Exhibit R-2, RDT&E Budget Item Justification: PB 2015 Navy											Date: March 2014	
Appropriation/Budget Activity 1319: *Research, Development, Test & Evaluation, Navy I* BA 7: *Operational Systems Development*					R-1 Program Element (Number/Name) PE 0303140N *I Information Sys Security Program*							
COST ($ in Millions)	**Prior Years**	**FY 2013**	**FY 2014**	**FY 2015 Base**	**FY 2015 OCO #**	**FY 2015 Total**	**FY 2016**	**FY 2017**	**FY 2018**	**FY 2019**	**Cost To Complete**	**Total Cost**
Total Program Element	317.124	27.723	23.514	23.053	-	23.053	25.423	21.848	22.393	23.000	Continuing	Continuing
0734: *Communications Security R&D*	311.460	25.284	21.113	19.171	-	19.171	23.327	19.723	20.282	20.814	Continuing	Continuing
3230: *Information Assurance*	5.664	2.439	2.401	3.882	-	3.882	2.096	2.125	2.111	2.186	Continuing	Continuing

The FY 2015 OCO Request will be submitted at a later date.

A. Mission Description and Budget Item Justification

The 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 the protection of the Navy's National Security Systems and Information (NSSI). ISSP 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, ISSP provides architectures, products, and services based on mission impacts, information criticality, threats, vulnerabilities, and required defensive countermeasure capabilities.

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, DoD Directives 8500.01, O-8530.01, and 8570.01, the new DoD Instruction (DoDI)8500.01, NIST 800-53 rev 4 IA control catalog, new DoDI 8510.01, and CNSS Instruction 1253.

FY15 will focus on ISSP efforts that address the risk management of cyberspace as defined in "The National Military Strategy for Cyberspace Operations", Chairman of the Joint Chiefs of Staff, Dec 2006, defensive Information Operations (IO) as defined in Joint Publication 3-13, and Defensive Cyberspace Operations (DCO) as defined in Joint Publication 3-12, which includes the capabilities to protect, detect, restore, and respond. ISSP provides the Navy with the following cyber security elements: (1) defense of NSSI, including the Nuclear Command, Control, and Communications (NC3) system, naval weapons systems, critical naval infrastructure, joint time and navigation systems, and industrial control systems; (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 (CND) service provider operations; (4) assurance of the Navy's telecommunications infrastructure and the wireless spectrum; (5) assurance of joint-user cyberspace domains, using a defense-in-depth architecture; (6) assurance of the critical computing base and information store; (7) assurance of mobile and cloud computing; (8) supporting assurance technologies, including the Public Key Infrastructure (PKI) and Key Management(KM); and (9) Cyber remediation capabilities that will accelerate the Navy's ability to prevent, constrain and mitigate cyber-attacks and critical vulnerabilities as well as provide greater resiliency, awareness, data analytics, redundancy and diversity into the Navy's Defense-in-Depth (DiD) strategy.

Exhibit R-2, RDT&E Budget Item Justification: PB 2015 Navy	Date: March 2014
Appropriation/Budget Activity 1319: *Research, Development, Test & Evaluation, Navy I* BA 7: *Operational Systems Development*	**R-1 Program Element (Number/Name)** PE 0303140N *I Information Sys Security Program*

B. Program Change Summary ($ in Millions)	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO	FY 2015 Total
Previous President's Budget	26.307	23.531	27.548	-	27.548
Current President's Budget	27.723	23.514	23.053	-	23.053
Total Adjustments	1.416	-0.017	-4.495	-	-4.495
• Congressional General Reductions	-	-0.017			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	2.212	-			
• SBIR/STTR Transfer	-0.382	-			
• Program Adjustments	-	-	-0.015	-	-0.015
• Rate/Misc Adjustments	-0.001	-	-4.480	-	-4.480
• Congressional General Reductions Adjustments	-0.413	-	-	-	-

Change Summary Explanation

Schedule:

Computer Network Defense (CND):

- Due to the dynamically changing threat, CND Inc 2 Full Operational Capability (FOC) has shifted beyond the current Future Years Defense Program (FYDP) to align with Capabilities Production Document (CPD)
- Added CND Build Milestones
- Build 3 completion shifted from 2Q15 to 3Q15.
- Build 4 start shifted from 1Q15 to 2Q15. Build 4 completion shifted from 1Q16 to 2Q16.
- Build 5 start shifted from 4Q15 to 1Q16. Build 5 completion shifted from 4Q16 to 1Q17.

Navy Cryptography (Crypto):

- KG-45A FOC shifted from 4QFY13 to 1QFY14 due to fleet schedule changes
- Link 22 (L22) Preliminary Design Review (PDR) 1 & 2 coupled to maintain schedule
- L22 Technical Readiness Review (TRR) 1 shifted from 4QFY13 to 3QFY14, L22 TRR 2 shifted from 1QFY14 to 3QFY14, L22 Production Readiness Review shifted from 3QFY14 to 4QFY14, and L22 Full Development Delivery shifted from 3QFY14 to 4QFY14 due to changes in vendor's schedule.
- VINSON/Advanced Narrowband Digital Voice Terminal Crypto Modernization (VACM) Milestone C (MS C) shifted from 4QFY13 to 2QFY14, Initial Operational Test and Evaluation (IOT&E) start shifted from 4QFY13 to 4QFY14, Full Rate Production (FRP) decision shifted from 3QFY14 to 2QFY15, and Initial Operational Capability (IOC) shifted from 4QFY14 to 2QFY16, due to changes in Air Force schedule

Exhibit R-2, RDT&E Budget Item Justification: PB 2015 Navy	Date: March 2014
Appropriation/Budget Activity 1319: *Research, Development, Test & Evaluation, Navy I* BA 7: *Operational Systems Development*	**R-1 Program Element (Number/Name)** PE 0303140N *I Information Sys Security Program*

Electronic Key Management System (EKMS):
- Phase V FOC completed.

Key Management Infrastructure (KMI):
- Capability Increment 2 (CI-2) Spiral 2 (SP2) FOC shifted from Q3FY18 to Q1FY18 due change in fielding plan and in accordance with National Security Agency(NSA) Electronic Key Management System (EKMS) end of life date
- CI-2 Spiral 1 (SP1) Full Rate Production Decision (FRPD) and Full Rate Fielding Decision (FRFD) completed.

Public Key Infrastructure (PKI):
- PKI Inc2 Spiral 3 IOC shifted from 3QFY13 to 2QFY14 and Inc 2 FOC shifted from 2QFY14 to 4QFY15 due to testing schedule delays. The Defense Information Security Agency (DISA) is the Lead Agency for PKI.

Funding:
Project 3230 - FY15 $1.2M increase in funding supports the Weaselboard Program which is addressing an urgent Speed to Fleet initiative to assess the health and protection of shipboard systems and identify anomalous activity with Shipboard Supervisory Control and Data Acquisition (SCADA) information.

Exhibit R-2A, RDT&E Project Justification: PB 2015 Navy												Date: March 2014
Appropriation/Budget Activity 1319 / 7					R-1 Program Element (Number/Name) PE 0303140N / *Information Sys Security Program*				Project (Number/Name) 0734 / *Communications Security R&D*			
COST ($ in Millions)	**Prior Years**	**FY 2013**	**FY 2014**	**FY 2015 Base**	**FY 2015 OCO #**	**FY 2015 Total**	**FY 2016**	**FY 2017**	**FY 2018**	**FY 2019**	**Cost To Complete**	**Total Cost**
0734: *Communications Security R&D*	311.460	25.284	21.113	19.171	-	19.171	23.327	19.723	20.282	20.814	Continuing	Continuing
Quantity of RDT&E Articles	0.000	-	-	-	-	-	-	-	-	-		

The FY 2015 OCO Request will be submitted at a later date.

A. Mission Description and Budget Item Justification

The Information Systems Security Program (ISSP) Research Development Test & Evaluation (RDT&E) efforts provide Information Assurance (IA) and Defensive Cyberspace Operations (DCO) solutions to protect the forward deployed, bandwidth-limited, highly mobile Naval information subscriber and the associated command, control, and communications required to achieve the integrated military advantage from Net-Centric operations. ISSP addresses engineering design, development, modeling, simulation, test, and evaluation for the unique IA challenges associated with dispersed, bandwidth limited, and forward-tactical connected US Navy communications systems.

This project includes a rapidly evolving design and application engineering effort to modernize cryptographic equipment and ancillaries with state-of-the-art replacements to counter evolving and increasingly sophisticated threats, in accordance with the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510 requirements. Communication Security (COMSEC) and Transmission Security (TRANSEC) evolution are from stand-alone dedicated devices to embedded modules incorporating National Security Agency (NSA) approved cryptographic engines, loaded with the certified algorithms and key, and interconnected via industry-defined interfaces. This includes the Department of Defense (DoD) Global Information Grid (GIG) capability requirements document for the development of Content Based Encryption (CBE) and in the implementation of the Committee for National Security Systems (CNSS) Policy 15 on the "Use of Public Standards for the Sharing of Information among National Security Systems."

In addition to protecting national security information, ISSP RDT&E efforts provide enterprise-wide assurance for statutorily protected information, such as the 107 protected data types described in the federal task force on Controlled Unclassified Information (CUI) and in DoD Manual 5200.01 Volume 4. ISSP RDT&E efforts must also provide solutions to the most advanced state-sponsored and criminal-intent Advanced Persistent Threats (APT), including those to Platform Information Technology (PIT), weapons systems, Industrial Control Systems (ICS), and Supervisory Control and Data Acquisition (SCADA).

ISSP RDT&E efforts provide dynamic risk-managed IA solutions to the Navy information infrastructure, not just security devices placed within a network. Extensive effort will be placed on rapidly providing solutions required for the new DoD Instruction (DoDI) 8500.01, (CNSS) Instruction No. 1253, and National Institute of Science and Technology (NIST) Special Publication (SP) 800-53 IA control set, focused primarily on espionage and sabotage capable, state-sponsored APTs. Additional efforts include the implementation of data object security labeling and provenance metadata, also required by DoDI 8500.01, which is a major enabler for cross-domain data sharing. Few technology areas change as fast as telecommunications and computers; resulting in the need for continuous evaluation, development, and testing of IA products and cyber defense strategies. ISSP efforts in support of this environment include developing or applying: (1) new secure voice and secure data prototypes and protocols; (2) technology for a new Suite B capable programmable COMSEC and TRANSEC devices and software; (3) security appliances and software for

Exhibit R-2A, RDT&E Project Justification: PB 2015 Navy		Date: March 2014
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*

switched and routed networks; (4) technology to interconnect networks of dissimilar classification and need-to-know, known respectively as Cross Domain Solutions (CDS) and virtually secure environments (VSE); (5) techniques for assuring code and data residing in and transiting the Navy's computing base and information store; (6) Public Key Infrastructure (PKI) and associated access control technologies such as smartcards and similar security tokens; (7) Key Management (KM) devices such as Simple Key Loaders (SKL), COMSEC Material Work Stations (CMWS), and Key Management Infrastructure (KMI) equipment (Client Management (MGC)/ Advanced Key Processor (AKP) MGC/AKPs, High Assurance Protocol Equipment, Delivery Only Client (DOC) and Next Generation devices; (8) technologies that provide assured and persistent Identity and Access Management (IdAM) for persons, virtual instances, and connected devices; (9) technologies for assuring cloud and mobile operating environments and devices; (10) defensive cyber security technologies required to support strategic and tactical cyber operations in an Anti-Access, Area-Denial (A2AD) hostile environment; and (11) Cyber Remediation capabilities that will accelerate the Navy's ability to prevent, constrain and mitigate cyber-attacks and critical vulnerabilities as well as provide greater resiliency, awareness, data analytics, redundancy and diversity into the Navy's Defense-in-Depth (DiD) strategy.

FY 15 Highlights for Information Systems Security Programs (ISSP):

Computer Network Defense (CND): Continue to develop, integrate, and test CND Builds, DiD and SA technologies for knowledge-empowered CND operations for shore sites and afloat platforms. Continue to develop new capabilities for the Navy's C2 architecture and provide technical guidance to ensure CND requirements are met by CANES. Continue to implement DOD and USCC IA/cyber security tools and mandates into ONE-Net, IT-21 and excepted networks. Continue evaluation of needs derived from the stakeholders and CCSG, as well as develop, update, and integrate the CND/IA suites with adaptive defense, security sensors, incident reporting, correlation, packet capture processing, and situational awareness capabilities to provide increased DiD, perform near real-time analysis of events, and counter APT. Provide Vulnerability Remediation Asset Manager (VRAM) tool to include Online Compliance Reporting System (OCRS) and Continuous Monitoring Risk Scoring (CMRS) capabilities. Begin impact analysis of DODI 8500.01 IA controls implementation in CND. Initiate integration and testing of Secure Socket Layer (SSL) intercept to achieve compliance with Defense Information Security Agency (DISA)firewall security guidance. Continue to further efforts to virtualize CND capabilities and consolidating IA Services in the ONE-Net environment. Begin development and implementation of an optimal technical and governance solution for interception of outbound encrypted traffic. Start analysis to replace and assume acquisition management of Navy Cyber Defense Operations Command's (NCDOC) tactical sensor infrastructure. Continue to support C10F NCSA efforts, deploying integrated tools at the C10F MOC to support C2 of the CS; NCSA will provide near real-time risk assessments, actionable intelligence, and immediate mitigation courses of action for knowledge-empowered CND operations throughout the Navy. Continue to develop JCTD delivered VSE to segment networks and adaptively manage operational risks. Provide Cyber Remediation initiatives within the Navy's CND/IA program in order to achieve improved network defense and security wholeness.

Navy Cryptography (Crypto): Continue development of TRANSEC replacement product for legacy devices. Complete iApp development efforts and initiate iApp crypto integration into specific devices. Complete Link-22 MLLC full development and provide support for transition to production efforts. Continue providing security engineering support for modernization of space crypto systems, embeddable crypto modernization strategies, and Next Generation Crypto initiatives. Continue providing support for NSA certification authority, acquisition authority, and data testing for all CM efforts. Continue to coordinate internally with other programs to address future crypto modernization efforts to include DMR, CDLS/TCDL. Continue to investigate impacts of upcoming NSA security enhancements for crypto mod products to include Enhanced FireFly (EFF), hardware and software. Continue to research and study the Secure Telephone Equipment (STE) follow-on. Continue to provide VACM

Exhibit R-2A, RDT&E Project Justification: PB 2015 Navy		Date: March 2014
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*

technical engineering support on behalf of DoN. Achieve VACM's Full Rate Production (FRP) decision and complete VACM Initial Operational Test & Evaluation (IOT&E).

Key Management (KM): Perform capability, verification testing that includes DT and OT in support of KMI CI-2 Spiral 2/Spin 2 software Full Rate Fielding Decision (FRFD). Achieve IOC on KMI CI-2 Spiral 2/Spin 1. Continue transition strategy, Alteration Installation Team (AIT) transition packages and define requirements for incorporation of other KMI roles into Navy architecture. Continue defining capability requirements for KMI CI-3. Continue supporting KMI transition working group meetings, developing white papers and supporting documentation for KMI CI-3. Conduct Next Generation Fill Device verification testing of Navy COMSEC requirements. Continue migrating CMWS/DMD and other Next Generation Fill Devices, the follow on to Simple Key Loader (SKL) into the KMI environment. Continue development, engineering and testing to the iApp which will enhance KMI secure communications and the Navy's implementation of the KMI DOC configuration, on the afloat and subsurface networks with the NSA KMI Spiral 2 software baseline. Continue engineering support to KMI PMO and vendors to develop capabilities required for the Navy, Army, and Air Force. Achieve Tactical Key Loader (TKL) Full Operational Capability (FOC).

Public Key Infrastructure (PKI): Continue research, develop, and test Identity and Access Management (IdAM) technologies to support afloat and OCONUS networks. Continue development and testing of tools to support Non-Person Entity (NPE) certificates in tactical/austere environments. Begin research and evaluate PKI authentication capabilities to support mobile devices for afloat and OCONUS networks. Continue to research and develop the next version of Navy Certificate Validation Infrastructure (NCVI) to support Online Certificate Status Protocol (OCSP) on afloat and OCONUS networks. Begin providing PKI support in the software development efforts for afloat networks, to include Common Access Card (CAC), Cryptographic Log-On (CLO), SIPRNet Token, and NPE. Begin test and evaluation support for technologies coming from the DoD Program Management Office (PMO) for future integration into Navy networks. Continue to ensure Navy compliance with new PKI related cryptographic algorithms and certificate changes on the CAC, Alternate Logon Token (ALT), and SIPRNet hardware token. PKI Inc 2 will reach Full Operational Capability (FOC).

Information Assurance (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 Command, Control, Communications, Computers and Intelligence (C4I) systems. This includes the expanded requirements to provide complete IdAM.

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2013	FY 2014	FY 2015
Title: Computer Network Defense (CND)	9.700	7.533	8.398
Articles:	-	-	-
FY 2013 Accomplishments: Developed, integrated and tested Computer Network Defense (CND) Build 1 and initiated future builds. Ensured security of Navy networks met Department of Defense (DoD) mandates and initiatives for securing the Global Information Grid (GIG). Developed, integrated, and tested Defense-in-Depth (DiD) and Situational Awareness (SA) technologies for knowledge-empowered CND operations for afloat and shore installations. Supported the development and deployment of new capabilities into the Navy's architecture, as well as provided technical guidance to ensure CND requirements were met by Consolidated Afloat Networks and Enterprise Services (CANES). Supported DoD defined tools and capabilities including host based security tools, automation			

Exhibit R-2A, RDT&E Project Justification: PB 2015 Navy		Date: March 2014
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2013	FY 2014	FY 2015
of reporting, monitoring, analysis and response. Integrated CND capabilities to perform near real-time analysis of events and updated the CND Information Assurance (IA) suites with adaptive defense, incident reporting, correlation, and SA capabilities. Promoted Course of Action (COA) development analysis and execution to improve interoperability with the Global Network Operations (NetOps) Information Sharing Environment. Developed enhancements and evaluated needs derived from the CND Capabilities Steering Group (CSSG) to advance analysis and response to network threats. Leveraged the Ozone Widget framework and the US Cyber Command (USCC) Cyber Pilot architecture to start to deliver visualization and analysis tools in support of Fleet Cyber Command (FCC) / Commander Tenth Fleet (C10F) Cyber SA efforts at the C10F Maritime Operations Center (MOC). Achieved Full Rate Production (FRP). ***FY 2014 Plans:*** Continue to develop, integrate, and test CND Builds, DiD and SA technologies for knowledge-empowered CND operations for shore sites and afloat platforms. Continue to develop new capabilities for the Navy's Command and Control (C2) architecture and provide technical guidance to ensure CND requirements are met by CANES. Continue to implement DoD and USCC IA/ cyber security mandates into Outside the Continental United States (OCONUS) Navy Enterprise Network (ONE-Net), Information Technology for the 21st Century (IT-21), and excepted networks as required. Continue the evaluation of needs derived from the CCSG and develop, update, and integrate the CND/IA suites with adaptive defense, security sensors, incident reporting, correlation, packet capture processing and situational awareness capabilities to provide increased DiD, to perform near real-time analysis of events, and to counter Advanced Persistent Threats (APT). Further efforts to virtualize CND capabilities and consolidate IA services in the ONE-Net environment. Continue to support C10F Navy Cyber Situational Awareness (NCSA) efforts, deploying integrated tools at the C10F MOC to support C2 of the Communications Systems (CS); NCSA will provide near real-time risk assessments, actionable intelligence, and immediate mitigation courses of action for knowledge-empowered CND operations throughout the Navy. Develop and further the Joint Capability Technology Demonstration (JCTD) Virtual Secure Enclaves (VSE) to segment networks and adaptively manage operational risks. ***FY 2015 Plans:*** Continue to develop, integrate, and test CND Builds, DiD and SA technologies for knowledge-empowered CND operations for shore sites and afloat platforms. Continue to develop new capabilities for the Navy's C2 architecture and provide technical guidance to ensure CND requirements are met by CANES. Continue to implement DOD and USCC IA/cyber security tools and mandates into ONE-Net, IT-21 and excepted networks. Continue evaluation of needs derived from the stakeholders and CCSG, as well as develop, update, and integrate the CND/IA suites with adaptive defense, security sensors, incident reporting, correlation, packet capture processing, and situational awareness capabilities to provide increased DiD, perform near real-time analysis of events, and counter APT. Provide Vulnerability Remediation Asset Manager (VRAM) tool to include Online Compliance Reporting System (OCRS) and Continuous Monitoring Risk Scoring (CMRS) capabilities. Begin impact analysis of DODI 8500.01 IA controls implementation in CND. Initiate integration and testing of Secure Socket Layer (SSL) intercept to achieve compliance with Defense Information Security Agency (DISA)firewall security guidance. Continue to further efforts to			

Exhibit R-2A, RDT&E Project Justification: PB 2015 Navy		Date: March 2014
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2013	FY 2014	FY 2015
virtualize CND capabilities and consolidating IA Services in the ONE-Net environment. Begin development and implementation of an optimal technical and governance solution for interception of outbound encrypted traffic. Start analysis to replace and assume acquisition management of Navy Cyber Defense Operations Command's (NCDOC) tactical sensor infrastructure. Continue to support C10F NCSA efforts, deploying integrated tools at the C10F MOC to support C2 of the CS; NCSA will provide near real-time risk assessments, actionable intelligence, and immediate mitigation courses of action for knowledge-empowered CND operations throughout the Navy. Continue to develop JCTD delivered VSE to segment networks and adaptively manage operational risks. Provide Cyber Remediation initiatives within the Navy's CND/IA program in order to achieve improved network defense and security wholeness.			
Title: Navy Cryptography (Crypto)	9.964	7.850	6.381
Articles:	-	-	-
FY 2013 Accomplishments: Continued research, evaluation, and prioritization of cryptographic products for modernization. Continued coordination with the National Security Agency (NSA) and support to the Cryptographic Joint Algorithm Integrated Product Team (IPT). Continued identifying strategies to reduce the overall crypto inventory within the Department of the Navy (DoN) to realize long term cost savings. Continued providing systems engineering services in support of execution of the Link-22 Modernized Link Level Communications Security (MLLC) full development efforts including: Preliminary Design Review (PDR) 1&2, Test Readiness Review (TRR) 1&2, and Critical Design Review (CDR). Conducted research into making modern crypto devices Key Management Infrastructure (KMI) aware, focusing on the Intermediary Application (iApp) development. Continued Naval Research Laboratory (NRL) research into Secure Voice (SV). Provided technical engineering support on behalf of DoN in support of Air Force VINSON/Advanced Narrowband Digital Voice Terminal Crypto Modernization (VACM) and perform Navy system tests on Production Representative Engineering Development Models (PREDMs). Continued providing security engineering support for Office of Secretary of Defense (OSD) Chief Information Officer (CIO) Nuclear Command and Control (NC2)/ Nuclear Command, Control, and Communications (NC3) Crypto Modernization (CM) efforts on behalf of the Navy. Transitioned Transmission Security (TRANSEC) Request For Information (RFI) items for CM solutions and coordinated with the NSA and other services; continued TRANSEC study and analysis for replacement products for legacy devices. Continued investigation into crypto replacement strategies for ground terminals of space systems, as well as replacements for legacy/embeddable crypto. Continued providing support for NSA certification authority, acquisition support and data testing for all cryptographic modernization efforts.			
FY 2014 Plans: Complete TRANSEC study and analysis for a replacement product for legacy devices and initiate TRANSEC development efforts. Continue iApp development efforts focusing on incorporating functionality into specific Navy crypto devices, fill devices, and support products. Complete NRL's research into SV. Provide VACM technical engineering support on behalf of DoN, achieve Milestone C (MS C), perform Navy system tests on PREDMs, and initiate Initial Operational Test & Evaluation (IOT&E). Continue			

Exhibit R-2A, RDT&E Project Justification: PB 2015 Navy		Date: March 2014
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2013	FY 2014	FY 2015
providing security engineering support modernization of space crypto systems, embeddable crypto modernization strategies, and Next Generation Crypto initiatives. Coordinate internally with other programs to address future crypto modernization efforts to include Digital Modular Radio (DMR), Communication Data Link System (CDLS)/Tactical Common Data Link (TCDL). Investigate impacts of upcoming NSA security enhancements for crypto modernization products to include Enhanced Firefly, hardware and software. Research and study the Secure Telephone Equipment (STE) follow-on. Complete Link-22 MLLC Test Readiness Review (TRR)1&2, Preliminary Readiness Review (PRR), and deliver full development article. Continue providing support for NSA certification authority, acquisition authority, and data testing for all CM efforts. Achieve Full Operational Capability(FOC)of KG-45A devices. ***FY 2015 Plans:*** Continue development of TRANSEC replacement product for legacy devices. Complete iApp development efforts and initiate iApp crypto integration into specific devices. Complete Link-22 MLLC full development and provide support for transition to production efforts. Continue providing security engineering support for modernization of space crypto systems, embeddable crypto modernization strategies, and Next Generation Crypto initiatives. Continue providing support for NSA certification authority, acquisition authority, and data testing for all CM efforts. Continue to coordinate internally with other programs to address future crypto modernization efforts to include DMR, CDLS/TCDL. Continue to investigate impacts of upcoming NSA security enhancements for crypto mod products to include Enhanced FireFly (EFF), hardware and software. Continue to research and study the Secure Telephone Equipment (STE) follow-on. Continue to provide VACM technical engineering support on behalf of DoN. Achieve VACM's Full Rate Production (FRP) decision and complete VACM Initial Operational Test & Evaluation (IOT&E).			
Title: Key Management (KM)	2.619	2.641	2.022
Articles:	-	-	-
FY 2013 Accomplishments: Began capability, engineering, development, and verification testing support to Key Management Infrastructure (KMI) Capability Increment (CI)-2 Spiral 2 Spin 1. Continued transition strategy and defined requirements for incorporation of other KMI roles into Navy architecture. Continued supporting KMI transition working group meetings, developed white papers and supporting documentation for KMI. Continued requirements definition support to the development of the next generation fill device. Continued Migrating Communications Security (COMSEC) Material Work Station (CMWS)/Data Management Device (DMD) and other Next Generation Fill Devices to the KMI environment. Began shipboard bandwidth study in support of KMI Manager Client (MGC) architecture in the afloat operational environment. Began to define capability requirements for KMI CI-3. Provided 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. Provided engineering and analysis to the Intermediary Application (iApp) which will enhance KMI secure communications. Defined KMI Delivery Only Client (DOC) solution requirements. Completed Full Operation Test & Evaluation (FOT&E) KMI Spiral 1 test events and Spiral 1 Full Rate Fielding/			

Exhibit R-2A, RDT&E Project Justification: PB 2015 Navy		Date: March 2014
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2013	FY 2014	FY 2015
Production Decision. Tactical Key Loader (TKL) achieved Full Rate Production Decision (FRPD) and Initial Operational Capability (IOC). Electronic Key Management System (EKMS) Phase V achieved Full Operational Capability (FOC). ***FY 2014 Plans:*** Continue capability, engineering, development,verification testing, and perform Development Testing (DT), Operational Testing (OT) in support of KMI CI-2 Spiral 2/Spin 1 software Full Rate Fielding Decision (FRFD). Continue transition strategy and define requirements for incorporation of other KMI roles into Navy architecture. Continue defining capability requirements for KMI CI-3. Continue supporting KMI transition working group meetings, developing white papers and supporting documentation for KMI CI-3. Continue requirements definition support to the development of the Next Generation Fill Device. Continue migrating CMWS/DMD and other Next Generation Fill Devices to the KMI environment. Continue development engineering and testing to the iApp which will enhance KMI secure communications. Conduct shipboard bandwidth assessment with Spiral 2 Software in support of KMI MGC. Complete capability Subject Matter Expert (SME) support to National Security Agency (NSA) for Spiral 2/Spin 1. Continue engineering support to KMI Program Management Office (PMO) and vendors to develop capabilities required for the Navy, Army, and Air Force. ***FY 2015 Plans:*** Perform capability, verification testing that includes DT and OT in support of KMI CI-2 Spiral 2/Spin 2 software Full Rate Fielding Decision (FRFD). Achieve IOC on KMI CI-2 Spiral 2/Spin 1. Continue transition strategy, Alteration Installation Team (AIT) transition packages and define requirements for incorporation of other KMI roles into Navy architecture. Continue defining capability requirements for KMI CI-3. Continue supporting KMI transition working group meetings, developing white papers and supporting documentation for KMI CI-3. Conduct Next Generation Fill Device verification testing of Navy COMSEC requirements. Continue migrating CMWS/DMD and other Next Generation Fill Devices, the follow on to Simple Key Loader (SKL) into the KMI environment. Continue development, engineering and testing to the iApp which will enhance KMI secure communications and the Navy's implementation of the KMI DOC configuration, on the afloat and subsurface networks with the NSA KMI Spiral 2 software baseline. Continue engineering support to KMI PMO and vendors to develop capabilities required for the Navy, Army, and Air Force. Achieve Tactical Key Loader (TKL) Full Operational Capability (FOC).			
Title: Public Key Infrastructure (PKI)	0.398	0.409	0.315
Articles:	-	-	-
FY 2013 Accomplishments: Researched, analyzed and evaluated Public Key Infrastructure (PKI) enabled (PKE) products (Microsoft and non-Microsoft) such as Virtual Private Networks (VPNs), routers, switches, and servers for their suitability to support Navy requirements for Non-Person Entity (NPE) certificates and to support identity management and protection requirements. Provided systems engineering support for Secret Internet Protocol Router Network (SIPRNet) PKI enablement for Navy Programs of Record (POR). Researched and tested PKI solutions for non-Microsoft systems . Continue to support the manual and automatic enrollment and issuance			

Exhibit R-2A, RDT&E Project Justification: PB 2015 Navy		Date: March 2014
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2013	FY 2014	FY 2015
of PKI NPE certificates to Navy servers and devices. Continued to evaluate Defense Information Systems Agency's (DISA) auto-enrollment and registration services for DoD PKI enabled devices. Continued to research and evaluate new technologies and develop solutions to enable the Navy's PKI to process new cryptographic algorithms and new secure hash algorithms, to include Elliptic Curve Cryptography (ECC) and Secure Hash Algorithms (SHA)-256. Tested and evaluated DISA's Online Certificate Status Protocol (OCSP) enhancements for certificate authentication in the Navy afloat and ashore environment. Ensured interoperability of PKI with Computer Network Defense (CND) systems architecture. ***FY 2014 Plans:*** Complete development of PKI solutions, including the SIPRNet Shipboard Validation Authority (SVA) and Cryptographic Log-on (CLO) capability to non-Microsoft systems and Microsoft non-Domain services. Begin testing and evaluation of the NIPRNet Enterprise Alternate Token System (NEATS) for shore and afloat role-based tokens. Complete research and testing of DISA OCSP enhancements for certificate authentication in the Navy afloat and ashore environments. Continue to ensure Navy compliance and compatibility with new PKI related cryptographic algorithms, to include ECC and SHA-256. Ensure compliance and compatibility with certificate changes on the Common Access Card (CAC), Alternate Logon Token (ALT), and SIPRNet hardware token. Continue to ensure compatibility and interoperability of PKI with CND systems architecture. Continue to research and develop tools to support certificates for Non-Person Entity (NPE) devices and tactical/austere environments. Begin researching Identity and Access Management (IdAM) technologies to increase information security. Start investigating virtualization of Navy Certificate Validation Infrastructure (NCVI) servers. Achieve PKI Increment 2 Spiral 3 Initial Operational Capability (IOC). ***FY 2015 Plans:*** Continue to ensure Navy compliance and compatibility with new PKI related cryptographic algorithms, to include ECC and SHA-256. Continue to ensure Navy compliance and compatibility with certificate changes on the CAC, ALT, and SIPRNet hardware token. Complete testing and evaluation of NEATS to support role-based token issuance for afloat and Outside of the Continental United States (OCONUS) networks. Continue to ensure compatibility and interoperability of PKI with CND systems architecture. Complete NPE research and development efforts and begin testing tools to support NPE certificates in tactical/ austere environments. Continue to research and begin development and testing of IdAM technologies to increase information security support afloat and OCONUS networks. Begin research and evaluation of PKI authentication capabilities to support mobile devices for afloat and OCONUS networks. Continue to investigate virtualization of NCVI servers and begin research and development of the next version of NCVI to support OCSP on afloat and OCONUS networks. Begin providing PKI support in the software development efforts for afloat networks, to include CAC, CLO, SIPRNet Token, and NPE. Begin test and evaluation support for technologies coming from the DoD Program Management Office (PMO) for future integration into Navy networks. Achieve PKI Increment 2 Spiral 3 Full Operational Capability (FOC).			
Title: Information Assurance (IA) Services	2.603	2.680	2.055

Exhibit R-2A, RDT&E Project Justification: PB 2015 Navy		Date: March 2014
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2013	FY 2014	FY 2015
Articles:	-	-	-
FY 2013 Accomplishments: Continued to provide security systems engineering support for the development of DoD and 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 SYSCOM via the IA Trusted Architecture (TA) to ensure the security design and integration of Computer Adaptive Network Defense-in-Depth (CANDiD) products and services is consistent across the Navy for major initiatives such as the future afloat, ashore, and OCONUS networks. 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 2014 Plans: Continue to provide security systems engineering support for the development of DoD and DoN IA architectures and the transition of new technologies to address Navy IA challenges. Provide updates to 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 cybersecurity 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 2015 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. Continue to provide updates to reflect emerging priorities and address Navy specific threats. Continue to coordinate IA activities across the virtual SYSCOM via the IA TA to ensure the security design and integration of cybersecurity products and services is consistent across the Navy for major initiatives such as the future afloat, ashore, and OCONUS networks. Continue to provide IA risk analysis and recommended risk mitigation strategies for Navy critical networks and C4I systems. Continue to 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.			
Accomplishments/Planned Programs Subtotals	25.284	21.113	19.171

Exhibit R-2A, RDT&E Project Justification: PB 2015 Navy		Date: March 2014
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost
• OPN/3415: *Info Sys Security Program (ISSP)*	123.918	133.530	110.766	-	110.766	144.125	81.580	86.039	89.929	Continuing	Continuing

Remarks

D. Acquisition Strategy

Computer Network Defense (CND): The CND Acquisition Category (ACAT) IVT program is a layered protection strategy, using Commercial Off-The-Shelf (COTS) and Government Off-The-Shelf (GOTS) hardware and software products that collectively provide an effective network security infrastructure. The rapid advance of cyber technology requires an efficient process for updating CND tools deployed to afloat and shore platforms. Recognizing the need for future CND capability improvements, CND implements an evolutionary acquisition strategy that delivers CND capabilities in multiple builds and functionality releases that address validated requirements.

Navy Cryptography (Crypto): Modernized crypto devices will replace legacy crypto in accordance with the Chairman of the Joint Chiefs of Staff (CJCS) mandate (CJCS Instruction 6510) as well as the National Security Agency (NSA) planned decertification, which improves the security of the Navy's data in transit. Link-22 Modernized Link Level Communications Security (MLLC has a two-step development phase. Preliminary development was completed with prototype and is now in full development to obtain initial product baseline. Strategies followed by other lead agencies include VINSON/Advanced Narrowband Digital Voice Terminal Crypto Modernization (VACM) and KG-3X which has the United States Air Force (USAF) as contract lead.

Key Management Infrastructure (KMI): KMI, an NSA led Joint ACAT program, is the next generation Electronic Key Management System (EKMS) that provides the infrastructure for management, ordering and distribution of key material as well as directly supporting the key requirements of all Crypto modernization efforts. KMI will follow an increment/spiral development strategy. KMI will continue to develop alternative architecture implementations for communities within the Navy.

Public Key Infrastructure (PKI): DoD PKI is a Joint ACAT program under the guidance of NSA Acquisition Executive (AE) as Program Manager (PM) and the DoD Chief Information Officer (CIO) as the Milestone Decision Authority (MDA). The Navy PKI project is the Navy element of the DoD PKI ACAT program. The Navy PKI program supports the DoD-wide implementation of PKI products and services across Navy afloat, non-Navy Marine Corps Intranet (NMCI), and OCONUS networks.

E. Performance Metrics

Computer Network Defense (CND):
* Provide the ability to protect from, react to, and restore operations after an intrusion or other catastrophic event through validated contingency plans for 100% of CND systems.
* 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.

Exhibit R-2A, RDT&E Project Justification: PB 2015 Navy		Date: March 2014
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*

* Defend against the unauthorized use of a host or application, particularly operating systems, by development and/or integration of host-based intrusion prevention system design solutions for 100% of authorized Navy enclaves.
* Continue to develop and provide Cyber Situational Awareness (CSA) to the Commander United States Tenth Fleet (C10F) Maritime Operations Center (MOC).

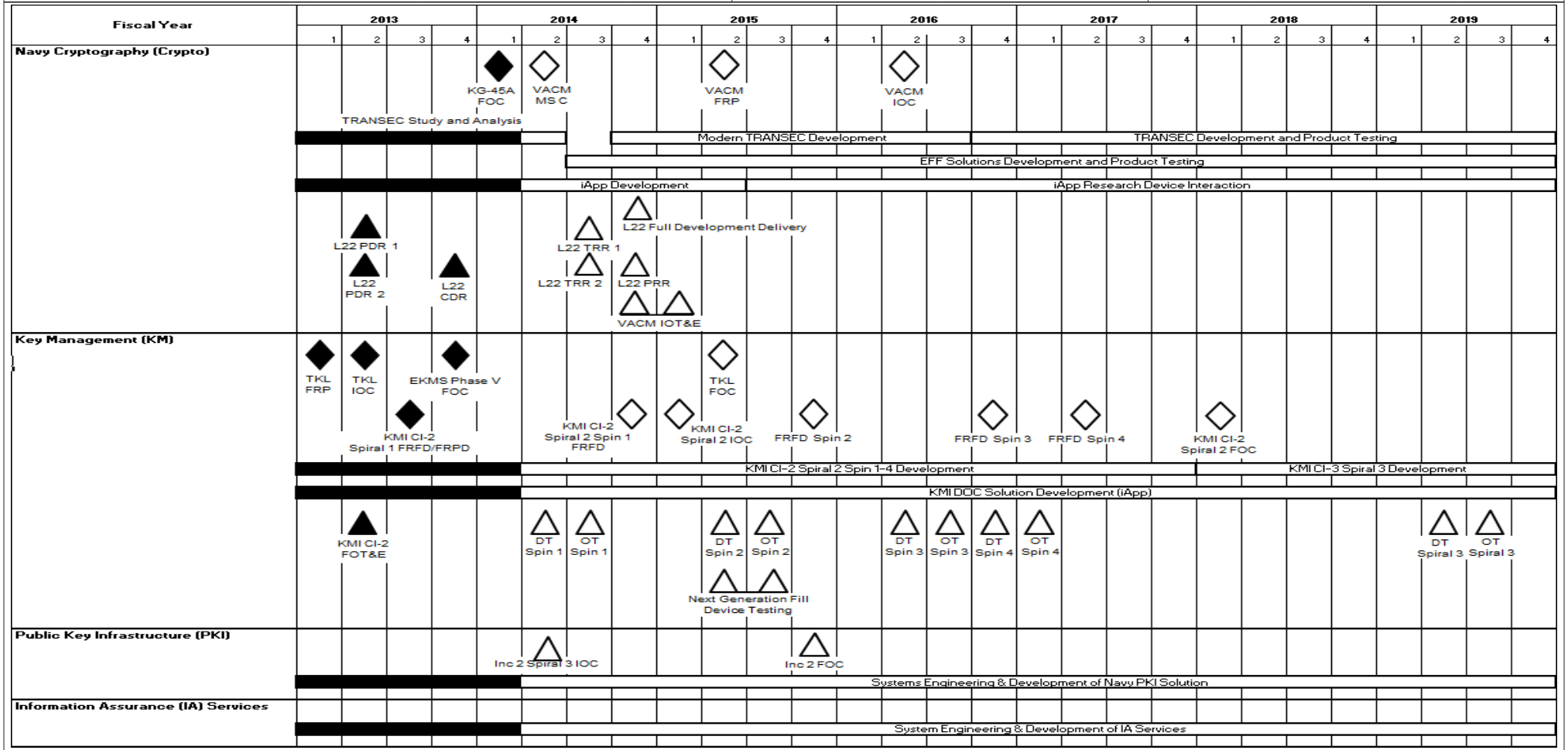
Navy Cryptography (Crypto):
* Meet 100% of Chairman of the Joint Chiefs of Staff Instruction (CJCSI 6510) Cryptographic Modernization (CM) requirements within the current FYDP by conducting a gap analysis and building a CM roadmap and implementation plan to allow the Navy NETWAR FORCEnet Enterprise to establish operational priorities based on risk assessments. The gap analysis is an effort to analyze current integrated legacy cryptographic devices within the Department of the Navy (DoN) inventory with known algorithm vulnerability dates, assess lifecycle sustainment issues, and identify transition device schedules, where they exist.
* Meet 100% of Top Secret (TS) and SECRET CJCSI 6510 by fielding modern cryptographic devices or request "key extension" via the Joint Staff Military Communications-Electronics Board (MCEB).
* Increase the functionality of cryptographic devices by replacing 2 legacy cryptographic devices with 1 modern device, where possible, and identify and implement modern small form factor, multi-channel cryptos (e.g., KIV-7M replacing KIV-7HS, KIV-7HSB, KG-84, KWR-46, KL-51, etc.).

Key Management (KM):
* Meet 100% of submarine and US Coast Guard key management requirements in order to replace existing Electronic Key Management System (EKMS) Tier 2 systems with a Key Management Infrastructure (KMI)/Delivery Only Client (DOC) solution Intermediary Application (iApp).
* Complete engineering efforts and testing of iApp to be transitioned to submarines and US Coast Guard Cutters to begin FY16.
* Incorporate 100% of the Communication Security (COMSEC) Manager Workstation (CMWS) requirements into the iApp baseline.
* Provide and refine Navy unique requirements into the National Security Agency (NSA) KMI Capability Increment (CI)-3 Capability Development Document (CDD).

Public Key Infrastructure (PKI):
* Provide integration support to ensure Navy networks and Programs of Record (POR) comply with DoD PKI requirements on NIPRNet and SIPRNet, per DoDI 8520.02.
* Ensure 100% interoperability with DoD and Federal partners by researching and evaluating enhanced cryptographic algorithms and DoD certificate changes.

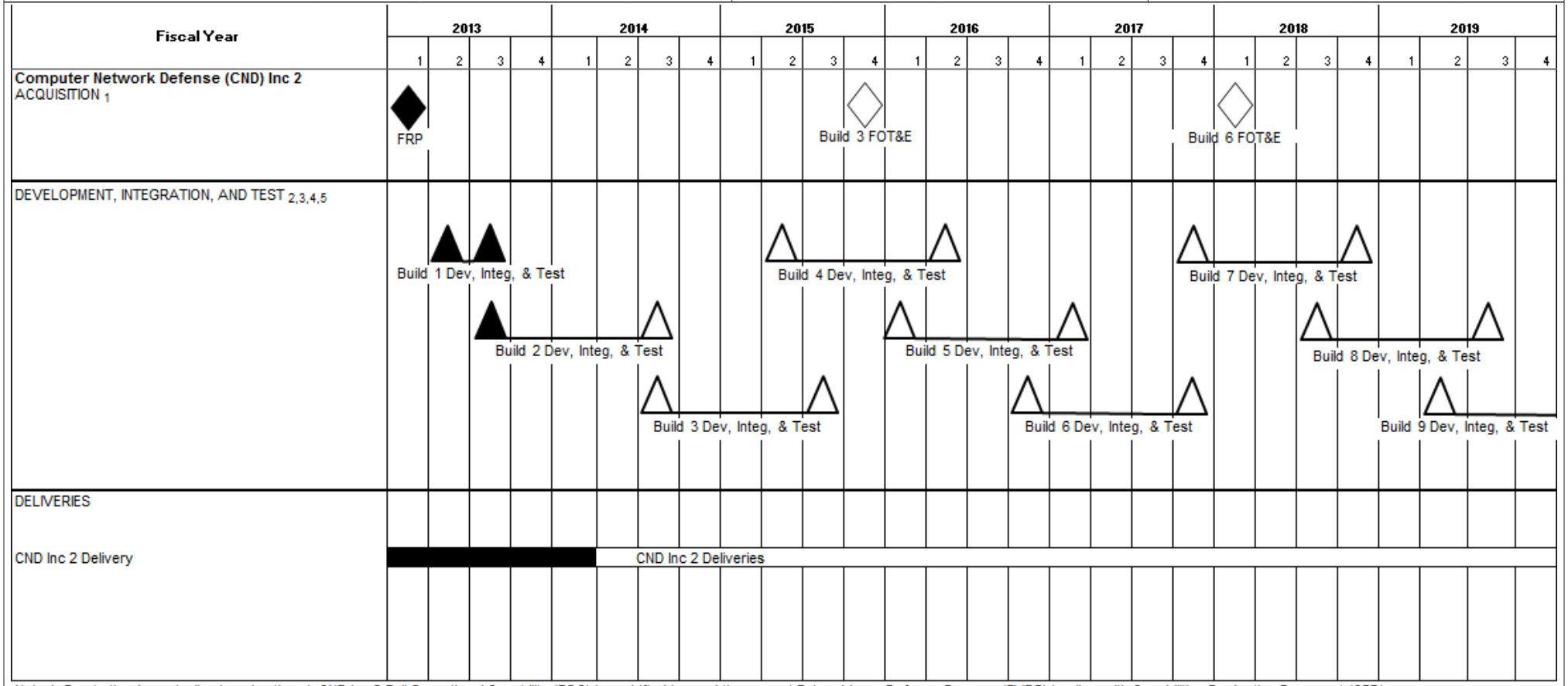
Information Assurance (IA) Services:
* Ensure 100% interoperability and application of commercial standards compliance for ISSP products by researching and conducting selective evaluations, integrating and testing commercial-off-the-shelf/Non-Developmental Item IA security products. Evaluation may include defensible network boundary capabilities such as firewalls, secure routers and
switches, guards, Virtual Private Networks (VPN), and network Intrusion Prevention Systems (IPS).
* Provide 100% of the services delineated in OPNAVINST 5239.1C by serving as the Navy's Information Assurance (IA) technical lead by developing IA risk analysis and recommended risk mitigation strategies for critical Navy networks and C4I systems.
* Coordinate IA activities across the Navy Enterprise via the IA Trusted Architecture (TA) to measure effectiveness of Navy networks. Ensure the security design and integration of Computer Adaptive Network Defense-in-Depth (CANDiD) products and services and that they are 100% interoperable and operationally acceptable across the Navy for major initiatives such as the future afloat, ashore, and Outside the Continental United States (OCONUS) networks.

Exhibit R-4, RDT&E Schedule Profile: PB 2015 Navy		Date: March 2014
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*



Reference "R2 - Change Summary Explanation" for notes

Exhibit R-4, RDT&E Schedule Profile: PB 2015 Navy		**Date:** March 2014
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*



Note 1: Due to the dynamically changing threat, CND Inc 2 Full Operational Capability (FOC) has shifted beyond the current Future Years Defense Program (FYDP) to align with Capabilities Production Document (CPD)
Note 2: Added CND Build Milestones
Note 3: Build 3 completion shifted from 2Q15 to 3Q15.
Note 4: Build 4 start shifted from 1Q15 to 2Q15. Build 4 completion shifted from 1Q16 to 2Q16.
Note 5: Build 5 start shifted from 4Q15 to 1Q16. Build 5 completion shifted from 4Q16 to 1Q17.

Exhibit R-2A, RDT&E Project Justification: PB 2015 Navy											Date: March 2014	
Appropriation/Budget Activity 1319 / 7					R-1 Program Element (Number/Name) PE 0303140N / *Information Sys Security Program*				Project (Number/Name) 3230 / *Information Assurance*			
COST ($ in Millions)	**Prior Years**	**FY 2013**	**FY 2014**	**FY 2015 Base**	**FY 2015 OCO #**	**FY 2015 Total**	**FY 2016**	**FY 2017**	**FY 2018**	**FY 2019**	**Cost To Complete**	**Total Cost**
3230: *Information Assurance*	5.664	2.439	2.401	3.882	-	3.882	2.096	2.125	2.111	2.186	Continuing	Continuing
Quantity of RDT&E Articles	0.000	-	-	-	-	-	-	-	-	-		

The FY 2015 OCO Request will be submitted at a later date.

A. Mission Description and Budget Item Justification

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

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

This project includes funds for advanced technology development, test and evaluation of naval information systems security based on leading edge technologies that will improve information assurance (e.g., situational awareness and information infrastructure protection) across all command echelons to tactical units afloat and war fighters ashore. This effort will provide the research to develop a secure seamless interoperable, common operational environment of networked information systems in the battle space and for monitoring and protecting the information infrastructure from malicious activities. This effort will provide naval forces a secure capability and basis in its achievement of protection from unauthorized access and misuse, and optimized IA resource allocations in the information battle space. This program will also develop core technology to: (1) improve network infrastructure resistance and resiliency to attacks; (2) enable the rapid development and certification of security-aware applications and information technologies in accordance with the Common Criteria for IA and IA-enabled information technology products by the National Security Telecommunications and Information Systems Security Instructions; and (3) measure the effectiveness and efficiency of IA defensive capabilities under naval environments.

The program will develop common architectural frameworks that facilitate integration of network security capabilities, enable effective seamless interoperation, and contribute to a common consistent picture of the networked environment with respect to information assurance and security. This effort will address the need for a common operational picture for IA, as well as assessment of security technology critical to the success of the mission. This effort will also initiate requirements definition for situational awareness capabilities to support computer network defense in a highly-distributed, homogeneous, and heterogeneous networks including mobile and 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

Exhibit R-2A, RDT&E Project Justification: PB 2015 Navy		Date: March 2014
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 3230 / *Information Assurance*

configurations of network security components to implement changes in real time or near real time. Program will also initiate requirements definition for secure coalition data exchange and interoperation among security levels and classifications, and ensure approaches address various security level technologies as well as emerging architectural methods of providing interoperability across different security levels. Examine multi-level aware applications and technologies including databases, web browsers, routers/switches, etc. Efforts will also initiate infrastructure protection efforts as the Navy develops network centric architectures and warfare concepts, ensuring an evolutionary development of security architectures and products for IA that addresses Navy infrastructure requirements. IA will ensure the architectures evolve to provide proper protection as technology, DoD missions, and threats continuously evolve. IA includes defensive protections as well as intrusion monitoring (sensors), warning mechanisms, and response capabilities in the architecture. Ensure the unique security and performance requirements of tactical systems, including those operating various security levels are addressed. Also, the program will initiate the efforts to conceptualize new network centric warfare technology to protect our assets, such as secure network gateways, routers, components and tools that improve the survivability of Navy networks. Last, IA will provide systems security engineering, certification and accreditation support for high-confidence naval information systems and ensure certification and accreditation approaches are consistent with Navy and DoD requirements.

FY15 : Continue development of new network security demands addressing nation-state level sponsored activity. Incorporate security services to thwart Denial of Network Service (DNS) attacks, distributed denial of service, botnet and other sophisticated attacks.

Increase in funding supports the Weaselboard Program which is addressing an urgent Speed to Fleet initiative to assess the health and protection of shipboard systems and identify anomalous activity with Shipboard Supervisory Control and Data Acquisition (SCADA) information.

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2013	FY 2014	FY 2015
Title: Information Assurance (IA)	2.439	2.401	3.882
Articles:	-	-	-

FY 2013 Accomplishments:
Continued the development of new network security technology focused on addressing nation-state level sponsored activity. Successfully characterizing certain attacks/profiles to increase detection rates of the technology- focusing on embedded malicious code and exfiltration of data from host environments. Continued development of attribution technology, focusing on nation-state activities across network boundaries that obfuscate traffic using techniques such as anonymization. Continued the development of a new high assurance boundary controller to protect Navy and Marine Corps data and resources from attack incorporating security services to thwart Denial of Network Service (DNS) attacks, distributed denial of service attacks, and botnet attacks, as well as sophisticated attacks to control the core, operating environment and ensuring essential robust communications are available through the boundary controller to provide continuity of operations during nation state sponsored attacks. Incremental technology demonstrated in representative Navy networks. Continued the development of mobile security techniques that introduce time- and location-based security parameters for geo-location and asset protection and management addressing the specific issues of geo-location and mapping in Global Positioning System (GPS)-constrained environments. Continued the development of critical cryptographic technology to support Navy unique platforms and requirements, such as Unmanned Autonomous Systems (UASs) ensuring the technology addresses the limited size, weight and power issues, and multiple data

Exhibit R-2A, RDT&E Project Justification: PB 2015 Navy		Date: March 2014
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 3230 / *Information Assurance*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2013	FY 2014	FY 2015
classification processing requirements, as well as providing on-the-fly programmability of mission data and key material to support various missions. Several critical milestones (e.g., PDR) achieved. Continued systems security engineering, certification and accreditation support for high-confidence naval information systems and ensure certification and accreditation approaches are consistent with Navy and DoD requirements. Continued development of a security framework for a federated cross-domain service oriented architecture (SOA) ensuring the framework addresses all critical aspects of SOA including cross-domain service discovery, identity management, and service invocation, while minimizing inference attacks. Continued the development of a security framework for mobile communication devices that allows the use/integration of commercial technology in a secure manner with initial efforts focusing on identity management, secure data storage, processing and exchange.			
FY 2014 Plans: Continue the development of new network security technology focused on addressing nation state level sponsored activity. Continue the development of a security framework for a federated, cross-domain SOA ensuring the framework addresses all critical aspects of SOA including cross-domain service discovery, identity management, and service invocation, while minimizing inference attacks. Continue the development of a security framework for mobile communication devices that allows the use/integration of commercial technology in a secure manner, such as to support the integration of Droid and/or iPhone devices. Continue the efforts focused on identity management and secure data storage, processing and exchange. Continue the development of mobile security techniques that introduce time and location based security parameters for geo-location and asset protection and management while addressing the specific issues of geo-location and mapping in GPS-constrained environments. Continue the development of critical cryptographic technology to support Navy unique platforms and requirements such as UAS ensuring the technology addresses the limited size, weight and power issues, and multiple data classification processing requirements, while as providing on-the-fly programmability of mission data and key material to support various missions such as COMSEC, ELINT, SIGINT, etc. Continue systems security engineering, certification and accreditation support for high-confidence naval information systems and ensure certification and accreditation approaches are consistent with Navy and DoD requirements. Complete the characterization of attacks/profiles to increase detection rates of the technology, especially for identifying new/emerging malicious code. Complete the development of attribution technology, focusing on nation-state activities across network boundaries that obfuscate traffic using techniques such as anonymization. Complete the incorporation of security services to thwart DNS attacks, distributed denial of service attacks, and botnet attacks, as well as sophisticated attacks to control the core operating environment. Initiate the development of new sensing and instrumentation technology to support attack prediction and to measure the effectiveness of network security technology. Initiate the development of technology to provide prediction/early warning sensing of impending attacks based on network traffic and user behavior.			
FY 2015 Plans: Continue at a reduced level of effort the development of a security framework for mobile communication devices. Emphasize addressing the security issues associated with bring-your-own-device/bring-your-own-application (BYOD/BYOA), such as to support the integration of Droid and/or iPhone devices. Continue at a reduced level of effort the development of new network			

Exhibit R-2A, RDT&E Project Justification: PB 2015 Navy		Date: March 2014
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 3230 / *Information Assurance*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2013	FY 2014	FY 2015
security technology focused on addressing nation state level sponsored activity. Continue at a reduced level of effort the development of enabling technology building blocks for identity management and secure data storage, processing and exchange. Initiate and complete the Weaselboard Project to study and assess vulnerabilities with Shipboard Supervisory Control and Data Acquisition (SCADA) information which conducts an operational demonstration on a Naval platform.			
Accomplishments/Planned Programs Subtotals	2.439	2.401	3.882

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

E. Performance Metrics

Protection of Navy and joint information from hostile exploitation and attack.