

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2013 Navy									DATE: February 2012		
APPROPRIATION/BUDGET ACTIVITY				R-1 ITEM NOMENCLATURE							
1319: Research, Development, Test & Evaluation, Navy BA 7: Operational Systems Development				PE 0303140N: Information Sys Security Program							
COST (\$ in Millions)	FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total	FY 2014	FY 2015	FY 2016	FY 2017	Cost To Complete	Total Cost
Total Program Element	24.988	37.196	26.307	-	26.307	26.532	25.984	25.314	25.754	Continuing	Continuing
0734: Communications Security R&D	22.077	22.418	23.641	-	23.641	23.771	23.326	22.637	23.021	Continuing	Continuing
3230: Information Assurance	2.911	2.778	2.666	-	2.666	2.761	2.658	2.677	2.733	Continuing	Continuing
9999: Congressional Adds	-	12.000	-	-	-	-	-	-	-	0.000	12.000

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, and Department of Defense (DoD) Directives 8500.01E, O-8530.01, and 8570.01.

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, and 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. 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 means that Navy cyberspace is a higher value and more vulnerable target. 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, an adversary often has access to the technologies they want 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 war fighter the essential information trust characteristics of availability, confidentiality, integrity, authentication, and non-repudiation. Information Assurance (IA), a key supporting cyber security activity, 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.

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2013 Navy		DATE: February 2012
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>
<p>The ISSP program provides the Navy with the following cyber security elements: (1) defense of 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 use 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 a Public Key Infrastructure (PKI). 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.</p> <p>All ISSP 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 standards bodies in ISSP-related matters include International Organization for Standardization, American National Standards Institute, Institute of Electrical and Electronics Engineers, Internet Engineering Task Force, World Wide Web Consortium, and National Institute of Standards and Technologies. The joint interoperability required in today's telecommunications systems makes standards compliance a must and the ISSP RDT&E program complies with the joint technical architecture. The FORCEnet architecture and standards documents reflect this emphasis on interoperable standards.</p> <p>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 standards bodies themselves. When necessary to protect mission critical systems specified in the Clinger/Cohen Act, ISSP RDT&E develops or tailors commercial and government technologies, standards, and processes to meet Navy-unique requirements; prototypes systems or portions of systems and examines their utility in operational Navy settings; and, provides 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.</p> <p>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).</p> <p>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.</p> <p>Major focus areas in FY13:</p> <p>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</p>		

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2013 Navy		DATE: February 2012
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>
<p>and ashore platforms. Continue to develop new capabilities into the Navy's Command and Control (C2) architecture via (Maritime Tactical Command and Control (MTC2)) 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 automation of reporting, monitoring, analysis and response as well as providing modernized patch management and host based security agent tools. For Maritime Operation Center (MOC) efforts in FY13, CND will leverage the Ozone Widget framework and the US Cyber Command Cyber Pilot architecture to deliver visualization and analysis tools in support of a NetOps COP at the C10F MOC.</p> <p>CND: Maritime Operations Center (MOC) - Assess the cyberspace network operations information dominance roadmap and as is architecture. Research government and industry automated autonomous information environment NetOps Common Operational Picture (COP) set of tools to provide the MOC the ability to maintain Command and Control (C2) of secure Communications Systems (CS) and conduct C2 Cyberspace NetOps. Integrate Cyberspace NetOps in the "to be" Navy C2 architecture.</p> <p>Cryptographic (Crypto)/Crypto Modernization - Continue the Link-22 Modernized Link Level Communications Security (COMSEC) (MLLC), Very High Frequency (VHF)/ Ultra High Frequency (UHF) Wideband Tactical Secure Voice Cryptologic Equipment (VINSON)/Advanced Narrowband Digital Voice Terminal (ANDVT) Cryptographic Modernization (VACM), and Link-16 CM development efforts, and start the Suite B Navy implementation, Crypto Priority (Red) List, Key Management Infrastructure (KMI) Awareness for devices (e.g., iApp development), and Navy Crypto Future Requirements development efforts. Continue development of a crypto modernization plan for transmission security (TRANSEC) with National Security Agency (NSA) and other services.</p> <p>Key Management Infrastructure (KMI) - Continue KMI transition planning, strategy and requirements definition for incorporation of other KMI roles into Navy architecture. Begin capability, engineering development and verification testing support to KMI Capability Increment (CI)-2 Spiral 2 Spin 2. Continue supporting KMI transition working group meetings, Working Integrated Product Teams (WIPTs), Joint Working Groups (JWG), and developing white papers and supporting documentation for KMI. Provide requirements definition support of the next generation fill device and KMI CI-3. Investigate alternative KMI architecture implementations for submarine and other communities within the Navy. 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.</p> <p>Public Key Infrastructure (PKI) - Continue to develop Secret Internet Protocol Router Network (SIPRNet) PKI solutions, including the SIPRNet Validation Authority and Hardware Token. 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 new certificates on the Common Access Card (CAC). Research and develop tools to support certificates for Non-Person Entity (NPE) devices.</p>		

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2013 Navy	DATE: February 2012
---	----------------------------

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>
---	--

B. Program Change Summary (\$ in Millions)	FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total
Previous President's Budget	25.934	25.229	25.902	-	25.902
Current President's Budget	24.988	37.196	26.307	-	26.307
Total Adjustments	-0.946	11.967	0.405	-	0.405
• Congressional General Reductions	-	-0.033			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	12.000			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-0.810	-			
• Program Adjustments	-	-	0.534	-	0.534
• Rate/Misc Adjustments	-	-	-0.129	-	-0.129
• Congressional General Reductions Adjustments	-0.136	-	-	-	-

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

Project: 9999: *Congressional Adds*

Congressional Add: *Cyber Security Research (Cong)*

Congressional Add Subtotals for Project: 9999

Congressional Add Totals for all Projects

FY 2011	FY 2012
-	12.000
-	12.000
-	12.000

Change Summary Explanation

TKL Contract Award slipped from 2QFY11 to 3QFY11, IOC slipped from 4QFY12 to 1QFY13 and FOC slipped 4QFY14 to 1QFY15 due to delay in contract negotiations.

KMI CI-2 MS C slipped from 2QFY11 to 1QFY12 and IOC shifted from 2QFY12 to 3QFY12 due to NSA schedule changes; FOC slipped from 4QFY14 to 1QFY17 to align to Chief of Naval Operations (CNO) ship availability.

KMI CI-2 OA2 slipped from 4QFY11 to 3QFY12, IOT&E slipped from 1QFY12 to 3QFY12 due to NSA test schedule delays.

TKL production First Article (FA) test slipped from 4QFY11 to 1QFY12 due to contract award delays.

TKL Full Rate Production (FRP) Decision slipped from 2QFY12 to 3QFY12 due to contract award delays.

KMI CI-2 Spiral 1 LRIP contract award slipped from 1QFY12 to 2QFY12 due to NSA schedule changes.

KMI CI-2 Spiral 1 FRP slipped from 2QFY12 to 1QFY13; Spiral 2 FRP slipped from 4QFY13 to 1QFY14 due to NSA schedule changes.

EKMS Phase V Software (SW) delivery end date shifted from 2QFY14 back to 1QFY13 due to accelerated fielding plan.

TKL deliveries slipped from 1QFY12 to 4QFY14 to 1QFY13 to 1QFY15 due to contract award delay.

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2013 Navy		DATE: February 2012
APPROPRIATION/BUDGET ACTIVITY		R-1 ITEM NOMENCLATURE
1319: <i>Research, Development, Test & Evaluation, Navy</i> BA 7: <i>Operational Systems Development</i>		PE 0303140N: <i>Information Sys Security Program</i>
<p>KMI CI-2 Spiral 2 delivery Start Date slipped from 1QFY13 to 3QFY13 due to NSA schedule changes.</p> <p>KG-3X Inc 2 FRP Decision slipped from 2QFY11 to 4QFY11 due to contract delays. FRP Decision is driven by USAF (as lead service). KG-45A FOC moved up from 2QFY13 to 1QFY13 due to battlegroup availability. KW-46M IOC slipped from 2QFY11 to 2QFY12 to meet Common Submarine Radio Room (CSRR) Increment 1 v3 IOC. VACM MS C slipped from 1QFY13 to 3QFY13 and IOC slipped from 1QFY14 to 3QFY14 due to delay in US Air Force source selection. Milestones are driven by USAF (as lead service). KW-46M integration test slipped from 1QFY12 to 2QFY12 due to availability of Naval Undersea Warfare Center (NUWC) test lab. KG-3X Inc 2 delivery moved up from 3QFY13 to 4QFY12 to meet the NSA cease key date. KW-46M Common Submarine Radio Room (CSRR) delivery changed from 3QFY11 to 2QFY12 and 4QFY15 to 2QFY18 to meet CSRR inc 1v3 IOC. AN/PYQ-20 (C) delivery moved up from 4QFY14 to 1QFY13 due to ship/ submarine availability. VACM FRP delivery Start Date slipped from 3QFY13 to 1QFY14 due to Contract Award delay.</p> <p>CND Inc 2 IOC slipped from 1QFY11 to 4QFY12 to match Capabilities Production Document (CPD) signed 13 AUG 2010. CND MOC Network Operations (NetOps) Common Operational Picture (COP) development efforts transitioned to CND beginning in FY12 to continue development of Cyber MOC capabilities and "to be" architecture. CND Inc 2 deliveries represent system refreshes/ updates and continue beyond FOC.</p> <p>PKI Inc 2, Spiral 3 IOC slipped from 2QFY13 to 3QFY13 due to NSA/DISA schedule delays. PKI Inc 2, Spiral 1 IOT&E slipped from 2QFY11 to 3QFY11 due to NSA/DISA schedule delays.</p>		

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Navy									DATE: February 2012		
APPROPRIATION/BUDGET ACTIVITY 1319: Research, Development, Test & Evaluation, Navy BA 7: Operational Systems Development				R-1 ITEM NOMENCLATURE PE 0303140N: Information Sys Security Program				PROJECT 0734: Communications Security R&D			
COST (\$ in Millions)	FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total	FY 2014	FY 2015	FY 2016	FY 2017	Cost To Complete	Total Cost
0734: Communications Security R&D	22.077	22.418	23.641	-	23.641	23.771	23.326	22.637	23.021	Continuing	Continuing
Quantity of RDT&E Articles	0	0	0	0	0	0	0	0	0		

A. Mission Description and Budget Item Justification

The Information Systems Security Program (ISSP) Research Development Test & Evaluation (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 Information Assurance (IA) challenges associated with the highly mobile, dispersed, bandwidth limited, and forward-tactical connected US Navy communications systems.

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

This project includes a rapidly evolving design and application engineering effort to modernize national security-grade (Type-1) cryptographic equipment and ancillaries with state-of-the-art replacements in order to counter evolving and increasingly sophisticated threats, 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) continuing through FY2013.

In addition to protecting national security information, ISSP RDT&E must provide enterprise-wide assurance for statutorily protected information under the Privacy Act of 1974, Computer Matching and Privacy Protection Act of 1988, Medical Records Confidentiality Act of 1995, Model State Public Health Privacy Act, 45 Code of Federal Regulation subtitle A sub-chapter C, parts 160-164, 1999, and the Federal Education Records Privacy Act. ISSP RDT&E efforts must also provide assurance to the broad spectrum of Sensitive-but-Unclassified information such as financial, personnel, contractor proprietary, and procurement sensitive.

The ISSP today includes more than legacy COMSEC and network security technology. IA or defensive information operations exist to counter a wide variety of threats. ISSP activities cover all telecommunications systems, and RDT&E projects must provide protection, detection, and reaction capabilities to the operational commander. ISSP RDT&E provides dynamic risk managed IA solutions to the Navy information infrastructure, not just security devices placed within a network.

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Navy		DATE: February 2012
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>
<p>Few technology areas change as fast as telecommunications and computers, and IA must keep pace. This results in the continuing need to evaluate, develop, and/or test IA products and approaches. Technology-based efforts include developing or applying: (1) new secure voice prototypes; (2) technology for a new family of programmable COMSEC and TRANSEC modules; (3) security appliances and software for switched and routed networks; (4) technology to interconnect networks 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 (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) and Next Generation devices.</p> <p>The resulting expertise applies to a wide variety of Navy development programs that integrate IA technology. Unlike traditional single-product development programs, the ISSP RDT&E holds a unique Navy-enterprise responsibility.</p> <p>ISSP efforts conclude with continuously monitored, certified and accredited systems supported within Navy cyber operational environment. Achieving and maintaining this milestone requires:</p> <ul style="list-style-type: none"> * Evolving techniques for defense of National Security Systems 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; * Communications Security (COMSEC) and process isolation techniques for securing the critical computing base and information store. <p>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.</p> <p>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 Electronic Key Management System (EKMS)/Key Management Infrastructure (KMI).</p> <p>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 PKI and Certificate Management Infrastructure technology, and the development of improved techniques for key and certificate management to support emerging, embedded cryptographic technology.</p> <p>ISSP RDT&E management will direct a program that:</p>		

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Navy		DATE: February 2012
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>
<ul style="list-style-type: none"> * Ensures the Navy's cyber domain implements a consistent joint and Federal Enterprise cyber security architecture; * Rapidly develops, deploys, and versions cyber security measures across all seven layers of the ISO Open Systems Interconnection Reference Model and for all CNSSI 1253 Information Assurance (IA) controls (best practices); * Ensures that all data within Navy Enterprise is protected in accordance with its classification and mission criticality, as required by law; * Provides 10th Fleet and Fleet Cyber Command (FLTCYBERCOM) 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 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. <p>Maritime Operations Center (MOC) networks will operate and share information with multiple partners and 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's) 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 to monitor and visualize network traffic to provide a locally generated, fused situational awareness picture for battle watch decision-making will be provided. NetOps COP provides the Commander with near immediate risk assessment, actionable intelligence and immediate mitigation courses of action and attribution of on-going CS Protection events in order to enable the apportionment of forces with exacting control in response to national objectives.</p> <p>FY 13 Highlights for Information Systems Security Program (ISSP),</p> <p>Computer Network Defense (CND) - Continue to implement Department of Defense (DoD)/Enterprise-wide IA and CND 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 (e.g., 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 new Commander Tenth Fleet (C10F) Maritime Operations Center (MOC). Continue to integrate CND capabilities to perform near real-time analysis of events</p>		

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Navy		DATE: February 2012
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>
<p>and Advanced Persistent Threat (APT). Update the CND IA suites with adaptive defense, incident reporting, correlation, 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. 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)s 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.</p> <p>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 a NetOps COP at the C10F MOC.</p> <p>Cryptographic (Crypto)/Crypto Modernization (CM) - Continue systems and security engineering support Link-22 Modernized Link Level Communications Security (COMSEC) (MLLC) full development effort., Very High Frequency (VHF)/ Ultra High Frequency (UHF) Wideband Tactical Secure Voice Cryptologic Equipment (VINSON)/Advanced Narrowband Digital Voice Terminal (ANDVT) Cryptographic Modernization (VACM), and Link-16 CM development efforts. Key Management Infrastructure (KMI) Awareness, Navy Future Crypto Requirements, Navy Crypto Mod Acceleration with joint services. Continue coordination of a Crypto Modernization Plan for Transmission Security (TRANSEC) with National Security Agency (NSA) and other services.</p> <p>Key Management Infrastructure (KMI) - Continue transition strategy and define requirements for incorporation of other KMI roles into Navy architecture (e.g., Controlling Authority, Command Authority). Provide capability, engineering development and verification testing support to KMI Capability Increment (CI)-2. Provide engineering services to the CRYPTO MOD programs (iApp) to ensure crypto devices are being designed with Key Management Infrastructure (KMI) capabilities specifically Over the Network Keying and are Network enabled. Begin requirements definition efforts for the next generation fill device and KMI CI-3. Investigate alternative KMI architecture implementations for submarine and other communities within the Navy. 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.</p> <p>Public Key Infrastructure (PKI) - Continue to develop Secret Internet Protocol Router Network (SIPRNet) PKI solutions, including the SIPRNet Validation Authority and Hardware Token. 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 new certificates on the Common Access Card (CAC). Research and develop tools to support certificates for Non-Person Entity (NPE) devices.</p> <p>IA Services - Continue to provide security systems engineering support for the development of DoD and Navy IA architectures and the transition of new technologies to address Navy IA challenges. Provide IA risk analysis and recommended risk mitigation strategies for Navy networks and C4I systems.</p>		
B. Accomplishments/Planned Programs (\$ in Millions, Article Quantities in Each)		
Title: Computer Network Defense (CND)		
		FY 2011
		FY 2012
		FY 2013
		7.714
		8.394
		9.871
Articles:		0
		0
		0

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Navy			DATE: February 2012			
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 2011	FY 2012	FY 2013
FY 2011 Accomplishments: Supported Department of Defense (DoD) mandated network security tools including the acceleration of Host Based Security Systems (HBSS) for all afloat SIPRNet enclaves in response to United States Strategy Command (USSTRATCOM) Communications Tasking Order (CTO) 10-133. Continued testing of adaptive reactive-defense capabilities, improved incident correlation, and situation awareness reporting. Conducted engineering activities in support of extending boundary defense capabilities to afloat platforms. Addressed Computer Network Defense (CND) capabilities required to support Information Assurance (IA) management of virtual machine and Virtual network environments from a tiered enclave organizational level, network operations intermediate level, and global enterprise management level. Conducted successful developmental test and operational assessment of CND Increment 2 systems. Accomplished transition from Abbreviated Acquisition Program (AAP) to Acquisition Category (ACAT) IV program of record and completed DoD 5000 requirements in support of Milestone C. CND Increment 2 received MS C approval 16 AUG 2011. Acquisition Decision Memorandum (ADM) authorized procurement of 49 LRIP systems.						
FY 2012 Plans: Incorporate DoD mandated network security tools into the next sub-increment of CND afloat and ashore design. Efforts include deployments of HBSS to afloat Navy Internet Protocol Router Network (NIPRNet) enclaves, network mapping and leak detection solutions, and configuration compliance and remediation tools. Develop Navy implementations of these DoD-mandated tools and capabilities. With the guidance of the Navy CND Capabilities Integrated Product Team (IPT), determine the capability needs that will need to be implemented in sub-increments. Begin CND Increment 2 technology insertion cycles (rapid acquisition) to address current and emergent real world threats, performance improvements, and end-of-life issues. Continue meeting Increment 2 Capability Production Document (CPD) performance parameters and address key system attributes. Support Initial Operational Test and Evaluation (IOT&E) and associated readiness reviews for CND Increment 2 to achieve Full-Rate Production (FRP) decision.						
FY 2013 Plans: Continue to ensure that security of Navy networks will 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 installations. Continue to support 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 of 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 IA suites with adaptive defense, incident reporting, correlation, and situational awareness capabilities. Continue to develop, integrate, and test Defense-in-Depth and situational awareness technologies for knowledge-empowered CND operations for afloat						

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Navy		DATE: February 2012	
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 2011	FY 2012
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.			
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 Network Operations (NetOps) Common Operational Picture (COP) at the C10F MOC.			
Title: Crypto/Crypto Modernization		8.339	7.656
Articles:		0	0
FY 2011 Accomplishments: Continued research, evaluation, and prioritization of modernization for cryptographic products. Continued coordination with the Information Systems Security Program Office (ISSPO), joint services, and the National Security Agency (NSA), including representing the Navy at the National Cryptographic Solutions Management Office's Crypto Solution Technical Advisory Group (CSTAG). Continued identifying strategies to reduce the overall crypto inventory within the Department of the Navy (DoN) to realize long term cost savings. Continued to support the on-going Cryptographic Joint Algorithm Integrated Project Team (IPT). Continued development for the Link 16 Cryptographic Modernization. Provided Link 22 cryptographic modernization and engineering support on the Modernized Link Level Communications Security (COMSEC) (MLLC). KW-46 Modernization continued with assisting the NSA/IS with finalization of keying material generation. AN/PYQ-20 engineering support throughout fielding as Trusted Agents (TA) for the certification and accreditation, supporting on fielding strategy, and other miscellaneous items. Continued Secure Voice (SV) RDT&E efforts such as Small Business Innovation Research (SBIR) oversight, and Naval Research Laboratory (NRL's) research into SV emerging technologies and related technical products, support to Air Force lead Very High Frequency (VHF)/Ultra High Frequency (UHF) Wideband Tactical Secure Voice Cryptologic Equipment (VINSON)/Advanced Narrowband Digital Digital Voice Terminal (ANDVT) Cryptographic Modernization (VACM) program and continue supporting ASD (NII)NC2/ NC3 CM. Initiated major pre-acquisition and development efforts for Department of the Army Materiel Annex (DAMA). Coordinated a Crypto Modification plan for Transmission Security (TRANSEC) with NSA and other services. Navy VACM efforts have included continued refinement of Navy (and dependent assets (e.g., USCG, USMC, MSC) inventory numbers, VACM Integrated Test Team (ITT) participation, continued research and discussion about fielding options. Performed a Saville Voice study that resulted in a significant reduction in the number of VACM replacement units needed. Provided NC2/NC3 engineering support for Communications Security (COMSEC) used within the strategic communications architecture.			
FY 2012 Plans: Continue research, evaluation, and prioritization of cryptographic products. Continue coordination with the Information Systems Security Program (ISSP) Office and the NSA, including representing the Navy at the CSTAG. Continue identifying strategies			

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Navy			DATE: February 2012		
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 2011	FY 2012	FY 2013
<p>to reduce the overall crypto inventory within the DoN to realize long term cost savings. Continue to support the on-going Cryptographic Joint Algorithm IPT. Provide consistent IA engineering support for the development and integration of CM products. Provide research into disposition of devices on the Crypto Priority (Red) List. Conduct research into Key Management Infrastructure (KMI) awareness for devices (e.g., iApp development). Continue development for the Link 16 CM through performing technical Analysis of Alternatives (AoA) for vendor Type 1 Crypto devices and security architecture implementations, conducting security risk analysis, reviewing security requirement specifications/test plans, developing systems engineering documents into technical documentation to ensure the implementation of robust IA solutions, and providing Subject Matter Experts (SME) technical support to multi-functional Link-16 CM development teams. Provide Link 22 cryptographic modernization and engineering support on the Modernized Link Level COMSEC (MLLC), to include finalizing development of various engineering documents and specifications to support development. 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 the fielding. KW-46M work entails integration testing, Emergency Action Message (EAM) and Targeting Change Message (TCM) certifications, and installation into the Common Submarine Radio Room (CSRR). Continue Secure Voice (SV) RDT&E efforts and NRL's research into SV emerging technologies and related technical products, support to Air Force led VACM program and continue supporting ASD (NII) NC2/ NC3 CM Coordinate a Crypto Mod plan for TRANSEC with NSA and other services.</p> <p>FY 2013 Plans:</p> <p>Continue research, evaluation, and prioritization of cryptographic products. Continue coordination with NSA, including representing the Navy at the CSTAG and support to the Cryptographic Joint Algorithm Integrated Project Team (IPT). Continue identifying strategies to reduce the overall crypto inventory within the DoN to realize long term cost savings. Continue to provide research into disposition of devices on the Crypto Priority (Red) list. Continue systems and security engineering support for the Link-22 Modernized Link Level COMSEC (MLLC) during the full development effort. Conduct research into KMI Awareness for devices (e.g., iApp development). Provide consistent IA engineering support for the development and integration of CM products. Continue development for the Link 16 CM through performing technical Analysis of AoA for vendor Type 1 Crypto devices and security architecture implementations. KW-46M work entails integration testing, Emergency Action Message (EAM) and Targeting Change Message (TCM) certifications, and installation into the Common Submarine Radio Room (CSRR). Continue NRL's research into SV emerging technologies and related technical products, support to Air Force led VACM program and continue supporting ASD (NII)NC2/ NC3 CM. Coordinate a Crypto Mod plan for TRANSEC with NSA and other services. For Secure Voice, conduct and witness all test, evaluations, and certifications required during VINSON ANDVT (VACM) Development Test (DT), and Operational Test (OT).</p>					
<p>Title: Key Management Infrastructure (KMI)</p> <p align="right">Articles:</p>			2.456 0	2.708 0	2.665 0

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Navy		DATE: February 2012		
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 2011	FY 2012	FY 2013
FY 2011 Accomplishments: Continued finalizing the Department of the Navy (DoN) KMI architecture and roll out strategy for deployment. Identified any issues pertaining to transition from Electronic Key Management System (EKMS) to Key Management System (KMI) pertaining to capabilities and connectivity to Naval networks. Provided engineering support in review of all necessary documentation for Navy Independent Logistics Assessment and National Security Agency (NSA) Milestone C Acquisition Decision Memorandum. This determined Navy transition for full rate production within the Navy for KMI Capability Increment (CI)-2. Continued engineering efforts for Navy transition and test planning for KMI CI-2 Manager Client/Advanced Key Processor (MGC/AKP). Continued developing Navy implementation plan for KMI CI-2 to support Navy programs of record and EKMS end of life. Provided technical support to National Security Agency (NSA) for KMI CI-2 Spiral 1 Development Testing and Evaluation, Operational Assessment (OA), Initial Operational Testing and Evaluation (IOT&E).				
FY 2012 Plans: 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 support documentation for KMI. Begin engineering and development efforts for KMI CI-2 Spiral 2 Spin 1 for incorporation into Navy architectures and networks. Testing KMI Manager Client/Advanced Key Processors (AKP) at selected pilot sites in support of NSA full rate production decision. Provide requirements definition support to the development of the next generation fill device. Migrate Communications Security (COMSEC) Material Work Station/Data Management Device and other next generation fill devices to the KMI environment. Provide research and analysis to a centralized configuration management and crypto unit inventory tracking tool which will improve EKMS and Crypto product management. Provide 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 KMI 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 support documentation for KMI. 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. 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.				
Title: Public Key Infrastructure (PKI)		0.741	0.408	0.404
Articles:		0	0	0
FY 2011 Accomplishments:				

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Navy		DATE: February 2012	
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 2011	FY 2012
<p>Tested and evaluated security and functionality of Public Key Infrastructure (PKI) tokens, readers, and middleware for Secure Internet Protocol Router Network (SIPRNet). Researched and evaluated tools to support Non-Person Entity (NPE) certificates. Analyzed and evaluated new application updates (including Windows and non-Windows Operating Systems) for integration into Navy PKI environments. Evaluated commercial off-the-shelf products that can support coalition information sharing. Designed and developed PKI SIPRNet expansion to support Global Information Grid (GIG) identity management and protection requirements. Evaluated automated on-line network device (e.g., workstations, routers, switches) certificate issuance infrastructure. Completed Department of Defense (DoD) 5000 requirements to achieve PKI Increment 2 Spiral 2 Milestone C and completed PKI Increment 2 Spiral 1 Initial Operational Test and Evaluation (IOT&E).</p> <p>FY 2012 Plans: Research, analyze and evaluate 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. Provide systems engineering support for SIPRNet PKI enabling to Navy Programs of Record (POR) for integration. This includes research, analysis, and evaluation of PKI enabled products and methods to support the manual and automatic enrollment and issuance of PKI NPE certificates to Navy servers and devices. Evaluate Defense Information Systems Agency's (DISA) auto-enrollment and registration services for Phases II and III of DoD PKI enabled Implementation. Research, analyze, and evaluate PKI enabled products for non-Microsoft devices and systems (e.g., Linux, Apple, servers, router, switches). Explore enhancements of PKI related cryptographic algorithms.</p> <p>FY 2013 Plans: Continue to research, analyze and evaluate PK enabled (PKE) products (Microsoft and non-Microsoft) such as VPNs, routers, switches, and servers for their suitability to support Navy requirements for NPE certificates and to support GIG identity management and protection requirements. Continue to provide systems engineering support for SIPRNet PKI enablement to Navy POR for integration. Continue to support the manual and automatic enrollment and issuance of PKI NPE certificates to Navy servers and devices. Continue to evaluate DISA's auto-enrollment and registration services for DoD PKI enabled devices. Continue to research and evaluate new technologies and develop solutions to enable the Navy's Public Key Infrastructure 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.</p>			
<p>Title: Electronic Key Management System (EKMS)</p> <p align="right">Articles:</p> <p>FY 2011 Accomplishments:</p>		0.176 0	-
			-

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Navy		DATE: February 2012	
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 2011	FY 2012
Finalized Navy EKMS Phase V hardware and software development for afloat and ashore as well as submarine community. Conducted Virtual Private Network (VPN) testing and prepared all necessary installation documentation to support this effort. Identified any functional deficiencies within EKMS Phase V for inclusion into the Key Management Infrastructure (KMI) Capability Increment (CI)-2 architecture. Continued to provide technical design support to EKMS programs of record (Advanced Extremely High Frequency (AEHF) and Mobile User Objective System (MUOS)) for architectures. Continued to define EKMS technology gaps in preparation to the transition to KMI. Identified technical solutions for EKMS sustainment until KMI CI-2.			
Title: Information Assurance (IA) Services		2.651	2.752
Articles:		0	0
FY 2011 Accomplishments: Continued to provide 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 IA master plan that reflect emerging priorities and address Navy specific threats. Coordinated IA activities across the virtual System and Materiel Command (SYSCOM) via the IA Trusted Agent (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, and 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 develop guidance and procedures for the design and integration of risk mitigation strategies via appropriate IA controls.			
FY 2012 Plans: Continue to provide security systems engineering support for the development of DoD and DoN IA architectures and the transition of new technologies to address Navy IA challenges. Provide updates to the Navy IA master plan that reflect emerging priorities and address Navy specific threats. Coordinate IA activities across the virtual System Command (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 2013 Plans:			

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Navy							DATE: February 2012					
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 2011		FY 2012		FY 2013	
Continue to provide security systems engineering support for the development of DoD and DoN IA architectures and the transition of new technologies to address Navy IA challenges. Provide updates to the Navy IA master plan that reflect emerging priorities and address Navy specific threats. Coordinate IA activities across the virtual SYSCOM via the IA TA to ensure the security design and integration of 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.												
Title: Maritime Operations Center (MOC) FY 2012 Plans: Maritime Operations Center (MOC) funding transitions to Computer Network Defense (CND) funding line to continue development of Cyber MOC capabilities. MOC will conduct Analysis of Alternatives (AoA) and evaluate the 10th Fleet operational data feeds and prepare a project plan to integrate these feeds to a set of Network Operations (NetOps) Common Operational Picture (COP) tools and maximize NetOps watch standard effectiveness.							Articles: -		0.500 0		-	
Accomplishments/Planned Programs Subtotals							22.077		22.418		23.641	
C. Other Program Funding Summary (\$ in Millions)												
Line Item		FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total	FY 2014	FY 2015	FY 2016	FY 2017	Cost To Complete	Total Cost
• OPN/3415: Info Sys Security Program (ISSP)		113.737	109.394	144.104	0.000	144.104	142.507	136.454	125.421	125.641	Continuing	Continuing
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.												
Key Management Infrastructure (KMI) - KMI is the next generation EKMS system that is net centric in nature, providing the infrastructure for management, ordering and distribution of key material as well as directly supporting the key requirements of all Crypto modernization efforts. Navy will continue to provide and refine Navy unique requirements into the NSA KMI CI-2 Spiral 2 Spin 2 capability. In parallel, KMI will continue to define Navy operational architecture and requirements for roll out of this new capability in the Fiscal Year 2013. Provide and refine Navy unique requirements into the NSA KMI CI-3 Capability Development Document (CDD). Investigate alternative KMI architecture implementations for submarine and other communities within the Navy.												

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Navy		DATE: February 2012
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>
<p>Cryptographic Modernization (CM) - The procurement and fielding of Modernized Crypto devices such as the KG-3X Inc 2, KG-45A, AN-PYQ-20(v)(c) (formerly KL-51M), KW-46M, KG-175D, KG-175A, KG-3X Suites, K02 Replacement, Very High Frequency (VHF)/Ultra High Frequency (UHF) Wideband Tactical Secure Voice Cryptologic Equipment (VINSON)/Advanced Narrowband Digital Voice Terminal (ANDVT) Cryptographic modernization (VACM), Common Submarine Radio Room (CSRR), Walburn, and 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.</p> <p>Computer Network Defense (CND) - The CND program procures equipment to secure Navy network information systems. Procurements within the CND equipment line include: Firewall components which provide protection for networks from unauthorized users, Virtual Private Networks (VPN's) which provide encrypted "Point-to-Point" virtual communication networks, Intrusion Prevention Systems (IPS), Administrator Access Control, Network Security tools and Filtering routers. CND procurements will also include Department of Defense (DoD) Information Assurance (IA) certification and accreditation process end-to-end certification and accreditation support tool, to provide enterprise-wide visibility into security posture. The rapid advance of cyber technology requires an efficient process for updating CND tools deployed to afloat and shore platforms. Recognizing the need for future CND capability improvements, CND will be implementing an evolutionary acquisition strategy that delivers CND capability in multiple increments and functionality releases that address validated requirements.</p> <p>Maritime Operations Center (MOC) - This Research Development Test & Evaluation (RDT&E) line supports an incremental acquisition strategy. MOC utilizes a System of Systems (SoS) and incremental approach in achieving global network of Navy Maritime organizations through Builds as defined by OPNAV N2/N6F41/C10F.</p> <p>E. Performance Metrics</p> <p>Key Management Infrastructure (KMI):</p> <ul style="list-style-type: none"> * Install KMI Manager Client/Advanced Key Processor (MGC/AKPs Spiral 2/Spin2) at selected pilot sites to support Initial Operational Capability (IOC). * Conduct Navy 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 by 4QFY13. * Complete engineering efforts and test planning for the KMI CI-2 (Spiral 2/Spin 2) transition. <p>Cryptographic Modernization (CM):</p> <ul style="list-style-type: none"> * Meet 100% of TOP SECRET (TS) and SECRET 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, hardware sustainment issues, and identify transition device schedules if one exists. * Meet 100% of TS and SECRET CJCSI 6510 by fielding modern cryptographic devices or request "recertification" via the Joint Staff Military Communications-Electronics Board (MCEB). 		

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Navy		DATE: February 2012
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>
<p>* Increase the functionality cryptographic devices by replacing 2 legacy cryptographic devices with 1 modern device where possible and identify and implement modern small form factor, multi channel cryptos. (e.g., KIV-7M replacing KIV-7HS, KIV-7HSB, KG-84, KWR-46, KL-51, etc.)</p> <p>Computer Network Defense (CND):</p> <p>* Provide the ability to protect from, react to, and restore operations after an intrusion or other catastrophic event through validated Contingency Plans (CPs) for 100% of CND systems.</p> <p>* 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.</p> <p>* 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.</p> <p>Information Assurance (IA) services:</p> <p>* Ensure 100% interoperability and application of commercial standards compliance for ISSP products by researching and conducting selective evaluations, to integrate and test of commercial-off-the-shelf/Non-Developmental Item 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).</p> <p>* 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.</p> <p>* Coordinate IA activities across the Navy Enterprise via the IA Trusted Agent (TA) to measure effectiveness of Navy networks and ensure the security design and integration of Computer Adaptive Network Defense-in-Depth (CANDiD) products and services is 100% interoperable and operationally acceptable across the Navy for major initiatives such as the future afloat, ashore, and OCONUS networks.</p> <p>Maritime Operations Center (MOC):</p> <p>Develop and provide Network Operations (NetOps) Common Operational Picture (COP) for C10F.</p>		

UNCLASSIFIED

Exhibit R-3, RDT&E Project Cost Analysis: PB 2013 Navy											DATE: February 2012			
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 Base		FY 2013 OCO		FY 2013 Total				
Cost Category Item	Contract Method & Type	Performing Activity & Location	Total Prior Years Cost	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Cost To Complete	Total Cost	Target Value of Contract	
Systems Engineering	WR	SSC PAC/ SSC LANT:San Diego, CA/ Charleston, SC	22.710	7.685	Dec 2011	7.428	Dec 2012	-		7.428	Continuing	Continuing	Continuing	
Systems Engineering	WR	NRL:Washington, DC	0.600	0.278	Dec 2011	0.280	Dec 2012	-		0.280	Continuing	Continuing	Continuing	
Systems Engineering - Link 22	C/CPAF	Northrup Grumman:Washington, DC	-	0.105	Nov 2011	0.106	Nov 2012	-		0.106	Continuing	Continuing	Continuing	
Systems Engineering (MOC)	WR	SSC PAC:San Diego, CA	-	0.500	Dec 2011	1.000	Dec 2012	-		1.000	Continuing	Continuing	Continuing	
Systems Engineering	WR	NUWC:Newport, RI	0.608	-		-		-		-	Continuing	Continuing	Continuing	
Systems Engineering	WR	FNMO:Monterey, CA	0.480	-		-		-		-	Continuing	Continuing	Continuing	
Software Development	C/CPAF	SAIC:San Diego, CA	32.877	-		-		-		-	Continuing	Continuing	Continuing	
Software Development	WR	SSC PAC/ SSC LANT:San Diego, CA/ Charleston, SC	11.029	-		-		-		-	Continuing	Continuing	Continuing	
Software Development	WR	NRL:Washington, DC	19.196	1.299	Dec 2011	1.322	Dec 2012	-		1.322	Continuing	Continuing	Continuing	
Primary Hardware Development (PY)	WR	Various:Various	102.136	-		-		-		-	Continuing	Continuing	Continuing	
Primary Hardware Development	WR	SSC PAC:San Diego, CA	2.554	-		-		-		-	Continuing	Continuing	Continuing	
Primary Hardware Development	WR	NRL:Washington, DC	0.970	-		-		-		-	Continuing	Continuing	Continuing	
Subtotal			193.160	9.867		10.136		-		10.136				
Support (\$ in Millions)				FY 2012		FY 2013 Base		FY 2013 OCO		FY 2013 Total				
Cost Category Item	Contract Method & Type	Performing Activity & Location	Total Prior Years Cost	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Cost To Complete	Total Cost	Target Value of Contract	
Architecture	WR	SSC PAC/ SSC LANT:San Diego, CA/ Charleston, SC	-	0.849	Dec 2011	0.856	Dec 2012	-		0.856	Continuing	Continuing	Continuing	

UNCLASSIFIED

Exhibit R-3, RDT&E Project Cost Analysis: PB 2013 Navy										DATE: February 2012			
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 Base		FY 2013 OCO		FY 2013 Total			
Cost Category Item	Contract Method & Type	Performing Activity & Location	Total Prior Years Cost	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Cost To Complete	Total Cost	Target Value of Contract
Architecture	C/CPFF	BAH:San Diego, CA	-	0.774	Oct 2011	0.782	Oct 2012	-		0.782	Continuing	Continuing	Continuing
Requirements Analysis	WR	Various:Various	-	0.978	Dec 2011	0.988	Dec 2012	-		0.988	Continuing	Continuing	Continuing
Studies & Design	WR	Various:Various	-	0.777	Dec 2011	0.783	Dec 2012	-		0.783	Continuing	Continuing	Continuing
Studies & Design	WR	SSC PAC/ SSC LANT:San Diego, CA/ Charleston, SC	-	1.674	Dec 2011	1.691	Dec 2012	-		1.691	Continuing	Continuing	Continuing
Systems Engineering Spt	WR	NRL:Washington, DC	-	0.183	Dec 2011	0.185	Dec 2012	-		0.185	Continuing	Continuing	Continuing
Systems Engineering Spt	WR	Various:Various	-	1.678	Dec 2011	1.690	Dec 2012	-		1.690	Continuing	Continuing	Continuing
Systems Engineering Spt	WR	SSC PAC/ SSC LANT:San Diego, CA/ Charleston, SC	-	1.183	Dec 2011	2.000	Dec 2012	-		2.000	Continuing	Continuing	Continuing
Subtotal			-	8.096		8.975		-		8.975			
Test and Evaluation (\$ in Millions)				FY 2012		FY 2013 Base		FY 2013 OCO		FY 2013 Total			
Cost Category Item	Contract Method & Type	Performing Activity & Location	Total Prior Years Cost	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Cost To Complete	Total Cost	Target Value of Contract
System DT&E	WR	NUWC:Newport, RI	0.623	0.075	Dec 2011	0.076	Dec 2012	-		0.076	Continuing	Continuing	Continuing
System DT&E	WR	SSC LANT:Charleston, SC	-	0.260	Dec 2011	0.262	Dec 2012	-		0.262	Continuing	Continuing	Continuing
System DT&E	WR	SSC PAC:San Diego, CA	34.778	-		-		-		-	Continuing	Continuing	Continuing
System OT&E	WR	COTF:Norfolk, VA	0.125	0.115	Dec 2011	0.116	Dec 2012	-		0.116	Continuing	Continuing	Continuing
Subtotal			35.526	0.450		0.454		-		0.454			
Management Services (\$ in Millions)				FY 2012		FY 2013 Base		FY 2013 OCO		FY 2013 Total			
Cost Category Item	Contract Method & Type	Performing Activity & Location	Total Prior Years Cost	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Cost To Complete	Total Cost	Target Value of Contract
Acquisition Management	C/CPFF	BAH:San Diego, CA	-	1.457	Dec 2011	1.472	Dec 2012	-		1.472	Continuing	Continuing	Continuing

UNCLASSIFIED

Exhibit R-3, RDT&E Project Cost Analysis: PB 2013 Navy										DATE: February 2012			
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 Base		FY 2013 OCO		FY 2013 Total			
Cost Category Item	Contract Method & Type	Performing Activity & Location	Total Prior Years Cost	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Cost To Complete	Total Cost	Target Value of Contract
Financial Management/ Cost Estimating	C/CPFF	Various:Various	-	0.679	Oct 2011	0.686	Oct 2012	-		0.686	Continuing	Continuing	Continuing
Travel	WR	SPAWAR:San Diego, CA	-	0.119	Oct 2011	0.120	Oct 2012	-		0.120	Continuing	Continuing	Continuing
Program Management	WR	SSC PAC/ SSC LANT:San Diego, CA/ Charleston, SC	-	0.294	Dec 2011	0.297	Dec 2012	-		0.297	Continuing	Continuing	Continuing
Program Management	WR	SSC PAC:San Diego, CA	1.213	-		-		-		-	Continuing	Continuing	Continuing
Program Management	C/CPFF	BAH:San Diego, CA	19.205	1.456	Oct 2011	1.501	Oct 2012	-		1.501	Continuing	Continuing	Continuing
Subtotal			20.418	4.005		4.076		-		4.076			
			Total Prior Years Cost	FY 2012		FY 2013 Base		FY 2013 OCO		FY 2013 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals			249.104	22.418		23.641		-		23.641			
Remarks													

UNCLASSIFIED

Exhibit R-4, RDT&E Schedule Profile: PB 2013 Navy		DATE: February 2012
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>

UNCLASSIFIED

Exhibit R-4, RDT&E Schedule Profile: PB 2013 Navy		DATE: February 2012
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>

UNCLASSIFIED

Exhibit R-4, RDT&E Schedule Profile: PB 2013 Navy		DATE: February 2012
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>

UNCLASSIFIED

Exhibit R-4, RDT&E Schedule Profile: PB 2013 Navy		DATE: February 2012
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>

UNCLASSIFIED

Exhibit R-4, RDT&E Schedule Profile: PB 2013 Navy		DATE: February 2012
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>

UNCLASSIFIED

Exhibit R-4, RDT&E Schedule Profile: PB 2013 Navy		DATE: February 2012
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>

UNCLASSIFIED

Exhibit R-4, RDT&E Schedule Profile: PB 2013 Navy		DATE: February 2012
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>

UNCLASSIFIED

Exhibit R-4A, RDT&E Schedule Details: PB 2013 Navy			DATE: February 2012
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				
EKMS - Phase V FOC	3	2014	3	2014
TKL - Contract Award	3	2011	3	2011
TKL - IOC	1	2013	1	2013
TKL - FOC	1	2015	1	2015
KMI CI-2 MS C	1	2012	1	2012
KMI CI-2 - IOC	3	2013	3	2013
KMI CI-2 - FOC	1	2017	1	2017
KMI CI-2 DT&E	2	2011	2	2011
KMI CI-2 - OA2	3	2012	3	2012
KMI CI-2 - IOT&E	3	2012	3	2012
TKL - FA Test	1	2012	1	2012
TKL - FRP Decision	3	2012	3	2012
KMI CI-2 Contract Award	2	2012	2	2012
KMI CI-2 - Spiral 1 FRP	1	2013	1	2013
KMI CI-2 - Spiral 2 FRP	1	2014	1	2014
EKMS - Phase V SW	1	2011	1	2013
EKMS SKL - Deliveries	1	2011	3	2013
TKL - Deliveries	1	2013	1	2015
KMI CI-2 Spiral 1 LRIP Deliveries	4	2012	4	2012
KMI CI-2 - Spiral 2 Deliveries	3	2013	1	2017
KMI CI-2 - Next Generation Fill Device	1	2013	1	2017

UNCLASSIFIED

Exhibit R-4A, RDT&E Schedule Details: PB 2013 Navy			DATE: February 2012		
APPROPRIATION/BUDGET ACTIVITY 1319: Research, Development, Test & Evaluation, Navy BA 7: Operational Systems Development		R-1 ITEM NOMENCLATURE PE 0303140N: Information Sys Security Program		PROJECT 0734: Communications Security R&D	
		Start		End	
Events by Sub Project		Quarter	Year	Quarter	Year
CRYPTO KG-3X - Inc 2 MS C/LRIP		2	2011	2	2011
CRYPTO KG 3X - Inc 2 FRP Decision		4	2011	4	2011
CRYPTO KG-45A - FOC		1	2013	1	2013
CRYPTO KW-46M - IOC		2	2012	2	2012
CRYPTO Link 22 MLLC - Prototype Award		2	2011	2	2011
CRYPTO VACM - MS C		3	2013	3	2013
CRYPTO VACM - IOC		3	2014	3	2014
CRYPTO VACM LRIP		3	2013	3	2013
CRYPTO VACM FRP		4	2013	4	2013
CRYPTO KG 3X - Inc 2 IOT&E		2	2011	2	2011
CRYPTO KW-46M - NUWC Integration Test		2	2012	2	2012
CRYPTO VACM IOT&E		4	2013	1	2014
CRYPTO KG-3X - Inc 2 Deliveries		1	2012	3	2012
CRYPTO KW-46M - CSRR Deliveries		2	2012	4	2017
CRYPTO AN-PYQ-20(v)(c)-(formerly KL-51M) Deliveries		1	2011	1	2013
CRYPTO KG-45A - Deliveries		1	2011	1	2013
CRYPTO Link-22 - MLLC Prototype Delivery		2	2012	2	2012
CRYPTO VACM LRIP Deliveries		3	2013	1	2014
CRYPTO VACM FRP Deliveries		1	2014	1	2017
PKI - Inc 2 Spiral 2 MS C		3	2011	3	2011
PKI - Inc 2 Spiral 3 IOC		3	2013	3	2013
PKI - Inc 2 FOC		2	2014	2	2014
PKI - Inc 2 Spiral 1 IOT&E		3	2011	3	2011
CND - Inc 2 MS C		4	2011	4	2011
CND - Inc 2 IOC		4	2012	4	2012

UNCLASSIFIED

Exhibit R-4A, RDT&E Schedule Details: PB 2013 Navy			DATE: February 2012	
APPROPRIATION/BUDGET ACTIVITY 1319: Research, Development, Test & Evaluation, Navy BA 7: Operational Systems Development	R-1 ITEM NOMENCLATURE PE 0303140N: Information Sys Security Program		PROJECT 0734: Communications Security R&D	
	Start		End	
Events by Sub Project	Quarter	Year	Quarter	Year
CND - Inc 2 FOC	4	2016	4	2016
CND - Inc 2 DT	3	2011	3	2011
CND - Inc 2 OA	3	2011	3	2011
CND - Inc 2 IOT&E	3	2012	3	2012
CND - Inc 2 LRIP	4	2011	3	2012
CND - Inc 2 FRP Decision	4	2012	4	2012
CND - Inc 2 Delivery	1	2012	4	2017

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Navy									DATE: February 2012		
APPROPRIATION/BUDGET ACTIVITY 1319: Research, Development, Test & Evaluation, Navy BA 7: Operational Systems Development				R-1 ITEM NOMENCLATURE PE 0303140N: Information Sys Security Program				PROJECT 3230: Information Assurance			
COST (\$ in Millions)	FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total	FY 2014	FY 2015	FY 2016	FY 2017	Cost To Complete	Total Cost
3230: Information Assurance	2.911	2.778	2.666	-	2.666	2.761	2.658	2.677	2.733	Continuing	Continuing
Quantity of RDT&E Articles	0	0	0	0	0	0	0	0	0		

A. Mission Description and Budget Item Justification

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

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

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

The program will develop common architectural frameworks that facilitate integration of network security capabilities, enable effective seamless 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. Initiate requirements definition for situation awareness capabilities to support computer network defense in highly distributed, homogeneous, and heterogeneous networks including mobile and embedded networked devices. This effort also includes the architectural definition of situational awareness and visualization capabilities to support active computer network defense and support underlying data mining and correlation tools. This includes addressing the capability to remotely manage and securely control the configurations of network security components to implement changes in real time or near real time. Initiate requirements definition for secure coalition data exchange and interoperability.

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Navy		DATE: February 2012		
APPROPRIATION/BUDGET ACTIVITY 1319: Research, Development, Test & Evaluation, Navy BA 7: Operational Systems Development	R-1 ITEM NOMENCLATURE PE 0303140N: Information Sys Security Program	PROJECT 3230: Information Assurance		
among security levels and classifications. Ensure approaches address various security level technologies as well as emerging architectural methods of providing interoperability across different security levels. Examine multi-level aware applications and technologies including databases, web browsers, routers/switches, etc. Initiate infrastructure protection efforts as the Navy develops network centric architectures and warfare concepts, ensuring an evolutionary development of security architectures and products for IA that addresses Navy infrastructure requirements. Ensure the architectures evolve to provide proper protection as technology, DoD missions, and the threat all evolve. Include defensive protections as well as intrusion monitoring (sensors), warning mechanisms, and response capabilities in the architecture. Ensure the unique security and performance requirements of tactical systems, including those operating various security levels are addressed. Initiate the efforts to conceptualize new network centric warfare technology to protect our assets, such as secure network gateways and routers, and components and tools that improve the survivability of Navy networks. Provide systems security engineering, certification and accreditation support for high-confidence naval information system and ensure certification and accreditation approaches are consistent with Navy and DoD requirements.				
Major focus area in FY13: Continue development of new network security 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 2011	FY 2012	FY 2013
Title: Information Assurance		2.911	2.778	2.660
Articles:		0	0	0
FY 2011 Accomplishments: Completed the development of the technology that protects, assesses and responds to attacks of the infrastructure framework and provided reconstitution capabilities/services; assessed in representative operational environments. Completed the development of modernized attack sensing and warning mechanisms based on new detection algorithms and data mining concepts, and response capabilities for the architecture/framework. Continued the development of a new high assurance boundary controller to protect Navy and Marine Corps data and resources from attack. Ensured the security services included, at a minimum, encryption and data malware analysis in the boundary controller as well as the ability to adjust routing of communications based on network stress levels. Continued the development of a high-assurance computing environment for Navy and Marine Corps use based on trusted platform technology. Continued the development of the appropriate core code, security messages and assurance functions required. Continued the development of new key and enabling technologies, management tools, and capabilities to address specific Navy and Marine Corps needs. Ensured the new solutions address distribution and management in bandwidth limited environments and tactical environments. Initiated the development of mobile security techniques that introduce time and location-based security parameters for geo-location and asset protection and management. Addressed the specific issues of geo-location and mapping in Global Positioning System (GPS) constrained environments. Continued systems security engineering, certification and accreditation support for high-confidence naval information systems and ensured certification and accreditation approaches are consistent with Navy and DoD requirements.				
FY 2012 Plans: Initiate the development of new network security technology focused on addressing nation state level sponsored activity. Address the growing threat by providing robust characterization of attacks/profiles to increase detection rates of the technology and to				

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Navy		DATE: February 2012	
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 2011	FY 2012
<p>support attribution of threat actions across network boundaries. Continue the development of a new high assurance boundary controller to protect Navy and Marine Corps data and resources from attack. Ensure the security services include, at a minimum, encryption and data malware analysis in the boundary controller as well as the ability to adjust routing of communications based on network threat-action levels. Complete the development of a high-assurance computing environment for Navy and Marine Corps use based on trusted platform technology. Complete the development of the appropriate core code, security messages and assurance functions required to ensure platform hardware and software protection. Complete the development of new key and enabling technologies, management tools, and capabilities to address specific Navy and Marine Corps needs. Ensure the new solutions address distribution and management in bandwidth limited environments and tactical environments. Continue the development of mobile security techniques that introduce time and location-based security parameters for geo-location and asset protection and management. Address the specific issues of geo-location and mapping in GPS constrained environments. Initiate the development of critical cryptographic technology to support Navy unique platforms and requirements. Ensure the technology addresses the limited size, weight and power issues, multiple data classification processing requirements, and provide on-the-fly programmability of mission data and key material to support various missions. Continue systems security engineering, certification and accreditation support for high-confidence naval information systems and ensure certification and accreditation approaches are consistent with Navy and DoD requirements.</p> <p>FY 2013 Plans:</p> <p>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. Incorporate 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. Ensure essential robust communications are available through the boundary controller to provide continuity of operations during nation state sponsored attacks. Initiate development of a security framework for a federated cross-domain service oriented architecture (SOA). Ensure 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 allow the use/integration of commercial technology in a secure manner. Initial efforts focus 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. Address 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 (e.g., unmanned autonomous systems (UASs)). Ensure the technology addresses the limited size, weight and power issues, multiple data classification processing requirements, and provide on-the-fly programmability of mission</p>			

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Navy		DATE: February 2012	
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 2011	FY 2012
data and key material to support various missions. Continue systems security engineering, certification and accreditation support for high-confidence naval information systems and ensure certification and accreditation approaches are consistent with Navy and DoD requirements.			
Accomplishments/Planned Programs Subtotals		2.911	2.778
			2.666
C. Other Program Funding Summary (\$ in Millions) N/A			
D. Acquisition Strategy This project funds advanced development, test and evaluation of naval information systems security based on leading edge technologies that will improve information assurance (e.g., situational awareness and information infrastructure protection) across all Command echelons to tactical units afloat and war fighters ashore. This effort will provide the research to develop a secure seamless interoperable, common operational environment of networked information systems in the battle space and for monitoring and protecting the information infrastructure from malicious activities. Technologies developed are not transitioned into a acquisition program within the ISSP OPN (BLI 3415) budget.			
E. Performance Metrics Cryptographic Modernization (CM): * Develop new emerging cryptographic technology for airborne applications by reducing the form-factor by 30%, and provide multi-channel, field reprogrammable cryptos that can be reprogrammed with algorithms in less than 1 minute. Increase throughput capabilities by 50% to meet high speed networks and develop new network-aware cryptographic technology to maximize bandwidth usage. Computer Network Defense (CND): * Develop new algorithms to provide real-time detection of nation state malware attacks against DoN networks. Detection algorithms shall be used by both host-based sensors and network sensors to provide a 100% detection of known/programmed malware. * Develop new malware analysis technology to decrease the analysis time by 50%, thus providing support for zero-day attacks. Wireless Security: * Develop new wireless signal discovery technology to increase detection by 30% and increase the bandwidth sensitivity by 20% thus allowing analysis and protection of DoN assets used in the wider emerging wireless spectrum.			

UNCLASSIFIED

Exhibit R-3, RDT&E Project Cost Analysis: PB 2013 Navy											DATE: February 2012		
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 Base		FY 2013 OCO		FY 2013 Total			
Cost Category Item	Contract Method & Type	Performing Activity & Location	Total Prior Years Cost	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Cost To Complete	Total Cost	Target Value of Contract
Development Support	Various	NRL:Washington, DC	2.998	2.778	Nov 2011	2.666	Nov 2012	-		2.666	Continuing	Continuing	Continuing
Subtotal			2.998	2.778		2.666		-		2.666			

	Total Prior Years Cost	FY 2012		FY 2013 Base		FY 2013 OCO		FY 2013 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	2.998	2.778		2.666		-		2.666			

Remarks

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Navy **DATE:** February 2012

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>
---	--	---

COST (\$ in Millions)	FY 2011	FY 2012	FY 2013 Base	FY 2013 OCO	FY 2013 Total	FY 2014	FY 2015	FY 2016	FY 2017	Cost To Complete	Total Cost
9999: <i>Congressional Adds</i>	-	12.000	-	-	-	-	-	-	-	0.000	12.000
Quantity of RDT&E Articles	0	0	0	0	0	0	0	0	0		

A. Mission Description and Budget Item Justification

Computer Network Defense (CND) will accelerate and improve 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 will focus on enabling development of Navy high speed tactical network sensors. Conduct systems engineering and architect Theater Network Operations and Security (TNSOC) modifications required to support ONE-Net environment security enhancements and network efficiencies. Establish lab environment that can support the development of Ozone Widget framework tools. Begin to develop the architecture and integrate 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. Determine optimal technical and governance solution for interception of outbound encrypted traffic, allowing for inspection and control. Update the CND development lab hardware 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 will also promote comprehensive implementation of Host Based Security Systems (HBSS) and other DoD mandated tools and capabilities.

B. Accomplishments/Planned Programs (\$ in Millions)

	FY 2011	FY 2012
Congressional Add: Cyber Security Research (Cong)	-	12.000
FY 2012 Plans: Computer Network Defense (CND) will accelerate and improve 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 will focus on enabling development of Navy high speed tactical network sensors. Conduct systems engineering and architect Theater Network Operations and Security (TNSOC) modifications required to support ONE-Net environment security enhancements and network efficiencies. Establish lab environment that can support the development of Ozone Widget framework tools. Begin to develop the architecture and integrate 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. Determine optimal technical and governance solution for interception of outbound encrypted traffic, allowing for inspection and control. Update the CND development lab hardware 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 will also promote comprehensive implementation of Host Based Security Systems (HBSS) and other DoD mandated tools and capabilities.		
Congressional Adds Subtotals	-	12.000

UNCLASSIFIED

Exhibit R-2A, RDT&E Project Justification: PB 2013 Navy		DATE: February 2012
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>
C. Other Program Funding Summary (\$ in Millions) N/A		
D. Acquisition Strategy Congressional Adds.		
E. Performance Metrics Congressional Adds.		

UNCLASSIFIED

Exhibit R-3, RDT&E Project Cost Analysis: PB 2013 Navy											DATE: February 2012		
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>					

Product Development (\$ in Millions)				FY 2012		FY 2013 Base		FY 2013 OCO		FY 2013 Total			
Cost Category Item	Contract Method & Type	Performing Activity & Location	Total Prior Years Cost	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Cost To Complete	Total Cost	Target Value of Contract
Systems Engineering	WR	SSC PAC/ SSC LANT:San Diego, CA/ Charleston, SC	-	10.090	May 2012	-		-		-	0.000	10.090	
Subtotal			-	10.090		-		-		-	0.000	10.090	

Support (\$ in Millions)				FY 2012		FY 2013 Base		FY 2013 OCO		FY 2013 Total			
Cost Category Item	Contract Method & Type	Performing Activity & Location	Total Prior Years Cost	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Cost To Complete	Total Cost	Target Value of Contract
Requirements Analysis	WR	NRL:Washington, DC	-	1.250	May 2012	-		-		-	0.000	1.250	
Subtotal			-	1.250		-		-		-	0.000	1.250	

Management Services (\$ in Millions)				FY 2012		FY 2013 Base		FY 2013 OCO		FY 2013 Total			
Cost Category Item	Contract Method & Type	Performing Activity & Location	Total Prior Years Cost	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Cost To Complete	Total Cost	Target Value of Contract
Management Services	C/CPFF	BAH:San Diego, CA	-	0.660	May 2012	-		-		-	0.000	0.660	
Subtotal			-	0.660		-		-		-	0.000	0.660	

			Total Prior Years Cost	FY 2012		FY 2013 Base		FY 2013 OCO		FY 2013 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals			-	12.000		-		-		-	0.000	12.000	

Remarks													