Exhibit R-2, RDT&E Budget Item Justification: PB 2017 Navy											Date: February 2016	
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 2015**	**FY 2016**	**FY 2017 Base**	**FY 2017 OCO**	**FY 2017 Total**	**FY 2018**	**FY 2019**	**FY 2020**	**FY 2021**	**Cost To Complete**	**Total Cost**
Total Program Element	370.451	22.655	28.081	38.510	-	38.510	39.701	31.128	31.399	32.092	Continuing	Continuing
0734: *Communications Security R&D*	359.957	18.773	25.953	36.987	-	36.987	37.302	28.755	29.182	29.828	Continuing	Continuing
3230: *Information Assurance*	10.494	3.882	2.128	1.523	-	1.523	2.399	2.373	2.217	2.264	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. 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. ISSP provides architectures, products, and services based on mission impacts, information criticality, threats, vulnerabilities, and required defensive countermeasure capabilities.

FY17 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 for Command, Control, Communications, Computers, & Intelligence (C4I) Afloat and Shore Networks, joint time and navigation systems, and industrial control systems using modern cryptographic solutions; (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 to include Task Force Cyber Awakening (TFCA) and Operation Rolling Tide (ORT)/Cyber Remediation capabilities that will accelerate the Navy's ability to prevent, constrain, and mitigate cyberattacks and critical vulnerabilities, as well as Navy Cyber Situational Awareness (NCSA) technologies that will provide greatly improved cyber threat intelligence and situational awareness, from external boundaries to tactical edge infrastructures; (4) assurance of the Navy's telecommunications infrastructure and the wireless spectrum; (5) SHARKCAGE provides the mechanisms to sense cyber threats across all Navy shore and afloat networks to reduce the complexities of monitoring, assessing, and detecting adversary activities across multiple enclaves (e.g. Non-secure Internet Protocol (IP) Router Network (NIPRNET), Secret Internet Protocol Router Network (SIPRNET), C4I, Combat Systems, Hull Mechanical & Electrical (HM&E), etc.); (6) assurance of joint-user cyberspace domains, using a defense-in-depth security architecture and its alignment with the Joint Regional Security Stack (JRSS); (7) assurance of the critical computing base and information store; (8) assurance of mobile and cloud computing; and (9) supporting assurance technologies, including the Public Key Infrastructure (PKI) and Key Management (KM).

Exhibit R-2, RDT&E Budget Item Justification: PB 2017 Navy					Date: February 2016
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 2015**	**FY 2016**	**FY 2017 Base**	**FY 2017 OCO**	**FY 2017 Total**
Previous President's Budget	23.016	28.102	29.595	-	29.595
Current President's Budget	22.655	28.081	38.510	-	38.510
Total Adjustments	-0.361	-0.021	8.915	-	8.915
• Congressional General Reductions	-	-0.021			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-0.361	0.000			
• Program Adjustments	0.000	0.000	11.600	-	11.600
• Rate/Misc Adjustments	0.000	0.000	-2.685	-	-2.685

Change Summary Explanation

Technical:
Computer Network Defense (CND):
- Additional capabilities to provide cyber security and Navy Cyber Situational Awareness (NCSA) for the Navy's portion of the Nuclear Command and Control Communications (NC3-N) system of systems.
- SHARKCAGE provides mechanisms to sense cyber threats across all Navy shore and afloat networks.

Navy Cryptography (Crypto):
- Advanced Cryptographic Capability (ACC) replaces legacy and combines legacy requirements with additional security enhancements.

Key Management (KM):
- KMI CI-3 Spiral 3 also referred to as KMI Tech Refresh.
- Intermediary Application (iApp) Development and Product Testing to extend through FY21 to incorporate KMI CI-3 Spiral 3 capabilities.

Schedule:
Computer Network Defense (CND):
- Due to the dynamic nature of cyber security CND builds were adjusted to include various Cyber Remediation capabilities to include: Operation Rolling Tide (ORT)/ Task Force Cyber Awakening (TFCA) / Navy Cyber Situational Awareness (NCSA).

Navy Cryptography (Crypto):

-VINSON/Advanced Narrowband Digital Voice Terminal (ANDVT) Cryptographic Modernization (VACM) Initial Operational Test and Evaluation (IOT&E) was completed in 2QFY15, Full Rate Production (FRP) decision shifted from 3QFY15 to 2QFY16 due to revised Air Force schedule. Initial Operational Capability (IOC) shifted from 3QFY16 to 4QFY16 due to revised estimated lead times from contract award to delivery.
- Link 22 (L22) Technical Readiness Review (TRR) 2 was completed in 2QFY15. L22 Full Development Delivery and L22 Production Readiness Review (PRR) shifted from 2QFY15 to 4QFY15 due to changes in vendor's schedule.
- Transmission Security (TRANSEC) studies and analysis continued through 4QFY16 and initiation of Modern TRANSEC development shifted from 3QFY15 to 3QFY16 to establish system of systems strategies across multiple Program of Records (PORs), due to support for Navy-wide and DoD-wide efforts. TRANSEC Development and Product Testing and Advanced Cryptographic Capability (ACC) Solutions Development and Product Tests ending 4QFY19 to meet fielding requirements for national mandates.

Key Management (KM):
- Key Management Infrastructure (KMI) Capability Increment-2 (CI-2) Spiral 2 Spin 1 Fielding Decision (FD) shifted from 2QFY15 to 3QFY15, to reflect actual date FD achieved.
- KMI CI-2 Spiral 2/Spin 2 Developmental Testing (DT) shifted from 2QFY15 to 2QFY16, CI-2 Spiral 2/Spin 2 Operational Assessment (OA) shifted from 3QFY15 to 2QFY16, and CI-2 Spiral 2/Spin 2 FD shifted from 4QFY15 to 4QFY16, in accordance with NSA schedule.
- KMI CI-2 Spiral 2/Spin 3 DT shifted from 2QFY16 to 4QFY16, CI-2 Spiral 2/Spin 3 OA shifted from 3QFY16 to 1QFY17, and CI-2 Spiral 2/Spin 3 FD shifted from 3QFY16 to 3QFY17, in accordance with NSA schedule.
- KMI CI-2 Spiral 2/Spin 4 DT shifted from 4QFY16 to 2QFY17, CI-2 Spiral 2/Spin4 OA shifted from 1QFY17 to 2QFY17, CI-2 Spiral 2/Spin 4 FD shifted from 2QFY17 to 3QFY17, in accordance with NSA schedule.
- KMI CI-2 Spiral 2/Spin 4 Full Operational Test and Evaluation (FOT&E) and Full Deployment Decision (FDD) included in 4QFY17, in accordance with NSA schedule.
- KMI CI-3 Spiral 3 / Technical Refresh Contract Award added in 2QFY19.
- Extended Intermediary Application (iApp) development effort out to FY21 to incorporate KMI CI-3 capabilities.
- KMI CI-3 Spiral 3/Spin 2 OA included in 1QFY21 and FD included in 2QFY21.

Funding:
Computer Network Defense (CND): Increase in FY17 supports cyber security system development for the Navy's portion of the Nuclear Command and Control Communications (NC3-N) system of systems; Navy Cyber Situational Awareness (NCSA) Common Operational Picture and other analytic development for NC3-N; Development of SHARKCAGE, which provides the mechanisms to sense cyber threats across all Navy shore and afloat networks to reduce the complexities of monitoring, assessing, and detecting adversary activities across multiple enclaves.

FY 2017 decrease in Information Systems Security Program RDTEN by $1.61M as required for the Department of the Navy to comply with the Bipartisan Budget Act of 2015.

The FY 2017 funding request was also reduced by $0.55M to account for the availability of prior year execution balances.

Exhibit R-2A, RDT&E Project Justification: PB 2017 Navy			Date: February 2016
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 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total	FY 2018	FY 2019	FY 2020	FY 2021	Cost To Complete	Total Cost
0734: *Communications Security R&D*	359.957	18.773	25.953	36.987	-	36.987	37.302	28.755	29.182	29.828	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) are evolving 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 Network (DoDIN) capability requirements document for the development of Content Based Encryption (CBE).

In addition to protecting national security information, the ISSP provides enterprise-wide cybersecurity 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 (i.e., C4I Afloat and Shore Networks), not just security devices placed within a network. Few technology areas change as fast as telecommunications, computers and network security, 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 cyberattacks and critical vulnerabilities and improve overall situational awareness of network status; (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 17 Highlights for Information Systems Security Programs (ISSP):

Exhibit R-2A, RDT&E Project Justification: PB 2017 Navy		Date: February 2016
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 and the advancement of critical TFCA and ORT/Cyber Remediation initiatives, that will accelerate the Navy's ability to prevent, constrain, analyze and mitigate cyberattacks and critical vulnerabilities, as well as NCSA capabilities that will provide greatly improved cyber threat intelligence and situational awareness; (2) Navy Crypto engineering efforts to modernize cryptographic equipment and ancillaries with state-of-the-art replacements to counter evolving and increasingly sophisticated threats to the Navy's telecommunications infrastructure and the wireless spectrum; (3) supporting assurance technologies, including EKMS/KMI and the PKI/IdAM; (4) Cybersecurity services that continue to provide security systems engineering support for the development of DoD and Department of Navy (DoN) cybersecurity architectures, alignment with JRSS, and the transition of new technologies to address Navy cybersecurity challenges.

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total
Title: Computer Network Defense (CND)	8.361	15.872	24.190	0.000	24.190
Articles:	-	-	-	-	-

FY 2015 Accomplishments:
Provided Operation Rolling Tide (ORT)/Cyber Remediation initiatives within the Navy's CND program in order to achieve improved network defense and security wholeness. Continued to develop, integrate, and test CND Builds, Defense-in-depth(DiD) and Situational Awareness (SA) technologies for knowledge-empowered CND operations for shore sites and Command, Control, Communications, Computers and Intelligence (C4I) afloat platforms. Continued to develop new capabilities for the Navy's Command and Control (C2) architecture and provided technical guidance to ensure CND requirements are met by Consolidated Afloat Networks and Enterprise Services (CANES). Continued to implement Department of Defense (DoD) and United States Cyber Command (USCC) cybersecurity tools and mandated tools into ONE-Net and C4I networks. Continued to evaluate needs derived from stakeholders and the CND Capabilities Steering Group (CCSG) and developed, updated, and integrated CND suites. Provided Vulnerability Remediation Asset Manager (VRAM) tool to include Online Compliance Reporting System (OCRS) capabilities and Assured Compliance Assessment Solution (ACAS) rollup. Began development and implementation of an optimal technical and governance solution for interception of outbound encrypted traffic. Initiated integration and testing of Secure Socket Layer (SSL) intercept to achieve compliance with Defense Information Security Agency (DISA) firewall security guidance. Continued to further efforts to virtualize CND capabilities and consolidate cybersecurity services in the ONE-Net environment. Started analysis to replace and assume acquisition management of Navy Cyber Defense Operations Command's (NCDOC) tactical sensor infrastructure. 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 C2 of the communications systems. Continued to develop Joint Capability

Exhibit R-2A, RDT&E Project Justification: PB 2017 Navy		Date: February 2016
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 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total
Technology Demonstration (JCTD) Virtual Secure Enclave (VSE) to segment networks and adaptively manage operational risks.					
FY 2016 Plans: Continue to develop 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 C4I 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 systems. Continue to develop JCTD VSE to segment networks and adaptively manage operational risks.					
FY 2017 Base Plans: Continue to develop Navy's portion of the Nuclear Command and Control Communications (NC3-N) and Ballistic Missile Defense (BMD) cyber security system of systems; Navy Cyber Situational Awareness (NCSA) Common Operational Picture and other analytic development for NC3-N; Development of SHARKCAGE, which provides the mechanisms to sense cyber threats across all Navy shore and afloat networks to reduce the complexities of monitoring, assessing, and detecting adversary activities across multiple enclaves (e.g. Nonsecure Internet Protocol (IP) Router Network (NIPRNET), Secret Internet Protocol Router Network (SIPRNET), C4I, Combat Systems, Hull Mechanical & Electrical (HM&E), etc.). Additionally, funding is for the development of event collection/analysis components for shore nodes and flyaway kits for deployed Cyber Protection Teams (CPT). Complete development and engineering efforts on ORT/Cyber Remediation initiatives. Continue to support					

Exhibit R-2A, RDT&E Project Justification: PB 2017 Navy		Date: February 2016
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 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total
C10F NCSA initiatives through the deployment of integrated Cyber SA tools that enhance C10F MOC ability to support/administer C2 of Navy networks and communication systems within Cyber Key Terrain (CKT) domain(s). Continue to develop, integrate, and test CND Inc 2 Builds, DiD, and SA technologies for knowledge-empowered CND operations for shore sites and afloat platforms within Navy's ONE-Net and C4I networks to achieve improved network defense and security wholeness. Continue to evaluate needs derived from stakeholders and the CCSG, and develop, update, and integrate CND suites. Continue to provide technical guidance to support deployment of new CND capabilities by CANES. Continue integration and testing of SSL intercept to achieve compliance with DISA firewall security guidance. Continue to implement DOD and USCC cybersecurity tools and mandates into ONE-Net and C4I networks. Continue efforts to further virtualize CND capabilities for more effective and cost-efficient deployment of cybersecurity technologies. Continue enhancing the VRAM tool per Fleet Cyber Command 10th Fleet (FCC/C10F) reporting requirements. Continue development and implementation of an optimal technical and governance solution for interception of outbound encrypted traffic. Continue to develop, integrate, and test solution to replace and assume acquisition management of NCDOC tactical sensor infrastructure. Continue to develop JCTD VSE to segment networks and adaptively manage operational risks. ***FY 2017 OCO Plans:*** N/A					
Title: Navy Cryptography (Crypto)	5.570	5.414	7.642	0.000	7.642
Articles:	-	-	-	-	-
FY 2015 Accomplishments: Delivered 10 Link-22 Modernized Link Level Communications Security (MLLC) Full Development units. Continued studies and analysis for Transmission Security (TRANSEC) replacement products, which included other Navy Program of Record (POR) interdependencies. Continued to provide security engineering support for modernization of Department of the Navy (DoN) crypto systems, embeddable crypto modernization strategies and Next Generation Crypto initiatives to include tactical radios and Communications Data Link System/Tactical Common Data Link (CDLS/TCDL). Continued to provide engineering support to National Security Agency (NSA) certification authority, acquisition authority, and data testing on all crypto modernization efforts. Continued to investigate impacts of upcoming NSA security enhancements for crypto modernization products to include Advanced Cryptographic Capability (ACC) efforts. Researched and studied the follow-on alternatives for Secure Telephone Equipment (STE) modernization. Continued to provide Vinson/Advanced Narrowband Digital Voice Terminal (ANDVT) Cryptographic Modernization (VACM) technical engineering support on behalf of DoN.					

Exhibit R-2A, RDT&E Project Justification: PB 2017 Navy		Date: February 2016
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 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total
Performed VACM Initial Operational Test & Evaluation (IOT&E). Continued to provide engineering support for the modernization of VACM ancillary devices. Completed Link-22 MLLC Test Readiness Review (TRR) 2. Completed Link-22 MLLC Production Readiness Review (PRR). ***FY 2016 Plans:*** Complete TRANSEC studies and analysis, deliver Analysis of Alternatives (AoA) replacement products and initiate development efforts to modernize legacy devices, which included other Navy Program of Record (POR) interdependencies, and initiate developmental testing across multiple products. Continue to provide security engineering support for modernization of DoN 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 ACC development and testing across multiple products. Achieve Full Rate Production (FRP) decision. Achieve VACM Initial Operational Capability (IOC). Continue modernization of VACM ancillary devices. ***FY 2017 Base Plans:*** Accelerate TRANSEC replacement products development and continue developmental testing across multiple products. Continue to provide security engineering support for modernization of DoN crypto systems, embeddable crypto modernization strategies, and Next Generation Crypto initiatives to include tactical radios and Communications Data Link System/Tactical Common Data Link (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. Continue ACC development and testing across multiple products. Continue modernization of VACM ancillary devices. Develop Navy strategy and implementation plan to modernize secure voice architectures within Navy networks. ***FY 2017 OCO Plans:*** N/A					
Title: Key Management (KM)	2.472	2.229	2.363	0.000	2.363
Articles:	-	-	-	-	-
FY 2015 Accomplishments: Achieved Key Management Infrastructure (KMI) Capability Increment (CI)-2 Spiral 2/Spin 1 Fielding Decision (FD). Continued to define KMI CI-3/Tech Refresh capability requirements. Continued migrating Communications Security (COMSEC) Material Workstation (CMWS) and the follow on to Simple Key Loader (SKL) into the KMI environment. Continued the development, engineering and testing of Intermediary Application					

Exhibit R-2A, RDT&E Project Justification: PB 2017 Navy		Date: February 2016
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 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total
(iApp), which enhanced the accounting for and distribution of KMI key delivery. Initiated Spiral 2/Spin 3 development efforts and provided engineering support to NSA to ensure Navy requirements were met. Initiated development and provided engineering support to NSA to ensure Navy requirements were met in KMI Spiral 2/ Spin 4 capabilities. ***FY 2016 Plans:*** Monitor and track capability verification testing to include vendor Development Testing (DT), Operational Assessment (OA) and achieve FD in support of KMI CI-2 Spiral 2/Spin 2. Complete Spiral 2/Spin 3 capability engineering, development, and vendor DT. Continue Spiral 2/Spin 4 capability engineering and development. Continue to define capability requirements for KMI CI-3/Tech Refresh. Continue migrating CMWS and the follow on to SKL into the KMI environment. Continue the development, engineering and testing to the Intermediary Application (iApp) which will enhance the accounting for and distribution of KMI key delivery. ***FY 2017 Base Plans:*** Continue to monitor and track capability verification testing to include vendor Operational Assessment (OA) and achieve Fielding Decision (FD) in support of KMI Capability Increment (CI)-2 Spiral 2/Spin 4. Complete Spiral 2/Spin 4 capability engineering, development and vendor Developmental Testing (DT), OA and achieve FD. Achieve Full Operational Test & Evaluation (FOT&E) and Full Deployment Decision (FDD) for KMI Spiral 2. Continue migrating CMWS and the follow on to SKL into the KMI environment. Initiate the development, engineering and testing of CI-3/Tech Refresh, including the integration of iApp, which will enhance the accounting for and distribution of KMI key delivery. ***FY 2017 OCO Plans:*** N/A					
Title: Public Key Infrastructure (PKI)	0.315	0.354	0.350	0.000	0.350
Articles:	-	-	-	-	-
FY 2015 Accomplishments: Continued Navy compliance and compatibility with DoD PKI implementation, cryptographic algorithms and development efforts, to include Computer Network Defense (CND), Elliptic Curve Cryptography (ECC), Secure Hash Algorithms (SHA-256), Navy Certificate Validation Infrastructure (NCVI), Common Access Card (CAC), Alternate Logon Token (ALT), and Secret Internet Protocol Router Network (SIPRNet) Token. Continued research, test and evaluation of Non-Classified Internet Protocol Router Network (NIPRNet) Enterprise Alternate Token System (NEATS), PKI authentication capabilities to support mobile devices, tools to support certificates					

Exhibit R-2A, RDT&E Project Justification: PB 2017 Navy		Date: February 2016
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 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total
for Non-Person Entity (NPE), and Identity and Access Management (IdAM) to support in tactical/austere environments and increase information security. ***FY 2016 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 the NEATS, and continue researching tools to support certificates for NPE. Continue researching and testing PKI authentication capabilities to support mobile devices, IdAM in tactical/ austere environments and increase information security, and begin Real-time Automated Personnel Identification System (RAPIDS) Operating Systems (OS) testing. ***FY 2017 Base Plans:*** Continue Navy compliance and compatibility with DoD PKI implementation, cryptographic algorithms and development efforts, to include CND, ECC, SHA-256 and other encryption methodologies, NCVI, CAC, ALT, and SIPRNet Token. Continue research, test and evaluation of NEATS, NPE, PKI authentication capabilities to support mobile devices, IdAM technologies, and RAPIDS OS. ***FY 2017 OCO Plans:*** N/A					
Title: Cybersecurity Services	2.055	2.084	2.442	0.000	2.442
Articles:	-	-	-	-	-
FY 2015 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. Continued to provide updates to reflect emerging priorities and address Navy specific threats. Continued to coordinate cybersecurity activities across the virtual 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. Continued to provide cybersecurity risk analysis and recommended risk mitigation strategies for Navy critical networks and C4I systems. Continued to coordinate with the Navy acquisition community to ensure cybersecurity requirements are identified and addressed within the development cycles for emerging Navy					

Exhibit R-2A, RDT&E Project Justification: PB 2017 Navy		Date: February 2016
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 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total
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 2016 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 2017 Base Plans:*** Begin coordination with Joint Information Environment (JIE) and Joint Management System (JMS) to ensure Navy architecture requirements for tactical networks are met. 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 2017 OCO Plans:*** N/A					
Accomplishments/Planned Programs Subtotals	18.773	25.953	36.987	0.000	36.987

Exhibit R-2A, RDT&E Project Justification: PB 2017 Navy		Date: February 2016
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 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total	FY 2018	FY 2019	FY 2020	FY 2021	Cost To Complete	Total Cost
• OPN/3415: *Info Sys Security Program (ISSP)*	101.110	135.687	85.694	-	85.694	91.581	99.749	102.197	105.659	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 Navy's cyber defense posture. 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.

Exhibit R-2A, RDT&E Project Justification: PB 2017 Navy		Date: February 2016
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 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 Command, Control, Communications, and Computers Executive Board (MC4EB).
* 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, integration with KMI Capability Increment (CI)-2, 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 to meet KMI CI-2 and KMI CI-3 capabilities.
* Refine and provide Navy unique requirements into the National Security Agency (NSA) KMI 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.

Exhibit R-2A, RDT&E Project Justification: PB 2017 Navy		Date: February 2016
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*

* 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 2017 Navy		Date: February 2016
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)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2015 Cost	FY 2015 Award Date	FY 2016 Cost	FY 2016 Award Date	FY 2017 Base Cost	FY 2017 Base Award Date	FY 2017 OCO Cost	FY 2017 OCO Award Date	FY 2017 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Hardware Development	Various	Various : Various	185.039	0.218	Dec 2014	0.268	Dec 2015	0.710	Dec 2016	-		0.710	Continuing	Continuing	Continuing
Hardware Development (WR)	WR	SSC LANT : Charleston, SC	3.921	0.684	Oct 2014	0.780	Oct 2015	0.862	Oct 2016	-		0.862	Continuing	Continuing	Continuing
Hardware Development (WR)	WR	SSC PAC : San Diego, CA	7.017	1.958	Oct 2014	2.235	Oct 2015	1.986	Oct 2016	-		1.986	Continuing	Continuing	Continuing
Hardware Development	C/CPFF	SSC LANT : Charleston, SC	0.479	0.576	Dec 2014	0.658	Dec 2015	0.000		-		0.000	Continuing	Continuing	Continuing
Hardware Development	C/CPFF	SSC PAC : San Diego, CA	1.170	1.084	Dec 2014	1.237	Dec 2015	1.045	Dec 2016	-		1.045	Continuing	Continuing	Continuing
Software Development	Various	Various : Various	66.200	0.000		2.265	Dec 2015	2.085	Dec 2016	-		2.085	Continuing	Continuing	Continuing
Software Development (WR)	WR	SSC LANT : Charleston, SC	1.530	2.020	Oct 2014	2.127	Oct 2015	1.671	Oct 2016	-		1.671	Continuing	Continuing	Continuing
Software Development (WR)	WR	SSC PAC : San Diego, CA	8.030	4.019	Oct 2014	5.961	Oct 2015	6.412	Oct 2016	-		6.412	Continuing	Continuing	Continuing
Software Development	C/CPFF	SSC LANT : Charleston, SC	1.313	1.789	Dec 2014	1.884	Dec 2015	3.891	Dec 2016	-		3.891	Continuing	Continuing	Continuing
Software Development	C/CPFF	SSC PAC : San Diego, CA	1.353	1.942	Dec 2014	3.794	Dec 2015	3.792	Dec 2016	-		3.792	Continuing	Continuing	Continuing
Software Development	MIPR	Defense Technical Information Center : Fort Belvoir, VA	0.839	0.603	Dec 2014	0.000		0.000		-		0.000	0.000	1.442	-
Software Development	MIPR	MITRE : McLean, VA	0.000	0.000		0.000		1.372	Dec 2016	-		1.372	Continuing	Continuing	Continuing
		Subtotal	276.891	14.893		21.209		23.826		-		23.826	-	-	-

Support ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2015 Cost	FY 2015 Award Date	FY 2016 Cost	FY 2016 Award Date	FY 2017 Base Cost	FY 2017 Base Award Date	FY 2017 OCO Cost	FY 2017 OCO Award Date	FY 2017 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Architecture	Various	Various : Various	4.467	0.460	Dec 2014	0.484	Dec 2015	0.000		-		0.000	Continuing	Continuing	Continuing
Architecture	WR	SSC LANT : Charleston, SC	0.440	0.806	Oct 2014	0.849	Oct 2015	0.413	Oct 2016	-		0.413	Continuing	Continuing	Continuing

Exhibit R-3, RDT&E Project Cost Analysis: PB 2017 Navy			Date: February 2016
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)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2015 Cost	FY 2015 Award Date	FY 2016 Cost	FY 2016 Award Date	FY 2017 Base Cost	FY 2017 Base Award Date	FY 2017 OCO Cost	FY 2017 OCO Award Date	FY 2017 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Architecture	WR	SSC PAC : San Diego, CA	0.210	0.220	Oct 2014	0.232	Oct 2015	0.923	Oct 2016	-		0.923	Continuing	Continuing	Continuing
Requirements Analysis	C/CPFF	BAH : San Diego, CA	5.274	0.220	Dec 2014	0.891	Dec 2015	3.704	Dec 2016	-		3.704	Continuing	Continuing	Continuing
Studies & Design	Various	Various : Various	4.050	0.359	Dec 2014	0.377	Dec 2015	0.224	Dec 2016	-		0.224	Continuing	Continuing	Continuing
Studies & Design	WR	NRL : Washington, DC	0.750	0.750	Dec 2014	0.790	Dec 2015	1.172	Dec 2016	-		1.172	Continuing	Continuing	Continuing
Systems Engineering	Various	Various : Various	3.044	0.000		0.000		0.000		-		0.000	0.000	3.044	-
Architecture	MIPR	MITRE : McLean, VA	0.000	0.000		0.000		0.363	Dec 2016	-		0.363	Continuing	Continuing	Continuing
Requirements Analysis	MIPR	MITRE : McLean, VA	0.000	0.000		0.000		0.363	Dec 2016	-		0.363	Continuing	Continuing	Continuing
Requirements Analysis	WR	SSC PAC : San Diego, CA	0.000	0.000		0.000		0.688	Oct 2016	-		0.688	Continuing	Continuing	Continuing
Studies & Design	WR	SSC PAC : San Diego, CA	0.000	0.000		0.000		0.688	Oct 2016	-		0.688	Continuing	Continuing	Continuing
Studies & Design	MIPR	MITRE : McLean, VA	0.000	0.000		0.000		0.363	Dec 2016	-		0.363	Continuing	Continuing	Continuing
		Subtotal	18.235	2.815		3.623		8.901		-		8.901	-	-	-

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2015 Cost	FY 2015 Award Date	FY 2016 Cost	FY 2016 Award Date	FY 2017 Base Cost	FY 2017 Base Award Date	FY 2017 OCO Cost	FY 2017 OCO Award Date	FY 2017 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
System DT&E	Various	Various : Various	37.789	0.423	Dec 2014	0.445	Dec 2015	1.545	Dec 2016	-		1.545	Continuing	Continuing	Continuing
System DT&E	WR	SSC PAC : San Diego, CA	0.000	0.000		0.000		0.688	Oct 2016	-		0.688	Continuing	Continuing	Continuing
System DT&E	WR	SSC LANT : Charleston, SC	0.000	0.000		0.000		0.250	Oct 2016	-		0.250	Continuing	Continuing	Continuing
		Subtotal	37.789	0.423		0.445		2.483		-		2.483	-	-	-

Exhibit R-3, RDT&E Project Cost Analysis: PB 2017 Navy		Date: February 2016
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*

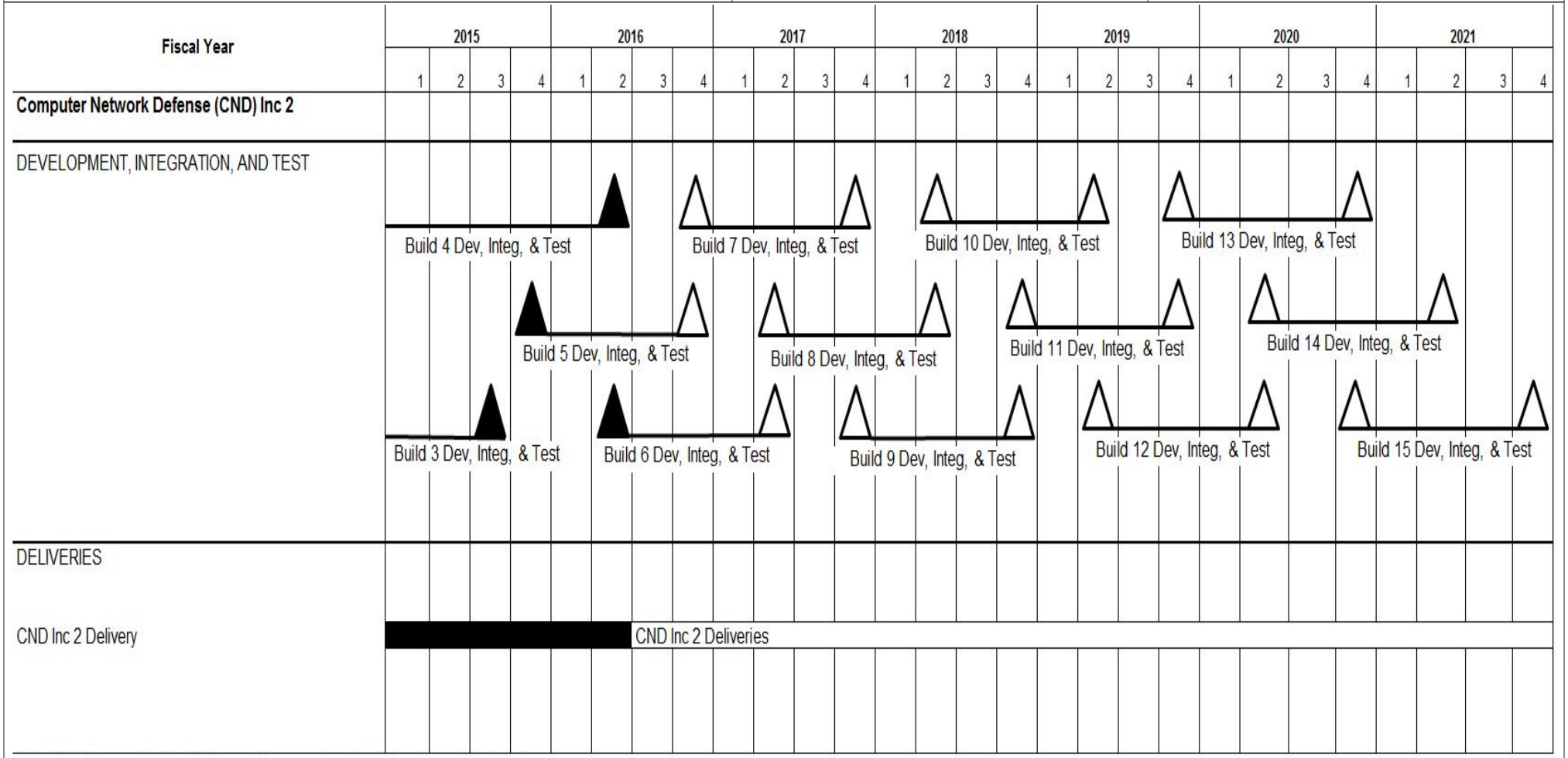
Management Services ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2015 Cost	FY 2015 Award Date	FY 2016 Cost	FY 2016 Award Date	FY 2017 Base Cost	FY 2017 Base Award Date	FY 2017 OCO Cost	FY 2017 OCO Award Date	FY 2017 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Program Management	C/CPFF	BAH : San Diego, CA	26.875	0.622	Dec 2014	0.656	Dec 2015	0.588	Dec 2016	-		0.588	Continuing	Continuing	Continuing
Travel	WR	SPAWAR : San Diego, CA	0.167	0.020	Oct 2014	0.020	Dec 2015	0.000		-		0.000	Continuing	Continuing	Continuing
Program Management (WR)	WR	SSC PAC : San Diego, CA	0.000	0.000		0.000		1.189	Oct 2016	-		1.189	Continuing	Continuing	Continuing
		Subtotal	27.042	0.642		0.676		1.777		-		1.777	-	-	-

	Prior Years	FY 2015		FY 2016		FY 2017 Base		FY 2017 OCO		FY 2017 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	359.957	18.773		25.953		36.987		-		36.987	-	-	-

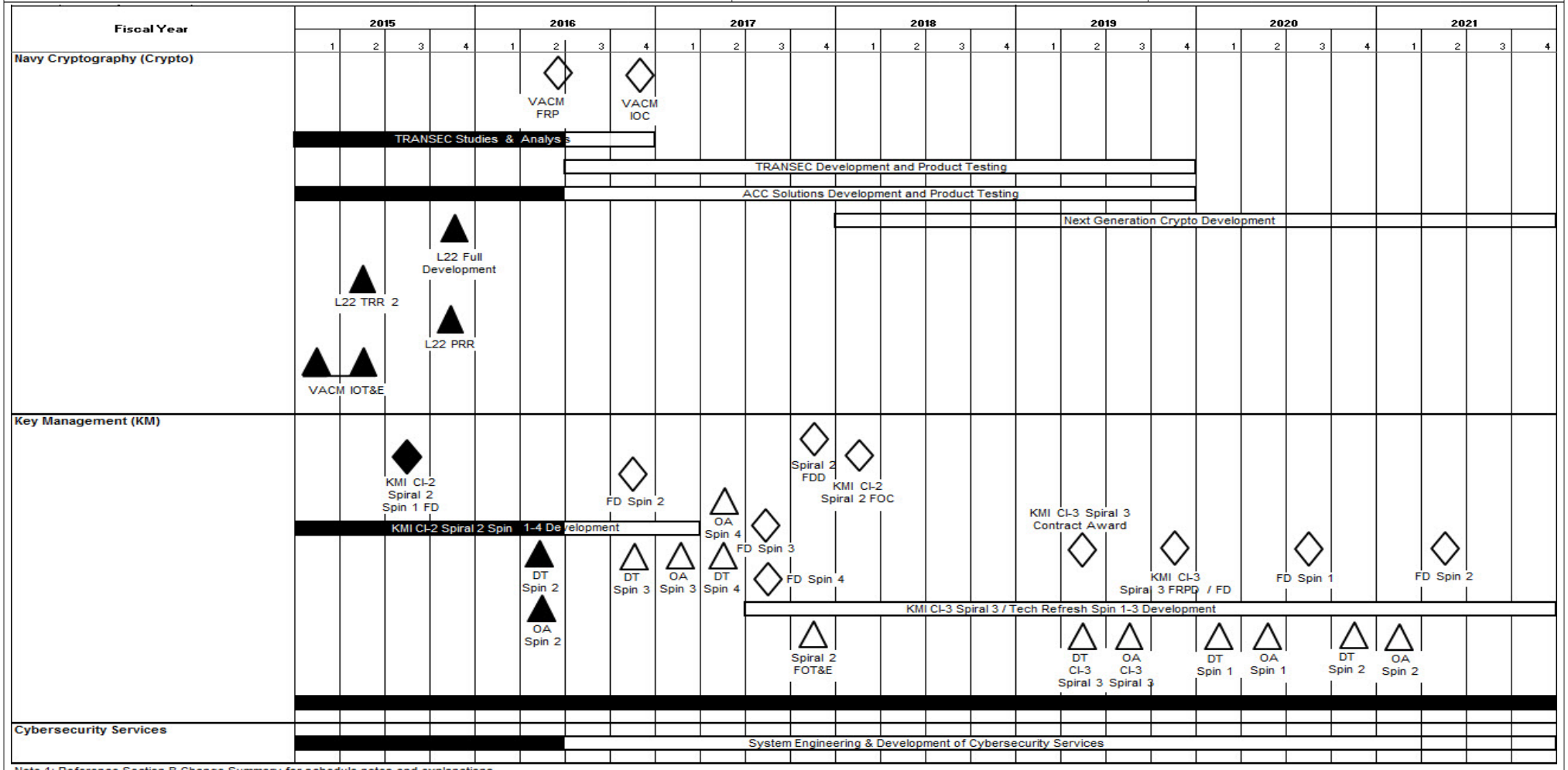
Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2017 Navy		Date: February 2016
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 2017 Navy		Date: February 2016
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 2017 Navy		Date: February 2016
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 3 Dev, Integ, & Test	3	2015	3	2015
CND - Build 4 Dev, Integ, & Test	2	2016	2	2016
CND - Build 5 Dev, Integ, & Test	4	2015	4	2016
CND - Build 6 Dev, Integ, & Test	2	2016	2	2017
CND - Build 7 Dev, Integ, & Test	4	2016	4	2017
CND - Build 8 Dev, Integ, & Test	2	2017	2	2018
CND - Build 9 Dev, Integ, & Test	4	2017	4	2018
CND - Build 10 Dev, Integ, & Test	2	2018	2	2019
CND - Build 11 Dev, Integ, & Test	4	2018	4	2019
CND - Build 12 Dev, Integ, & Test	2	2019	2	2020
CND - Build 13 Dev, Integ, & Test	4	2019	4	2020
CND - Build 14 Dev, Integ, & Test	2	2020	2	2021
CND - Build 15 Dev, Integ, & Test	4	2020	4	2021
CND - Inc 2 Deliveries	1	2015	4	2020
Crypto - VACM Full Rate Production (FRP) Decision	2	2016	2	2016
Crypto - VACM Initial Operational Capability (IOC)	4	2016	4	2016
Crypto - VACM Initial Operational Test & Evaluation (IOT&E)	1	2015	2	2015
Crypto - TRANSEC Studies & Analysis	1	2015	4	2016
Crypto - TRANSEC Development and Product Testing	3	2016	4	2019
Crypto - ACC Solutions Development and Product Testing	1	2015	4	2019
Crypto - Link 22 (L22) Full Development Article Delivery	4	2015	4	2015

Exhibit R-4A, RDT&E Schedule Details: PB 2017 Navy		Date: February 2016
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 Test Readiness Review (TRR) 2	2	2015	2	2015
Crypto - L22 Production Readiness Review (PRR)	4	2015	4	2015
Crypto - Next Generation Crypto Development	1	2018	4	2021
Key Management - KMI CI-2 Spiral 2 Spin 1 Fielding Decision (FD)	3	2015	3	2015
Key Management - FD Spiral 2 Spin 2	4	2016	4	2016
Key Management - FD Spiral 2 Spin 3	3	2017	3	2017
Key Management - FD Spiral 2 Spin 4	3	2017	3	2017
Key Management - KMI CI-2 Spiral 2 Full Operational Capability (FOC)	1	2018	1	2018
Key Management - KMI CI-2 Spiral 2 Spin 1-4 Development	1	2015	1	2017
Key Management - KMI CI-3 Spiral 3/Tech Refresh Spin 1-3 Development	3	2017	4	2021
Key Management - KMI Intermediary Application (iAPP) Development and Product Testing	1	2015	4	2021
Key Management - Development Testing (DT) CI-2 Spiral 2 Spin 2	2	2016	2	2016
Key Management - Operational Assessment (OA) CI-2 Spiral 2 Spin 2	2	2016	2	2016
Key Management - DT CI-2 Spiral 2 Spin 3	4	2016	4	2016
Key Management - OA CI-2 Spiral 2 Spin 3	1	2017	1	2017
Key Management - DT CI-2 Spiral 2 Spin 4	2	2017	2	2017
Key Management - OA CI-2 Spiral 2 Spin 4	2	2017	2	2017
Key Management - Spiral 2 Full Operational Test & Evaluation (FOT&E)	4	2017	4	2017
Key Management - Spiral 2 Full Deployment Decision (FDD)	4	2017	4	2017
Key Management - KMI CI-3 Spiral 3 Contract Award	2	2019	2	2019
Key Management - DT CI-3 Spiral 3	2	2019	2	2019
Key Management - OA CI-3 Spiral 3	3	2019	3	2019
Key Management - KMI CI-3 Spiral 3 Fielding Decision (FD)	4	2019	4	2019
Key Management - FD Spiral 3 Spin 1	3	2020	3	2020
Key Management - FD Spiral 3 Spin 2	2	2021	2	2021

Exhibit R-4A, RDT&E Schedule Details: PB 2017 Navy		Date: February 2016
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**
Key Management - DT CI-3 Spiral 3 Spin 1	1	2020	1	2020
Key Management - Operational Assessment (OA) CI-3 Spiral 3 Spin 1	2	2020	2	2020
Key Management - Development Testing (DT) CI-3 Spiral 3 Spin 2	4	2020	4	2020
Key Management - OA CI-3 Spiral 3 Spin 2	1	2021	1	2021
Cybersecurity - Systems Engineering & Development of Cybersecurity Services	1	2015	4	2021

Exhibit R-2A, RDT&E Project Justification: PB 2017 Navy											Date: February 2016	
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 2015**	**FY 2016**	**FY 2017 Base**	**FY 2017 OCO**	**FY 2017 Total**	**FY 2018**	**FY 2019**	**FY 2020**	**FY 2021**	**Cost To Complete**	**Total Cost**
3230: *Information Assurance*	10.494	3.882	2.128	1.523	-	1.523	2.399	2.373	2.217	2.264	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 2017 Navy		Date: February 2016
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.

FY17 : 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 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total
Title: Information Assurance (IA)	3.882	2.128	1.523	0.000	1.523
Articles:	-	-	-	-	-
FY 2015 Accomplishments: Continued the development of a security framework for mobile communication devices. The framework emphasized 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. Completed at a reduced level of effort the development of new network security technology focused on addressing nation state level sponsored activity. Completed at a reduced level of effort the development of enabling technology building blocks for identity management and secure data storage, processing and exchange. Completed the Weaselboard Project used to study and assess vulnerabilities with Shipboard Supervisory Control and Data Acquisition (SCADA) information that conducts an operational demonstration on a Naval platform.					
FY 2016 Plans: Continue the development of new sensing and instrumentation technology to measure the effectiveness of network security technology.					

Exhibit R-2A, RDT&E Project Justification: PB 2017 Navy		Date: February 2016
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 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total
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. Complete the development of new network security technology focused on addressing nation state level sponsored activity. Enhance the security framework for federated infrastructures to support newly developed cross-domain services/devices. 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 phone and tablet devices. 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 2017 Base Plans: Continue 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. Continue the development of technology to provide prediction/early warning sensing of impending attacks based on network traffic and user behavior. Provide initial response options/actions based on sensing predictions.					

Exhibit R-2A, RDT&E Project Justification: PB 2017 Navy		Date: February 2016
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 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total
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. Adapt the solution for other candidate platforms in support of mission requirements. 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 development of new sensing and instrumentation technology to measure the effectiveness/provide metrics of network security technology against nation state adversaries. Initiate the development of a new techniques/technology for discovering adversarial presence in Navy/DoD networks, especially for advanced persistent threats (APT) within the network infrastructure and components/ workstations. Efforts will focus on detection, isolation and remediation. ***FY 2017 OCO Plans:*** N/A					
Accomplishments/Planned Programs Subtotals	3.882	2.128	1.523	0.000	1.523

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 2017 Navy			Date: February 2016
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)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2015 Cost	FY 2015 Award Date	FY 2016 Cost	FY 2016 Award Date	FY 2017 Base Cost	FY 2017 Base Award Date	FY 2017 OCO Cost	FY 2017 OCO Award Date	FY 2017 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Development Support	Various	NRL : Washington, DC	10.494	3.882	Nov 2014	2.128	Nov 2015	1.523	Nov 2016	-		1.523	Continuing	Continuing	Continuing
		Subtotal	10.494	3.882		2.128		1.523		-		1.523	-	-	-

	Prior Years	FY 2015		FY 2016		FY 2017 Base		FY 2017 OCO		FY 2017 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	10.494	3.882		2.128		1.523		-		1.523	-	-	-

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2017 Navy		Date: February 2016
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 3230 / *Information Assurance*

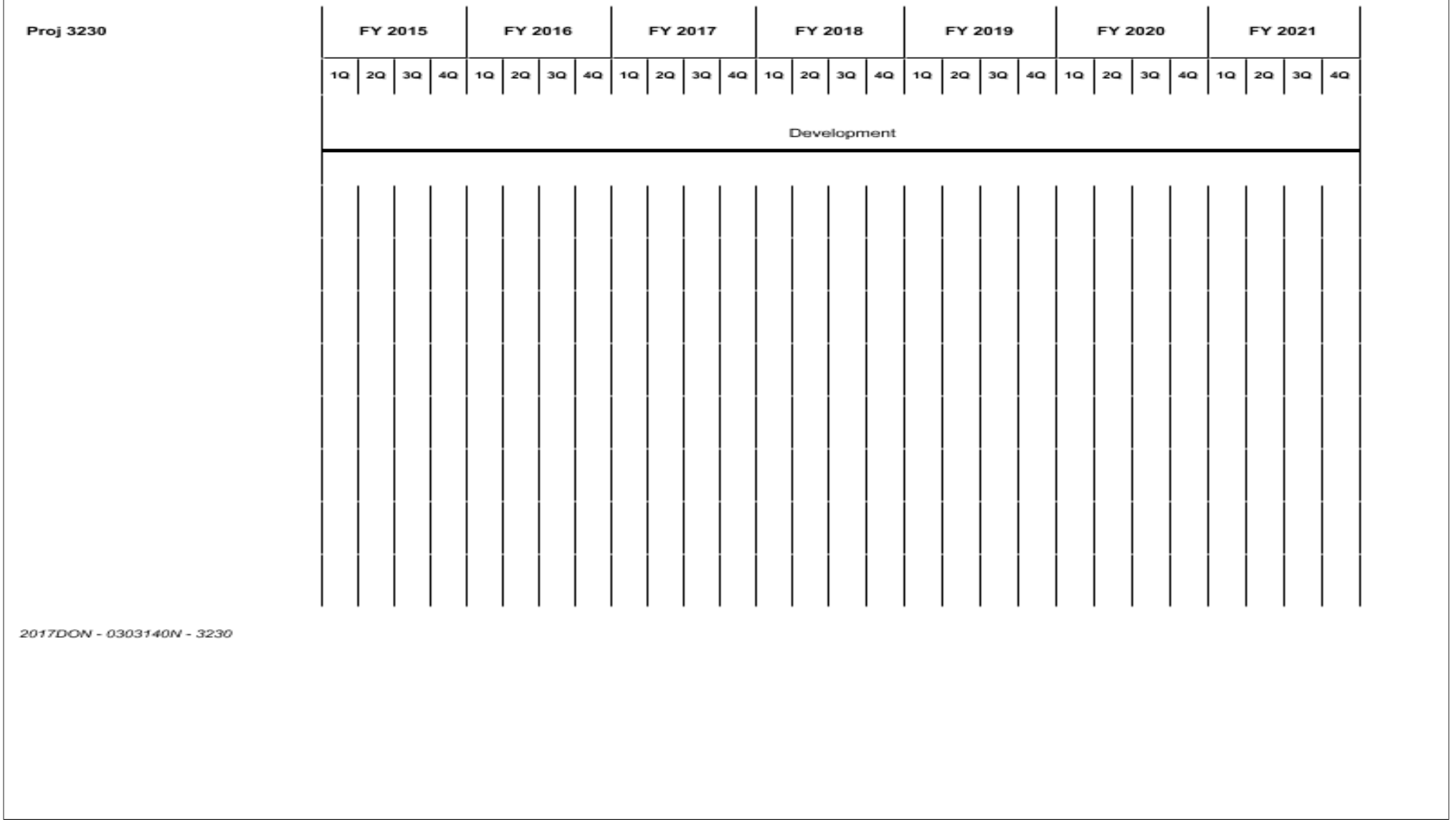


Exhibit R-4A, RDT&E Schedule Details: PB 2017 Navy		Date: February 2016
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 3230 / *Information Assurance*

Schedule Details

	Start		End	
Events by Sub Project	**Quarter**	**Year**	**Quarter**	**Year**
Proj 3230				
Development	1	2015	4	2021

THIS PAGE INTENTIONALLY LEFT BLANK