

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2014 Navy										DATE: April 2013		
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)	All Prior Years	FY 2012	FY 2013 [#]	FY 2014 Base	FY 2014 OCO ^{##}	FY 2014 Total	FY 2015	FY 2016	FY 2017	FY 2018	Cost To Complete	Total Cost
Total Program Element	253.780	38.747	26.307	23.531	-	23.531	27.548	26.217	25.802	26.215	Continuing	Continuing
0734: Communications Security R&D	250.782	24.081	23.641	21.130	-	21.130	24.865	23.544	23.034	23.429	Continuing	Continuing
3230: Information Assurance	2.998	2.666	2.666	2.401	-	2.401	2.683	2.673	2.768	2.786	Continuing	Continuing
9999: Congressional Adds	0.000	12.000	0.000	0.000	-	0.000	0.000	0.000	0.000	0.000	0.000	12.000

[#] FY 2013 Program is from the FY 2013 President's Budget, submitted February 2012

^{##} The FY 2014 OCO Request will be submitted at a later date

A. Mission Description and Budget Item Justification

Information Systems Security Program (ISSP) ensures the protection of Navy and joint cyberspace systems from exploitation and attack. Cyberspace systems include wired and wireless telecommunications systems, Information Technology (IT) systems, and the content processed, stored, or transmitted therein. ISSP includes protection of the Navy's National Security Systems and Information (NSSI).

ISSP is the Navy's implementation of statutory and regulatory requirements specified in Federal Information Security Management Act of 2002 (FISMA, 44 U.S.C. section 3541), the Computer Security Act of 1987 (Public Law 100-235), Privacy Act of 1974 (5 U.S.C. section 552a, Public Law No. 93-579), National Security Act of 1947 (Public Law 235), Comprehensive National Cyber security Initiative (CNCI) National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/ HSPD-23), National Security Directive 42, Presidential Decision Directive 63, Executive Order 13526, Appendix III of Office of Management and Budget (OMB) Circular A-130 Revised, Committee for National Security Systems (CNSS) Policy 22, Chairman Joint Chiefs of Staff Instructions 6510.01F and 6510.02D, Department of Defense (DoD) Directives 8500.01, O-8530.01, and 8570.01, the new DoD Instruction 8500.02, and CNSS Instruction 1253.

ISSP activities address the risk management of cyberspace defined in "The National Military Strategy for Cyberspace Operations", Chairman of the Joint Chiefs of Staff, Dec 2006, of defensive Information Operations (IO) defined in Joint Publication 3-13 including the capabilities to protect, detect, restore, and respond. ISSP supports the entire naval cyberspace domain from the mobile forward-deployed subscriber, through the ashore supporting critical information infrastructure, and the interconnection with other cyberspace domains. Navy cyberspace is a higher value and more vulnerable target due to the interconnectivity of naval and joint networks, connections to allied and coalition partners, connections to the public information infrastructure, and their use in naval and joint war fighting. Navy cyber systems face advanced attacks involving malicious changes to critical information, changes to the functionality of critical systems, denial of service (including jamming), and the destruction of systems and networks. Since many naval cyber systems are based on commercially available technologies, adversaries often have access to the technologies they seek to exploit.

Rapid changes in the underlying commercial and government cyber infrastructures makes cyber security an increasingly complex and dynamic problem. ISSP provides the Navy's warfighter the essential information trust characteristics of availability, confidentiality, integrity, authentication, and non-repudiation. Information

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2014 Navy		DATE: April 2013
APPROPRIATION/BUDGET ACTIVITY 1319: <i>Research, Development, Test & Evaluation, Navy</i> BA 7: <i>Operational Systems Development</i>		R-1 ITEM NOMENCLATURE PE 0303140N: <i>Information Sys Security Program</i>
Assurance (IA)/Computer Network Defense (CND), key supporting cyber security activities, must evolve quickly to meet the rapidly evolving threats and vulnerabilities. Implementing ISSP requires rapid acquisition approaches to stay ahead of nation-states, terrorists, and criminal organization adversaries, among others. The Information Systems Security Program (ISSP) provides the Navy with the following cyber security elements: (1) defense of Navy's National Security Systems and Information (NSSI); (2) assured separation of information levels and user communities, including allied, coalition, non-Governmental, Defense Industrial Base, and other public partners; (3) technologies supporting the Navy's Computer Network Defense Service Providers (CNDSP) operations; (4) assurance of the Navy's telecommunications infrastructure and the wireless spectrum; (5) assurance of joint-user cyberspace domains, using a defense-in-depth architecture; (6) assurance of the critical computing base and information store; and, (7) supporting assurance technologies, including the Public Key Infrastructure (PKI) and Key Management Infrastructure (KMI). The ISSP program must be rapid, predictive, adaptive, and tightly coupled to cyberspace technology. Through modeling and simulation of Department of Defense (DoD) and commercial cyberspace systems evolution, the ISSP program provides architectures, products, and services based on mission impacts, information criticality, threats, vulnerabilities, and required defensive countermeasure capabilities. All ISSP Research Development Test & Evaluation (RDT&E) efforts comply with the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113) as implemented through Office of Management and Budget (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 standard 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 connection of FORCEnet with the DoD Global Information Grid (GIG) requires all ISSP RDT&E activities to adopt a minimum standard of "best commercial IA practices." The ISSP program examines commercial technologies to determine their fit within Navy architectures, provides feedback to vendors about what the Navy requires, and participates in the standard 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 Information Assurance (IA) expertise and engineering to Navy and joint information system developments. All ISSP technology development efforts endeavor to solve specific Navy and joint IA problems using techniques that speed transition to procurement as soon as possible. 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 the 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 implements requirements in Executive Orders 12333 and 12958 and National Security Decision Directive 145.		

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2014 Navy		DATE: April 2013
APPROPRIATION/BUDGET ACTIVITY 1319: <i>Research, Development, Test & Evaluation, Navy</i> BA 7: <i>Operational Systems Development</i>		R-1 ITEM NOMENCLATURE PE 0303140N: <i>Information Sys Security Program</i>
Major focus areas in FY14 (By Program): Computer Network Defense (CND) - Continue to ensure that security of Navy networks meet the mandates and initiatives of DoD for securing the Global Information Grid (GIG). Continue to develop, integrate, and test defense-in-depth and situational awareness technologies for knowledge-empowered CND operations for afloat and ashore platforms. Continue to develop new capabilities for Navy's Command and Control (C2) architecture and provide technical guidance to ensure CND requirements are met by Consolidated Afloat Network Enterprise Service (CANES). Continue the development and integration of DoD defined tools and capabilities including adaptive defense, security sensors, automation of reporting, monitoring, analysis and response as well as providing modernized patch management, virtualization support, packet capture and processing, and host based security agent tools. Cryptographic (Crypto)/Crypto Modernization (CM) - Initiate development of a Transmission Security (TRANSEC) replacement product for legacy devices. Initiate Intermediary Application (iApp) development efforts and incorporate functionality into specific Navy crypto devices, fill devices support products, or Personal Digital Assistants (PDA). Complete Full Development effort for the Link-22 Modernized Link Level Communications Security (COMSEC) (MLLC) and begin planning transition to production. Conduct Navy system test on VINSON/Advanced Narrowband Digital Voice Terminal (ANDVT) Cryptographic Modernization (VACM) Low Rate Initial Production (LRIP) units. Complete Navy VACM training material development, and all required pre-installation documentation, materials and acquisition support. Continue providing security engineering support for modernization of space crypto systems, embeddable crypto strategies, Unmanned Vehicle/low power crypto, Next Generation crypto initiatives, disposable crypto for tactical apps, Layer 2 encryption, and Tactical Secure Voice (TSV) cross-banding. Continue NSA Certification Authority and acquisition authority for all CM products. Key Management Infrastructure (KMI) - Continue capability, verification testing support to KMI Capability Increment (CI) CI-2 Spiral 2 software. Continue transition strategy and define requirements for incorporation of other KMI roles in Navy architecture (e.g., Controlling Authority, Command Authority). Continue defining capability requirements for KMI CI-3. Continue supporting KMI transition working group meetings, developing white papers and supporting documentation for KMI CI-3. Continue requirements definition support to the development of the next generation fill device. Continue migrating COMSEC Material Work Station/Data Management Device and other next generation fill devices to the KMI environment. Continue engineering the Navy Enterprise system to a centralized configuration management and crypto unit inventory tracking tool, which will improve Electronic Key Management System (EKMS) Tier 3 Simple Key Loaders (SKL), Tactical Key Loaders (TKL), KMI, and Crypto product management. Continue development engineering and testing to the Intermediary Application (iApp) which will enhance KMI secure communications. Continue shipboard bandwidth study with Spiral 2 Software in support of KMI Delivery Only Client (DOC) architecture in the afloat operation environment. Public Key Infrastructure (PKI) - Develop Secret Internet Protocol Router Network (SIPRNet) PKI solutions, including the SIPRNet Validation Authority and Cryptographic Logon(CLO) capability to non-Microsoft systems and Microsoft non-Domain services. Research and test Defense Information Systems Agency (DISA) Online Certificate Status Protocol (OCSP) enhancements for certificate authentication in the Navy afloat and ashore environments. Ensure compatibility and interoperability of PKI with Computer Network Defense (CND) systems architecture. Ensure Navy compliance with new PKI related cryptographic algorithms and certificates changes on the Common Access Card (CAC), Alternate Logon Token (ALT), and SIPRNet hardware token. Research and develop tools to support certificates for Non-Person Entity (NPE) devices and tactical/austere environments. Research Identity and Access Management (IdAM) technologies to increase		

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2014 Navy	DATE: April 2013
---	-------------------------

APPROPRIATION/BUDGET ACTIVITY

1319: *Research, Development, Test & Evaluation, Navy*
 BA 7: *Operational Systems Development*

R-1 ITEM NOMENCLATURE

PE 0303140N: *Information Sys Security Program*

information security on the Global Information Grid (GIG). Investigate virtualization of Navy Certificate Validation Infrastructure (NCVI) servers with Hardware Security Modules.

Information Assurance (IA) Services - Continue to provide security systems engineering support for the development of Department of Defense (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 Command, Control, Communications, & Intelligence (C4I) systems. This includes the expanded requirements to provide complete Identity and Access Management (IdAM) solutions, expanded spectrum monitoring, and data object security and provenance labeling as required in the current DODI 8500.2 and the new DODI 8500.02 IA controls.

B. Program Change Summary (\$ in Millions)	FY 2012	FY 2013	FY 2014 Base	FY 2014 OCO	FY 2014 Total
Previous President's Budget	37.196	26.307	26.532	-	26.532
Current President's Budget	38.747	26.307	23.531	-	23.531
Total Adjustments	1.551	0.000	-3.001	-	-3.001
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	3.094	0.000			
• SBIR/STTR Transfer	-1.543	0.000			
• Program Adjustments	0.000	0.000	0.093	-	0.093
• Rate/Misc Adjustments	0.000	0.000	-3.094	-	-3.094

Congressional Add Details (\$ in Millions, and Includes General Reductions)

Project: 9999: *Congressional Adds*

 Congressional Add: *Cyber Security Research (Cong)*

	FY 2012	FY 2013
	12.000	-
Congressional Add Subtotals for Project: 9999	12.000	0.000
Congressional Add Totals for all Projects	12.000	0.000

Change Summary Explanation

CND Inc 2 IOC was achieved in advance of schedule, moved from 4QFY12 to 3QFY12.

CND Inc 2 IOT&E slipped from 3QFY12 to 4QFY12 due to delayed receipt of Operational Test results.

CND Inc 2 LRIP slipped from 3QFY12 to 4QFY12 due to delayed receipt of Operational Test results.

CND Inc 2 FRP Decision slipped from 4QFY12 to 1QFY13 due to delayed Acquisition Decision Memorandum (ADM) approval.

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2014 Navy		DATE: April 2013
APPROPRIATION/BUDGET ACTIVITY 1319: <i>Research, Development, Test & Evaluation, Navy</i> BA 7: <i>Operational Systems Development</i>		R-1 ITEM NOMENCLATURE PE 0303140N: <i>Information Sys Security Program</i>
CRYPTO KG-45A FOC slipped from 1QFY13 to 4QFY13 due to delay in fielding onboard 1 CG platform. CRYPTO VACM MS C slipped from 3QFY13 to 4QFY13 due to software delays per US Air Force (USAF) Program Office. Milestones are driven by USAF as the lead service. CRYPTO VACM IOC slipped from 3QFY14 to 4QFY14 due to software development delays. CRYPTO VACM LRIP slipped from 3QFY13 to 4QFY13 due to software development delays. CRYPTO VACM FRP Decision slipped from 4QFY13 to 3QFY14 due to software development delays and contracting strategy moving to USAF contract sole source justification. CRYPTO KW-46M Common Submarine Radio Room (CSRR) integration test end date slipped from 2QFY12 to 1QFY13 due to availability of Naval Undersea Warfare Center (NUWC) test lab. CRYPTO VACM IOT&E end date slipped from 1QFY14 to 2QFY14 due to software development delays. CRYPTO KG-45A deliveries end date shifted from 1QFY13 to 4QFY13 due to delay in fielding onboard 1 CG platform. CRYPTO Link-22 MLLC Prototype delivery end date shifted from 2QFY12 to 3QFY12 due to contract performance issues (SAFENET). CRYPTO VACM LRIP deliveries shifted from 3QFY13 to 2QFY14 due to change in delivery schedule. CRYPTO VACM FRP delivery start date shifted from 1QFY14 to 4QFY14 due to software development delays. TKL IOC slipped from 1QFY13 to 2QFY13 and FOC slipped from 1QFY15 to 2QFY15 due to late Acquisition Decision Memorandum (ADM) approval and contract award. KMI CI-2 IOC is a NSA driven milestone and equipment was funded by NSA at limited Navy sites; IOC shifted from 3QFY12 to 4QFY12 due to NSA test schedule delays. KMI CI-2 FOC slipped from 1QFY17 to 3QFY18 to align to Chief of Naval Operations (CNO) ship availabilities. KMI CI-2 IOT&E is a NSA driven milestone and equipment was funded by NSA at limited Navy sites; slipped from 3QFY12 to 4QFY12 due to NSA test schedule delays. TKL production First Article (FA) test was completed 2QFY12. TKL Full Rate Production (FRP) Decision slipped from 3QFY12 to 1QFY13 due to Milestone Decision Authority (MDA) decision on FRP events. KMI CI-2 Spiral 1 LRIP contract was awarded 4QFY12. KMI Spiral 1 FRP slipped from 1QFY13 to 2QFY13 due to NSA test schedule delays. KMI Spiral 2 FRP slipped from 1QFY14 to 4QFY14 due to NSA schedule delays. EKMS Phase V SW delivery end date shifted from 1QFY13 to 2QFY13 due to final fielding. SKL delivery end date shifted from 3QFY13 to 4QFY15 due to later fielding of Next Generation Fill Devices to coincide with KMI Over the Network Key (OTNK) capability. TKL delivery start date shifted from 1QFY13 to 3QFY13 due to delay in Full Rate Fielding Decision (FRFD). KMI CI-2 Spiral 1 LRIP deliveries shifted from 4QFY12 to 1QFY14 through 3QFY14 due to NSA test schedule delays.		

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2014 Navy		DATE: April 2013
APPROPRIATION/BUDGET ACTIVITY 1319: <i>Research, Development, Test & Evaluation, Navy</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140N: <i>Information Sys Security Program</i>	
KMI CI-2 Spiral 2 delivery start date shifted from 3QFY13 to 4QFY14 due to NSA schedule changes; Delivery end date shifted from 1QFY17 to 3QFY18 due to CNO availabilities of ships. Next Generation Fill Device delivery start date shifted from 1QFY13 to 1QFY16 to support Crypto Mod initiative for KMI awareness and will coincide with NSA KMI OTNK capability in FY15. Funding: FY 2014 \$3M reduction will descope Cyber Security Research efforts (\$2.5M) and Crypto systems engineering efforts (\$0.5M). Technical: N/A		

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2014 Navy										DATE: April 2013		
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)	All Prior Years	FY 2012	FY 2013 [#]	FY 2014 Base	FY 2014 OCO ^{##}	FY 2014 Total	FY 2015	FY 2016	FY 2017	FY 2018	Cost To Complete	Total Cost
0734: Communications Security R&D	250.782	24.081	23.641	21.130	-	21.130	24.865	23.544	23.034	23.429	Continuing	Continuing
Quantity of RDT&E Articles	0	0	0	0		0	0	0	0	0		

[#] FY 2013 Program is from the FY 2013 President's Budget, submitted February 2012

^{##} The FY 2014 OCO Request will be submitted at a later date

A. Mission Description and Budget Item Justification

The Information Systems Security Program (ISSP) Research Development Test & Evaluation (RDT&E) 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 United States (US) Navy communications systems.

ISSP RDT&E personnel work closely with the Navy's Information Operations (IO) - Exploit (Signals Intelligence (SI)) and IO - Attack (Information Warfare (IW)) 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 products integrate 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 to counter evolving and increasingly sophisticated threats, in accordance with The Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510 requirements. Communication Security (COMSEC) and Transmission Security (TRANSEC) evolution are from stand-alone dedicated devices to embedded modules incorporating National Security Agency (NSA) approved cryptographic engines, loaded with the certified algorithms and key, and interconnected via industry-defined interfaces. This includes the Department of Defense (DoD) Global Information Grid (GIG) capability requirements document for the development of Content Based Encryption (CBE).

North Atlantic Treaty Organization (NATO) Improved Link Eleven (NILE) is a cooperative development project for Link 22 involving 7 nations: United States, Germany, France, United Kingdom, Canada, Italy and Spain. The US is responsible for all coordination of Information Security (INFOSEC) activities under the NILE project. In addition, the US controls the release of the crypto capability to the nations and all potential 3rd parties. The current Link 22 crypto (Link Level Crypto (LLC)) is obsolete and needs to be modernized per NSA and CJCS Crypto Modernization mandates.

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2014 Navy		DATE: April 2013
APPROPRIATION/BUDGET ACTIVITY 1319: <i>Research, Development, Test & Evaluation, Navy</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140N: <i>Information Sys Security Program</i>	PROJECT 0734: <i>Communications Security R&D</i>
In addition to protecting national security information, ISSP RDT&E efforts 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. ISSP RDT&E must also provide solutions to the most advanced state-sponsored and criminal-intent advanced persistent threats, including those to platform Information Technology (IT), weapons systems, Industrial Control (ICS), and Supervisory Control and Data Acquisition (SCADA). The Information Systems Security Program (ISSP) today includes more than legacy Communication Security (COMSEC) and network security technology. Information Assurance (IA) or defensive Information Operations (IO) 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 Research Development Test & Evaluation (RDT&E) efforts provide dynamic risk-managed IA solutions to the Navy information infrastructure, not just security devices placed within a network. Extensive effort will be placed on rapidly providing solutions required for the new DODI 8500.02, CNSSI 1253, and NIST SP 800-53 IA control set, focused primarily on espionage and sabotage capable, state-sponsored advanced persistent threats. Additional efforts will include the implementation of data object security labeling and provenance metadata, also required by DODI 8500.02, which is a major enabler for cross domain data sharing. 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 (TRANSEC) 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 SmartCards and similar security tokens; (7) Electronic Key Management System (EKMS) devices such as Simple Key Loaders (SKL), COMSEC Material Work Stations (CMWS), and Key Management Infrastructure (KMI) equipment (Client Management (MGC)/Advanced Key Processor (AKP) MGC/AKPs, High Assurance Protocol Equipment, Delivery Only Client (DOC) and Next Generation devices. ISSP efforts conclude with continuously monitored, certified, and accredited systems supported within Navy cyber operational environments. Achieving and maintaining this milestone requires: * Evolving techniques for defense of National Security Systems (NSS) and Information against advanced persistent threats, including process, control, and sensor layers; * Approved techniques for the assured separation of information levels and user communities, including allied, coalition, non-Governmental, Defense Industrial Base, and other public partners; * Rapid deployment of technologies supporting the Navy's Computer Network Defense Service Providers (CNDSP) operations; * Hardware and software to assure end-to-end resilience of the Navy's telecommunications infrastructure and availability of the critical wireless spectrum resource; * High robustness interfaces with joint user and platform cyberspace domains, using a defense-in-depth architecture;		

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2014 Navy		DATE: April 2013
APPROPRIATION/BUDGET ACTIVITY 1319: <i>Research, Development, Test & Evaluation, Navy</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140N: <i>Information Sys Security Program</i>	PROJECT 0734: <i>Communications Security R&D</i>
* COMSEC and process isolation techniques for securing the critical computing base and information store. The cyberspace domain has virtually eliminated the traditional distinction between telecommunications and information systems. Because cyber security is a cradle-to-grave enterprise-wide discipline, this program applies the set of best practices embodied within the Committee on National Security Systems Instruction (CNSSI) 1253. Of special note is the Navy's cyber security role in the joint Cryptographic Modernization Program, required by Chairman of the Joint Chiefs of Staff Instructions (CJCSI) 6510.02D, providing high assurance and other cryptographic technologies protecting cyber systems. The parallel Security Management Infrastructure (SMI) program develops, evaluates, and applies new emerging technologies and enhanced capabilities to the EKMS/KMI. Additional efforts will focus on the architecture, design, and development of systems to manage the security parameters (e.g., 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 EKMS/KMI Infrastructure technology, and the development of improved techniques for key and certificate management. Information Systems Security Program (ISSP) Research Development Test & Evaluation (RDT&E) management will direct a program that: * Ensures the Navy's cyber domain implements consistent joint and enterprise cyber security architecture; * Rapidly develops and deploys the latest versions of cyber security measures across all seven layers of the Information Organization of Standardization (ISO) Open Systems Interconnection Reference Model and for all Committee on National Security Systems Instruction (CNSSI) 1253 Information Assurance (IA) controls (best practices); * Ensures that all data within the Navy Enterprise is protected in accordance with its classification and mission criticality, as required by law; * Provides Fleet Cyber Command and Commander U.S. Tenth Fleet (C10F) with integrated tools and techniques to protect, detect, restore, and respond to cyber events and incidents; * Supports the Navy Computer Network Defense (CND) provider by enabling cyber situational awareness; * Defends against and detects the unauthorized modification or disclosure of data outside the Navy cyber domain, such as in the WikiLeaks incident; * Provides a risk-managed means of selectively allowing information to flow across the enclave boundary while ensuring proper marking and provenance; * Provides strong authentication of users accessing services from Navy cyberspace; * Defends against the unauthorized use of a host or application, particularly operating systems, control and process systems, and supervisory control and data acquisition systems; * Maintains cyber security configuration management of all hosts to track patches and system configuration changes; * Ensures adequate defenses against subversive acts of trusted people and systems, both internal and external; * Provides a Communications Security (COMSEC) infrastructure that supports key, privilege, and certificate management; and that enables positive identification of individuals utilizing network services; and, * Provides a continuous monitoring, analysis, assessment, situational awareness, and response infrastructure.		

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2014 Navy		DATE: April 2013
APPROPRIATION/BUDGET ACTIVITY 1319: <i>Research, Development, Test & Evaluation, Navy</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140N: <i>Information Sys Security Program</i>	PROJECT 0734: <i>Communications Security R&D</i>
Maritime Operations Center (MOC) networks will operate and share information with multiple partners in varying circumstances. The MOCs will receive integrated tools to maintain a Network Operations (NetOps) Common Operational Picture (COP) and support Command and Control (C2) of the Communications Systems (CS) through the ability to analyze and develop Courses of Action (COA) to manage C2 cyberspace operations. This includes CYBER Surveillance, bandwidth monitoring, INTEL situational awareness tools, and network health monitoring. NetOps COP will provide a proactive view and enhanced security tool for use by CYBER network managers. NetOps COP ensures validity of the COP, network health, and provides operator synchronization with Information Operations (IO), and situational awareness of the cyber battle space. A combination of software tools, interoperable enabling hardware and processes will be provided to monitor and visualize network traffic and to provide a locally-generated, fused situational awareness picture for battle watch decision making. 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 14 Highlights for Information Systems Security Programs (ISSP): Computer Network Defense (CND) - Continue to implement Department of Defense (DoD)/Information Assurance (IA)/CND Enterprise Solutions Steering Group (ESSG) tools into Outside the Continental United States (US) Navy Enterprise Network (ONE-Net), Information Technology for the 21st Century (IT-21), and other networks such as Cyber Asset Reduction & Security (CARS) as required. Support the DoD/ESSG development and integration of CND capabilities into the Navy's architecture and support the addition of these capabilities into the Commander U.S. Tenth Fleet (C10F) Maritime Operations Center (MOC). Continue to integrate CND capabilities to perform near real-time analysis of events and Advanced Persistent Threats (APT). Update the Computer Network Defense (CND) Information Assurance (IA) suites with adaptive defense, security sensors, incident reporting, correlation, packet capture and processing, and situational awareness capabilities. Achieve cost and performance efficiencies by consolidating IA services in the Outside the Continental United States (US) Navy Enterprise Network (ONE-Net) environment and by furthering efforts to virtualize CND capabilities. Continue to develop, integrate, and test defense-in-depth and situational awareness technologies for knowledge-empowered CND operations for afloat and ashore platforms. Promote Course of Action (COA) development analysis and execution to improve interoperability with the Global NetOps Information Sharing Environment. Develop enhancements and continue evaluation of needs derived from the CND Capabilities Steering Group to advance analysis and response to network threats. CND will continue to deploy integrated tools at the C10F MOC in order to maintain Cyber Situational Awareness (CSA) to support Command and Control (C2) of the Communications Systems (CS). CSA provides near immediate risk assessments, actionable intelligence and immediate mitigation COAs and attribution of on-going CS protection events in order to enable the apportionment of forces with exacting control in response to national objectives. Develop and further Joint Capability Technology Demonstration (JCTD) delivered capability to adaptively manage risks to operational networks throughout an Area of Responsibility to provide defense-in-depth by functionally segmenting networks through the deployment of Virtual Secure Enclaves (VSE) and utilization of black core transport services to protect key cyber terrain. Cryptographic (Crypto)/Crypto Modernization (CM) - Initiate development of a Transmission Security (TRANSEC) replacement product for legacy devices. Initiate Intermediary Application (iApp) development efforts and incorporate functionality into specific Navy crypto devices, fill devices support products, or Personal Digital Assistants (PDA). Complete Full Development effort for the Link-22 Modernized Link Level Communications Security (COMSEC) (MLLC) and begin planning transition to production. Conduct Navy system test on VINSON/Advanced Narrowband Digital Voice Terminal (ANDVT) Cryptographic Modernization (VACM) Low Rate Initial Production (LRIP) units. Complete Navy VACM training material development, and all required pre-installation documentation, materials and acquisition support.		

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2014 Navy		DATE: April 2013		
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		
Continue providing security engineering support for modernization of space crypto systems, embeddable crypto strategies, Unmanned Vehicle/low power crypto, Next Generation crypto initiatives, disposable crypto for tactical apps, Layer 2 encryption, and Tactical Secure Voice (TSV) cross-banding. Continue National Security Agency (NSA) certification authority and acquisition authority for all CM products.				
Key Management Infrastructure (KMI) - Continue capability, verification testing support to KMI Capability Increment (CI) CI-2 Spiral 2 software. Continue transition strategy and define requirements for incorporation of other KMI roles into Navy architecture (e.g., Controlling Authority, Command Authority). Continue defining capability requirements for KMI CI-3. Continue supporting KMI transition working group meetings, developing white papers and supporting documentation for KMI CI-3. Continue requirements definition support to the development of the next generation fill device. Continue migrating COMSEC Material Work Station/Data Management Device and other next generation fill devices to the KMI environment. Continue engineering the Navy Enterprise system to a centralized configuration management and crypto unit inventory tracking tool, which will improve Electronic Key Management System (EKMS) Tier 3 Simple Key Loaders (SKL), Tactical Key Loaders (TKL), KMI and Crypto product management. Continue development engineering and testing to the Intermediary Application (iApp) which will enhance KMI secure communications. Begin shipboard bandwidth study in support of KMI Delivery Only Client (DOC) architecture in the afloat operational environment.				
Public Key Infrastructure (PKI) - Develop Secret Internet Protocol Router Network (SIPRNet) PKI solutions, including the SIPRNet Validation Authority and Cryptographic Logon (CLO) capability to non-Microsoft systems and Microsoft non-Domain services. Research and test Defense Information Systems Agency (DISA) Online Certificate Status Protocol (OCSP) enhancements for certificate authentication in the Navy afloat and ashore environments. Ensure compatibility and interoperability of PKI with CND systems architecture. Ensure Navy compliance with new PKI related cryptographic algorithms and certificate changes on the Common Access Card (CAC), Alternate Logon Token (ALT), and SIPRNet hardware token. Research and develop tools to support certificates for Non-Person Entity (NPE) devices and tactical/austere environments. Research Identity and Access Management (IdAM) technologies to increase information security on the Global Information Grid (GIG). Investigate virtualization of Navy Certificate Validation Infrastructure (NCVI) servers with Hardware Security Modules.				
Information Assurance (IA) Services - Continue to provide security systems engineering support for the development of Department of Defense (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. This includes the expanded requirements to provide complete Identity and Access Management (IdAM) solutions, expanded spectrum monitoring, and data object security and provenance labeling as required in current DODI 8500.2 and the new DODI 8500.02 IA controls.				
B. Accomplishments/Planned Programs (\$ in Millions, Article Quantities in Each)		FY 2012	FY 2013	FY 2014
Title: Computer Network Defense (CND)		7.844	9.871	7.539
Articles:		0	0	0
FY 2012 Accomplishments:				
Incorporated DoD mandated network security tools into the next sub-increment of CND afloat and ashore design. Efforts included deployments of Host Based Security Systems (HBSS) to afloat Non-Secure Internet Protocol Router Network (NIPRNet) enclaves, network mapping and leak detection solutions, and configuration compliance and remediation tools. Developed the Navy implementation of DoD-mandated tools and capabilities with the guidance of the Navy CND Capabilities Integrated Product Team (IPT). Began CND Increment 2 technology insertion cycles (rapid acquisition) to address current and emergent real world threats,				

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2014 Navy		DATE: April 2013	
APPROPRIATION/BUDGET ACTIVITY 1319: <i>Research, Development, Test & Evaluation, Navy</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140N: <i>Information Sys Security Program</i>	PROJECT 0734: <i>Communications Security R&D</i>	
B. Accomplishments/Planned Programs (\$ in Millions, Article Quantities in Each)		FY 2012	FY 2013
performance improvements, and end-of-life issues. Continued meeting Increment 2 Capability Production Document (CPD) performance parameters and addressed key system attributes. Supported Developmental Test (DT), Initial Operational Test and Evaluation (IOT&E) and associated readiness reviews required for CND Increment 2 to achieve Full-Rate Production (FRP) decision. FY 2013 Plans: Continue to ensure that security of Navy networks will meet DOD mandates and initiatives for securing the Global Information Grid (GIG). Continue to develop, integrate, and test defense-in-depth and situational awareness technologies for knowledge-empowered CND operations for afloat and shore installations. Continue to support the development and deployment of new capabilities into the Navy's architecture and provide technical guidance to ensure CND requirements are met by Consolidated Afloat Networks and Enterprise Services (CANES). Continue to support DoD defined tools and capabilities including automation of reporting, monitoring, analysis and response as well as providing modernized patch management and host based security agent tools. Continue to integrate CND capabilities to perform near real-time analysis of events and Advanced Persistent Threat (APT). Update the CND Information Assurance (IA) suites with adaptive defense, incident reporting, correlation, and situational awareness capabilities. Promote Course of Action (COA) development analysis and execution to improve interoperability with the Global Network Operations (NetOps) Information Sharing Environment. Develop enhancements and continue evaluation of needs derived from the CND Capabilities Steering Group to advance analysis and response to network threats. Commander United States Tenth Fleet (C10F) Maritime Operations Center (MOC) - Leverage the Ozone Widget framework and the US Cyber Command Cyber Pilot architecture to deliver visualization and analysis tools in support of NetOps Common Operational Picture (COP) at the C10F MOC. FY 2014 Plans: Continue to ensure that security of Navy networks meet Department of Defense (DoD) mandates and initiatives for securing the GIG. Continue to develop, integrate, and test defense-in-depth and situational awareness technologies for knowledge-empowered Computer Network Defense (CND) operations for afloat and shore platforms. Continue to develop new capabilities for the Navy's Command and Control (C2) architecture and provide technical guidance to ensure CND requirements are met by Consolidated Afloat Network Enterprise Service (CANES). Continue the development and integration of DoD defined tools and capabilities including adaptive defense, security sensors, automation of reporting, monitoring, analysis, and response, as well as providing modernized patch management and host based security agent tools. Continue to implement DoD/Information Assurance (IA)/CND Enterprise Solutions Steering Group (ESSG) tools into Outside the Continental US Navy Enterprise Network (ONE-Net), Information Technology for the 21st Century (IT-21), and other networks such as Cyber Asset Reduction & Security (CARS) as required. Support the DoD/ESSG development and integration of CND capabilities into the Navy's architecture and support the addition of these capabilities into the Commander United States Tenth Fleet (C10F) MOC. Continue to integrate CND capabilities to perform near real-time analysis of events and Advanced Persistent Threat (APT). Update the CND IA suites with adaptive			

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2014 Navy		DATE: April 2013	
APPROPRIATION/BUDGET ACTIVITY 1319: <i>Research, Development, Test & Evaluation, Navy</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140N: <i>Information Sys Security Program</i>	PROJECT 0734: <i>Communications Security R&D</i>	
B. Accomplishments/Planned Programs (\$ in Millions, Article Quantities in Each)		FY 2012	FY 2013
defense, incident reporting, correlation, packet capture and processing, and situational awareness capabilities. Achieve cost and performance efficiencies by consolidating IA services in the ONE-Net environment and by furthering efforts to virtualize CND capabilities. Promote Course of Action (COA) development analysis and execution to improve interoperability with the Global NetOps Information Sharing Environment. Develop enhancements and continue evaluation of needs derived from the CND Capabilities Steering Group to advance analysis and response to network threats. Determine optimal technical and governance solutions for interception of outbound encrypted traffic, allowing for inspection and control. CND will continue to deploy integrated tools at the C10F MOC in order to maintain Cyber Situational Awareness (CSA) to support C2 of the Communications Systems (CS). CSA provides near real time risk assessments, actionable intelligence, mitigation COAs and attribution of on-going CS Protection events. Develop a Joint Capability Technology Demonstration (JCTD)-delivered capability to adaptively manage risks to operational networks throughout an Area of Responsibility to provide defense-in-depth by functionally segmenting networks through the deployment of Virtual Secure Enclaves (VSE) and utilization of black core transport services to protect key cyber terrain.			
Title: Crypto/Crypto Modernization (CM)			
Articles:			
FY 2012 Accomplishments: Continued research, evaluation, and prioritization of cryptographic products in coordinaton with the Information Systems Security Program (ISSP) Office and the National Security Agency (NSA). Continued identifying strategies to reduce the overall crypto inventory within the Department of the Navy (DoN) to realize long term cost savings. Continue to support the on-going Cryptographic Joint Algorithm Integrated Product Team (IPT) and representing the Navy at the Crypto Products Team (CPT) IPT. Provided consistent Information Assurance (IA) engineering support for the development and integration of Crypto Mod (CM) products. Researched disposition and replacement of devices on the Crypto Priority (Red) List. Conducted research into making modern crypto devices Key Management Infrastructure (KMI) aware (e.g., iApp development). Continued supporting the development for the Link-16 CM through: (1) performing technical Analysis of Alternatives (AoA) for vendor Type 1 Crypto devices and security architecture implementations; (2) conducting security risk analysis; (3) reviewing security requirement specifications/ test plans; (4) developing systems engineering documents into technical documentation to ensure the implementation of robust IA solutions; and (5) providing Subject Matter Experts (SME)technical support to multi-functional Link-16 CM development teams. Provided Link-22 cryptographic modernization management and engineering support to the Modernized Link Level Communications Security (COMSEC) (MLLC) effort, to include finalizing development of various engineering documents and specifications to support development, as well as testing, of the Link-22 Proof of Concept units. North Atlantic Treaty Organization (NATO) Improved Link Eleven (NILE) is a cooperative development project for Link-22 involving 7 nations: United States, Germany, France, United Kingdom, Canada, Italy and Spain. The United States (US) is responsible for all coordination of Information Security (INFOSEC) activities under the NILE project. In addition, the US controls the release of the crypto capability to the nations and all potential 3rd parties. The current Link-22 crypto Link Level Crypto (LLC), is obsolete and needs to be		10.251 0	8.052 0
			7.857 0

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2014 Navy		DATE: April 2013		
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 2012	FY 2013	FY 2014
modernized per NSA and CJCS Crypto Modernization mandates. Funds will keep the Modernized Link Level Crypto (MLLC) effort on schedule. Facilitated KW-46 Modernization Enterprise Change Request (ECR) process to consolidate test reports for the Material Licensing Tracking System (MLTS) testing at Naval Undersea Warfare Center (NUWC), and assist with fielding. KW-46M work entailed integration testing, Emergency Action Message (EAM) and Targeting Change Message (TCM) certifications, and integration into the Common Submarine Radio Room (CSRR). Continued Secure Voice (SV) RDT&E efforts and Naval Research Laboratory's (NRL) research into Secure Voice (SV) emerging technologies and related technical products. Provided technical support from the Navy perspective to Air Force led VINSON/Advanced Narrowband Digital Voice Terminal Crypto Modernization (VACM) program, as well as continued support to Office of Secretary of Defense (OSD) Chief Information Officer (CIO) Nuclear Command & Control, Nuclear Command Control & Communications (NC2/NC3) Crypto Modernization (CM). Began coordinating a Crypto Mod plan for Transmissions Security (TRANSEC) modernization with NSA and other services. Began investigating Government off the Shelf (GOTS)/Commercial off the Shelf (COTS) crypto technology refresh strategies, updating OPNAVINST 2300.4G, identifying baseline for Crypto graphic equipment suite for Afloat environment, space systems/embeddable crypto modernization strategy, and system engineering support for Unmanned Aerial Vehicle (UAV)/Lower Powercryptographic solutions. Provided acquisition support, National Security Agency (NSA) Certification Authority, and data testing.				
FY 2013 Plans: Continue research, evaluation, and prioritization of cryptographic products for modernization. Continue coordination with NSA and support to the Cryptographic Joint Algorithm Integrated Product Team (IPT). Continue identifying strategies to reduce the overall crypto inventory within the Department of the Navy (DoN) to realize long term cost savings. Continue to provide research into replacement/modernization of devices on the Crypto Priority (Red) list. Continue providing systems engineering services in support of execution of the Link-22 Modernized Link Level COMSEC (MLLC) Full Development effort. This will include interfacing with the NATO NILE Program Management Office (PMO), NSA, Northrup Grumman (NG) and the vendor to ensure all development activities continue as scheduled, all contract documentation is reviewed and that all program requirements are met. Conduct research into making modern crypto devices Key Management Infrastructure (KMI) Aware focusing on the Intermediary Application (iApp) (development or similar product). Provide consistent Information Assurance (IA) engineering support for the development and integration of CM products. Continue development for the Link-16 CM through performing technical Analysis of Analysis of Alternatives (AoA) for vendor Type 1 Crypto devices and security architecture implementations. Complete all outstanding KW-46M integration testing to support installation as part of the Common Submarine Radio Room (CSRR) deployment. Continue Naval Research Laboratory's (NRL) research into Secure Voice (SV) technology and begin development of a cross-banding technology to support VINSON/Advanced Narrowband Digital Voice Terminal Crypto Modernization (VACM) introduction into Navy secure voice gateways architecture. Provide technical support on behalf of DoN, as well as supporting Air Force VACM Development Test (DT) and Operational Test (OT) and Navy system tests on production representative Engineering Development Models (EDM). Conduct Navy VACM Independent Logistics Assessment (ILA) and provide support to Milestone C (MS C) decision. Continue providing security engineering support for Office of Secretary of Defense (OSD) Chief				

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2014 Navy		DATE: April 2013		
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 2012	FY 2013	FY 2014
Information Officer (CIO) NC2/ NC3 Crypto Modernization (CM) efforts on behalf of the Navy. Transition Transmission Security (TRANSEC) Request For Information (RFI) items into potential CM solutions and coordinate with the National Security Agency and other services. Complete the update of OPNAVINST 2300.4G. Continue investigation into crypto replacement strategies for ground terminals of space systems, as well as replacements for legacy/embeddable crypto. Complete initial system engineering support (Request for Information development) to Unmanned Vehicle/low power crypto options and determine way forward for Navy modernization. Research potential solutions for disposable crypto for tactical apps and Layer 2 encryption techniques. Continue providing support for National Security Agency (NSA) Certification Authority, acquisition support and data testing for all cryptographic modernization efforts. FY 2014 Plans: Initiate development of a TRANSEC replacement product for legacy devices. Initiate intermediary Application (iApp) development efforts and incorporate functionality into specific Navy crypto devices, fill devices, support products, and Personal Digital Assistants (PDA). Conduct Navy system test on VACM Low Rate Initial Production (LRIP) units. Complete Navy VACM training material development and all required pre-installation documentation and materials, and acquisition support. Continue providing security engineering support for modernization of space crypto systems, embeddable crypto modernization strategies, Unmanned Aerial Vehicle (UAV)/Lower Power crypto way ahead, Next Generation Crypto (Post 2018) initiatives, disposable crypto for tactical apps, Layer 2 encryption and Tactical Secure Voice (TSV) cross-banding. Complete Full Development effort for the Link-22 Modernized Link Level Communications Security (COMSEC) (MLLC) and begin planning transition to production. This includes close coordination efforts with North Atlantic Treaty Organization (NATO) Improved Link Eleven (NILE) Program Management Office (PMO), NATO Nations, NSA, and the vendor to ensure all development activities continue as scheduled, all contract documentation is reviewed, and that all program requirements are met. Continue providing for NSA Certification Authority, acquisition authority, and data testing for all CM efforts.				
Title: Key Management Infrastructure (KMI) Articles:		2.532 0	2.665 0	2.643 0
FY 2012 Accomplishments: Continued transition strategy and defined requirements for incorporation of other Key Management Infrastructure (KMI) roles into Navy architecture (e.g., Controlling Authority, Command Authority). Continued supporting KMI transition working group meetings, developing white papers and supporting documentation for KMI. Began engineering and development efforts for KMI Capability Increment (CI) CI-2 Spiral 2 Spin 1 for incorporation into Navy architectures and networks. Tested KMI Manager Client(MGC)/Advanced Key Processors (AKP) at selected pilot sites in support of National Security Agency (NSA) full rate production decision. Provided requirements definition support to the development of the next generation fill device. Migrated Communications Security (COMSEC) Material Work Station/Data Management Device and other next generation fill devices to the KMI environment. Provided research and analysis to a centralized configuration management and crypto unit inventory tracking tool which will				

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2014 Navy		DATE: April 2013	
APPROPRIATION/BUDGET ACTIVITY 1319: <i>Research, Development, Test & Evaluation, Navy</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140N: <i>Information Sys Security Program</i>	PROJECT 0734: <i>Communications Security R&D</i>	
B. Accomplishments/Planned Programs (\$ in Millions, Article Quantities in Each)		FY 2012	FY 2013
improve Electronic Key Management System (EKMS) and Crypto product management. Began research and analysis to the Intermediary application (iApp) which will enhance KMI secure communications.			
FY 2013 Plans: Begin capability, engineering development and verification testing support to Key Management Infrastructure (KMI) Capability Increment (CI)-2 Spiral 2 Spin 2. Continue transition strategy and define requirements for incorporation of other KMI roles into Navy architecture (e.g., Controlling Authority, Command Authority). Continue supporting KMI transition working group meetings, developing white papers and supporting documentation for KMI. Continue requirements definition support to the development of the next generation fill device. Continue Migrating Communications Security (COMSEC) Material Work Station/Data Management Device and other next generation fill devices to the KMI environment. Begin shipboard bandwidth study in support of KMI Manager Client (MGC) architecture in the afloat operational environment. Begin to define capability requirements for KMI CI-3. Provide engineering and analysis to a centralized configuration management and crypto unit inventory tracking tool which will improve Electronic Key Management System (EKMS) and Crypto product management. Provide engineering and analysis to the Intermediary Application (iApp) which will enhance KMI secure communications. Define KMI Delivery Only Client (DOC) solution requirements.			
FY 2014 Plans: Continue capability, verification testing support to KMI CI-2 Spiral 2 software. Continue transition strategy and define requirements for incorporation of other KMI roles into Navy architecture (e.g., Controlling Authority, Command Authority). Continue defining capability requirements for KMI CI-3. Continue supporting KMI transition working group meetings, developing white papers and supporting documentation for KMI CI-3. Continue requirements definition support to the development of the next generation fill device. Continue migrating COMSEC Material Work Station/Data Management Device and other next generation fill devices to the KMI environment. Continue engineering the Navy Enterprise system to a centralized configuration management and crypto unit inventory tracking tool, which will improve EKMS Tier 3 Simple Key Loader (SKL), Tactical Key Loader (TKL), KMI, and Crypto product management. Continue development engineering and testing to the Intermediary Application (iApp) which will enhance KMI secure communications. Continue shipboard bandwidth study with Spiral 2 Software in support of KMI MGC and begin bandwidth study in support of KMI DOC architecture in the afloat operational environment.			
Title: Public Key Infrastructure (PKI)		0.381	0.404
Articles:		0	0
FY 2012 Accomplishments: Researched, analyzed and evaluated Public Key Infrastructure (PKI) enabled products such as Virtual Private Networks (VPN), routers, switches, servers, and Secret Internet Protocol Router Network (SIPRNet) Token Management System for their suitability to support Navy needs for Non-Person Entity (NPE) certificates and Global Information Grid (GIG) identity management and protection requirements. Provided systems engineering support for SIPRNet Public Key Infrastructure (PKI) enabling to Navy			

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2014 Navy		DATE: April 2013		
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 2012	FY 2013	FY 2014
Programs of Record (POR) for integration. This included research, analysis, and evaluation of PKI enabled products and methods to support the manual and automatic enrollment and issuance of PKI NPE certificates to Navy servers and devices. Evaluated Defense Information Systems Agency's (DISA) auto-enrollment and registration services for Phases II and III of Department of Defense (DoD) PKI-enabled Implementation. Researched, analyzed, and evaluated PKI enabled products for non-Microsoft devices and systems (e.g., Linux, Apple, servers, router, switches). Explored enhancements of PKI related cryptographic algorithms. Researched advancements of Navy Certificate Validation Infrastructure (NCVI) configurations to utilize DISA's Robust Certificate Validation Services (RCVS) capability for Online Certificate Status Protocol (OCSP).				
FY 2013 Plans: Continue to research, analyze and evaluate Public Key (PK)-enabled (PKE) products (Microsoft and non-Microsoft) such as Virtual Private Networks (VPNs), routers, switches, and servers for their suitability to support Navy requirements for Non-Person Entity (NPE) certificates and to support Global Information Grid (GIG) identity management and protection requirements. Continue to provide systems engineering support for SIPRNet Public Key Infrastructure (PKI) enablement to Navy Program of Record (POR) for integration to include research and support for non-Microsoft systems PKI solutions. Continue to support the manual and automatic enrollment and issuance of PKI NPE certificates to Navy servers and devices. Continue to evaluate Defense Information Systems Agency's (DISA) auto-enrollment and registration services for Department of Defense (DoD) PKI enabled devices. Continue to research and evaluate new technologies and develop solutions to enable the Navy's PKI to process new cryptographic algorithms and new secure hash algorithms (e.g., SHA-256, Elliptic Curve Cryptography). Test and evaluate DISA Online Certificate Status Protocol (OCSP) enhancements for certificate authentication in the Navy afloat and ashore environment. Continue to ensure interoperability of PKI with Computer Network Defense (CND) systems architecture.				
FY 2014 Plans: Develop Secret Internet Protocol Router Network (SIPRNet) PKI solutions, including the SIPRNet Validation Authority and Cryptographic Logon (CLO) capability to non-Microsoft systems and Microsoft non-Domain services. Research and test DISA OCSP enhancements for certificate authentication in the Navy afloat and ashore environments. Ensure compatibility and interoperability of PKI with CND systems architecture. Ensure Navy compliance with new PKI related cryptographic algorithms and certificate changes on the Common Access Card (CAC), Alternate Logon Token (ALT), and SIPRNet hardware token. Research and develop tools to support certificates for Non-Person Entity (NPE) devices and tactical/austere environments. Research Identity and Access Management (IdAM) technologies to increase information security on the GIG. Investigate virtualization of Navy Certificate Validation Infrastructure (NCVI) servers with Hardware Security Modules.				
Title: Information Assurance (IA) Services		2.573	2.649	2.682
Articles:		0	0	0
FY 2012 Accomplishments:				

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2014 Navy		DATE: April 2013	
APPROPRIATION/BUDGET ACTIVITY 1319: <i>Research, Development, Test & Evaluation, Navy</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140N: <i>Information Sys Security Program</i>	PROJECT 0734: <i>Communications Security R&D</i>	
B. Accomplishments/Planned Programs (\$ in Millions, Article Quantities in Each)		FY 2012	FY 2013
Provided security systems engineering support for the development of Department of Defense (DoD) and Department of the Navy (DoN) Information Assurance (IA) architectures and the transition of new technologies to address Navy IA challenges. Provided updates to the Navy Information Assurance (IA) master plan that reflect emerging priorities and addressed Navy specific threats. Coordinated IA activities across the virtual System Command (SYSCOM) via the IA Trusted Architecture (TA) to ensure the security design and integration of Computer Adaptive Network Defense In Depth (CANDiD) 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. Provided IA risk analysis and recommended risk mitigation strategies for Navy critical networks and Command, Control, Communications, Computers & Intelligence (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. Continued to evaluate products for security issues and developed guidance and procedures for the design and integration of risk mitigation strategies via appropriate Information Assurance (IA) controls. FY 2013 Plans: Continue to provide security systems engineering support for the development of Department of Defense (DoD) and Department of the Navy (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 Computer Adaptive Network Defense-in-Depth (CANDiD) 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. FY 2014 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 Trusted Architecture (TA) to ensure the security design and integration of Computer Adaptive Network Defense-in-Depth (CANDiD) 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. Extensive effort will be placed on rapidly providing solutions			

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2014 Navy							DATE: April 2013				
APPROPRIATION/BUDGET ACTIVITY 1319: <i>Research, Development, Test & Evaluation, Navy</i> BA 7: <i>Operational Systems Development</i>				R-1 ITEM NOMENCLATURE PE 0303140N: <i>Information Sys Security Program</i>			PROJECT 0734: <i>Communications Security R&D</i>				
B. Accomplishments/Planned Programs (\$ in Millions, Article Quantities in Each)							FY 2012	FY 2013	FY 2014		
required for the new DODI 8500.02, CNSSI 1253, and NIST SP 800-53 IA control set, focused primarily on espionage and sabotage capable, state-sponsored advanced persistent threats.											
Title: Maritime Operations Center (MOC)							0.500	0.000	0.000		
Articles:							0				
FY 2012 Accomplishments: Maritime Operations Center (MOC) funding transitioned to the Computer Network Defense (CND) funding line to continued development of Cyber MOC capabilities. MOC conducted an Analysis of Alternatives (AoA), evaluated the 10th Fleet operational data feeds, prepared a project plan to integrate these feeds to a set of Network Operations (NetOps) Common Operational Picture (COP) tools, and maximized NetOps watch standard effectiveness.											
Accomplishments/Planned Programs Subtotals							24.081	23.641	21.130		
C. Other Program Funding Summary (\$ in Millions)											
Line Item	FY 2012	FY 2013	FY 2014 Base	FY 2014 OCO	FY 2014 Total	FY 2015	FY 2016	FY 2017	FY 2018	Cost To Complete	Total Cost
• OPN/3415: <i>Info Sys Security Program (ISSP)</i>	93.960	144.104	133.530		133.530	149.744	138.948	93.142	95.397	Continuing	Continuing
Remarks											
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 (CI-2). Products that are procured and fielded include: Tactical Key Loader, Simple Key Loader, Next Generation Fill devices.											
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. Products that are procured and fielded include: Advanced Key Processor (AKP), Management Client (MGC - computer , printer, scanner, monitors, key boards, hard drives, Type -1 tokens, card reader and mice), and High Assurance Internet Protocol Encryption devices. Navy will continue to provide and refine Navy unique requirements into the NSA KMI CI-2 Spiral 2 Spin 2 capability. In parallel, KMI will: (1) continue to define Navy operational architecture and requirements for roll-out (limited) of this new capability in the Fiscal Year 2014; (2) provide and refine Navy unique requirements into the NSA KMI CI-3 Capability Development Document (CDD); and (3) investigate alternative KMI architecture implementations for submarine and other communities within the Navy.											

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2014 Navy		DATE: April 2013
APPROPRIATION/BUDGET ACTIVITY 1319: <i>Research, Development, Test & Evaluation, Navy</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140N: <i>Information Sys Security Program</i>	PROJECT 0734: <i>Communications Security R&D</i>
Cryptographic Modernization (CM) - The procurement and fielding of Modernized Crypto devices such as the KG-3X Inc 2, KG-45A, AN-PYQ-20 (formerly KL-51M), KW-46M, KG-175D, KG-175A, Very High Frequency (VHF)/Ultra High Frequency (UHF) Wideband Tactical Secure Voice Cryptologic Equipment (VINSON)/Advanced Narrowband Digital Voice Terminal (ANDVT) Cryptographic modernization (VACM), KIV-7M WALBURN and SAVILLE Communications Security (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 information system networks. Procurements within the CND equipment line include: Firewall components which provide protection for networks from unauthorized users, Virtual Private Networks (VPN) which provide encrypted "Point-to-Point" virtual communication networks, Intrusion Prevention Systems (IPS), Administrator Access Control, Network Security tools and Filtering routers. 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 implements an evolutionary acquisition strategy that delivers CND capabilities in multiple builds and functionality releases that address validated requirements. E. Performance Metrics Key Management Infrastructure (KMI): * Install KMI Manager Client/Advanced Key Processor (MGC/AKP) Spiral 1 at selected pilot sites to support Initial Operational Capability (IOC). MGC/AKP Spiral 2 installs delayed to FY15 due to NSA Spiral 2 capability schedule change. * Conduct Navy MGC/AKP Spiral 2 testing across relevant networks (e.g., Navy/Marine Corp Internet/Next Generation(NMCI/NGEN), Integrated Shipboard Network System/Consolidated Afloat Networks and Enterprise Services (ISNS/CANES), Base Level Information Infrastructure Outside the Continental United States (OCONUS) Navy Enterprise Network (BLII ONEnet)) to support Navy-wide deployment in preparation for FY15 Spiral 2 fielding. * Complete engineering efforts and test planning for the KMI CI-2 (Spiral 2) transition planned to begin FY15. * Provide and refine Navy unique requirements into the NSA KMI CI-3 Capability Development Document (CDD). Cryptographic Modernization (CM): * Meet 100% of Chairman of the Joint Chiefs of Staff Instruction (CJCSI 6510) Cryptographic Modernization (CM) 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 Department of the Navy (DoN) inventory with known algorithm vulnerability dates, assess lifecycle sustainment issues, and identify transition device schedules, where they exist. * Meet 100% of Top Secret (TS) and SECRET CJCSI 6510 by fielding modern cryptographic devices or request "key extension" via the Joint Staff Military Communications-Electronics Board (MCEB). * Increase the functionality of 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 (CP) for 100% of CND systems.		

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2014 Navy		DATE: April 2013
APPROPRIATION/BUDGET ACTIVITY 1319: <i>Research, Development, Test & Evaluation, Navy</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140N: <i>Information Sys Security Program</i>	PROJECT 0734: <i>Communications Security R&D</i>
* 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 enclaves. * 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 enclaves. * Continue to develop and provide Cyber Situational Awareness (CSA) to the Commander United States Tenth Fleet (C10F) Maritime Operations Center (MOC). Information Assurance (IA) services: * Ensure 100% interoperability and application of commercial standards compliance for ISSP products by researching and conducting selective evaluations, integrating and testing commercial-off-the-shelf/Non-Developmental Item IA security products. 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 Information Assurance (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 Trusted Agent (TA) to measure effectiveness of Navy networks. Ensure the security design and integration of Computer Adaptive Network Defense-in-Depth (CANDiD) products and services and that they are 100% interoperable and operationally acceptable across the Navy for major initiatives such as the future afloat, ashore, and Outside the Continental United States (OCONUS) networks. Maritime Operations Center (MOC): *Develop and provide Network Operations (NetOps) Common Operational Picture (COP) for C10F.		

UNCLASSIFIED

Exhibit R-3, RDT&E Project Cost Analysis: PB 2014 Navy												DATE: April 2013			
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 2012		FY 2013		FY 2014 Base		FY 2014 OCO		FY 2014 Total			
Cost Category Item	Contract Method & Type	Performing Activity & Location	All Prior Years	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Cost To Complete	Total Cost	Target Value of Contract
Systems Engineering	WR	SSC PAC/ SSC LANT:San Diego, CA/ Charleston, SC	22.710	7.932	Dec 2011	7.534	Dec 2012	4.968	Dec 2013	-		4.968	Continuing	Continuing	Continuing
Systems Engineering	WR	NRL:Washington, DC	0.600	0.278	Dec 2011	0.280	Dec 2012	0.247	Dec 2013	-		0.247	Continuing	Continuing	Continuing
Systems Engineering - Link 22	C/CPAF	Northrup Grumman:Washington, DC	0.000	0.599	Nov 2012	0.000		0.000		-		0.000	Continuing	Continuing	Continuing
Primary Hardware Development - Link 22	C/CPAF	SAFENET:Columbia, MD	0.000	2.600	Aug 2012	0.000		0.000		-		0.000	0.000	2.600	
Systems Engineering (MOC)	WR	SSC PAC:San Diego, CA	0.000	0.500	Dec 2011	1.000	Dec 2012	0.000		-		0.000	Continuing	Continuing	Continuing
Systems Engineering	WR	NUWC:Newport, RI	0.608	0.000		0.000		0.119	Dec 2013	-		0.119	Continuing	Continuing	Continuing
Systems Engineering	WR	FNMO:Monterey, CA	0.480	0.000		0.000		0.000		-		0.000	Continuing	Continuing	Continuing
Systems Engineering (NCDOD)	WR	SSC LANT:Charleston, SC	0.000	0.000		0.000		0.100	Dec 2013	-		0.100	0.000	0.100	
Software Development	C/CPAF	SAIC:San Diego, CA	32.877	0.000		0.000		0.000		-		0.000	Continuing	Continuing	Continuing
Software Development	WR	SSC PAC/ SSC LANT:San Diego, CA/ Charleston, SC	11.029	0.000		0.000		0.632	Dec 2013	-		0.632	Continuing	Continuing	Continuing
Software Development	WR	NRL:Washington, DC	19.196	1.299	Dec 2011	1.322	Dec 2012	1.475	Dec 2013	-		1.475	Continuing	Continuing	Continuing
Primary Hardware Development (PY)	WR	Various:Various	102.136	0.000		0.000		0.000		-		0.000	Continuing	Continuing	Continuing
Primary Hardware Development	WR	SSC PAC:San Diego, CA	2.554	0.000		0.000		0.000		-		0.000	Continuing	Continuing	Continuing
Primary Hardware Development	WR	NRL:Washington, DC	0.970	0.000		0.000		0.000		-		0.000	Continuing	Continuing	Continuing
Subtotal			193.160	13.208		10.136		7.541		0.000		7.541			

UNCLASSIFIED

Exhibit R-3, RDT&E Project Cost Analysis: PB 2014 Navy												DATE: April 2013			
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 2012		FY 2013		FY 2014 Base		FY 2014 OCO		FY 2014 Total			
Cost Category Item	Contract Method & Type	Performing Activity & Location	All Prior Years	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Cost To Complete	Total Cost	Target Value of Contract
Architecture	WR	SSC PAC/ SSC LANT:San Diego, CA/ Charleston, SC	0.000	0.849	Dec 2011	0.856	Dec 2012	1.062	Dec 2013	-		1.062	Continuing	Continuing	Continuing
Requirements Analysis	WR	NRL:Washington, DC	0.000	0.978	Dec 2011	0.988	Dec 2012	0.000		-		0.000	Continuing	Continuing	Continuing
Studies & Design	WR	NRL:Washington, DC	0.000	0.777	Dec 2011	0.783	Dec 2012	0.000		-		0.000	Continuing	Continuing	Continuing
Studies & Design	WR	SSC PAC/ SSC LANT:San Diego, CA/ Charleston, SC	0.000	1.674	Dec 2011	1.691	Dec 2012	2.753	Dec 2013	-		2.753	Continuing	Continuing	Continuing
Systems Engineering Spt	WR	NRL:Washington, DC	0.000	0.183	Dec 2011	0.185	Dec 2012	0.175	Dec 2013	-		0.175	Continuing	Continuing	Continuing
Systems Engineering Spt	WR	SSC PAC/ SSC LANT:San Diego, CA/ Charleston, SC	1.678	1.183	Dec 2011	3.690	Dec 2012	3.153	Dec 2013	-		3.153	Continuing	Continuing	Continuing
Architecture	C/CPFF	BAH:San Diego, CA	0.000	0.774	Dec 2011	0.000		0.795	Nov 2013	-		0.795	0.000	1.569	
Requirements Analysis	C/CPFF	BAH:San Diego, CA	0.000	0.000		0.782	Dec 2012	0.805	Dec 2013	-		0.805	0.000	1.587	
Subtotal			1.678	6.418		8.975		8.743		0.000		8.743			
Test and Evaluation (\$ in Millions)				FY 2012		FY 2013		FY 2014 Base		FY 2014 OCO		FY 2014 Total			
Cost Category Item	Contract Method & Type	Performing Activity & Location	All Prior Years	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Cost To Complete	Total Cost	Target Value of Contract
System DT&E	WR	NUWC:Newport, RI	0.623	0.075	Dec 2011	0.076	Dec 2012	0.119	Dec 2013	-		0.119	Continuing	Continuing	Continuing
System DT&E	WR	SSC LANT:Charleston, SC	0.000	0.260	Dec 2011	0.999	Dec 2012	0.826	Dec 2013	-		0.826	Continuing	Continuing	Continuing
System DT&E	WR	SSC PAC:San Diego, CA	34.778	0.000		0.978	Dec 2012	0.727	Dec 2013	-		0.727	Continuing	Continuing	Continuing
System OT&E	WR	COTF:Norfolk, VA	0.125	0.115	Dec 2011	0.116	Dec 2012	0.361	Dec 2013	-		0.361	Continuing	Continuing	Continuing
Subtotal			35.526	0.450		2.169		2.033		0.000		2.033			

UNCLASSIFIED

Exhibit R-3, RDT&E Project Cost Analysis: PB 2014 Navy												DATE: April 2013			
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)				FY 2012		FY 2013		FY 2014 Base		FY 2014 OCO		FY 2014 Total			
Cost Category Item	Contract Method & Type	Performing Activity & Location	All Prior Years	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Cost To Complete	Total Cost	Target Value of Contract
Financial Management/ Cost Estimating	C/CPFF	INDUS/BAH 1.6:San Diego, CA	0.000	0.679	Oct 2011	0.686	Oct 2012	0.000		-		0.000	Continuing	Continuing	Continuing
Travel	WR	SPAWAR:San Diego, CA	0.000	0.119	Oct 2011	0.025	Oct 2012	0.025	Oct 2013	-		0.025	Continuing	Continuing	Continuing
Program Management	WR	SSC PAC/ SSC LANT:San Diego, CA/ Charleston, SC	0.000	0.294	Dec 2011	0.392	Dec 2012	0.097	Dec 2013	-		0.097	Continuing	Continuing	Continuing
Program Management	WR	SSC PAC:San Diego, CA	1.213	0.000		0.000		0.000		-		0.000	Continuing	Continuing	Continuing
Program Management	C/CPFF	BAH:San Diego, CA	19.205	1.456	Oct 2011	0.642	Oct 2012	1.316	Oct 2013	-		1.316	Continuing	Continuing	Continuing
Acquisition Management	C/CPFF	BAH:San Diego, CA	0.000	1.457	Dec 2011	0.616	Oct 2012	1.375	Oct 2013	-		1.375	0.000	3.448	
Subtotal			20.418	4.005		2.361		2.813		0.000		2.813			
			All Prior Years	FY 2012		FY 2013		FY 2014 Base		FY 2014 OCO		FY 2014 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals			250.782	24.081		23.641		21.130		0.000		21.130			
Remarks															

UNCLASSIFIED

Exhibit R-4, RDT&E Schedule Profile: PB 2014 Navy

DATE: April 2013

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*

Fiscal Year	2012				2013				2014				2015				2016				2017				2018			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Acquisition Milestones																												
CND Inc 2 IOC (Note 1)			▲																									
			CND Inc 2 IOC																									
CND Inc 2 FOC																				△								
																				CND Inc 2 FOC								
Test & Evaluation Milestones																												
Operational Test (O/T)																												
CND Inc 2 IOT&E (Note 2)				▲																								
				CND Inc 2 IOT&E																								
Production Milestones																												
CND Inc 2 LRIP Start/Complete (Note 3)				▲																								
				CND Inc 2 LRIP Complete																								
CND Inc 2 FRP Decision (Note 4)					▲																							
					CND Inc 2 FRP Decision																							
Deliveries																												
CND Inc 2 Delivery	▲																											

Note 1: CND Inc 2 IOC achieved in advance of schedule, moved from 4QFY12 TO 3QFY12.

Note 2: CND Inc 2 IOT&E slipped from 3QFY12 TO 4QFY12 due to delayed receipt of Operational Test results.

Note 3: CND Inc 2 LRIP slipped from 3QFY12 to 4QFY12 due to delayed receipt of Operational Test results.

Note 4: CND Inc 2 FRP Decision slipped from 4QFY12 to 1QFY13 due to delayed Acquisition Decision Memorandum (ADM) approval.

UNCLASSIFIED

Exhibit R-4, RDT&E Schedule Profile: PB 2014 Navy

DATE: April 2013

APPROPRIATION/BUDGET ACTIVITY

1319: Research, Development, Test & Evaluation, Navy

BA 7: Operational Systems Development

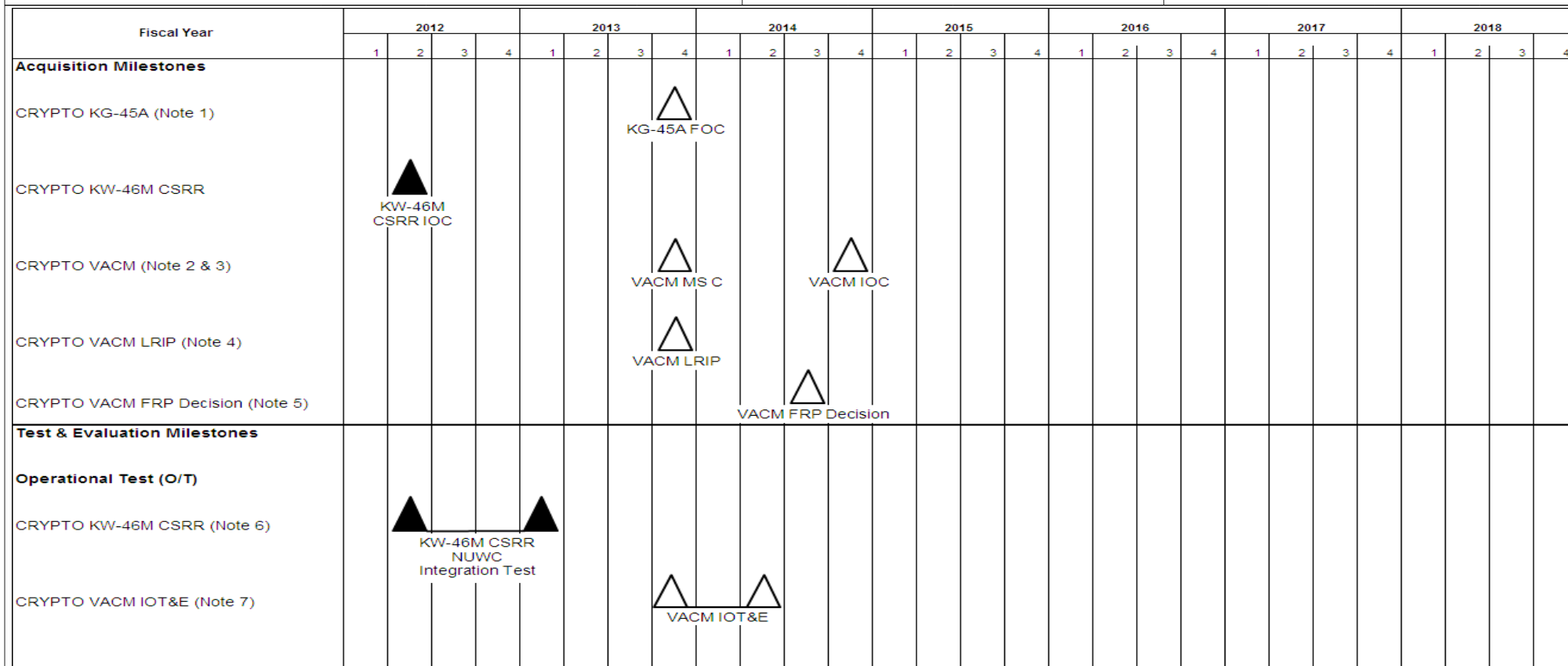
R-1 ITEM NOMENCLATURE

PE 0303140N: Information Sys Security

Program

PROJECT

0734: Communications Security R&D



Note 1: CRYPTO KG-45A FOC slipped from 1QFY13 to 4QFY13 due to delay in fielding onboard 1 CG platform.

Note 2: CRYPTO VACM MS C slipped from 3QFY13 to 4QFY13 due to software development delays per US Air Force (USAF) Program Office. Milestones are driven by USAF as the lead service.

Note 3: CRYPTO VACM IOC slipped from 3QFY13 to 4QFY13 due to software development delays.

Note 4: CRYPTO VACM LRIP slipped from 3QFY13 to 4QFY13 due to software development delays.

Note 5: CRYPTO VACM FRP Decision slipped from 4QFY13 to 3QFY14 due to software development delays and contracting strategy moving to USAF contract sole source justification.

Note 6: CRYPTO KW-46M Common Submarine Radio Room (CSRR) integration test end date slipped from 2QFY12 to 1QFY13 due to availability of Naval Undersea Warfare Center (NUWC) test lab.

Note 7: CRYPTO VACM IOT&E end date slipped from 1QFY14 to 2QFY14 due to software development delays.

UNCLASSIFIED

Exhibit R-4, RDT&E Schedule Profile: PB 2014 Navy

DATE: April 2013

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

Fiscal Year	2012				2013				2014				2015				2016				2017				2018			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Deliveries																												
CRYPTO KG-3X Inc 2	▲			▲																								
CRYPTO AN-PYQ-20 (formerly KL-51M)								▲																				
CRYPTO KG-45A (Note 1)												▲																
CRYPTO Link - 22 MLLC (Note 2)		▲	▲									▲																
CRYPTO VACM LRIP Deliveries (Note 3)												▲																
CRYPTO VACM FRP Deliveries (Note 4)													▲															

Note 1: CRYPTO KG-45A Deliveries end date shifted from 1QFY13 to 4QFY13 due to delay in fielding onboard 1 CG platform.

Note 2: CRYPTO Link-22 MLLC Prototype delivery end date shifted from 2QFY12 to 3QFY12 due to contract performance issues (SAFENET).

Note 3: CRYPTO VACM LRIP deliveries shifted from 3QFY13 to 2QFY14 due to change in delivery schedule.

Note 4: CRYPTO VACM FRP delivery Start Date shifted from 1QFY14 to 4QFY14 due to software development delays.

UNCLASSIFIED

Exhibit R-4, RDT&E Schedule Profile: PB 2014 Navy **DATE:** April 2013

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*

Fiscal Year	2012				2013				2014				2015				2016				2017				2018			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Acquisition Milestones																												
EKMS Phase V																												
TKL (Note 1)																												
KMI CI-2 (Note 2 & 3)																												
Test & Evaluation Milestones																												
Operational Test (O/T)																												
KMI CI-2 IOT&E (Note 4)																												
KMI CI-2 OA2																												

Note 1: TKL IOC slipped from 1QFY13 to 2QFY13 and FOC slipped from 1QFY15 to 2QFY15 due to late Acquisition Decision Memorandum (ADM) approval and contract award.

Note 2: KMI CI-2 IOC is a NSA driven milestone and equipment was funded by NSA at limited Navy sites; IOC shifted from 3QFY12 to 4QFY12 due to NSA test schedule delays;

Note 3: KMI CI-2 FOC slipped from 1QFY17 to 3QFY18 to align to Chief of Naval Operations (CNO) ship availabilities.

Note 4: KMI CI-2 IOT&E is a NSA driven milestone and equipment was funded by NSA at limited Navy sites; slipped from 3QFY12 to 4QFY12 due to NSA test schedule delays.

UNCLASSIFIED

PE 0303140N: *Information Sys Security Program*
Navy

R-1 Line #201

R-1 ITEM NOMENCLATURE

PE 0303140N: Information Sys Security Program

0734: *Communications Security R&D*[illegible]

Note 2: TKL Full Rate Production (FRP) Decision slipped from 3QFY12 to 1QFY13 due to MDA (Milestone Decision Authority) decision on FRP events.

Note 4: KMI Spiral 1 FRP slipped from 1QFY13 to 2QFY13 due to NSA test schedule delays.

Note 5: KMI Spiral 2 FRP slipped from 1QFY14 to 4QFY14 due to NSA schedule delays.

Note 6: EKMS Phase V SW delivery end date delayed from 1QFY13 to 2QFY13 due to final fielding.

Note 7: SKL Delivery end date shifted from 3QFY13 to 4QFY15 due to later fielding of Next Generation Fill Devices to coincide with KMI Over the Network Key (OTNK) capability.

Note 8: TKL Delivery start date shifted one quarter from 1QFY13 to 3QFY13 due to delay in Full Rate Fielding Decision (FRFD).

Note 9: KMI CI-2 Spiral 1 LRIP deliveries shifted from 4QFY12 to 1QFY14 through 3QFY14 due to NSA test schedule delays.

Note 10: KMI CI-2 Spiral 2 delivery start date shifted from 3QFY13 to 4QFY14 due to NSA schedule changes; Delivery end date shifted from 1QFY17 to 3QFY18 due to CNO availabilities of ships.

Note 11: Next Generation Fill Device delivery start date shifted from 1QFY13 to 1QFY16 to support Crypto Mod initiative for KMI awareness and will coincide with NSA KMI OTNK capability in FY15.

UNCLASSIFIED

Exhibit R-4, RDT&E Schedule Profile: PB 2014 Navy																DATE: April 2013												
APPROPRIATION/BUDGET ACTIVITY										R-1 ITEM NOMENCLATURE								PROJECT										
1319: Research, Development, Test & Evaluation, Navy										PE 0303140N: Information Sys Security Program								0734: Communications Security R&D										
BA 7: Operational Systems Development																												
Fiscal Year	2012				2013				2014				2015				2016				2017				2018			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Acquisition Milestones																												
PKI Inc 2, Spiral 1 & 2																												
	PKI Inc 2, Spiral 1 & 2 IOC																											
PKI Inc 2, Spiral 3 IOC																												
							PKI Inc 2, Spiral 3 IOC																					
PKI Inc 2 FOC																												
									PKI Inc 2 FOC																			

UNCLASSIFIED

Exhibit R-4A, RDT&E Schedule Details: PB 2014 Navy			DATE: April 2013
APPROPRIATION/BUDGET ACTIVITY 1319: <i>Research, Development, Test & Evaluation, Navy</i> BA 7: <i>Operational Systems Development</i>	R-1 ITEM NOMENCLATURE PE 0303140N: <i>Information Sys Security Program</i>	PROJECT 0734: <i>Communications Security R&D</i>	

Schedule Details

Events by Sub Project	Start		End	
	Quarter	Year	Quarter	Year
Proj 0734				
CND - Inc 2 IOC	3	2012	3	2012
CND - Inc 2 FOC	4	2016	4	2016
CND - Inc 2 IOT&E	4	2012	4	2012
CND - Inc 2 LRIP	1	2012	4	2012
CND - Inc 2 FRP Decision	1	2013	1	2013
CND - Inc 2 Delivery	1	2012	4	2018
CRYPTO KG-45A - FOC	4	2013	4	2013
CRYPTO KW-46M CSRR - IOC	2	2012	2	2012
CRYPTO VACM - MS C	4	2013	4	2013
CRYPTO VACM - IOC	4	2014	4	2014
CRYPTO VACM - LRIP	4	2013	4	2013
CRYPTO VACM - FRP Decision	3	2014	3	2014
CRYPTO KW-46M CSRR - NUWC Integration Test	2	2012	1	2013
CRYPTO VACM - IOT&E	4	2013	2	2014
CRYPTO KG-3X - Inc 2 Deliveries	1	2012	4	2012
CRYPTO AN-PYQ-20 (formerly KL-51M) - Deliveries	1	2012	1	2013
CRYPTO KG-45A - Deliveries	1	2012	4	2013
CRYPTO Link-22 - MLLC Prototype Delivery	2	2012	3	2012
CRYPTO Link-22 - MLLC Full Scale Delivery	3	2014	3	2014
CRYPTO VACM - LRIP Deliveries	2	2014	2	2014
CRYPTO VACM - FRP Deliveries	4	2014	4	2018

UNCLASSIFIED

Exhibit R-4A, RDT&E Schedule Details: PB 2014 Navy			DATE: April 2013	
APPROPRIATION/BUDGET ACTIVITY 1319: <i>Research, Development, Test & Evaluation, Navy</i> BA 7: <i>Operational Systems Development</i>		R-1 ITEM NOMENCLATURE PE 0303140N: <i>Information Sys Security Program</i>		PROJECT 0734: <i>Communications Security R&D</i>
		Start		End
Events by Sub Project		Quarter	Year	Quarter
				Year
EKMS - Phase V FOC		3	2014	3
TKL - IOC		2	2013	2
TKL - FOC		2	2015	2
KMI CI-2 - MS C		1	2012	1
KMI CI-2 - Spiral 1 IOC		4	2012	4
KMI CI-2 - Spiral 2 FOC		3	2018	3
KMI CI-2 - IOT&E		4	2012	4
KMI CI-2 - OA2		3	2012	3
TKL - FA Test		2	2012	2
TKL - FRP Decision		1	2013	1
KMI CI-2 - Spiral 1 LRIP Contract Award		4	2012	4
KMI CI-2 - Spiral 1 FRP HW		2	2013	2
KMI CI-2 - Spiral 2 FRP SW		4	2014	4
EKMS - Phase V SW		1	2012	2
EKMS - SKL Deliveries		1	2012	4
TKL - Deliveries		3	2013	2
KMI CI-2 - Spiral 1 LRIP Deliveries		1	2014	3
KMI CI-2 - Spiral 2 Deliveries		4	2014	3
Next Generation Fill Device		1	2016	4
PKI - Inc 2 Spiral 1 & 2 IOC		1	2012	1
PKI - Inc 2 Spiral 3 IOC		3	2013	3
PKI - Inc 2 FOC		2	2014	2

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2014 Navy										DATE: April 2013		
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)	All Prior Years	FY 2012	FY 2013 [#]	FY 2014 Base	FY 2014 OCO ^{##}	FY 2014 Total	FY 2015	FY 2016	FY 2017	FY 2018	Cost To Complete	Total Cost
3230: Information Assurance	2.998	2.666	2.666	2.401	-	2.401	2.683	2.673	2.768	2.786	Continuing	Continuing
Quantity of RDT&E Articles	0	0	0	0		0	0	0	0	0		

[#] FY 2013 Program is from the FY 2013 President's Budget, submitted February 2012

^{##} The FY 2014 OCO Request will be submitted at a later date

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 expands significantly 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 be divorced from 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: (1) improve network infrastructure resistance and resiliency to attacks; (2) 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 (3) 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 interoperability, 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. This effort will also initiate requirements definition for situational awareness capabilities to support computer network defense in a highly-distributed, homogeneous, and heterogeneous networks including mobile and

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2014 Navy		DATE: April 2013		
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		
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. Program will also initiate requirements definition for secure coalition data exchange and interoperation among security levels and classifications, and 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. Efforts will also 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. IA will ensure the architectures evolve to provide proper protection as technology, DoD missions, and threats continuously evolve. IA includes 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. Also, the program will initiate the efforts to conceptualize new network centric warfare technology to protect our assets, such as secure network gateways, routers, components and tools that improve the survivability of Navy networks. Last, IA will provide 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.				
Major focus areas in FY14: Continue development of new network security demands addressing nation-state level sponsored activity. Incorporate security services to thwart DNS attacks, distributed denial of service, botnet and other sophisticated attacks.				
B. Accomplishments/Planned Programs (\$ in Millions, Article Quantities in Each)		FY 2012	FY 2013	FY 2014
Title: Information Assurance		2.666	2.666	2.40
Articles:		0	0	0
FY 2012 Accomplishments:				
Continued the development of new network security technology focused on addressing nation state level sponsored activity and successfully characterized several attacks/profiles to improve detection rates of the technology and to support attribution of threat actions across network boundaries. Continued the development of a new high assurance boundary controller to protect Navy and Marine Corps data and resources from attack ensuring 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. Continued the development of mobile security techniques that introduce time- and location-based security parameters for geo-location and asset protection and management. Continued 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. Completed the development of a high-assurance computing environment for Navy and Marine Corps use based on trusted platform technology. Completed the development of the appropriate core code, security messages and assurance functions required to ensure platform hardware and software protection. Completed the development of new key and enabling technologies to address specific Navy and Marine Corps needs. Ensure the new solutions address distribution and management in bandwidth limited environments and tactical environments. Initiated the development of critical cryptographic technology that support Navy unique platforms and requirements ensuring the technology addresses the limited size, weight and				

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2014 Navy			DATE: April 2013		
APPROPRIATION/BUDGET ACTIVITY 1319: <i>Research, Development, Test & Evaluation, Navy</i> BA 7: <i>Operational Systems Development</i>		R-1 ITEM NOMENCLATURE PE 0303140N: <i>Information Sys Security Program</i>		PROJECT 3230: <i>Information Assurance</i>	
B. Accomplishments/Planned Programs (\$ in Millions, Article Quantities in Each)			FY 2012	FY 2013	FY 2014
power issues, and multiple data classification processing requirements, as well as, providing on-the-fly programmability of mission data and key material to support various missions. FY 2013 Plans: Continue the development of new network security technology focused on addressing nation-state level sponsored activity. Continue characterizing attacks/profiles to increase detection rates of the technology- focusing on embedded malicious code and exfiltration of data from host environments. Continue development of attribution technology, focusing on nation-state activities across network boundaries that obfuscate traffic using techniques such as anonymization. Continue the development of a new high assurance boundary controller to protect Navy and Marine Corps data and resources from attack incorporating security services to thwart Denial of Network Service (DNS) attacks, distributed denial of service attacks, and botnet attacks, as well as sophisticated attacks to control the core, operating environment and ensuring essential robust communications are available through the boundary controller to provide continuity of operations during nation state sponsored attacks. Continue the development of mobile security techniques that introduce time- and location-based security parameters for geo-location and asset protection and management addressing the specific issues of geo-location and mapping in Global Positioning System (GPS)-constrained environments. Continue the development of critical cryptographic technology to support Navy unique platforms and requirements, such as unmanned autonomous systems (UASs) ensuring the technology addresses the limited size, weight and power issues, and multiple data classification processing requirements, as well as providing 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. Initiate development of a security framework for a federated cross-domain service oriented architecture (SOA) ensuring the framework addresses all critical aspects of SOA including cross-domain service discovery, identity management, and service invocation, while minimizing inference attacks. Initiate the development of a security framework for mobile communication devices that allows the use/integration of commercial technology in a secure manner with initial efforts focusing on identity management, secure data storage, processing and exchange. FY 2014 Plans: Continue the development of new network security technology focused on addressing nation state level sponsored activity. Continue the development of a security framework for a federated, cross-domain service-oriented architecture (SOA) ensuring the framework addresses all critical aspects of SOA including cross-domain service discovery, identity management, and service invocation, while minimizing inference attacks. Continue the development of a security framework for mobile communication devices that allows the use/integration of commercial technology in a secure manner, such as to support the integration of Droid and/or iPhone devices. Continue the efforts focused on identity management and secure data storage, processing and exchange. Continue the development of mobile security techniques that introduce time and location-based security parameters for geo-location and asset protection and management while addressing the specific issues of geo-location and mapping in Global Positioning System (GPS)-constrained environments. Continue the development of critical cryptographic technology to support					

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2014 Navy		DATE: April 2013	
APPROPRIATION/BUDGET ACTIVITY 1319: <i>Research, Development, Test & Evaluation, Navy</i> BA 7: <i>Operational Systems Development</i>		R-1 ITEM NOMENCLATURE PE 0303140N: <i>Information Sys Security Program</i>	PROJECT 3230: <i>Information Assurance</i>
B. Accomplishments/Planned Programs (\$ in Millions, Article Quantities in Each)		FY 2012	FY 2013
Navy unique platforms and requirements such as unmanned autonomous systems (UASs) ensuring the technology addresses the limited size, weight and power issues, and multiple data classification processing requirements, while as providing on-the-fly programmability of mission data and key material to support various missions such as COMSEC, ELINT, SIGINT, etc. 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. Complete the characterization of attacks/profiles to increase detection rates of the technology, especially for identifying new/emerging malicious code. Complete the development of attribution technology, focusing on nation-state activities across network boundaries that obfuscate traffic using techniques such as anonymization. Complete the incorporation of security services to thwart DNS attacks, distributed denial of service attacks, and botnet attacks, as well as sophisticated attacks to control the core operating environment. Initiate the development of new sensing and instrumentation technology to support attack prediction and to measure the effectiveness of network security technology. Initiate the development of technology to provide prediction/early warning sensing of impending attacks based on network traffic and user behavior.			
Accomplishments/Planned Programs Subtotals		2.666	2.666
C. Other Program Funding Summary (\$ in Millions) N/A			
Remarks			
D. Acquisition Strategy N/A			
E. Performance Metrics Protection of Navy and joint information and information systems from hostile exploitation and attack			

UNCLASSIFIED

Exhibit R-3, RDT&E Project Cost Analysis: PB 2014 Navy												DATE: April 2013		
APPROPRIATION/BUDGET ACTIVITY 1319: <i>Research, Development, Test & Evaluation, Navy</i> BA 7: <i>Operational Systems Development</i>							R-1 ITEM NOMENCLATURE PE 0303140N: <i>Information Sys Security Program</i>				PROJECT 3230: <i>Information Assurance</i>			

Support (\$ in Millions)				FY 2012		FY 2013		FY 2014 Base		FY 2014 OCO		FY 2014 Total			
Cost Category Item	Contract Method & Type	Performing Activity & Location	All Prior Years	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Cost To Complete	Total Cost	Target Value of Contract
Development Support	Various	NRL:Washington, DC	2.998	2.666	Nov 2011	2.666	Nov 2012	2.401	Nov 2013	-		2.401	Continuing	Continuing	Continuing
Subtotal			2.998	2.666		2.666		2.401		0.000		2.401			

	All Prior Years	FY 2012	FY 2013	FY 2014 Base	FY 2014 OCO	FY 2014 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	2.998	2.666	2.666	2.401	0.000	2.401			

Remarks

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2014 Navy									DATE: April 2013			
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)	All Prior Years	FY 2012	FY 2013 [#]	FY 2014 Base	FY 2014 OCO ^{##}	FY 2014 Total	FY 2015	FY 2016	FY 2017	FY 2018	Cost To Complete	Total Cost
9999: Congressional Adds	0.000	12.000	0.000	0.000	-	0.000	0.000	0.000	0.000	0.000	0.000	12.000
Quantity of RDT&E Articles	0	0	0	0		0	0	0	0	0		
# FY 2013 Program is from the FY 2013 President's Budget, submitted February 2012												
## The FY 2014 OCO Request will be submitted at a later date												
A. Mission Description and Budget Item Justification												
Computer Network Defense (CND) accelerates and improves the cyber security, situational awareness, and efficiencies of OCONUS Naval Enterprise Network (ONE-Net) and Information Technology for the 21st Century (IT-21) networks. Efforts focus on enabling development of Navy high speed tactical network sensors. Efforts also include the conduct of systems engineering and architect Theater Network Operations and Security (TNSOC) modifications required to support ONE-Net environment security enhancements and network efficiencies. Funding establishes a lab environment that can support the development of Ozone Widget framework tools. Also, CND develops the architecture and integrated tools that support the automation of certification and accreditation processes in-line with Defense Information Systems Agency (DISA) imperatives for continuous network monitoring and risk scoring. Funding is used to determine optimal technical and governance solution for interception of outbound encrypted traffic, allowing for inspection and control. Last, CND will be updated development lab hardware will be updated to ensure Charleston Network Operations Center (CHASNOC), SSC Pacific Afloat, and End-to-End (E2C) labs contain the most current CND cyber security technologies. This also promoted comprehensive implementation of Host Based Security Systems (HBSS) and other DoD mandated tools and capabilities.												
B. Accomplishments/Planned Programs (\$ in Millions)								FY 2012	FY 2013			
Congressional Add: Cyber Security Research (Cong)								12.000	-			
FY 2012 Accomplishments: Computer Network Defense (CND) accelerated and improved the cyber security, situational awareness, and efficiency of OCONUS Naval Enterprise Network (ONE-Net) and Information Technology for the 21st Century (IT-21) networks. Efforts focused on enabling development of Navy high speed tactical network sensors. Conducted systems engineering and architect Theater Network Operations and Security (TNSOC) modifications required to support ONE-Net environment security enhancements and network efficiencies. Established a lab environment that can support the development of Ozone Widget framework tools. Began the development of the architecture and integrated tools that support the automation of certification and accreditation processes in line with Defense Information Systems Agency (DISA) imperatives for continuous network monitoring and risk scoring. Determined optimal technical and governance solution for interception of outbound encrypted traffic, allowing for inspection and control. Updated the CND development lab hardware to ensure Charleston Network Operations Center (CHASNOC), SSC Pacific Afloat, and End-to-End (E2C) labs												

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2014 Navy		DATE: April 2013	
APPROPRIATION/BUDGET ACTIVITY 1319: <i>Research, Development, Test & Evaluation, Navy</i> BA 7: <i>Operational Systems Development</i>		R-1 ITEM NOMENCLATURE PE 0303140N: <i>Information Sys Security Program</i>	PROJECT 9999: <i>Congressional Adds</i>

B. Accomplishments/Planned Programs (\$ in Millions)	FY 2012	FY 2013
contain the most current CND cyber security technologies. This also promoted comprehensive implementation of Host Based Security Systems (HBSS) and other DoD mandated tools and capabilities.		
Congressional Adds Subtotals	12.000	0.000

C. Other Program Funding Summary (\$ in Millions)
N/A

Remarks

D. Acquisition Strategy
Congressional Adds.

E. Performance Metrics
Congressional Adds.

UNCLASSIFIED

Exhibit R-3, RDT&E Project Cost Analysis: PB 2014 Navy												DATE: April 2013			
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					
Product Development (\$ in Millions)				FY 2012		FY 2013		FY 2014 Base		FY 2014 OCO		FY 2014 Total			
Cost Category Item	Contract Method & Type	Performing Activity & Location	All Prior Years	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Cost To Complete	Total Cost	Target Value of Contract
Primary Hardware Development	WR	SSC PAC:San Diego, CA	0.000	0.064	May 2012	0.000		0.000		-		0.000	0.000	0.064	
Primary Hardware Development	WR	NRL:Washington, DC	0.000	0.200	Apr 2012	0.000		0.000		-		0.000	0.000	0.200	
Primary Hardware Development	C/CPFF	SSC LANT:Charleston, SC	0.000	1.733	Jul 2012	0.000		0.000		-		0.000	0.000	1.733	
Software Development	WR	SSC PAC:San Diego, CA	0.000	2.600	Jul 2012	0.000		0.000		-		0.000	0.000	2.600	
Software Development	C/CPFF	DITC:Ft. Belvoir, VA	0.000	1.300	Jan 2013	0.000		0.000		-		0.000	0.000	1.300	
Systems Engineering	WR	SSC PAC:San Diego, CA	0.000	1.144	Oct 2012	0.000		0.000		-		0.000	0.000	1.144	
Systems Engineering	C/CPFF	ESC/CAA:Hanscomb AFB, MA	0.000	0.050	Oct 2012	0.000		0.000		-		0.000	0.000	0.050	
Subtotal			0.000	7.091		0.000		0.000		0.000		0.000	0.000	7.091	
Support (\$ in Millions)				FY 2012		FY 2013		FY 2014 Base		FY 2014 OCO		FY 2014 Total			
Cost Category Item	Contract Method & Type	Performing Activity & Location	All Prior Years	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Cost To Complete	Total Cost	Target Value of Contract
Requirements Analysis	WR	SSC PAC:San Diego, CA	0.000	0.235	Nov 2012	0.000		0.000		-		0.000	0.000	0.235	
Requirements Analysis	C/CPFF	SSC LANT:Charleston, SC	0.000	0.103	Jun 2012	0.000		0.000		-		0.000	0.000	0.103	
Architecture	WR	SSC PAC:San Diego, CA	0.000	1.672	May 2012	0.000		0.000		-		0.000	0.000	1.672	
Studies & Design	WR	SSC PAC:San Diego, CA	0.000	0.315	Nov 2012	0.000		0.000		-		0.000	0.000	0.315	
Studies & Design	C/CPFF	BAH:San Diego, CA	0.000	0.234	Dec 2012	0.000		0.000		-		0.000	0.000	0.234	
Subtotal			0.000	2.559		0.000		0.000		0.000		0.000	0.000	2.559	

UNCLASSIFIED

Exhibit R-3, RDT&E Project Cost Analysis: PB 2014 Navy												DATE: April 2013			
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			
Test and Evaluation (\$ in Millions)				FY 2012		FY 2013		FY 2014 Base		FY 2014 OCO		FY 2014 Total			
Cost Category Item	Contract Method & Type	Performing Activity & Location	All Prior Years	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Cost To Complete	Total Cost	Target Value of Contract
System DT&E	WR	SSC LANT:Charleston, SC	0.000	0.415	May 2012	0.000		0.000		-		0.000	0.000	0.415	
System DT&E	WR	NRL:Washington, DC	0.000	0.425	Apr 2012	0.000		0.000		-		0.000	0.000	0.425	
System DT&E	C/CPFF	BAH:San Diego, CA	0.000	0.350	Dec 2012	0.000		0.000		-		0.000	0.000	0.350	
System DT&E	WR	SSC PAC:San Diego, CA	0.000	0.767	May 2012	0.000		0.000		-		0.000	0.000	0.767	
Subtotal			0.000	1.957		0.000		0.000		0.000		0.000	0.000	1.957	
Management Services (\$ in Millions)				FY 2012		FY 2013		FY 2014 Base		FY 2014 OCO		FY 2014 Total			
Cost Category Item	Contract Method & Type	Performing Activity & Location	All Prior Years	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Cost To Complete	Total Cost	Target Value of Contract
Acquisition Management	C/CPFF	BAH:San Diego, CA	0.000	0.393	Dec 2012	0.000		0.000		-		0.000	0.000	0.393	
Subtotal			0.000	0.393		0.000		0.000		0.000		0.000	0.000	0.393	
			All Prior Years	FY 2012		FY 2013		FY 2014 Base		FY 2014 OCO		FY 2014 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals			0.000	12.000		0.000		0.000		0.000		0.000	0.000	12.000	
Remarks															