Exhibit R-2, RDT&E Budget Item Justification: PB 2012 Navy										DATE: February 2011	
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 2010**	**FY 2011**	**FY 2012 Base**	**FY 2012 OCO**	**FY 2012 Total**	**FY 2013**	**FY 2014**	**FY 2015**	**FY 2016**	**Cost To Complete**	**Total Cost**
Total Program Element	31.422	25.934	25.229	-	25.229	25.902	26.388	26.416	25.801	Continuing	Continuing
0734: *Communications Security R&D*	24.262	22.921	22.451	-	22.451	23.146	23.551	23.569	22.924	Continuing	Continuing
3230: *Information Assurance*	2.181	3.013	2.778	-	2.778	2.756	2.837	2.847	2.877	Continuing	Continuing
9999: *Congressional Adds*	4.979	-	-	-	-	-	-	-	-	0.000	4.979

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 an easier attacked and higher value target. The types of possible attacks continue 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 IA elements: (1) assure separation of information levels and user communities, including coalition partners; (2) assurance of the telecommunications infrastructure; (3) assurance of joint user enclaves, using a defense-in-depth architecture; (4) assurance of the computing base and information store; and, (5) supporting assurance technologies, including a Public Key Infrastructure (PKI). 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.

Exhibit R-2, RDT&E Budget Item Justification: PB 2012 Navy	DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	R-1 ITEM NOMENCLATURE PE 0303140N: *Information Sys Security Program*

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, American National Standards Institute, Institute of Electrical and Electronics Engineers, Internet Engineering Task Force, World Wide Web Consortium, and National Institute of Standards and Technologies. 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 the Clinger/Cohen Act, 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.

Maritime Operations Center (MOC) will respond to new technologies and advanced hardware and software tools to support the development and deployment towards automated autonomous computer network operations (CNO) network operations (NETOPS).

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 FY12:
Computer Network Defense (CND) - Continue to ensure that security of Navy networks will meet the mandates and initiatives of DoD for securing the GIG by continued development of system management capabilities to enforce proactive afloat/shore fleet level security policies across the Navy computer network. Continue the development and testing of security situational awareness technologies for knowledge-empowered CND operations for both afloat/shore installations. Continue to develop capabilities into Common Computing Environment (CCE) and Afloat Core Services (ACS) and provide technical guidance to ensure CND requirements are met by Consolidated Afloat Network Enterprise Service (CANES). Continue the development of patch management and host based security agent tools that promote the integration of CND capabilities (monitoring, detecting, analyzing, and responding).

Cryptographic (Crypto)/Crypto Modernization (CM) - Continue the Link-22 Modernized Link Level Communications Security (COMSEC) (MLLC), Very High Frequency (VHF)/Ultra High Frequency (UHF) Wideband Tactical Secure Voice Cryptologic Equipment (VINSON)/Advanced Narrowband Digital Voice Terminal (ANDVT) Cryptographic Modernization (VACM), and Link-16 CM development efforts, and start the Suite B Navy Implementation, Portable Radio Program (PRP), Demand Assigned Multiple Access (DAMA), Secure Voice Over Internet Protocol (SVoIP) and Navy Crypto Future Requirements development efforts. Develop a crypto modernization plan for transmission security (TRANSEC) with National Security Agency (NSA) and other services.

Exhibit R-2, RDT&E Budget Item Justification: PB 2012 Navy	DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	**R-1 ITEM NOMENCLATURE** PE 0303140N: *Information Sys Security Program*

Electronic Key Management System (EKMS)/Key Management Infrastructure (KMI). Continue EKMS to KMI transition planning. Continue transition strategy and define requirements for incorporation of other KMI roles into Navy architecture. Provide support to KMI Capability Increment 3 kickoff and program implementation. Continue supporting KMI transition working group meetings, developing white papers and support documentation for KMI. Provide requirements definition support of the next generation fill device.

Public Key Infrastructure (PKI) - Continue to develop Secret Internet Protocol Router Network (SIPRNet) PKI solutions, including the SIPR Validation Authority (SVA), and SIPR Hardware Token.

MOC - Assess the cyberspace network operations information dominance roadmap and as is architecture. Investigate government and industry automated autonomous information environment network operations (NETOPS) common operational picture (COP) set of tools for applicability to provide the Maritime Operations Center the ability to maintain Command and Control (C2) of secure Communications Systems (CS) through the ability to analyze and determine optimal method of conducting C2 cyberspace NETOPS. Develop the cyberspace NETOPS to be architecture.

B. Program Change Summary ($ in Millions)	FY 2010	FY 2011	FY 2012 Base	FY 2012 OCO	FY 2012 Total
Previous President's Budget	29.049	25.934	27.660	-	27.660
Current President's Budget	31.422	25.934	25.229	-	25.229
Total Adjustments	2.373	-	-2.431	-	-2.431
• Congressional General Reductions		-			
• Congressional Directed Reductions		-			
• Congressional Rescissions	-	-			
• Congressional Adds		-			
• Congressional Directed Transfers		-			
• Reprogrammings	2.924	-			
• SBIR/STTR Transfer	-0.243	-			
• Program Adjustments	-	-	-2.136	-	-2.136
• Section 219 Reprogramming	-0.285	-	-	-	-
• Rate/Misc Adjustments	-	-	-0.295	-	-0.295
• Congressional General Reductions Adjustments	-0.023	-	-	-	-

Congressional Add Details ($ in Millions, and Includes General Reductions)	FY 2010	FY 2011
Project: 9999: *Congressional Adds*		
Congressional Add: *Universal Description, Discovery and Integration*	4.979	-
	4.979	-

Exhibit R-2, RDT&E Budget Item Justification: PB 2012 Navy	DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 1319: *Research, Development, Test & Evaluation, Navy* BA 7: *Operational Systems Development*	**R-1 ITEM NOMENCLATURE** PE 0303140N: *Information Sys Security Program*

Congressional Add Details ($ in Millions, and Includes General Reductions)	FY 2010	FY 2011
Congressional Add Subtotals for Project: 9999		
Congressional Add Totals for all Projects	4.979	-

Change Summary Explanation

Schedule:
EKMS TKL production FA Test slipped from 2Q 2010 to 4Q 2011 due to contract delays and NSA testing requirements. No RDT&E funding impact.
EKMS TKL production FRP decision slipped from 3Q 2010 to 2Q 2012 due to contract delays and NSA strategy requiring First Article (FA) test to be completed first. No RDT&E funding impact.

Crypto - Link -22 MLLC prototype contract award slipped from 1Q 2011 to 2Q 2011 due to delays in source selection process. No risk to FY11 effort.
Crypto - VACM MS C slipped from 4Q 2012 to 1Q 2013 due to delay in US Air Force source selection.
Crypto - KW-46M production integration test moved from 4Q 2010 to 2Q 2011 due to delay in NSA providing certified Test key for testing. No RDT&E funding impact.

CND Inc 2 CPD slipped from 3Q 2010 to 4Q 2010 due to delay of mission area determination. No RDT&E funding impact.
CND Inc 2 DT Assist/OA slipped from 2Q 2011 to 3Q 2011 due to delay in Critical Design Renew (CDR)/Test Readiness Review (TRR) schedule and revised testing schedule from COMOPTEVFOR. No RDT&E funding impact.
CND Inc 2 Production RFP and contract award milestones removed from schedule. Existing contract strategy was deeemed sufficient.

Funding:
($-2.186M) from PB11 to PB12 in FY12 reduction reflects ramp down of CND, CMPO and KMI systems engineering efforts.

Technical: N/A

Exhibit R-2A, RDT&E Project Justification: PB 2012 Navy			DATE: February 2011
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 2010	FY 2011	FY 2012 Base	FY 2012 OCO	FY 2012 Total	FY 2013	FY 2014	FY 2015	FY 2016	Cost To Complete	Total Cost
0734: *Communications Security R&D*	24.262	22.921	22.451	-	22.451	23.146	23.551	23.569	22.924	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 (TRANSEC) evolution is from stand-alone dedicated devices to embedded modules incorporating NSA approved cryptographic engines, loaded with the certified algorithms and key, and interconnected via industry-defined interfaces. This includes the DoD Global Information Grid (GIG) 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 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 information such as financial, personnel, contractor proprietary, and procurement sensitive.

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 TRANSEC modules; (3) security appliances and software for switched and routed networks; (4) technology to interconnect networks

Exhibit R-2A, RDT&E Project Justification: PB 2012 Navy		DATE: February 2011
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*

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 SmartCards and similar security tokens); (7) Electronic Key Management System devices (Simple Key Loaders, COMSEC Material Work Stations (CMWS)) and Key Management Infrastructure equipment (Client Management (MGC)/Advanced Key Processor (AKP) MGC/AKPs, High Assurance Protocol Equipment) and Next Generation devices.

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 RDT&E 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 (SMI) 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 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.

Exhibit R-2A, RDT&E Project Justification: PB 2012 Navy		DATE: February 2011
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*

* 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 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.

Maritime Operations Center (MOC) networks will operate and share information with multiple partners and in varying circumstances. The MOCs will receive incremental tools toward maintaining a proactive automated autonomous information environment NETOPS Common Operational Picture (COP) set of tools to support Command and Control (C2) of the Communications Systems (CS) through the ability to analyze and determine optimal method of dominating C2 cyberspace operations. This includes CYBER Surveillance, bandwidth monitoring, INTEL situational awareness tool and network health monitoring. NETOPS COP will provide a proactive view and enhanced security tool for use of CYBER network managers. NETOPS COP enhances execution of Open Public Local Access Network during all phases by ensuring validity of the COP, network health, information operations, and battlespace awareness. A combination of software tools, interoperable enabling hardware and processes to monitor and visualize network traffic to provide a locally generated, fused situational awareness picture for battle watch decision-making will be provided. NETOPS COP provides the Commander with near immediate risk assessment, actionable intelligence and immediate mitigation courses of action and attribution of on-going CS Protection events in order to enable the apportionment of forces with exacting control in response to national objectives.

FY 12 Highlights for ISSP, Computer Network Defense and Maritime Operations Center (MOC):

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 (UDOP) to enhance Security Information Manager (SIM) tools with adaptive reactive-defense capabilities, improve incident correlation and situation awareness reporting. Begin development of computer-network evaluation capabilities to perform real-time analysis of events. Develop enhancements that advance CND analysis and response capabilities to network threats. Begin development of CND Increment 2 technology insertion cycles.

Exhibit R-2A, RDT&E Project Justification: PB 2012 Navy		DATE: February 2011
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*

Cryptographic (Crypto)/Crypto Modernization (CM) - Continue the Link-22 Modernized Link Level Communications Security (COMSEC) (MLLC), Very High Frequency (VHF)/Ultra High Frequency (UHF) Wideband Tactical Secure Voice Cryptologic Equipment (VINSON)/Advanced Narrowband Digital Voice Terminal (ANDVT) Cryptographic Modernization (VACM), and Link-16 CM development efforts, and start the Suite B Navy Implementation, Portable Radio Program (PRP), Key Management Infrastructure (KMI) Awareness, Demand Assigned Multiple Access (DAMA) , Secure Voice Over Internet Protocol (SVoIP), Navy Future Crypto Requirements, Navy Crypto Mod Acceleration with joint services. Coordinate a Crypto Modernization Plan for Transmission Security (TRANSEC) with NSA and other services.

Electronic Key Management System (EKMS) - Finalize any EKMS to KMI transition issues. Migrate COMSEC Material Work Station/Data Management Device (CMWS/DMD) and other Tier 3 devices to the KMI environment. Explore transition planning for CMWS/DMD to operate in the KMI environment.

Key Management Infrastructure (KMI) - Continue transition strategy and define requirements for incorporation of other KMI roles into Navy architecture (i.e. Controlling Authority, Command Authority. Provide support to KMI CI-3 kickoff and program implementation. Providing engineering services to the CRYPTO MOD programs to ensure crypto devices are being designed with KMI capabilities specifically Over the Network Keying and are Network enabled. Begin requirements definition efforts for the Next Generation Fill Device.

PKI - Research and develop tools to support device (non-human) certificates. Design and develop PKI expansion to support GIG 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.

Maritime Operations Center (MOC) - Respond to new technologies and advanced hardware and software tools to support the development and deployment towards automated autonomous Computer Network Operations (CNO) NETOPS.

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2010	FY 2011	FY 2012
Title: Computer Network Defense (CND)	9.955	8.010	8.410
Articles:	0	0	0
FY 2010 Accomplishments: Developed a process to assign asset criticality at the host and application level. Advanced development of proactive insider threat countermeasures and application layer security risk monitoring. Continued to develop UDOP to enhance Security Information Manager (SIM) tools. Continued research to analyze IA capabilities to support Early Adopters systems with selective and autonomic settings on the CND posture as a proactive response to threat attack sensors and vulnerability indications. Addressed 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. Began transition to CANES with CND capabilities			

Exhibit R-2A, RDT&E Project Justification: PB 2012 Navy		DATE: February 2011
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 Programs ($ in Millions, Article Quantities in Each)	FY 2010	FY 2011	FY 2012
in support of CCE and ACS. Progressed towards completing DoD 5000 requirements to achieve MS C and determining developmental , operational and joint interoperability test requirements for CND Increment 2. ***FY 2011 Plans:*** Develop Joint Task Force/Global Network Operations Department of Defense (JTF-GNO/DoD) mandated network security tools (assured compliance assessment solution (ACAS), Host-Based Security System version upgrades into the CND Afloat and Shore design to protect against emergent threats. Continue the development of UDOP to enhance SIM tools with adaptive reactive-defense capabilities, improve incident correlation and situation awareness reporting. Continue the development of CND capabilities in support of CCE and 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. Standardize/modularize and collapse shore architecture design . Finalize test requirements for CND Increment 2. Complete DoD 5000 requirements to achieve MS C. Continue lab testing and support OA for CND Increment 2. ***FY 2012 Plans:*** Incorporate U.S. Cyber Command (USCYBERCOM)/DoD mandated network security tools into the CND Afloat and Shore Increment 2 design to improve Layered Defense-in-Depth (DiD) capability. Begin development of CND Increment 2 technology insertion cycles (rapid acquisition) to address current and emergent realworld threats, performance improvements, and end-of-life issues to continue meeting Increment 2 Capability Production Document (CPD) performance parameters and address key system attributes (enhanced Situational Awareness/Sensor Grid, Tier 3 SIM, data correlation, integrated DiD, enhanced Command & Control (C2) capabilities). Develop capabilities to perform real-time analysis of events. Continue to develop enhancements that advance CND analysis and response capabilities to network threats. Continue CND capabilities design coordination with CCE and ACS capabilities. Support test readiness reviews and events (Operational Assessment, DT Assist and Initial Operational Test and Evaluation (IOT&E)) for CND Increment 2.			
Title: Crypto/Crypto Modernization	8.024	8.658	7.673
Articles:	0	0	0
FY 2010 Accomplishments: Continued research, evaluation, and prioritization of cryptographic products such as Demand Assigned Multiple Access (DAMA), portable tactical radios, Single Channel Ground and Airborne Radio System, Integrated Broadcast Service Multi Mission Advanced Tactical Terminal, Telemetry, and various embedded devices. Continued coordination with the Information Systems Security Office, joint services, and the National Security Agency (NSA), including representing the Navy at the Cryptographic Solutions Technical Advisory Group (CSTAG). Continued identifying strategies to reduce the overall crypto inventory within the			

Exhibit R-2A, RDT&E Project Justification: PB 2012 Navy		DATE: February 2011
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 Programs ($ in Millions, Article Quantities in Each)	FY 2010	FY 2011	FY 2012
DoN to realize long term cost savings. Continued providing consistent Information Assurance (IA) engineering support for the development and integration of Crypto Mod products. Continued to support the on-going Cryptographic Joint Algorithm Integrated Product Team (IPT). Transitioned 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 VINSON/ANDVT Cryptographic Modernization (VACM) program (providing documentation review, as well as SV technical, acquisition, logistic, test and evaluation support). Continued development of Link 22 Modernized Link Level COMSEC (MLLC), Link 16 Crypto Mod (CM), KW-46M in support of the Fleet Submarine Broadcast System, KG-3X Inc 2 and VACM, while finalizing the development of AN-PYQ-20(v)(c) (formerly KL-51M) efforts in support of the submarine off-line encryption requirement. Continued Crypto voice standardization based on the Variable Data Rate, Voice Compression Algorithm. Supported Assistant Secretary of Defense (ASD) (Networks and Information Integration (NII)) Nuclear Command Control and Communications (NC3) Crypto Modernization.			
FY 2011 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 CSTAG. Continue identifying strategies to reduce the overall crypto inventory within the DoN 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 Crypto Mod and Link 22 MLLC, KW-46M. Continue SV 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 DAMA, SV Over Internet Protocol (SVoIP) Test & Evaluation (T&E). Coordinate a Crypto Mod plan for Transmission Security (TRANSEC) with NSA and other services.			
FY 2012 Plans: Continue research, evaluation, and prioritization of cryptographic products. Continue coordination with the Information Systems Security Office and the NSA, including representing the Navy at the CSTAG. Continue identifying strategies to reduce the overall crypto inventory within the DoN 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 through performing technical analysis of alternatives (AoA) for vendor Type 1 Crypto devices and security architecture implementations, conducting security risk analysis, reviewing security requirement specifications/test plans, developing systems engineering documents into technical documentation to ensure the implementation of robust IA solutions, and providing SME technical support to multi-functional Link-16 CM development teams. Continue development for the Link 22 MLLC through overseeing system integration, verification and validation (IV&V) efforts and acceptance testing, conducting security risk analysis/reduction, interpreting the Information Assurance Security Requirements Directive (IASRD) and providing recommendations			

Exhibit R-2A, RDT&E Project Justification: PB 2012 Navy		DATE: February 2011
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 Programs ($ in Millions, Article Quantities in Each)	FY 2010	FY 2011	FY 2012
towards the NSA certification process. KW-46M work entails integration testing, Emergency Action Message (EAM) and Targeting Change Message (TCM) certifications, and installation into the Common Submarine Radio Room (CSRR). Continue SV RDT&E efforts such as SBIR oversight, and NRL's research into SV emerging technologies and related technical products, support to Air Force led VACM program and continue supporting ASD (NII) NC3 CM. Initiate major pre-acquisition and development efforts for DAMA, SVoIP and T&E. Coordinate a Crypto Mod plan for TRANSEC with NSA and other services.			
Title: Key Management Infrastructure (KMI) ***Articles:*** ***FY 2010 Accomplishments:*** Continued finalizing the DoN KMI architecture and roll out strategy for deployment. Identified any issues pertaining to transition from EKMS to KMI pertaining to capabilities and connectivity to Naval networks. Provided engineering support in review of all necessary documentation for Navy Independent Logistics Assessment and National Security Agency (NSA) Milestone C Acquisition Decision Memorandum. This determined Navy transition for full rate production within the Navy for Capability Increment (CI-2). Continued engineering efforts for Navy transition and test planning for KMI CI-2 Manager Client/Advanced Key Processor (MGC/AKP). Continued developing Navy implementation plan for KMI CI-2 to support Navy programs of record and EKMS end of life. ***FY 2011 Plans:*** Provide technical support to National Security Agency for KMI CI-2 Spiral 1 Development Testing and Evaluation, OA, Initial Operational Testing and Evaluation (IOT&E), Milestone C. Continue to support engineering and development efforts for KMI CI-2 and incorporation into Navy architectures and networks. Testing KMI Manager Client/Advanced Key Processors at selected pilot sites in support of OA and IOT&E. ***FY 2012 Plans:*** Continue transition strategy and define requirements for incorporation of other KMI roles into Navy architecture (i.e., Controlling Authority, Command Authority). Continue supporting KMI transition working group meetings, developing white papers and support documentation for KMI. Migrate COMSEC Material Work Station/Data Management Device and other Tier 3 devices to the KMI environment. Begin support to KMI CI-3 kickoff and program implementation. Provide requirements definition support to the development of the Next Generation Fill Device.	2.383 0	2.549 0	2.708 0
Title: Public Key Infrastructure (PKI) ***Articles:*** ***FY 2010 Accomplishments:*** Initiated 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. Performed research and development	0.703 0	0.769 0	0.408 0

Exhibit R-2A, RDT&E Project Justification: PB 2012 Navy		DATE: February 2011
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 Programs ($ in Millions, Article Quantities in Each)	FY 2010	FY 2011	FY 2012
of solutions to resolve technical challenges and the tools required for continued deployment of Navy, non-Navy, Marine Corps Internet/Cryptographic Log On and Navy Certificate Validation Infrastructure/Online Certificate Status Protocol Afloat. Researched and developed tools to support device (non-human) certificates. Performed security and functionality testing and evaluation of PKI tokens and readers to support Tactical PKI and Homeland Security Presidential Directive-12 (HSPD-12) implementation. Supported 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 PKI environments. Provided evaluation of Commercial-Off-The-Shelf (COTS) products that can support coalition information sharing. Initiated test and evaluation of HSPD-12 token and middleware as part of the transition to stronger algorithms. Researched and developed tools to support PKI with Internet Protocol Version 6 and Suite B implementation. ***FY 2011 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 GIG identity management and protection requirements onto the SIPRNet. Evaluate automated on-line network device (e.g., workstations, routers, switches) certificate issuance infrastructure. Complete DoD 5000 requirements to achieve Milestone C. ***FY 2012 Plans:*** Research, analyze and evaluate Public Key Infrastructure (PKI) enabled products such as VPNs, routers, and switches, for their suitability to support Navy needs for device (Non-Person Entities) certificates. Analyze and evaluate PKI enabled products to support GIG identity management and protection requirements, such as the evolution of SIPRNET Token issuance workstations, SIPRNET Tokens, Middleware, and servers (Microsoft Domain Controllers, Web Server, Validation Authorities). Provide systems engineering support for SIPR PKI enabling to Navy Program of Records (POR) for integration. This includes research, analysis, and evaluation of PKI enabled products and methods to support the manual and automatic enrollment and issuance of PKI certificates to Navy servers and devices known as Non-Person Entities (NPE), and evaluation of DISA's auto-enrollment and registration services for Phases II and III of DoD PKI enabled Implementation. Research, analyze, and evaluate PKI enabled products for non-Microsoft devices and systems (e.g. Linux, Apple, servers, router, switches).			
Title: Electronic Key Management System (EKMS) ***Articles:*** ***FY 2010 Accomplishments:***	0.413 0	0.183 0	-

Exhibit R-2A, RDT&E Project Justification: PB 2012 Navy		DATE: February 2011
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 Programs ($ in Millions, Article Quantities in Each)	FY 2010	FY 2011	FY 2012
EKMS Phase V: Finalized Navy EKMS Phase V hardware and software development for ashore and afloat as well as submarine community. Conducted Virtual Private Network tested and deployed to two Pilots and prepared all necessary installation documentation to support this effort. Identified any functional deficiencies within EKMS Phase V for inclusion into the KMI CI-2 architecture. Defined phase out approach and transition strategy of EKMS to KMI. Continued to provide technical design support to EKMS programs of record (IFF Mode 5 & AEHF) for architectures. Continued to define EKMS technology gaps in preparation to the transition to KMI. Identified technical solutions for EKMS sustainment until KMI CI-2. ***FY 2011 Plans:*** Continue to define EKMS technology gaps in preparation to the transition to KMI. Identify technical solutions for EKMS sustainment until KMI CI-2. Continue EKMS systems engineering to support technology issues as a result of the introduction of KMI into the dual mode environment. Finalize any EKMS to KMI transition issues. Migrate COMSEC Material Work Station/Data Management Device and other Tier 3 devices to the KMI environment.			
Title: Information Assurance (IA) Services (formerly IA Architecture)	2.784	2.752	2.752
Articles:	0	0	0
FY 2010 Accomplishments: Continued 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. Supported the ongoing development of the Navy IA Master Plan and coordinated IA activities across the virtual System Command (SYSCOM) via the IA Technical Authority (TA) to ensure the security design and integration of Computer Network Defense-in-Depth (CNDiD) products and services is consistent across the Navy for major initiatives such as the future afloat, ashore, and OCONUS networks. Provided IA 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 PDA security readiness of Naval wireless networks and mobile computing devices. Continued to evaluate products for security issues and developed guidance and procedures for the design and integration of risk mitigation strategies via appropriate IA controls. ***FY 2011 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 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			

Exhibit R-2A, RDT&E Project Justification: PB 2012 Navy		DATE: February 2011
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 Programs ($ in Millions, Article Quantities in Each)	FY 2010	FY 2011	FY 2012
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. ***FY 2012 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 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.			
Title: Maritime Operations Center (MOC) ***Articles:*** ***FY 2012 Plans:*** Maritime Operations Center (MOC) will respond to new technologies and advanced hardware and software tools to support the development and deployment towards automated autonomous CNO NETOPS.	-	-	0.500 0
Accomplishments/Planned Programs Subtotals	24.262	22.921	22.451

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2010	FY 2011	FY 2012 Base	FY 2012 OCO	FY 2012 Total	FY 2013	FY 2014	FY 2015	FY 2016	Cost To Complete	Total Cost
• OPN/3415: *Info Sys Security Program (ISSP)*	108.210	120.529	119.857	0.000	119.857	122.470	129.847	138.779	131.491	0.000	871.183
• OPN/8106: *Maritime Operations Center (MOC)*	6.110	6.248	6.508	0.000	6.508	8.347	7.151	8.194	9.377	0.000	51.935

D. Acquisition Strategy

EKMS Phase V -The 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 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 RDT&E funding over the Future Years Defense Program (FYDP) to ensure the Navy infrastructure evolves with the EKMS phases, supports additional

Exhibit R-2A, RDT&E Project Justification: PB 2012 Navy		DATE: February 2011
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*

devices certified by NSA and supports the migration of EKMS to KMI CI-2. This will require potential modifications to the Navy EKMS architecture including the local management device and associated software. NSA certified Commercial-Off-The-Shelf/Government-Off-The-Shelf (COTS/GOTS) devices are procured to support Navy requirements.

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-3 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 2012.

Cryptographic Modernization (CM) - The procurement and fielding of Modernized Crypto devices such as the KG-3X Inc 2, KG-45A, AN-PYQ-20(v)(c) (formerly KL-51M), KW-46M, KG-175D, KG-175A, KG-3X Suites, K02 Replacement, VACM, SubCM Common Submarine Radio Room (CSRR), Walburn, and COMSEC Crypto Serial Replacement 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.

Computer Network Defense (CND) - The CND program procures equipment to secure Navy network information systems. Procurements within the CND equipment line include: Firewall components which provide protection for networks from unauthorized users, Virtual Private Networks (VPN's) which provide encrypted "Point-to-Point" virtual communication networks, Intrusion Prevention Systems, Administrator Access Control, Network Security tools and Filtering routers. CND procurements will also include DoD IA certification and accreditation process end-to-end certification and accreditation support tool, to provide enterprise-wide visibility into security posture. The rapid advance of cyber technology requires an efficient process for updating CND tools deployed to afloat and shore platforms. Recognizing the need for future CND capability improvements, CND will be implementing an evolutionary acquisition strategy that delivers CND capability in multiple increments and functionality releases that address validated requirements.

Maritime Operations Center (MOC) - This RDT&E line supports an incremental acquisition strategy. MOC utilizes a System of Systems (SoS) and incremental approach in achieving global network of Navy Maritime organizations through Builds as defined by OPNAV N2/N6F41.

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) to achieve Commander Operational Test and Evaluation Force (COMOPTEVFOR) support for Navy-wide deployment.
* Complete 100% of engineering efforts for Navy transition and test planning for the KMI CI-2 clients and AKPs to ensure successful Navy transition to KMI in accordance with EKMS end of life priorities and objectives.
* Complete development and transition to production the Tactical Key Loader (TKL) to achieve 100% acceptance of First Article, NSA Certification testing and COMOPTEVFOR determination of suitability for production.

Cryptographic Modernization (CM):

Exhibit R-2A, RDT&E Project Justification: PB 2012 Navy		DATE: February 2011
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*

* Meet 100% of TOP SECRET (TS) and SECRET Chairman of Joint Chiefs of Staff Instruction (CJCSI 6510) cryptographic modernization requirements within the current 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. The gap analysis is an effort to analyze current integrated legacy cryptographic devices within the DoN inventory with known algorithm vulnerability dates, hardware sustainment issues, and identify transition device schedules if one exists.
* 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).
* 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, KG-84, 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(COTS)/Non-Developmental Item IA security products. Evaluation may include defensible network boundary capabilities such as firewalls, secure routers and switches, guards, Virtual Private Networks, and network Intrusion Prevention Systems.
* 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 TA to measure effectiveness of Navy networks and ensure the security design and integration of CNDiD products and services is 100% interoperable and operationally acceptable across the Navy for major initiatives such as the future afloat, ashore, and OCONUS networks.

Maritime Operations Center (MOC):
Provide and demonstrate NETOPS COP on a yearly basis via warfighter interface venues.

Exhibit R-3, RDT&E Project Cost Analysis: PB 2012 Navy		DATE: February 2011
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)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Total Prior Years Cost	FY 2011 Cost	FY 2011 Award Date	FY 2012 Base Cost	FY 2012 Base Award Date	FY 2012 OCO Cost	FY 2012 OCO Award Date	FY 2012 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Primary Hardware Development	C/CPFF	VIASAT:Carlsbad, CA	7.282	-		-		-		-	0.000	7.282	
Primary Hardware Development	MIPR	MITRE:San Diego, CA	5.522	-		-		-		-	0.000	5.522	
Primary Hardware Development (PY)	WR	Various:Various	88.607	-		-		-		-	0.000	88.607	
Systems Engineering	WR	NUWC:Newport, RI	0.608	-		-		-		-	0.000	0.608	
Systems Engineering	WR	SSC PAC/LANT:San Diego, CA/Charleston, SC	11.105	11.605	Dec 2010	9.838	Dec 2011	-		9.838	0.000	32.548	
Systems Engineering	WR	NRL:Washington DC	0.300	0.300	Dec 2010	0.260	Dec 2011	-		0.260	0.000	0.860	
Systems Engineering	WR	FNMOC:Monterey, CA	0.240	0.240	Dec 2010	0.208	Dec 2011	-		0.208	0.000	0.688	
Primary Hardware Development	WR	SSC PAC:San Diego	1.264	1.290	Dec 2010	1.120	Dec 2011	-		1.120	0.000	3.674	
Primary Hardware Development	WR	NRL:Washington DC	0.480	0.490	Dec 2010	0.426	Dec 2011	-		0.426	0.000	1.396	
Primary Hardware Development	WR	Various:Various	0.725	-		-		-		-	0.000	0.725	
Software Development (Note 2)	C/CPAF	SAIC:San Diego, CA	32.877	-		-		-		-	0.000	32.877	
Software Development (Note 2)	WR	NRL:Washington, D.C.	4.587	1.705	Dec 2010	1.480	Dec 2011	-		1.480	0.000	7.772	
Software Development (Note 2)	WR	SSC PAC/LANT:San Diego, CA and Charleston, SC	6.719	4.310	Dec 2010	3.740	Dec 2011	-		3.740	0.000	14.769	
Software Development (Note 1,2)	WR	NRL:Washington, D.C.	12.904	-		-		-		-	0.000	12.904	
System Engineering (MOC)	WR	SSC PAC:San Diego, CA	-	-		0.500	Dec 2011	-		0.500	0.000	0.500	
		Subtotal	173.220	19.940		17.572		-		17.572	0.000	210.732	

Exhibit R-3, RDT&E Project Cost Analysis: PB 2012 Navy			DATE: February 2011
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)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Total Prior Years Cost	FY 2011 Cost	FY 2011 Award Date	FY 2012 Base Cost	FY 2012 Base Award Date	FY 2012 OCO Cost	FY 2012 OCO Award Date	FY 2012 Total Cost	Cost To Complete	Total Cost	Target Value of Contract

Remarks

Note 1: Funding realigned to Project 3230 beginning FY10
Note 2: Moved Software Development from 'Support' category to 'Product Development'

Support ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Total Prior Years Cost	FY 2011 Cost	FY 2011 Award Date	FY 2012 Base Cost	FY 2012 Base Award Date	FY 2012 OCO Cost	FY 2012 OCO Award Date	FY 2012 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Systems and Analysis	WR	SSC PAC/LANT:San Diego, CA/Charleston, SC	-	-		1.519	Dec 2011	-		1.519	0.000	1.519	
Software Development	WR	NRL:Washington, D.C.	-	-		0.256	Dec 2011	-		0.256	0.000	0.256	
		Subtotal	-	-		1.775		-		1.775	0.000	1.775	

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Total Prior Years Cost	FY 2011 Cost	FY 2011 Award Date	FY 2012 Base Cost	FY 2012 Base Award Date	FY 2012 OCO Cost	FY 2012 OCO Award Date	FY 2012 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Developmental Test	WR	SSC PAC:San Diego, CA	34.723	0.055	Dec 2010	0.106	Dec 2011	-		0.106	0.000	34.884	
Developmental Test	WR	NUWC:Newport, RI	0.263	0.360	Dec 2010	0.695	Dec 2011	-		0.695	0.000	1.318	
Operational Test	WR	OPTEVFOR:Norfolk, VA	0.080	0.045	Dec 2010	0.086	Dec 2011	-		0.086	0.000	0.211	
		Subtotal	35.066	0.460		0.887		-		0.887	0.000	36.413	

Management Services ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Total Prior Years Cost	FY 2011 Cost	FY 2011 Award Date	FY 2012 Base Cost	FY 2012 Base Award Date	FY 2012 OCO Cost	FY 2012 OCO Award Date	FY 2012 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Program Management	C/CPFF	BAH:San Diego, CA	17.264	1.941	Dec 2010	1.707	Dec 2011	-		1.707	0.000	20.912	
Program Management	WR		0.633	0.580	Dec 2010	0.510	Dec 2011	-		0.510	0.000	1.723	

Exhibit R-3, RDT&E Project Cost Analysis: PB 2012 Navy		DATE: February 2011
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*

Management Services ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Total Prior Years Cost	FY 2011 Cost	FY 2011 Award Date	FY 2012 Base Cost	FY 2012 Base Award Date	FY 2012 OCO Cost	FY 2012 OCO Award Date	FY 2012 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
		SSC PAC:San Diego, CA											
		Subtotal	17.897	2.521		2.217		-		2.217	0.000	22.635	

	Total Prior Years Cost	FY 2011 Cost	FY 2011 Award Date	FY 2012 Base Cost	FY 2012 Base Award Date	FY 2012 OCO Cost	FY 2012 OCO Award Date	FY 2012 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	226.183	22.921		22.451		-		22.451	0.000	271.555	

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2012 Navy		DATE: February 2011
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-4, RDT&E Schedule Profile: PB 2012 Navy		DATE: February 2011
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-4, RDT&E Schedule Profile: PB 2012 Navy		DATE: February 2011
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-4, RDT&E Schedule Profile: PB 2012 Navy		DATE: February 2011
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-4, RDT&E Schedule Profile: PB 2012 Navy		DATE: February 2011
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-4, RDT&E Schedule Profile: PB 2012 Navy		DATE: February 2011
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-4, RDT&E Schedule Profile: PB 2012 Navy		DATE: February 2011
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 2012 Navy		DATE: February 2011
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	
Events by Sub Project	**Quarter**	**Year**	**Quarter**	**Year**
Proj 0734				
EKMS Phase V IOC	3	2010	3	2010
EKMS Phase V FOC	3	2014	3	2014
EKMS TKL Contract Award	2	2011	2	2011
EKMS TKL IOC	4	2012	4	2012
EKMS TKL FOC	4	2014	4	2014
KMI CI-2 MS C	2	2011	2	2011
KMI CI-2 Inc 2 IOC	2	2012	2	2012
KMI CI-2 FOC	4	2014	4	2014
KMI CI-2 DT&E	2	2011	2	2011
KMI CI-2 IOT&E	3	2011	3	2011
KMI CI-2 OA2	2	2011	2	2011
EKMS TKL FA Test	4	2011	4	2011
EKMS TKL FRP Decision	2	2012	2	2012
KMI CI-2 Spiral 1 LRIP	3	2011	3	2011
KMI CI-2 Spiral 1 FRP	2	2012	2	2012
KMI CI-2 Spiral 2 FRP	4	2013	4	2013
EKMS Phase V S/W	3	2010	1	2013
EKMS SKL Deliveries	1	2010	3	2013
EKMS TKL Deliveries	1	2012	4	2014
KMI CI-2 Deliveries	3	2012	4	2016
KMI CI-2 Next Generation Fill Device	2	2013	4	2016

Exhibit R-4A, RDT&E Schedule Details: PB 2012 Navy		DATE: February 2011
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	
Events by Sub Project	**Quarter**	**Year**	**Quarter**	**Year**
CRYPTO KG-3X Inc 2 MS C/FRP	2	2011	2	2011
CRYPTO KG-45A FOC	2	2013	2	2013
CRYPTO KW-46M IOC	2	2011	2	2011
CRYPTO Link 22 MLLC - Prototype Award	2	2011	2	2011
CRYPTO VACM MS B	2	2010	2	2010
CRYPTO VACM MS C	1	2013	1	2013
CRYPTO VACM IOC	1	2014	1	2014
CRYPTO KG-45A NSA Cert Qual Test	1	2010	1	2010
CRYPTO AN-PYQ-20(v) (c) (formerly KL-51M) Development Test	3	2010	3	2010
CRYPTO KW-46 NUWC Integration Test	2	2011	2	2011
CRYPTO AN-PYQ-20(v) (c) (formerly KL-51M) Production Decision	4	2010	4	2010
CRYPTO KG-3X Inc 2 Deliveries	4	2011	2	2013
CRYPTO KW-46M CSRR Deliveries	3	2011	2	2015
CRYPTO AN-PYQ-20(v) (c) (formerly KL-51M) Deliveries	4	2010	4	2014
CRYPTO KG-45A Deliveries	3	2010	1	2013
CRYPTO Link 22 MLLC Prototype Delivery	2	2012	2	2012
CRYPTO VACM Deliveries	3	2013	4	2016
PKI Inc 2 MS C	3	2011	3	2011
PKI Inc 2 IOC	2	2013	2	2013
PKI Inc 2 FOC	2	2014	2	2014
PKI Inc 2 Spiral 2 IOT&E	2	2011	2	2011
CND Inc 2 CPD	4	2010	4	2010
CND Inc 2 MS C	4	2011	4	2011
CND Inc 2 IOC	4	2012	4	2012

Exhibit R-4A, RDT&E Schedule Details: PB 2012 Navy		DATE: February 2011
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	
Events by Sub Project	**Quarter**	**Year**	**Quarter**	**Year**
CND Inc 2 FOC	4	2016	4	2016
CND Inc 2 DT Assist	3	2011	3	2011
CND Inc 2 OA	3	2011	3	2011
CND Inc 2 IOT&E	3	2012	3	2012
CND Inc 2 LRIP	2	2012	4	2012
CND Inc 2 FRP Decision	4	2012	4	2012
CND Inc 2 Initial Delivery	2	2012	2	2012
MOC Systems of Systems (SoS) Development FY12 TRR	3	2012	3	2012
MOC Systems of Systems (SoS) Development FY14 TRR	3	2014	3	2014
MOC Systems of Systems (SoS) Development FY16 TRR	3	2016	3	2016
MOC Prototype Development Build 12 PTD	2	2013	2	2013
MOC Prototype Development Build 14 FY14 PTD	2	2014	2	2014
MOC Prototype Development Build 14 FY15 PTD	2	2015	2	2015
MOC Prototype Development Build 16 PTD	2	2016	2	2016
MOC Developmental Test FY14	4	2014	4	2014
MOC Developmental Test FY16	4	2016	4	2016
MOC Spiral 10 IOC	1	2010	1	2010
MOC Spiral 10 FOC	4	2011	4	2011
MOC Build 12 IOC	1	2012	1	2012
MOC Build 12 FOC	4	2013	4	2013
MOC Build 14 IOC	1	2014	1	2014
MOC Build 14 FOC	4	2015	4	2015
MOC Build 16 IOC	1	2016	1	2016
MOC Spiral 10	1	2010	4	2011

Exhibit R-4A, RDT&E Schedule Details: PB 2012 Navy		DATE: February 2011
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	
Events by Sub Project	**Quarter**	**Year**	**Quarter**	**Year**
MOC Build 12	1	2012	4	2013
MOC Build 14	1	2014	4	2015
MOC Build 16	1	2016	4	2016

Exhibit R-2A, RDT&E Project Justification: PB 2012 Navy			DATE: February 2011
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 2010	FY 2011	FY 2012 Base	FY 2012 OCO	FY 2012 Total	FY 2013	FY 2014	FY 2015	FY 2016	Cost To Complete	Total Cost
3230: *Information Assurance*	2.181	3.013	2.778	-	2.778	2.756	2.837	2.847	2.877	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 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 common operational picture for 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

Exhibit R-2A, RDT&E Project Justification: PB 2012 Navy		DATE: February 2011
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*

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 Programs ($ in Millions, Article Quantities in Each)	FY 2010	FY 2011	FY 2012
Title: Information Assurance	2.181	3.013	2.778
Articles:	0	0	0

FY 2010 Accomplishments:

Completed the development of the information sharing architecture that addresses data integrity, confidentiality and policy management throughout networks of varying classification levels. Evaluated the security services of the architecture and adjusted to ensure mission operations are supported. Continued the development of technology that protects, assesses and responds to attacks of the infrastructure architecture and provided reconstitution capabilities/services. Continued the development of modernized attack sensing and warning mechanisms based on new detection algorithms and data mining concepts, and response capabilities for the architecture. Completed the development of technology and tools to ensure the unique security and performance requirements of tactical wireless communication systems are addressed. Initiated the development of a new high assurance boundary controller to protect Navy and Marine Corps data and resources from attack. Provided security services including encryption and data malware analysis in the boundary controller. Initiated the development of a high-assurance computing environment for Navy and Marine Corps use based on trusted platform technology. Developed the appropriate core code, security messages and assurance functions required. Initiated the development of new key and enabling technologies, management tools, and capabilities to address specific Navy and Marine Corps needs. Ensured the new solutions address distribution and management of data and other requisite material. Continued systems security engineering, certification and accreditation support for high-confidence naval information systems and ensured certification and accreditation approaches are consistent with Navy and DoD requirements.

FY 2011 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

Exhibit R-2A, RDT&E Project Justification: PB 2012 Navy		DATE: February 2011
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 Programs ($ in Millions, Article Quantities in Each)	FY 2010	FY 2011	FY 2012
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 support for high-confidence naval information systems and ensure certification and accreditation approaches are consistent with Navy and DoD requirements.			
FY 2012 Plans: Initiate the development of new network security technology focused on addressing nation state level sponsored activity. Address the growing threat by providing robust characterization of attacks/profiles to increase detection rates of the technology and to support attribution of threat actions across network boundaries. 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 threat-action levels. Complete the development of a high-assurance computing environment for Navy and Marine Corps use based on trusted platform technology. Complete the development of the appropriate core code, security messages and assurance functions required to ensure platform hardware and software protection. Complete 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. Continue 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 GPS constrained environments. Initiate the development of critical cryptographic technology to support Navy unique platforms and requirements. Ensure the technology addresses the limited size, weight and power issues, multiple data classification processing requirements, and provide on-the-fly programmability of mission data and key material to support various missions. 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.			
Accomplishments/Planned Programs Subtotals	2.181	3.013	2.778

Exhibit R-2A, RDT&E Project Justification: PB 2012 Navy		DATE: February 2011
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*

C. Other Program Funding Summary ($ in Millions)

N/A

D. Acquisition Strategy

This project funds advanced 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. Technologies developed are not transitioned into a acquisition program within the ISSP BLI 3415 budget.

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 DoN 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 DoN assets used in the wider emerging wireless spectrum.

Exhibit R-3, RDT&E Project Cost Analysis: PB 2012 Navy		DATE: February 2011
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 2011 Cost	FY 2011 Award Date	FY 2012 Base Cost	FY 2012 Base Award Date	FY 2012 OCO Cost	FY 2012 OCO Award Date	FY 2012 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Development Support	WR	NRL:Washington, DC	2.181	3.013	Nov 2010	2.778	Nov 2011	-		2.778	Continuing	Continuing	Continuing
		Subtotal	2.181	3.013		2.778		-		2.778			

	Total Prior Years Cost	FY 2011		FY 2012 Base		FY 2012 OCO		FY 2012 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	2.181	3.013		2.778		-		2.778			

Remarks

Exhibit R-2A, RDT&E Project Justification: PB 2012 Navy			DATE: February 2011
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 2010	FY 2011	FY 2012 Base	FY 2012 OCO	FY 2012 Total	FY 2013	FY 2014	FY 2015	FY 2016	Cost To Complete	Total Cost
9999: *Congressional Adds*	4.979	-	-	-	-	-	-	-	-	0.000	4.979
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 Programs ($ in Millions)	FY 2010	FY 2011
Congressional Add: Universal Description, Discovery and Integration	4.979	-
FY 2010 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. Continued development of software design, functional and security test plans.		
Congressional Adds Subtotals	4.979	-

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 2012 Navy		DATE: February 2011
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 2011 Cost	FY 2011 Award Date	FY 2012 Base Cost	FY 2012 Base Award Date	FY 2012 OCO Cost	FY 2012 OCO Award Date	FY 2012 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Software Development Support	WR	SSC LANT:Charleston, SC	4.979	-		-		-		-	0.000	4.979	
		Subtotal	4.979	-		-		-		-	0.000	4.979	

	Total Prior Years Cost	FY 2011		FY 2012 Base		FY 2012 OCO		FY 2012 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	4.979	-		-		-		-	0.000	4.979	

Remarks