Exhibit R-2, **RDT&E Budget Item Justification:** PB 2016 Navy	**Date:** February 2015
Appropriation/Budget Activity 1319: *Research, Development, Test & Evaluation, Navy* **/** BA 7: *Operational Systems Development*	**R-1 Program Element (Number/Name)** PE 0303140N **/** *Information Sys Security Program*

COST ($ in Millions)	Prior Years	FY 2014	FY 2015	FY 2016 Base	FY 2016 OCO	FY 2016 Total	FY 2017	FY 2018	FY 2019	FY 2020	Cost To Complete	Total Cost
Total Program Element	344.847	25.604	23.016	28.102	-	28.102	29.595	28.829	22.823	23.292	Continuing	Continuing
0734: *Communications Security R&D*	336.744	23.213	19.134	25.974	-	25.974	27.474	26.725	20.644	21.069	Continuing	Continuing
3230: *Information Assurance*	8.103	2.391	3.882	2.128	-	2.128	2.121	2.104	2.179	2.223	Continuing	Continuing

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 through the implementation of statutory and regulatory requirements. Cyberspace systems include wired and wireless telecommunications systems, Information Technology (IT) systems, and the content processed, stored, or transmitted therein. The ISSP includes the protection of the Navy's National Security Systems and Information (NSSI). The 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, the ISSP provides architectures, products, and services based on mission impacts, information criticality, threats, vulnerabilities, and required defensive countermeasure capabilities.

FY16 will focus on efforts that address the risk management of cyberspace, which includes the capabilities to protect, detect, restore, and respond. The ISSP provides the Navy with the following cybersecurity 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 to include Task Force Cyber Awakening (TFCA) initiatives, specifically Navy Cyber Situational Awareness (NCSA) and Operation Rolling Tide (ORT)/Cyber Remediation capabilities that will accelerate the Navy's ability to prevent, constrain, and mitigate cyber-attacks and critical vulnerabilities; (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; and (8) supporting assurance technologies, including the Public Key Infrastructure (PKI) and Key Management (KM).

Exhibit R-2, **RDT&E Budget Item Justification:** PB 2016 Navy	**Date:** February 2015
Appropriation/Budget Activity 1319: *Research, Development, Test & Evaluation, Navy* **/** BA 7: *Operational Systems Development*	**R-1 Program Element (Number/Name)** PE 0303140N **/** *Information Sys Security Program*

B. Program Change Summary ($ in Millions)	**FY 2014**	**FY 2015**	**FY 2016 Base**	**FY 2016 OCO**	**FY 2016 Total**
Previous President's Budget	23.514	23.053	25.423	-	25.423
Current President's Budget	25.604	23.016	28.102	-	28.102
Total Adjustments	2.090	-0.037	2.679	-	2.679
• Congressional General Reductions	-	-0.037			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	2.100	-			
• SBIR/STTR Transfer	-0.010	-			
• Rate/Misc Adjustments	-	-	2.679	-	2.679

Change Summary Explanation

The FY 2016 funding request was reduced by $3.0 million to account for the availability of prior year execution balances.

Technical:
Computer Network Defense (CND):
- Additional capabilities to include network vulnerability remediation, security compliance reporting and mapping of Navy networks in order to accelerate advanced Task Force Cyber Awakening (TFCA) initiatives, specifically Navy Cyber Situational Awareness (NCSA) and Operation Rolling Tide (ORT)/Cyber Remediation

Navy Cryptography (Crypto):
- Intermediary Application (iApp) requirement will be met by Key Management iApp development initiative

Key Management (KM):
- Operational Test (OT) events changed to Operational Assessment (OA), since Full Rate Production (FRP) follow on tests are informal test events and do not require formal evaluations.
- Capability Increment 2 (CI-2) Spiral 2 Spin 1 Full Rate Fielding Decision (FRFD) event changed to a Fielding Decision (FD) since CI-2 FRFD completed in FY13
- Next Generation Fill Device was removed. Requirement will be met by Simple Key Loader (SKL) follow-on efforts.

Information Assurance (IA) / Cybersecurity:
- Replaced the term "IA" with "Cybersecurity" per Department of Defense Instruction (DoDI) 8500.01 March 14, 2014 update

Schedule:
Computer Network Defense (CND):

Exhibit R-2, **RDT&E Budget Item Justification:** PB 2016 Navy	**Date:** February 2015
Appropriation/Budget Activity 1319: *Research, Development, Test & Evaluation, Navy* / BA 7: *Operational Systems Development*	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*

- All CND builds were accelerated to include TCFA/NCSA/ORT/Cyber Remediation capabilities
- All CND build's "Development, Integration & Test" phase completion time increased from 5 to 6 quarters in order to incorporate new cyber remediation capabilities

Navy Cryptography (Crypto):
- VINSON/Advanced Narrowband Digital Voice Terminal (ANDVT) Cryptographic Modernization (VACM) Milestone C (MS C) shifted from 2QFY14 to 3QFY14 to reflect actual date milestone was achieved by Air Force (AF). Initial Operational Test and Evaluation (IOT&E) start shifted from 4QFY14 to 1QFY15, Full Rate Production (FRP) decision shifted from 2QFY15 to 3QFY15, and Initial Operational Capability (IOC) shifted from 2QFY16 to 3QFY16, due to (1) QTR shift in MS C.
- Link 22 (L22) Technical Readiness Review (TRR) 2 shifted from 3QFY14 to 2QFY15, L22 Full Development Delivery shifted from 4QFY14 to 2QFY15, and L22 Production Readiness Review (PRR) shifted from 4QFY14 to 2QFY15, due to changes in vendor's schedule
- Additional Transmission Security (TRANSEC) study and analysis continued to 2QFY15 and initiation of Modern TRANSEC development shifted from 4QFY14 to 3QFY15, due to National Security Agency (NSA) directives

Key Management (KM):
- Tactical Key Loader (TKL) Full Operational Capability (FOC) accelerated from 2QFY15 to 3QFY14 due to actual date FOC achieved
- CI-2 Spiral 2/Spin 1 Development Test (DT) shifted from 2QFY14 to 3QFY14 and CI-2 Spiral 2/Spin 1 OA shifted from 3QFY14 to 4QFY14, due to actual date Full Rate Field Decision (FRFD) achieved
- CI-2 Spiral 2/Spin 1 Fielding Decision (FD) shifted from 4QFY14 to 2QFY15 and CI-2 Spiral 2/Spin 3 FD accelerated from 4QFY16 to 3QFY16, in accordance with NSA schedule
- Removed Next Generation Field Device testing event.

Public Key Infrastructure (PKI):
- PKI R-4 removed; under $1M

Funding:
Computer Network Defense (CND): $7.5M increase in FY16 supports Task Force Cyber Awakening (TFCA), specifically Navy Cyber Situational Awareness (NCSA) and Operation Rolling Tide (ORT)/Cyber Remediation capabilities to include network vulnerability remediation, security compliance reporting and mapping of Navy networks in order to achieve improved network defense and security wholeness.

Exhibit R-2A, **RDT&E Project Justification:** PB 2016 Navy		**Date:** February 2015
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 2014	FY 2015	FY 2016 Base	FY 2016 OCO	FY 2016 Total	FY 2017	FY 2018	FY 2019	FY 2020	Cost To Complete	Total Cost
0734: *Communications Security R&D*	336.744	23.213	19.134	25.974	-	25.974	27.474	26.725	20.644	21.069	Continuing	Continuing
Quantity of RDT&E Articles		-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

The Information Systems Security Program (ISSP) Research Development Test & Evaluation (RDT&E) efforts provide cybersecurity 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. The ISSP addresses engineering design, development, modeling, simulation, test, and evaluation for the unique cybersecurity challenges associated with dispersed, bandwidth limited, and forward-tactical connected U.S. 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. Communications 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) Information Networks (DoDIN) capability requirements document for the development of Content Based Encryption (CBE).

In addition to protecting national security information, the ISSP provides enterprise-wide cyber security for statutorily protected information. The ISSP 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).

The ISSP provides dynamic risk-managed cybersecurity solutions to the Navy information infrastructure, not just security devices placed within a network. Extensive effort will be placed on rapidly providing solutions. Few technology areas change as fast as telecommunications and computers; resulting in the need for continuous evaluation, development, and testing of cybersecurity products and cyber defense strategies. The ISSP efforts in support of this environment include developing or applying: (1) Computer Network Defense (CND) cybersecurity technologies required to support strategic and tactical cyber operations; (2) Task Force Cyber Awakening (TFCA) initiatives, specifically Navy Cyber Situational Awareness (NCSA) and Operation Rolling Tide (ORT)/Cyber Remediation capabilities that will accelerate the Navy's ability to prevent, constrain, and mitigate cyber-attacks and critical vulnerabilities; (3) technology to interconnect networks of dissimilar classification and need-to-know, known respectively as Cross Domain Solutions (CDS) and Virtual Secure Enclaves (VSE); (4) new Cryptography secure voice and secure data prototypes and protocols and associated technology for capable programmable COMSEC and TRANSEC devices and software; (5) Key Management (KM); (6) Public Key Infrastructure (PKI) and associated access control technologies that provide assured and persistent Identity and Access Management (IdAM) for persons, virtual instances, and connected devices.

FY 16 Highlights for Information Systems Security Programs (ISSP):

Exhibit R-2A, **RDT&E Project Justification:** PB 2016 Navy		**Date:** February 2015
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*

ISSP efforts that address the risk management of cyberspace, which includes the capabilities to protect, detect, restore, and respond to the following: (1) Technologies supporting the Navy's Computer Network Defense (CND) service provider operations to TFCA initiatives, specifically NCSA and ORT/Cyber Remediation capabilities that will accelerate the Navy's ability to prevent, constrain, and mitigate cyber-attacks and critical vulnerabilities; (2) Navy Crypto engineering efforts to modernize cryptographic equipment and ancillaries with state-of-the-art replacements to counter evolving and increasingly sophisticated threats assurance of the Navy's telecommunications infrastructure and the wireless spectrum; (3) supporting assurance technologies, including Key Management (KM) and the Public Key Infrastructure (PKI); (4) Cybersecurity Services that continue to provide security systems engineering support for the development of DoD and Department of Navy (DoN) cybersecurity architectures and the transition of new technologies to address Navy cybersecurity challenges.

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	**FY 2014**	**FY 2015**	**FY 2016 Base**	**FY 2016 OCO**	**FY 2016 Total**
Title: Computer Network Defense (CND)	7.533	8.361	15.893	-	15.893
Articles:	-	-	-	-	-

FY 2014 Accomplishments:
Provided initial Operation Rolling Tide (ORT)/Cyber Remediation analysis within the Navy's CND program in order to achieve improved network defense and security wholeness. Developed, integrated and tested CND Build 2 and initiated future builds. Ensured Navy networks met Department of Defense (DoD) mandates and initiatives for securing the DoD Information Networks (DoDIN). 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, and provided technical guidance to ensure CND requirements were met by Consolidated Afloat Networks and Enterprise Services (CANES). Implemented DoD and US Cyber Command (USCC) cybersecurity mandates. Evaluated needs derived from the CND Capabilities Steering Group (CCSG) and developed, updated, and integrated the CND suites. Furthered efforts to virtualize CND capabilities and consolidate cybersecurity services in the ONE-Net environment. Continued to support Command 10th Fleet (C10F) Navy Cyber Situational Awareness (NCSA) efforts by deploying integrated tools at the C10F Maritime Operations Center (MOC) to support Command and Control (C2) of the communications systems. Developed and furthered the Joint Capability Technology Demonstration (JCTD) Virtual Secure Enclaves (VSE) to segment networks and adaptively manage operational risks.

FY 2015 Plans:
Continue to provide ORT/Cyber Remediation initiatives within the Navy's CND program in order to achieve improved network defense and security wholeness. 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 cybersecurity tools and mandated

Exhibit R-2A, **RDT&E Project Justification:** PB 2016 Navy		**Date:** February 2015
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 2014**	**FY 2015**	**FY 2016 Base**	**FY 2016 OCO**	**FY 2016 Total**
tools into ONE-Net and IT-21 networks. Continue to evaluate needs derived from stakeholders and the CCSG, and develop, update, and integrate CND suites. Provide Vulnerability Remediation Asset Manager (VRAM) tool to include Online Compliance Reporting System (OCRS) capabilities and Assured Compliance Assessment Solution (ACAS) rollup. Begin development and implementation of an optimal technical and governance solution for interception of outbound encrypted traffic. 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 consolidate cybersecurity services in the ONE-Net environment. 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 by deploying integrated tools at the C10F MOC to support C2 of the communications systems. Continue to develop JCTD delivered VSE to segment networks and adaptively manage operational risks. ***FY 2016 Base Plans:*** $7.5M increase supports Task Force Cyber Awakening (TFCA), specifically NCSA and ORT/Cyber Remediation initiatives. Funding will provide additional capabilities within the Navy's CND program in order to accelerate advanced cybersecurity initiatives to achieve improved network defense and security wholeness. Additional capabilities to include network vulnerability remediation, security compliance reporting, mapping of Navy networks in order to automate real time cybersecurity capabilities critical to the warfighter and will support C2 of Cyber by providing a Data-as-a-Service capability to monitor the cyber environment (CE) by ingesting data from numerous data feeds then plan and direct kinetic/non-kinetic operations within the CE. 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 cybersecurity tools and mandates into ONE-Net and IT-21 networks. Continue to evaluate needs derived from stakeholders and the CCSG, and develop, update, and integrate CND suites. Provide VRAM tool to include OCRS and Continuous Monitoring Risk Score (CMRS) capabilities. Continue to develop and implement an optimal technical and governance solution for interception of outbound encrypted traffic. Continue integration and testing of SSL intercept to achieve compliance with DISA firewall security guidance. Further efforts to virtualize CND capabilities and consolidate cybersecurity services in the ONE-Net environment. Continue analysis to replace and assume acquisition management of NCDOC tactical sensor infrastructure. Continue to support C10F NCSA efforts by deploying integrated tools at the C10F MOC to support C2 of the communications					

Exhibit R-2A, **RDT&E Project Justification:** PB 2016 Navy		**Date:** February 2015
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 2014**	**FY 2015**	**FY 2016 Base**	**FY 2016 OCO**	**FY 2016 Total**
systems. Continue to develop JCTD delivered VSE to segment networks and adaptively manage operational risks. ***FY 2016 OCO Plans:*** N/A					
Title: Navy Cryptography (Crypto)	9.950	5.931	5.414	-	5.414
Articles:	-	-	-	-	-
FY 2014 Accomplishments: Continued initial Transmission Security (TRANSEC) study and continued analysis for a replacement product for legacy devices and investigated strategies for TRANSEC development efforts. Provided Vinson/Advanced Narrowband Digital Voice Terminal (ANDVT) Cryptographic Modernization (VACM) technical engineering support on behalf of Navy, achieved Milestone C (MS C), and performed Navy system integration tests on Production Representative Engineering Design Models (PREDMs). Continued to provide security engineering support for modernization of space crypto systems, embeddable crypto modernization strategies, and Next Generation Crypto initiatives, tactical radios, and Communication Data Link System (CDLS)/Tactical Common Data Link (TCDL). Investigated impacts of upcoming National Security Agency (NSA) security enhancements for crypto modernization products to include Enhanced FireFly (EFF) and initiated development and testing efforts. Completed Link-22 Modernized Link Level Communications Security (MLLC) Test Readiness Review (TRR) 1 and continued to provide Navy engineering support to NSA for certification authority, acquisition authority and data testing on all crypto modernization efforts. Initiated engineering support for the modernization of VACM ancillary devices on behalf of Navy. Achieved Full Operational Capability (FOC) of KG-45A devices. ***FY 2015 Plans:*** Deliver 10 Link-22 MLLC Full Development units. Continue studies and analysis for TRANSEC replacement products and initiate development efforts for legacy devices, to include other Navy Program of Record (POR) interdependencies. Continue to provide security engineering support for modernization of space crypto systems, embeddable crypto modernization strategies, and Next Generation Crypto initiatives to include tactical radios and CDLS/TCDL. Continue to provide engineering support to NSA certification authority, acquisition authority and data testing on all crypto modernization efforts. Continue to investigate impacts of upcoming NSA security enhancements for crypto modernization products to include EFF efforts. Research and study the follow-on alternatives for Secure Telephone Equipment (STE) modernization. Continue to provide VACM technical engineering support on behalf of DoN. Perform VACM Initial Operational Test & Evaluation (IOT&E) and achieve Full Rate Production (FRP) decision. Continue to provide engineering support for the modernization of VACM					

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)

	FY 2014	FY 2015	FY 2016 Base	FY 2016 OCO	FY 2016 Total

ancillary devices. Complete Link-22 Modernized Link Level Communications Security (MLLC) Test Readiness Review (TRR) 2. Complete Link-22 MLLC Production Readiness Review (PRR).

FY 2016 Base Plans:
Continue development of TRANSEC replacement products and initiate developmental testing across multiple products. Continue to provide security engineering support for modernization of space crypto systems, embeddable crypto modernization strategies, and Next Generation Crypto initiatives to include tactical radios and CDLS/TCDL. Continue to provide support for NSA certification authority, acquisition authority and data testing for all Crypto Modernization efforts. Continue to investigate impacts of upcoming NSA security enhancements for crypto modernization products. Initiate EFF development and testing across multiple products. Achieve VACM Initial Operational Capability (IOC). Complete modernization of VACM ancillary devices.

FY 2016 OCO Plans:
N/A

	FY 2014	FY 2015	FY 2016 Base	FY 2016 OCO	FY 2016 Total
Title: Key Management (KM)	2.641	2.472	2.229	-	2.229
Articles:	-	-	-	-	-

FY 2014 Accomplishments:
Continued capability, engineering, development, verification testing, monitored vendor Developmental Testing (DT), and Operational Assessment (OA) completion in support of 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 to define capability requirements for KMI CI-3. Continued migrating Communications Security (COMSEC) Material Work Station (CMWS) to the KMI environment. Continued the development, engineering and testing of Key Management Infrastructure Intermediary Application (iApp) which will enhance the accounting for and distribution of KMI key delivery for afloat networks. Conducted shipboard bandwidth assessment with Spiral 2 in support of KMI Management Client (MGC). Initiated Spiral 2/Spin 2 development and test efforts. Continued to provide engineering support to National Security Agency (NSA) to ensure Navy requirements are met in KMI Spiral 2/Spin 2. Achieved Tactical Key Loader (TKL) FOC.

FY 2015 Plans:
Achieve KMI CI-2 Spiral 2/Spin 1 Fielding Decision (FD). Continue to monitor and track capability verification testing to include vendor DT, OA and achieve FD in support of KMI CI-2 Spiral 2/Spin 2. Continue to define KMI CI-3 capability requirements. Continue migrating CMWS, the follow on to Simple Key Loader (SKL) into the KMI

Exhibit R-2A, **RDT&E Project Justification:** PB 2016 Navy		**Date:** February 2015
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 2014**	**FY 2015**	**FY 2016 Base**	**FY 2016 OCO**	**FY 2016 Total**
environment. Continue the development, engineering and testing of iApp which will enhance the accounting for and distribution of KMI key delivery for afloat networks. Initiate Spiral 2/Spin 3 development efforts and provide engineering support to NSA to ensure Navy requirements are met. ***FY 2016 Base Plans:*** Continue Spiral 2/Spin 3 capability engineering, development, vendor DT, and OA and achieve FD on KMI CI-2 Spiral 2/Spin 3. Continue to define capability requirements for KMI CI-3. Continue migrating CMWS, the follow on to SKL into the KMI environment. Complete the development, engineering and testing to the iApp which will enhance the accounting for and distribution of KMI key delivery for afloat networks. Initiate development and provide engineering support to NSA to ensure Navy requirements are met in KMI Spiral 2/Spin 4 capabilities and complete vendor DT for KMI Spiral 2/Spin 4. ***FY 2016 OCO Plans:*** N/A					
Title: Public Key Infrastructure (PKI)	0.409	0.315	0.354	-	0.354
Articles:	-	-	-	-	-
FY 2014 Accomplishments: Completed development of PKI solutions, including the SECRET Internet Protocol Router Network (SIPRNet) Shipboard Validation Authority (SVA) and Cryptographic Log-on (CLO) capability to non-Microsoft systems and Microsoft non-Domain services. Completed research on microsoft and non-microsoft PKI solutions for Navy Program of Record (POR). Completed research and testing of Defense Information Systems Agency (DISA) Online Certificate Status Protocol (OCSP) enhancements for certificate authentication in the Navy afloat and shore environments. Completed investigating virtualization of Navy Certificate Validation Infrastructure (NCVI) servers. Continued to ensure Navy compliance and compatibility with new PKI-related cryptographic algorithms, to include Elliptic Curve Cryptography (ECC) and Secure Hash Algorithms (SHA-256). Ensured compliance and compatibility with certificate changes on the Common Access Card (CAC), Alternate Logon Token (ALT), and SIPRNet hardware token. Continued to ensure compatibility and interoperability of PKI with Computer Network Defense (CND) systems architecture. Began testing and evaluation of the Non-Classified Internet Protocol Router Network (NIPRNet) Enterprise Alternate Token System (NEATS) for shore and afloat role-based tokens. Continued to research and develop tools to support certificates for Non-Person Entity (NPE) devices and tactical/austere environments. Began researching Identity and Access Management (IdAM) technologies to increase information security. ***FY 2015 Plans:***					

Exhibit R-2A, **RDT&E Project Justification:** PB 2016 Navy		**Date:** February 2015
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 2014**	**FY 2015**	**FY 2016 Base**	**FY 2016 OCO**	**FY 2016 Total**
Continue Navy compliance and compatibility with DoD PKI implementation, cryptographic algorithms and development efforts, to include CND, ECC, SHA-256, NCVI, CAC, ALT, and SIPRNet Token. Continue research, test and evaluation of NEATS, PKI authentication capabilities to support mobile devices, tools to support certificates for NPE and IdAM to support in tactical/austere environments and increase information security. ***FY 2016 Base Plans:*** Continue Navy compliance and compatibility with DoD PKI implementation, cryptographic algorithms and development efforts, to include CND, ECC, SHA-256, NCVI, CAC, ALT, and SIPRNet Token. Continue research, test and evaluation of NEATS, PKI authentication capabilities to support mobile devices, tools to support certificates for NPE and IdAM in tactical/austere environments and increase information security. ***FY 2016 OCO Plans:*** N/A					
Title: Cybersecurity Services	2.680	2.055	2.084	-	2.084
Articles:	-	-	-	-	-
FY 2014 Accomplishments: Continued to provide security systems engineering support for the development of DoD and DoN cybersecurity architectures and the transition of new technologies to address Navy cybersecurity challenges. Provided updates to reflect emerging priorities and address Navy specific threats. Coordinated cybersecurity activities across the virtual Systems Command (SYSCOM) via the Cybersecurity Trusted Architecture (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 Outside the Continental United States (OCONUS) networks. Provided cybersecurity 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 cybersecurity 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 cybersecurity controls. ***FY 2015 Plans:*** Continue to provide security systems engineering support for the development of DoD and DoN cybersecurity architectures and the transition of new technologies to address Navy cybersecurity challenges. Continue to provide updates to reflect emerging priorities and address Navy specific threats. Continue to coordinate					

Exhibit R-2A, RDT&E Project Justification: PB 2016 Navy		**Date:** February 2015
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 2014	FY 2015	FY 2016 Base	FY 2016 OCO	FY 2016 Total

cybersecurity activities across the virtual SYSCOM via the Cybersecurity 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 cybersecurity risk analysis and recommended risk mitigation strategies for Navy critical networks and C4I systems. Continue to coordinate with the Navy acquisition community to ensure cybersecurity 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 cybersecurity controls.

FY 2016 Base Plans:
Continue to provide security systems engineering support for the development of DoD and DoN cybersecurity architectures and the transition of new technologies to address Navy cybersecurity challenges. Continue to provide updates to reflect emerging priorities and address Navy specific threats. Continue to coordinate cybersecurity activities across the virtual SYSCOM via the Cybersecurity 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 cybersecurity risk analysis and recommended risk mitigation strategies for Navy critical networks and C4I systems. Continue to coordinate with the Navy acquisition community to ensure cybersecurity 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 cybersecurity controls.

FY 2016 OCO Plans:
N/A

	FY 2014	FY 2015	FY 2016 Base	FY 2016 OCO	FY 2016 Total
Accomplishments/Planned Programs Subtotals	23.213	19.134	25.974	-	25.974

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2014	FY 2015	FY 2016 Base	FY 2016 OCO	FY 2016 Total	FY 2017	FY 2018	FY 2019	FY 2020	Cost To Complete	Total Cost
• OPN/3415: *Info Sys Security Program (ISSP)*	125.902	108.002	135.687	-	135.687	82.905	85.848	86.376	88.273	Continuing	Continuing

Remarks

Exhibit R-2A, RDT&E Project Justification: PB 2016 Navy		**Date:** February 2015
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*

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. Strategies followed by other lead agencies include VINSON/Advanced Narrowband Digital Voice Terminal Crypto Modernization (VACM) and KG-3X which are led by the United States Air Force (USAF).

Key Management (KM): Key Management Infrastructure (KMI) is a NSA led Joint ACAT I program. It 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. The KMI program will continue to develop alternative architecture implementations for communities within the Navy to implement Intermediary Application (iApp) as a key management solution.

Public Key Infrastructure (PKI): Department of Defense (DoD) PKI is an ACAT I program led by the NSA and the DoD Chief Information Officer (CIO) who are the Milestone Decision Authority (MDA). The Navy PKI project supports the DoD-wide implementation of PKI products and services across Navy afloat, non-Navy Marine Corps Intranet (NMCI), and Outside the Continental United States (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.
* 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 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 Fiscal Year Defense Plan (FYDP) by conducting a gap analysis and building a CM roadmap and implementation plan to allow the Navy Network Warfare Command (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, identify, and implement modern small form factor, multi-channel cryptography devices (e.g., KIV-7M replacing KIV-7HS, KIV-7HSB, KG-84, KWR-46, KL-51, etc.).

Key Management (KM):
* Meet 100% of DON, US Coast Guard (USCG) key management requirements. USCG and Military Sealift Command (MSC) replace existing Electronic Key Management System (EKMS) Tier 2 systems with a Key Management Infrastructure (KMI) Intermediary Application (iApp). Littoral Combat Ship (LCS) implements iApp to automate key deliver to the platforms.
* Complete iApp engineering efforts, testing and begin transition to LCS, USCG Cutters and MSC in FY17.
* Incorporate 100% of the Communication Security (COMSEC) Manager Workstation (CMWS) requirements into the iApp baseline.
* Refine and provide 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 Department of Defense (DoD) PKI requirements on Non-Classified Internet Protocol Router Network (NIPRNet) and SECRET Internet Protocol Router Network (SIPRNet), per Department of Defense Instruction (DoDI) 8520.02.
* Ensure 100% interoperability with DoD and Federal partners by researching and evaluating enhanced cryptographic algorithms and DoD certificate changes.

Cybersecurity Services:
* Ensure 100% interoperability and application of commercial standards compliance for Information Systems Security Program (ISSP) products by researching and conducting selective evaluations, integrating and testing commercial-off-the-shelf/Non-Developmental Item cybersecurity 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 cybersecurity technical lead by developing cybersecurity risk analysis and recommended risk mitigation strategies for critical Navy networks and Command, Control, Communications, Computers, and Intelligence (C4I) systems.
* Coordinate cybersecurity activities across the Navy Enterprise via the Cybersecurity 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-3, RDT&E Project Cost Analysis: PB 2016 Navy			**Date:** February 2015
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*	

Product Development ($ in Millions)				**FY 2014**		**FY 2015**		**FY 2016 Base**		**FY 2016 OCO**		**FY 2016 Total**			
Cost Category Item	**Contract Method & Type**	**Performing Activity & Location**	**Prior Years**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Cost To Complete**	**Total Cost**	**Target Value of Contract**
Hardware Development	Various	Various : Various	179.534	0.653	Dec 2013	0.218	Dec 2014	0.268	Dec 2015	-		0.268	Continuing	Continuing	Continuing
Hardware Development (WR)	WR	SSC LANT : Charleston, SC	3.696	0.225	Dec 2013	0.741	Dec 2014	0.780	Dec 2015	-		0.780	Continuing	Continuing	Continuing
Hardware Development (WR)	WR	SSC PAC : San Diego, CA	4.898	2.119	Dec 2013	2.122	Dec 2014	2.235	Dec 2015	-		2.235	Continuing	Continuing	Continuing
Hardware Development	C/CPFF	Raytheon : Los Angeles, CA	2.212	2.640	Apr 2014	-		-		-		-	-	4.852	-
Hardware Development	C/CPFF	SSC LANT : Charleston, SC	0.000	0.479	Dec 2013	0.625	Dec 2014	0.658	Dec 2015	-		0.658	Continuing	Continuing	Continuing
Hardware Development	C/CPFF	SSC PAC : San Diego, CA	0.000	1.170	Dec 2013	1.175	Dec 2014	1.237	Dec 2015	-		1.237	Continuing	Continuing	Continuing
Software Development	Various	Various : Various	65.410	0.790	Dec 2013	-		-		-		-	Continuing	Continuing	Continuing
Software Development (WR)	WR	SSC LANT : Charleston, SC	0.000	1.530	Dec 2013	2.020	Dec 2014	2.127	Dec 2015	-		2.127	Continuing	Continuing	Continuing
Software Development (WR)	WR	SSC PAC : San Diego, CA	3.464	4.566	Dec 2013	4.019	Dec 2014	5.982	Dec 2015	-		5.982	Continuing	Continuing	Continuing
Software Development	C/CPFF	SSC LANT : Charleston, SC	0.000	1.313	Dec 2013	1.789	Dec 2014	1.884	Dec 2015	-		1.884	Continuing	Continuing	Continuing
Software Development	C/CPFF	SSC PAC : San Diego, CA	0.000	1.353	Dec 2013	1.942	Dec 2014	3.794	Dec 2015	-		3.794	Continuing	Continuing	Continuing
Software Development	MIPR	Defense Technical Information Center : Fort Belvoir, VA	0.000	0.839	Dec 2013	0.603	Dec 2014	2.265	Dec 2015	-		2.265	Continuing	Continuing	Continuing
		Subtotal	259.214	17.677		15.254		21.230		-		21.230	-	-	-

Support ($ in Millions)				**FY 2014**		**FY 2015**		**FY 2016 Base**		**FY 2016 OCO**		**FY 2016 Total**			
Cost Category Item	**Contract Method & Type**	**Performing Activity & Location**	**Prior Years**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Cost To Complete**	**Total Cost**	**Target Value of Contract**
Architecture	Various	Various : Various	2.275	0.792	Dec 2013	0.460	Dec 2014	0.484	Dec 2015	-		0.484	Continuing	Continuing	Continuing

Exhibit R-3, **RDT&E Project Cost Analysis:** PB 2016 Navy			**Date:** February 2015
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*	

Support ($ in Millions)

				FY 2014		FY 2015		FY 2016 Base		FY 2016 OCO		FY 2016 Total			
Cost Category Item	**Contract Method & Type**	**Performing Activity & Location**	**Prior Years**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Cost To Complete**	**Total Cost**	**Target Value of Contract**
Architecture	WR	SSC LANT : Charleston, SC	0.000	0.440	Dec 2013	0.806	Dec 2014	0.849	Dec 2015	-		0.849	Continuing	Continuing	Continuing
Architecture	WR	SSC PAC : San Diego, CA	0.000	0.210	Dec 2013	0.220	Dec 2014	0.232	Dec 2015	-		0.232	Continuing	Continuing	Continuing
Architecture	MIPR	Dept of Energy : Washington, DC	0.000	1.400	Feb 2014	-		-		-		-	-	1.400	-
Requirements Analysis	Various	Various : Various	4.071	1.203	Dec 2013	0.220	Dec 2014	0.891	Dec 2015	-		0.891	Continuing	Continuing	Continuing
Studies & Design	Various	Various : Various	4.050	-		0.359	Dec 2014	0.377	Dec 2015	-		0.377	Continuing	Continuing	Continuing
Studies & Design	WR	NRL : Washington, DC	0.000	0.750	Dec 2013	0.750	Dec 2014	0.790	Dec 2015	-		0.790	Continuing	Continuing	Continuing
Systems Engineering	Various	Various : Various	3.044	-		-		-		-		-	-	3.044	-
		Subtotal	13.440	4.795		2.815		3.623		-		3.623	-	-	-

Test and Evaluation ($ in Millions)

				FY 2014		FY 2015		FY 2016 Base		FY 2016 OCO		FY 2016 Total			
Cost Category Item	**Contract Method & Type**	**Performing Activity & Location**	**Prior Years**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Cost To Complete**	**Total Cost**	**Target Value of Contract**
System DT&E	Various	Various : Various	37.665	0.124	Dec 2013	0.423	Dec 2014	0.445	Dec 2015	-		0.445	Continuing	Continuing	Continuing
		Subtotal	37.665	0.124		0.423		0.445		-		0.445	-	-	-

Management Services ($ in Millions)

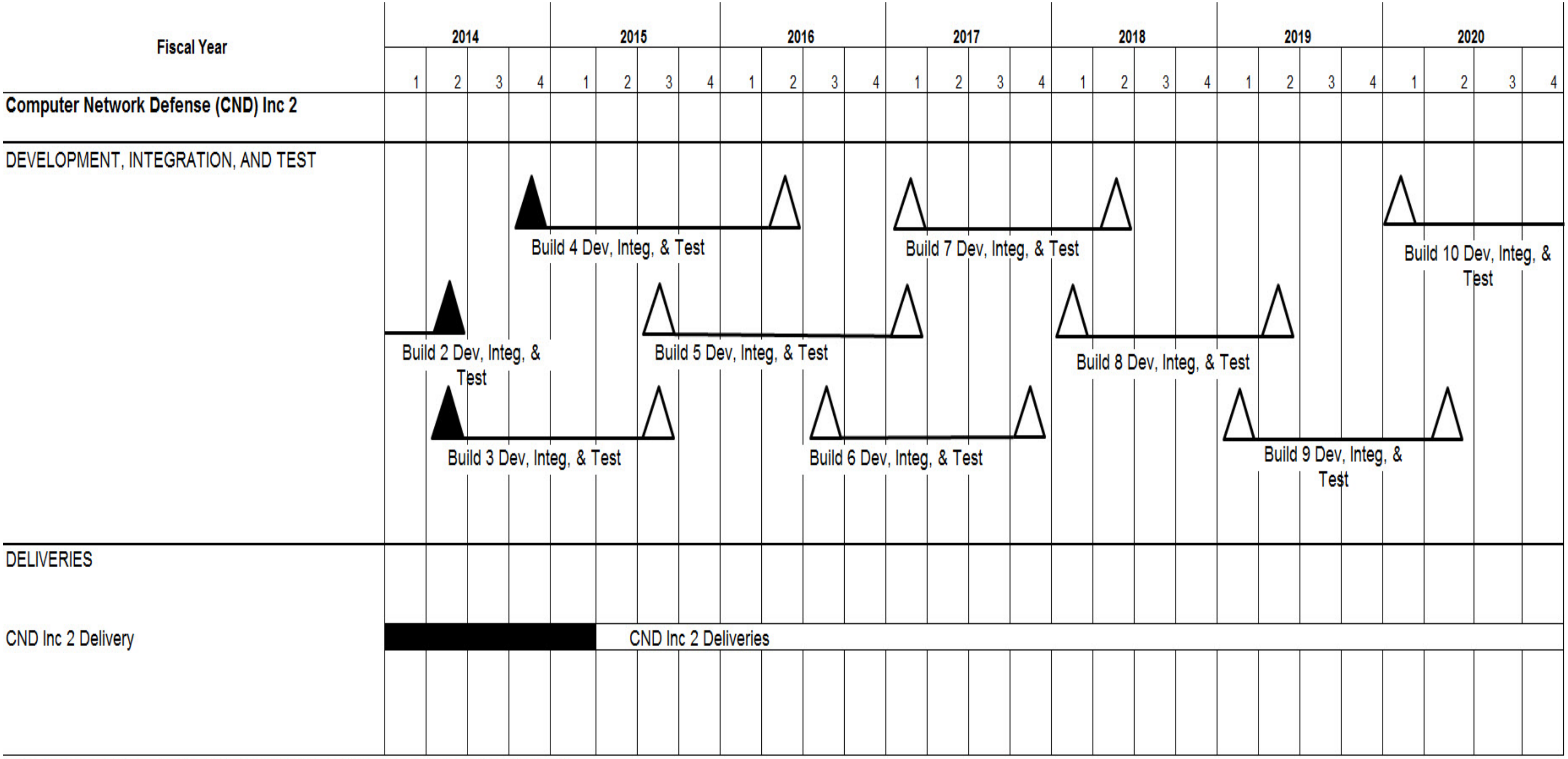
				FY 2014		FY 2015		FY 2016 Base		FY 2016 OCO		FY 2016 Total			
Cost Category Item	**Contract Method & Type**	**Performing Activity & Location**	**Prior Years**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Cost To Complete**	**Total Cost**	**Target Value of Contract**
Program Management	C/CPFF	BAH : San Diego, CA	26.286	0.589	Dec 2013	0.622	Dec 2014	0.656	Dec 2015	-		0.656	Continuing	Continuing	Continuing
Travel	WR	SPAWAR : San Diego, CA	0.139	0.028	Oct 2013	0.020	Oct 2014	0.020	Dec 2015	-		0.020	Continuing	Continuing	Continuing
		Subtotal	26.425	0.617		0.642		0.676		-		0.676	-	-	-

Exhibit R-3, **RDT&E Project Cost Analysis:** PB 2016 Navy		**Date:** February 2015
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*

	Prior Years	FY 2014		FY 2015		FY 2016 Base		FY 2016 OCO		FY 2016 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	336.744	23.213		19.134		25.974		-		25.974	-	-	-

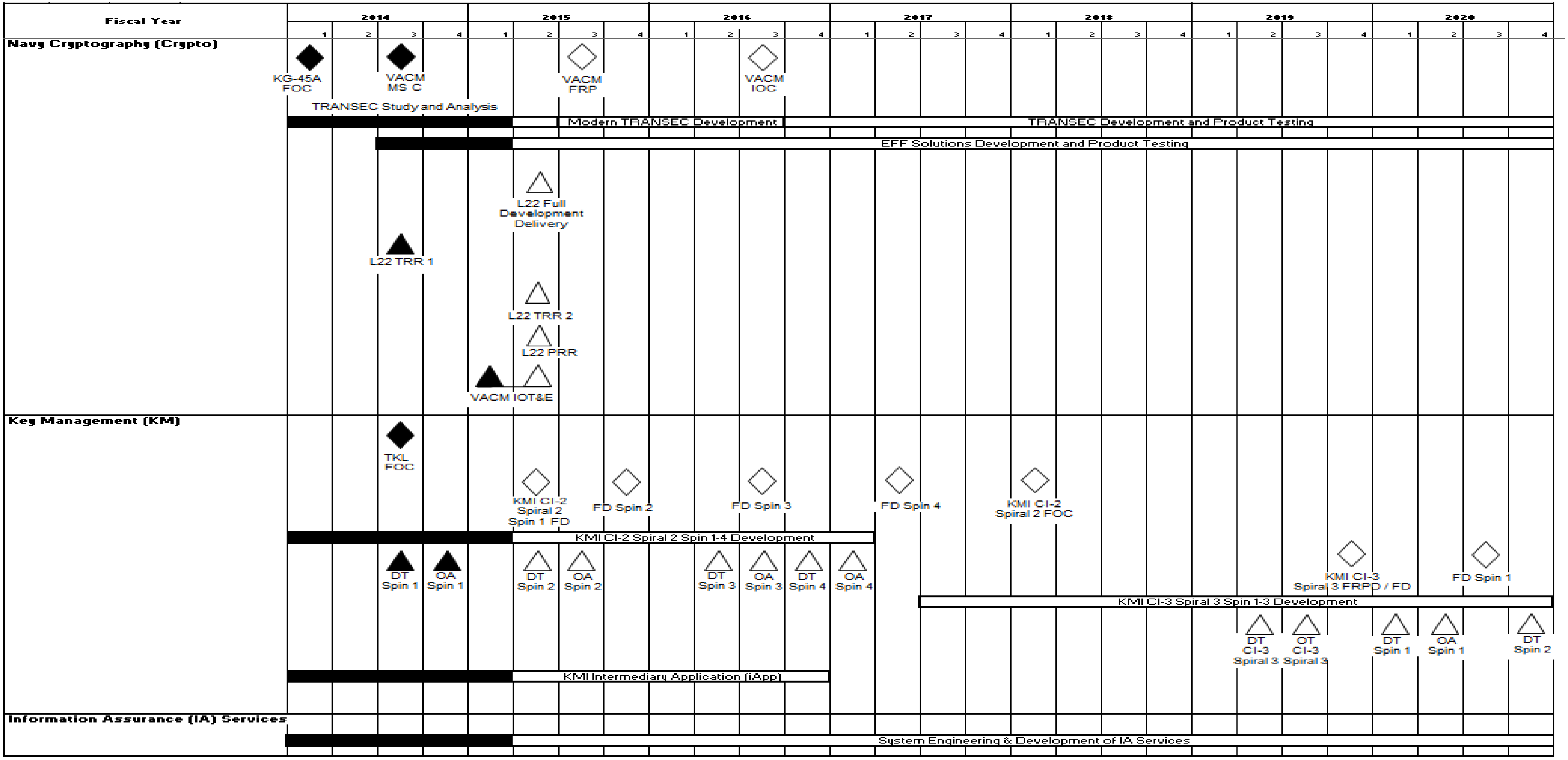
Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2016 Navy		**Date:** February 2015
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: Reference Section B Change Summary for schedule notes and explanations

Exhibit R-4, RDT&E Schedule Profile: PB 2016 Navy		**Date:** February 2015
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: Reference Section B Change Summary for schedule notes and explanations

Exhibit R-4A, RDT&E Schedule Details: PB 2016 Navy		**Date:** February 2015
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*

Schedule Details

	Start		**End**	
Events by Sub Project	**Quarter**	**Year**	**Quarter**	**Year**
Proj 0734				
CND - Build 2 Dev, Integ, & Test	1	2014	2	2014
CND - Build 3 Dev, Integ, & Test	2	2014	3	2015
CND - Build 4 Dev, Integ, & Test	4	2014	2	2016
CND - Build 5 Dev, Integ, & Test	3	2015	4	2016
CND - Build 6 Dev, Integ, & Test	3	2016	4	2017
CND - Build 7 Dev, Integ, & Test	1	2017	2	2018
CND - Build 8 Dev, Integ, & Test	1	2018	2	2019
CND - Build 9 Dev, Integ, & Test	1	2019	2	2020
CND - Build 10 Dev, Integ, & Test	1	2020	4	2020
CND - Inc 2 Deliveries	1	2014	4	2020
Crypto - KG-45A FOC	1	2014	1	2014
Crypto - VACM MS C	3	2014	3	2014
Crypto - VACM FRP	3	2015	3	2015
Crypto - VACM IOC	3	2016	3	2016
Crypto - VACM IOT&E	1	2015	2	2015
Crypto - TRANSEC Study & Analysis	1	2014	2	2015
Crypto - TRANSEC Development and Product Testing	3	2015	4	2020
Crypto - EFF Solutions Development and Product Testing	3	2014	4	2020
Crypto - L22 TRR 1	3	2014	3	2014
Crypto - L22 Full Development Article Delivery	2	2015	2	2015
Crypto - L22 TRR 2	2	2015	2	2015

Exhibit R-4A, **RDT&E Schedule Details:** PB 2016 Navy		**Date:** February 2015
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*

	Start		**End**	
Events by Sub Project	**Quarter**	**Year**	**Quarter**	**Year**
Crypto - L22 PRR	2	2015	2	2015
Key Management - TKL FOC	3	2014	3	2014
Key Management - KMI CI-2 Spiral 2 Spin 1 FD	2	2015	2	2015
Key Management - FD Spin 2	4	2015	4	2015
Key Management - FD Spin 3	3	2016	3	2016
Key Management - FD Spin 4	2	2017	2	2017
Key Management - KMI CI-2 Spiral 2 FOC	1	2018	1	2018
Key Management - KMI CI-2 Spiral 2 Spin 1-4 Development	1	2014	1	2017
Key Management - KMI CI-3 Spiral 3 Spin 1-3 Development	3	2017	4	2020
Key Management - KMI Intermediary Application (iAPP)	1	2014	4	2016
Key Management - DT CI-2 Spiral 2 Spin 1	3	2014	3	2014
Key Management - OA CI-2 Spiral 2 Spin 1	4	2014	4	2014
Key Management - DT CI-2 Spiral 2 Spin 2	2	2015	2	2015
Key Management - OA CI-2 Spiral 2 Spin 2	3	2015	3	2015
Key Management - DT CI-2 Spiral 2 Spin 3	2	2016	2	2016
Key Management - OA CI-2 Spiral 2 Spin 3	3	2016	3	2016
Key Management - DT CI-2 Spiral 2 Spin 4	4	2016	4	2016
Key Management - OA CI-2 Spiral 2 Spin 4	1	2017	1	2017
Key Management - DT CI-3 Spiral 3	2	2019	2	2019
Key Management - OT CI-3 Spiral 3	3	2019	3	2019
Key Management - KMI CI-3 Spiral 3 FRPD/FD	4	2019	4	2019
Key Management - FD Spin 1	3	2020	3	2020
Key Management - DT CI-3 Spiral 3 Spin 1	1	2020	1	2020
Key Management - OA CI-3 Spiral 3 Spin 1	2	2020	2	2020
Key Management - DT CI-3 Spiral 3 Spin 2	4	2020	4	2020

Exhibit R-4A, **RDT&E Schedule Details:** PB 2016 Navy		**Date:** February 2015
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*

	Start		**End**	
Events by Sub Project	**Quarter**	**Year**	**Quarter**	**Year**
Cybersecurity - Systems Engineering & Development of Cybersecurity Services	1	2014	4	2020

Exhibit R-2A, **RDT&E Project Justification:** PB 2016 Navy		**Date:** February 2015
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 2014	FY 2015	FY 2016 Base	FY 2016 OCO	FY 2016 Total	FY 2017	FY 2018	FY 2019	FY 2020	Cost To Complete	Total Cost
3230: *Information Assurance*	8.103	2.391	3.882	2.128	-	2.128	2.121	2.104	2.179	2.223	Continuing	Continuing
Quantity of RDT&E Articles		-	-	-	-	-	-	-	-	-		

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 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

Exhibit R-2A, **RDT&E Project Justification:** PB 2016 Navy		**Date:** February 2015
Appropriation/Budget Activity 1319 **/** 7	**R-1 Program Element (Number/Name)** PE 0303140N **/** *Information Sys Security Program*	**Project (Number/Name)** 3230 **/** *Information Assurance*

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.

FY16 : 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.

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	**FY 2014**	**FY 2015**	**FY 2016 Base**	**FY 2016 OCO**	**FY 2016 Total**
Title: Information Assurance (IA)	2.391	3.882	2.128	-	2.128
Articles:	-	-	-	-	-
FY 2014 Accomplishments: Continued the development of new network security technology focused on addressing nation state level sponsored activity. Continued 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. Continued 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. Continued the efforts focused on identity management and secure data storage, processing and exchange. Continued 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.					

Exhibit R-2A, **RDT&E Project Justification:** PB 2016 Navy		**Date:** February 2015
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 2014**	**FY 2015**	**FY 2016 Base**	**FY 2016 OCO**	**FY 2016 Total**
Continued 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. Continued systems security engineering, certification and accreditation support for high-confidence naval information systems and ensure certification and accreditation approaches are consistent with Navy and DoD requirements. Completed the characterization of attacks/profiles to increase detection rates of the technology, especially for identifying new/emerging malicious code. Completed the development of attribution technology, focusing on nation-state activities across network boundaries that obfuscate traffic using techniques such as anonymization. Completed 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. Completed the development of a security framework for a federated, cross-domain services oriented architecture (SOA) ensuring the framework addresses all critical aspects of SOA including service discovery, identity management, and service invocation, while minimizing inference attacks. Completed the development of several 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. Completed the characterization of several nation state sponsored attacks/profiles that were used to increase detection rates of DoD sensor technology. Initiated the development of new sensing and instrumentation technology to support attack prediction and to measure the effectiveness of network security technology.					

Exhibit R-2A, **RDT&E Project Justification:** PB 2016 Navy		**Date:** February 2015
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 2014**	**FY 2015**	**FY 2016 Base**	**FY 2016 OCO**	**FY 2016 Total**
Initiated 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 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. ***FY 2016 Base Plans:*** Continue the development of new sensing and instrumentation technology to support attack prediction and to measure the effectiveness of network security technology. Continue the development of technology to provide prediction/early warning sensing of impending attacks based on network traffic and user behavior. Continue the development of critical cryptographic technology to support Navy unique platforms and requirements such as UASs (e.g., UAVs, UUV) 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.					

Exhibit R-2A, **RDT&E Project Justification:** PB 2016 Navy		**Date:** February 2015
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 2014**	**FY 2015**	**FY 2016 Base**	**FY 2016 OCO**	**FY 2016 Total**
Complete 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. Complete the development of new network security technology focused on addressing nation state level sponsored activity. Enhance the security framework for a federated SOA infrastructure to support cross-domain services. Complete the efforts focused developing enabling technology building blocks for identity management and secure data storage, processing and exchange. Initiate the development of new host-based security technology focused on addressing data-at-rest requirements, protection of the operating system and applications from nation state-sponsored activities, and methods for system and software updates that do not invalidate the security framework of the host workstation. ***FY 2016 OCO Plans:*** N/A					
Accomplishments/Planned Programs Subtotals	2.391	3.882	2.128	-	2.128

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.

Exhibit R-3, **RDT&E Project Cost Analysis:** PB 2016 Navy		**Date:** February 2015
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 3230 / *Information Assurance*

Support ($ in Millions)				**FY 2014**		**FY 2015**		**FY 2016 Base**		**FY 2016 OCO**		**FY 2016 Total**			
Cost Category Item	**Contract Method & Type**	**Performing Activity & Location**	**Prior Years**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Award Date**	**Cost**	**Cost To Complete**	**Total Cost**	**Target Value of Contract**
Development Support	Various	NRL : Washington, DC	8.103	2.391	Nov 2013	3.882	Nov 2014	2.128	Nov 2015	-		2.128	Continuing	Continuing	Continuing
		Subtotal	8.103	2.391		3.882		2.128		-		2.128	-	-	-

	Prior Years	**FY 2014**		**FY 2015**		**FY 2016 Base**		**FY 2016 OCO**		**FY 2016 Total**	**Cost To Complete**	**Total Cost**	**Target Value of Contract**
Project Cost Totals	8.103	2.391		3.882		2.128		-		2.128	-	-	-

Remarks

Exhibit R-4, **RDT&E Schedule Profile:** PB 2016 Navy		**Date:** February 2015
Appropriation/Budget Activity 1319 **/** 7	**R-1 Program Element (Number/Name)** PE 0303140N **/** *Information Sys Security Program*	**Project (Number/Name)** 3230 **/** *Information Assurance*

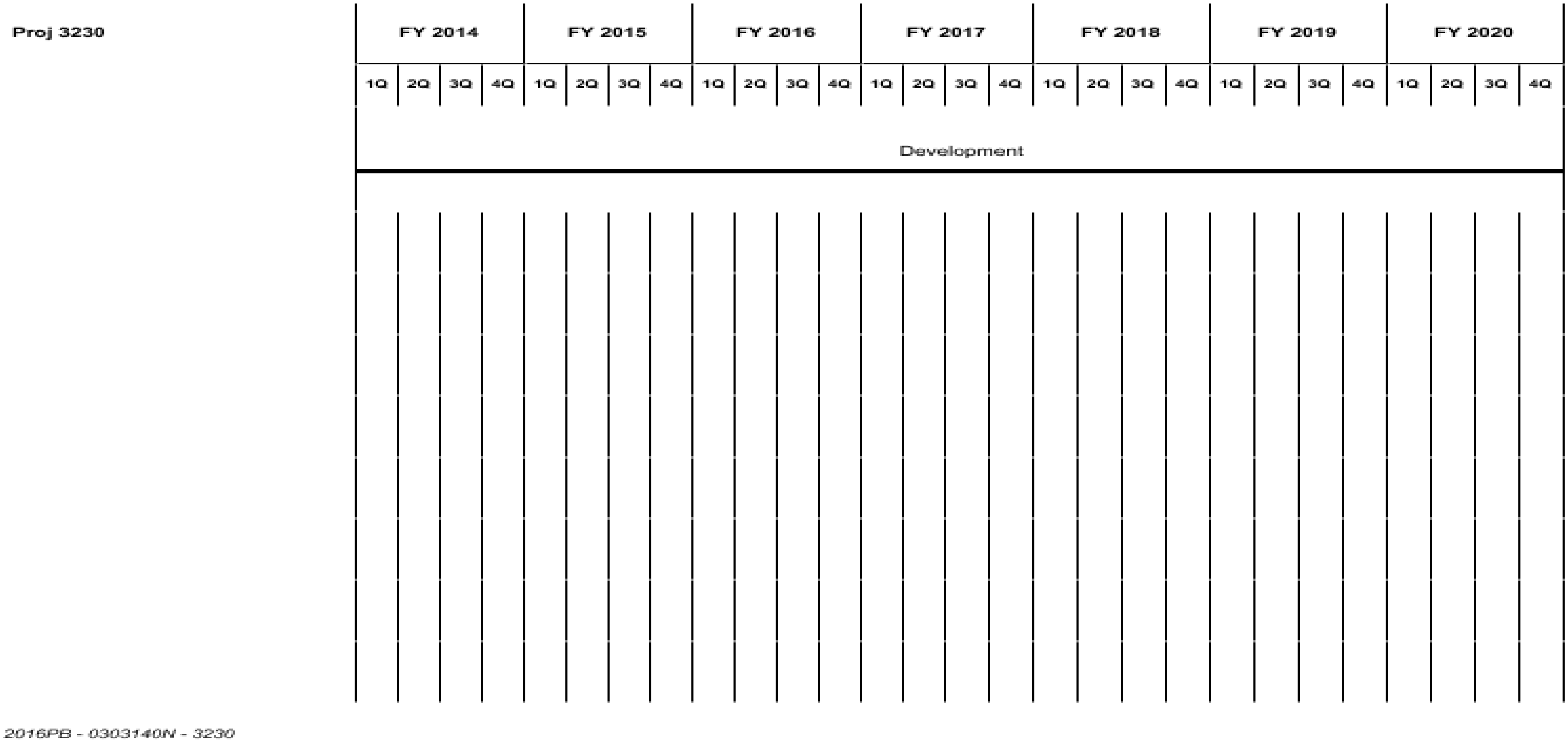


Exhibit R-4A, **RDT&E Schedule Details:** PB 2016 Navy		**Date:** February 2015
Appropriation/Budget Activity 1319 **/** 7	**R-1 Program Element (Number/Name)** PE 0303140N **/** *Information Sys Security Program*	**Project (Number/Name)** 3230 **/** *Information Assurance*

Schedule Details

	Start		**End**	
Events by Sub Project	**Quarter**	**Year**	**Quarter**	**Year**
Proj 3230				
Development	1	2014	4	2020