013 Estimate	FY 2014 Estimate	FY 2015 Estimate	Cost To Complete	Total Cost
3230: *Information Assurance*	0.000	2.191	3.013	0.000	3.013	3.023	3.098	3.179	3.219	Continuing	Continuing
Quantity of RDT&E Articles	0	0	0	0	0	0	0	0	0		

A. Mission Description and Budget Item Justification

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

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

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

The program will develop common architectural frameworks that facilitate integration of network security capabilities, enable effective seamless interoperation, and contribute to a common consistent picture of the networked environment with respect to information assurance and security. This effort will address the need for a

Exhibit R-2A, RDT&E Project Justification: PB 2011 Navy		DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 3230: *Information Assurance*

common operational picture for Information Assurance (IA), as well as assessment of security technology critical to the success of the mission. Initiate requirements definition for situation awareness capabilities to support computer network defense in highly distributed, homogeneous, and heterogeneous networks including mobile and embedded networked devices. This effort also includes the architectural definition of situational awareness and visualization capabilities to support active computer network defense and support underlying data mining and correlation tools. This includes addressing the capability to remotely manage and securely control the configurations of network security components to implement changes in real time or near real time. Initiate requirements definition for secure coalition data exchange and interoperation among security levels and classifications. Ensure approaches address various security level technologies as well as emerging architectural methods of providing interoperability across different security levels. Examine multi-level aware applications and technologies including databases, web browsers, routers/switches, etc. Initiate infrastructure protection efforts as the Navy develops network centric architectures and warfare concepts, ensuring an evolutionary development of security architectures and products for IA that addresses Navy infrastructure requirements. Ensure the architectures evolve to provide proper protection as technology, DoD missions, and the threat all evolve. Include defensive protections as well as intrusion monitoring (sensors), warning mechanisms, and response capabilities in the architecture. Ensure the unique security and performance requirements of tactical systems, including those operating various security levels are addressed. Initiate the efforts to conceptualize new network centric warfare technology to protect our assets, such as secure network gateways and routers, and components and tools that improve the survivability of Navy networks. Provide systems security engineering, certification and accreditation support for high-confidence naval information system and ensure certification and accreditation approaches are consistent with Navy and DoD requirements.

B. Accomplishments/Planned Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
Information Assurance	0.000	2.191	3.013	0.000	3.013
FY 2010 Plans: Complete the development of the information sharing architecture that addresses data integrity, confidentiality and policy management throughout networks of varying classification levels. Evaluate the security services of the architecture and adjust to ensure mission operations are supported. Continue the development of technology that protects, assesses and responds to attacks of the infrastructure architecture and provide reconstitution capabilities/services. Continue the development of modernized attack sensing and warning mechanisms based on new detection algorithms and data mining concepts, and response capabilities for the architecture. Complete the development of technology and tools to ensure the unique security and performance requirements of tactical wireless communication systems are addressed. Initiate the development of a new high assurance boundary controller to protect Navy and Marine Corps data and resources from attack. Provide security services					

Exhibit R-2A, RDT&E Project Justification: PB 2011 Navy		DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 3230: *Information Assurance*

B. Accomplishments/Planned Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
including encryption and data malware analysis in the boundary controller. Initiate the development of a high-assurance computing environment for Navy and Marine Corps use based on trusted platform technology. Develop the appropriate core code, security messages and assurance functions required. Initiate the development of new key and enabling technologies, management tools, and capabilities to address specific Navy and Marine Corps needs. Ensure the new solutions address distribution and management of data and other requisite material. Continue systems security engineering, certification and accreditation support for high-confidence naval information systems and ensure certification and accreditation approaches are consistent with Navy and DoD requirements. *FY 2011 Base Plans:* Complete the development of the technology that protects, assesses and responds to attacks of the infrastructure framework and provide reconstitution capabilities/services. Assess in representative operational environments. Complete the development of modernized attack sensing and warning mechanisms based on new detection algorithms and data mining concepts, and response capabilities for the architecture/framework. Continue the development of a new high assurance boundary controller to protect Navy and Marine Corps data and resources from attack. Ensure the security services include, at a minimum, encryption and data malware analysis in the boundary controller as well as the ability to adjust routing of communications based on network stress levels. Continue the development of a high-assurance computing environment for Navy and Marine Corps use based on trusted platform technology. Continue the development of the appropriate core code, security messages and assurance functions required. Continue the development of new key and enabling technologies, management tools, and capabilities to address specific Navy and Marine Corps needs. Ensure the new solutions address distribution and management in bandwidth limited environments and tactical environments. Initiate the development of mobile security techniques that introduce time and location-based security parameters for geo-location and asset protection and management. Address the specific issues of geo-location and mapping in Global Positioning System (GPS) constrained environments. Continue systems security engineering, certification and accreditation					

Exhibit R-2A, RDT&E Project Justification: PB 2011 Navy		DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 3230: *Information Assurance*

B. Accomplishments/Planned Program ($ in Millions)

	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total
support for high-confidence naval information systems and ensure certification and accreditation approaches are consistent with Navy and DoD requirements.					
Accomplishments/Planned Programs Subtotals	0.000	2.191	3.013	0.000	3.013

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2009	FY 2010	FY 2011 Base	FY 2011 OCO	FY 2011 Total	FY 2012	FY 2013	FY 2014	FY 2015	Cost To Complete	Total Cost
• OPN/3415: *Info Sys Security Program (ISSP)*	100.725	110.214	120.529	0.000	120.529	125.713	129.595	137.727	150.491	Continuing	Continuing

D. Acquisition Strategy

N/A

E. Performance Metrics

Cryptographic Modernization (CM):
. Develop new emerging cryptographic technology for airborne applications by reducing the form-factor by 30%, and provide multi-channel, field reprogrammable cryptos that can be reprogrammed with algorithms in less than 1 minute. Increase throughput capabilities by 50% to meet high speed networks and develop new network-aware cryptographic technology to maximize bandwidth usage.

Computer Network Defense (CND):
. Develop new algorithms to provide real-time detection of nation state malware attacks against Department of Navy networks. Detection algorithms shall be used by both host-based sensors and network sensors to provide a 100% detection of known/programmed malware.
. Develop new malware analysis technology to decrease the analysis time by 50%, thus providing support for zero-day attacks.

Wireless Security:
. Develop new wireless signal discovery technology to increase detection by 30% and increase the bandwidth sensitivity by 20% thus allowing analysis and protection of Department of Navy assets used in the wider emerging wireless spectrum.

Exhibit R-3, RDT&E Project Cost Analysis: PB 2011 Navy		DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 3230: *Information Assurance*

Support ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Total Prior Years Cost	FY 2010 Cost	FY 2010 Award Date	FY 2011 Base Cost	FY 2011 Base Award Date	FY 2011 OCO Cost	FY 2011 OCO Award Date	FY 2011 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Development Support	WR	NRL Washington, DC	0.000	2.191	Nov 2009	3.013	Nov 2010	0.000		3.013	Continuing	Continuing	Continuing
		Subtotal	0.000	2.191		3.013		0.000		3.013			

Remarks

	Total Prior Years Cost	FY 2010		FY 2011 Base		FY 2011 OCO		FY 2011 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	0.000	2.191		3.013		0.000		3.013			

Remarks

Exhibit R-2A, RDT&E Project Justification: PB 2011 Navy			DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 9999: *Congressional Adds*	

COST ($ in Millions)	FY 2009 Actual	FY 2010 Estimate	FY 2011 Base Estimate	FY 2011 OCO Estimate	FY 2011 Total Estimate	FY 2012 Estimate	FY 2013 Estimate	FY 2014 Estimate	FY 2015 Estimate	Cost To Complete	Total Cost
9999: *Congressional Adds*	6.682	4.979	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	24.598
Quantity of RDT&E Articles	0	0	0	0	0	0	0	0	0		

A. Mission Description and Budget Item Justification

Congressional Adds.

B. Accomplishments/Planned Program ($ in Millions)

	FY 2009	FY 2010
Congressional Add: Universal Description, Discovery and Integration *FY 2009 Accomplishments:* Continued systems engineering to cover continued interoperability requirements for the architecture which demand a common security model to be established. Continued engineering implementation and warfighter/military utility assessment, risk reduction, and operational demonstration. Implemented a prototype trusted discovery technology to demonstrate capabilities for integration in a high security, service orientated architecture environment. Began development of software design, functional and security test plans. *FY 2010 Plans:* Continue systems engineering to cover continued interoperability requirements for the architecture which demand a common security model to be established. Continue engineering implementation and warfighter/military utility assessment, risk reduction, and operational demonstration. Continue development of software design, functional and security test plans.	4.288	4.979
Congressional Add: TSG technology accreditation	2.394	0.000

Exhibit R-2A, RDT&E Project Justification: PB 2011 Navy		DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 9999: *Congressional Adds*

B. Accomplishments/Planned Program ($ in Millions)

	FY 2009	FY 2010
FY 2009 Accomplishments: Trans Enterprise Services Grid (TSG) Technology Accreditation (TA): Developed a capability within the Information Systems Security Program's (ISSP's) Computer Network Defense (CND) program. This work focused on the Vulnerability Remediation Asset Management (VRAM) program and effectively sending and receiving Secure Configuration Compliance Validation Initiative (SCCVI) data generated by Retina scans between the ship and Fleet Numeric Mission Operations Center (FNMOC) facility and receiving information back when applicable. This process required the manual intervention of shipboard personnel to collect system scan data, manually initiate a transfer of that data to the FNMOC facility, observe that transaction, manually flush the system of data in cases of failed attempts, ensure the mitigation of any orphaned data in flight during loss of network connection, manually restart the transfer of data, manually confirm the receipt of said data shoreside, and manually log the transaction for post audit purposes. This process consumed far more human attention and intervention than desired due to the fragile nature of afloat network connectivity and frequent disconnections. Initial efforts seeked to leverage the lessons learned throughout the Secure Legacy Application Integration with NCES (Network Centric Enterprises Services) (SLAIN) Small Business Innovative Research (SBIR) effort, along with complementary research and development efforts undertaken separately, to develop, accredit, and deploy VRAM enhancements that will provide the following four capabilities: Data persistence during the transfer of information Guaranteed delivery of VRAM data from ship to shore Provide an automated confirmation message to shipboard personnel that the scan data delivered successfully Reporting to be defined during development		
Congressional Adds Subtotals	6.682	4.979

Exhibit R-2A, RDT&E Project Justification: PB 2011 Navy		DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	**R-1 ITEM NOMENCLATURE** PE 0303140N: *Information Sys Security Program*	**PROJECT** 9999: *Congressional Adds*

C. Other Program Funding Summary ($ in Millions)

N/A

D. Acquisition Strategy

Congressional Adds.

E. Performance Metrics

Congressional Adds.

Exhibit R-3, RDT&E Project Cost Analysis: PB 2011 Navy		DATE: February 2010
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*	PROJECT 9999: *Congressional Adds*

Support ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Total Prior Years Cost	FY 2010 Cost	FY 2010 Award Date	FY 2011 Base Cost	FY 2011 Base Award Date	FY 2011 OCO Cost	FY 2011 OCO Award Date	FY 2011 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Software Development Support	WR	SSC Various	0.000	4.979	Mar 2010	0.000		0.000		0.000	0.000	4.979	Continuing
		Subtotal	0.000	4.979		0.000		0.000		0.000	0.000	4.979	

Remarks

	Total Prior Years Cost	FY 2010		FY 2011 Base		FY 2011 OCO		FY 2011 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	0.000	4.979		0.000		0.000		0.000	0.000	4.979	

Remarks