Exhibit R-2, RDT&E Budget Item Justification: FY 2018 Navy											Date: May 2017	
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 2016**	**FY 2017**	**FY 2018 Base**	**FY 2018 OCO**	**FY 2018 Total**	**FY 2019**	**FY 2020**	**FY 2021**	**FY 2022**	**Cost To Complete**	**Total Cost**
Total Program Element	393.106	29.491	38.510	50.269	-	50.269	53.013	49.927	45.859	39.056	Continuing	Continuing
0734: *Communications Security R&D*	378.730	27.371	36.987	47.854	-	47.854	50.623	47.697	43.585	36.738	Continuing	Continuing
3230: *Information Assurance*	14.376	2.120	1.523	2.415	-	2.415	2.390	2.230	2.274	2.318	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. The ISSP will extend cybersecurity and resiliency by addressing the acquisition and modernization of our platforms, systems, and information technology networks; by instituting quality assurance programs to protect critical warfighting capabilities to sustain the readiness of our cyber programs and systems. The ISSP cyberspace programs include wired and wireless telecommunications systems, Information Technology (IT) systems, and the content processed, stored, or transmitted therein. Cyberspace operations include both defensive and offensive measures, which preserve the ability to utilize friendly cyberspace capabilities; protect data, networks, net-centric capabilities, and other designated systems; and project power by the application of force in or through cyberspace. An attack, via cyberspace, targets an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. 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. The ISSP provides architectures, products, and services based on mission impacts, cybersecurity threats, information criticality, vulnerabilities, and required defensive countermeasure capabilities.

The ISSP focuses on efforts that address the risk management of cyberspace, which provides 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, Navy (NC3-N) 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 and cyber security tools; (2) technologies supporting the Navy's Computer Network Defense (CND) service provider that will accelerate the Navy's ability to prevent, constrain, and mitigate cyber attacks and critical vulnerabilities; (3) 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 Crypto telecommunications infrastructure and the wireless spectrum; (5) sensing cyber threats across all Navy shore and afloat networks to reduce the complexities of monitoring, assessing, and detecting adversary activities across multiple enclaves through the collection of tools in SHARKCAGE; (6) alignment to Navy's Insider Threat program; (7) assurance of joint-user cyberspace domains, using a Defense-In-Depth (DiD) security architecture and its alignment with the Joint Information Environment (JIE)/Joint Regional Security Stack (JRSS); (8) assurance technologies, including the Key Management (KM) and Public Key Infrastructure (PKI).

FY18 increase aligns to the following capabilities in support of National Defense due to recent cybersecurity threats:

Exhibit R-2, RDT&E Budget Item Justification: FY 2018 Navy	Date: May 2017
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*

(1) Modernize Navy Cryptography common software for Transmission Security (TRANSEC), including the KGV-11M crypto core, based on the THORNTON TRANSEC Algorithm Modernization (TTAM). Specification algorithm modernization is mandated by Chairman of the Joint Chiefs of Staff Instruction (CJCSN) 6510 to meet mandated National Security Agency (NSA) cease key dates. The TRANSEC algorithm modernization mandate protects critical UHF circuits from unauthorized access, spoofing, and denial of service.

(2) Accelerate SHARKCAGE development efforts to provide Defensive Cyberspace Operations (DCO) forces with the ability to detect adversary activities and analyze cyber attacks against Navy networks via protected, isolated networks, and integrate intelligence and Navy data to assess potential cyber threats. DCO are passive and active cyberspace defense activities that allow us to outmaneuver an adversary. SHARKCAGE will provide the capability to analyze active cyber threats and take actions to contain/stop threat activities. The data that is collected and analyzed via SHARKCAGE will be presented and visualized via the NCSA capability.

(3) Accelerate NCSA development activities that provide Navy forces near real-time cyber risk and readiness information of Navy networks and their associated mission impacts across the Navy enterprise as an enabler of assured Command and Control (C2). NCSA will also be able to receive cyber threat analysis from SHARKCAGE. As a result, operational level of war cyber situational awareness will be provided to Fleet Cyber Command (FCC) and Navy Geographic Maritime Operations Centers (MOC) through visualization capabilities via web-accessible cyber Common Operational Pictures (COP) established through the correlation of relevant cyber data sources; combining asset data, baseline configuration data, event data, and real-time threat data critical for defending Navy networks and Navy network infrastructure.

(4) Increase in Information Assurance supports investment in efforts to improve effectiveness of cyber defenses and critical infrastructure protection, and adequately fund continuing efforts. Increased investment in cyber defense includes programs addressing asset criticality and management and a new generation of cross-domain technology that focuses on critical infrastructure protection.

B. Program Change Summary ($ in Millions)	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total
Previous President's Budget	28.081	38.510	39.701	-	39.701
Current President's Budget	29.491	38.510	50.269	-	50.269
Total Adjustments	1.410	0.000	10.568	-	10.568
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	2.002	0.000			
• SBIR/STTR Transfer	-0.592	0.000			
• Program Adjustments	0.000	0.000	9.643	-	9.643
• Rate/Misc Adjustments	0.000	0.000	0.925	-	0.925

Change Summary Explanation

TECHNICAL:

Exhibit R-2, RDT&E Budget Item Justification: FY 2018 Navy	Date: May 2017
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*

Computer Network Defense (CND):
- Begin development, integration, and testing of Navy's Insider Threat program capabilities in order to fulfill the Presidential, Department of Defense (DoD), and Department of Navy (DoN) directives to reduce the risk of Insider Threats as well as provide enhancements to the Vulnerability Remediation Asset Manager (VRAM) to improve DoD cyber readiness.

Navy Cryptography (Crypto):
- Modernize KGV-11 to support National Security Agency (NSA) mandated cryptographic modernization, which provides for secure access to the Ultra High Frequency (UHF) Demand Assigned Multiple Access (DAMA) network.

Key Management (KM):
- Key Management Infrastructure (KMI) Capability Increment (CI)-2 Spiral 2/Spin 4 capabilities has been programmatically realigned from KMI CI-2 to KMI CI-3 per NSA.

SHARKCAGE & Navy Cyber Situational Awareness (NCSA):
- SHARKCAGE and NCSA development efforts previously budgeted under CND have been broken out for greater visibility into cybersecurity.

SCHEDULE:

CND:
- Due to the dynamic nature of cybersecurity and increasing complexity of technology CND builds were adjusted to include various cybersecurity/remediation capabilities to include Joint Regional Security Stack (JRSS), the Navy's Insider Threat Program as well as cybersecurity enhancements to the VRAM capability to improve DoD cyber readiness.

Crypto:
- VINSON/Advanced Narrowband Digital Voice Terminal (ANDVT) Cryptographic Modernization (VACM) Full Rate Production (FRP) decision was achieved in 3QFY16 in accordance with the revised United States Air Force (USAF) schedule.

- VACM Initial Operational Capability (IOC) accelerated from 4QFY16 to 3QFY16 due to the installations of operational Low Rate Initial Production (LRIP) devices on Nuclear Command, Control, and Communications, Navy (NC3-N) circuits and was achieved in 3QFY16.

- Transmission Security (TRANSEC) studies and analysis completion accelerated from 4QFY16 to 2QFY16 to prepare for NSA release of THORNTON TRANSEC Algorithm Modernization (TTAM) specifications in 3QFY16.

- TRANSEC Development and Product Testing extended from 4QFY19 to 3QFY20 to meet fielding requirements in accordance with national mandates.

- Advanced Cryptographic Capability (ACC) Solutions Development and Product Tests extended from 4QFY19 to 4QFY22 to meet fielding requirements in accordance with national mandates.

- KGV-11M key milestones added in accordance with the development schedule to support NSA mandated cryptographic modernization.

KM:
- KMI CI-2 Development updated to reflect development of Spiral 1 though Spiral 3 in accordance with NSA's schedule.

- KMI CI-2 Spiral 2 Spin 2 Fielding Decision (FD) updated from 4QFY16 to 4QFY17 in accordance with NSA's schedule.

- KMI CI-2 Spiral 2 Spin 3 FD removed in accordance with NSA's schedule.

- KMI CI-2 Spiral 2 Spin 4 Developmental Testing (DT), Operational Assessment (OA), and FD removed in accordance with NSA's schedule. KMI CI-2 Spiral 2 Spin 4 capability has been programmatically realigned from KMI CI-2 to KMI CI-3.

- KMI CI-2 Spiral 2 Full Deployment Decision (FDD) updated from 4QFY17 to 2QFY18 in accordance with NSA's schedule.

- KMI CI-2 Spiral 2 Spin 2, CI-2 Spiral 2 Spin 3, and CI-3 DT and OA events have been incorporated into Development, Integration, and Test cycles.

SHARKCAGE & NCSA:
- SHARKCAGE and NCSA development efforts previously budgeted under CND have been broken out for greater visibility into cybersecurity.

- SHARKCAGE and NCSA are planned Rapid Deployment Capability's (RDC). An RDC is the Navy's implementation of the Department of Defense (DoD) 5000 defined "Accelerated Acquisition Program." It provides the ability to react immediately to a newly discovered enemy threat(s) or potential enemy threat(s) through tailored procedures, to allow for fielding of mature capabilities based on Commercial Off-The-Shelf (COTS) and Non-Developmental Item (NDI) products within a two year period. At the end of that period SHARKCAGE and NCSA are planned to transition to respective ACAT programs.

FUNDING:

CND:
- SHARKCAGE and NCSA development efforts previously budgeted under CND have been broken out for greater visibility into cybersecurity.

- Additional funding provided for cybersecurity enhancements for VRAM to improve DoD cyber readiness.

Exhibit R-2, RDT&E Budget Item Justification: FY 2018 Navy	Date: May 2017
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*

Crypto:
- Increase in FY18 will develop and implement common software for TRANSEC modernization, including the KGV-11M crypto core, based on the TTAM. Specification algorithm modernization is mandated by Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510 to meet mandated NSA cease key dates. The TRANSEC algorithm modernization mandate protects critical UHF circuits from unauthorized access, spoofing, and denial of service.

SHARKCAGE:
- SHARKCAGE development efforts previously budgeted under CND have been broken out for greater visibility into cybersecurity.

- Increase in FY18 will accelerate SHARKCAGE development efforts to provide Defensive Cyberspace Operations (DCO) forces with the ability to detect adversary activities and analyze cyber attacks against Navy networks via protected, isolated networks, and integrate intelligence and Navy data to assess potential cyber threats. SHARKCAGE will provide the capability to analyze active cyber threats and take actions to contain/stop threat activities. The data that is collected and analyzed via SHARKCAGE will be presented and visualized via the NCSA capability.

NCSA:
- NCSA development efforts previously budgeted under CND have been broken out for greater visibility into cybersecurity.

- Increase in FY18 will accelerate NCSA development activities that provide Navy forces near real-time cyber risk and readiness information of Navy networks and their associated mission impacts across the Navy enterprise as an enabler of assured Command and Control (C2). NCSA will be able to receive cyber threat analysis from SHARKCAGE. As a result, operational level of war cyber situational awareness will be provided to Fleet Cyber Command (FCC) and Navy Geographic Maritime Operations Centers (MOC) through visualization capabilities via web-accessible cyber Common Operational Pictures (COP) established through the correlation of relevant cyber data sources; combining asset data, baseline configuration data, event data, and real-time threat data critical for defending Navy networks and Navy network infrastructure.

The FY 2018 funding request was reduced by $2.313 million to account for the availability of prior year execution balances.

Exhibit R-2A, RDT&E Project Justification: FY 2018 Navy											Date: May 2017	
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 2016**	**FY 2017**	**FY 2018 Base**	**FY 2018 OCO**	**FY 2018 Total**	**FY 2019**	**FY 2020**	**FY 2021**	**FY 2022**	**Cost To Complete**	**Total Cost**
0734: *Communications Security R&D*	378.730	27.371	36.987	47.854	-	47.854	50.623	47.697	43.585	36.738	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 extend our cybersecurity and resiliency, provide Defensive Cyberspace Operations (DCO), and cross domain solutions to protect data, Department of Defense information networks (DoDIN), net-centric operations, the forward deployed, and other designated systems in order to protect cyberspace and critical warfighting capabilities.

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 keys, 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).

Computer Network Defense (CND): The CND program provides cyberspace capabilities to secure the Cyber Domain. CND is a combination of hardware, software, sets of processes and protective measures that use computer networks to detect, monitor, protect, analyze and defend against network infiltrations resulting in service/ network denial, degradation and disruptions. CND enables a government or military institute/organization to defend against network attacks perpetrated by malicious or adversarial computer systems or networks.

Navy Cryptography (Crypto): Navy Crypto modernizes legacy cryptographic equipment which includes families of COMSEC and TRANSEC devices that are divided into crypto voice, crypto data, crypto products and associated ancillary devices. These devices provide modern cryptographic solutions to replace obsolete, legacy devices within the crypto categories.

Key Management (KM): KM monitors and tracks capability verification testing, as well as designs and tests capabilities to provide a net-centric, web based architecture for the ordering, management and distribution of all cryptographic key material to support Navy users, to include integration of Intermediary Application (iApp).

Public Key Infrastructure (PKI): The DoD PKI program, under the authority of the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD AT&L), develops and tests PKI equipment and is responsible for meeting statutory and regulatory requirements for the DoD PKI program. The Navy PKI program tests and implements products for afloat and shore non-Navy Marine Corps Intranet (NMCI) networks and institutionalizes Identity and Access Management (IdAM) so that person and non-person entities can securely access all authorized DoD resources.

Exhibit R-2A, RDT&E Project Justification: FY 2018 Navy		Date: May 2017
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*

SHARKCAGE: SHARKCAGE is a global, federated DCO enclave consisting of shore sensor nodes, DCO analysis workbenches, and analytic nodes. Utilizing one-way passive taps in a protected, isolated, classified environment, SHARKCAGE consolidates cyber event data from multiple platforms and networks, providing Navy DCO forces with a shared environment and common platform for integrated workflow, collaboration, and analysis. SHARKCAGE efficiently detects, correlates, and analyzes nation and non-nation state attacks against maritime Navy networks and the Naval Networking Environment (NNE).

Navy Cyber Situational Awareness (NCSA): NCSA is a command and control infrastructure that provides Navy commanders with timely, trusted, and comprehensive Situational Awareness (SA) of the cyberspace domain to include tailored, near real-time visualization of network health, vulnerabilities, and operational readiness through the correlation of data from multiple sources. NCSA combines asset data, baseline configuration data, and real-time threat data - critical for defending a fully-interconnected network infrastructure. NCSA enables early threat detection and timely decision making.

Cybersecurity Services: Cybersecurity Services develop cyber architecture and provides cybersecurity engineering for the DoD and Department of the Navy (DoN) cybersecurity interests based on the requirements prioritized by Fleet Cyber Command/Commander Tenth Fleet (FCC/C10F). Cybersecurity Services transitions new technologies to address current Navy cybersecurity challenges.

The ISSP focuses on efforts that address the risk management of cyberspace, which provides capabilities to protect, detect, restore and respond. The ISSP provides the Navy with the following cybersecurity elements: (1) defense of National Security Systems and Information (NSSI), including the Nuclear Command, Control, and Communications, Navy (NC3-N) 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 and cyber security tools; (2) technologies supporting the Navy's CND service provider that will accelerate the Navy's ability to prevent, constrain, and mitigate cyber attacks and critical vulnerabilities; (3) 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 Crypto telecommunications infrastructure and the wireless spectrum; (5) sensing cyber threats across all Navy shore and afloat networks to reduce the complexities of monitoring, assessing, and detecting adversary activities across multiple enclaves through the collection of tools in SHARKCAGE; (6) alignment to Navy's Insider Threat program; (7) assurance of joint-user cyberspace domains, using a Defense-In-Depth (DiD) security architecture and its alignment with the Joint Information Environment (JIE)/Joint Regional Security Stack (JRSS); (8) assurance technologies, including KM and PKI.

FY18 increase aligns to the following capabilities in support of National Defense due to recent cybersecurity threats:

(1) Modernize Navy Cryptography common software for Transmission Security (TRANSEC), including the KGV-11M crypto core, based on the THORNTON TRANSEC Algorithm Modernization (TTAM). Specification algorithm modernization is mandated by Chairman of the Joint Chiefs of Staff Instruction (CJCSN) 6510 to meet mandated National Security Agency (NSA) cease key dates. The TRANSEC algorithm modernization mandate protects critical UHF circuits from unauthorized access, spoofing, and denial of service.

(2) Accelerate SHARKCAGE development efforts to provide DCO forces with the ability to detect adversary activities and analyze cyber attacks against Navy networks via protected, isolated networks, and integrate intelligence and Navy data to assess potential cyber threats. DCO are passive and active cyberspace defense activities

that allow us to outmaneuver an adversary. SHARKCAGE will provide the capability to analyze active cyber threats and take actions to contain/stop threat activities. The data that is collected and analyzed via SHARKCAGE will be presented and visualized via the NCSA capability.

(3) Accelerate NCSA development activities that provide Navy forces near real-time cyber risk and readiness information of Navy networks and their associated mission impacts across the Navy enterprise as an enabler of assured Command and Control (C2). NCSA will also be able to receive cyber threat analysis from SHARKCAGE. As a result, operational level of war cyber situational awareness will be provided to FCC and Navy Geographic Maritime Operations Centers (MOC) through visualization capabilities via web-accessible cyber Common Operational Pictures (COP) established through the correlation of relevant cyber data sources; combining asset data, baseline configuration data, event data, and real-time threat data critical for defending Navy networks and Navy network infrastructure.

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total
Title: Computer Network Defense (CND)	17.290	24.190	14.039	0.000	14.039
Articles:	-	-	-	-	-

FY 2016 Accomplishments:
Continued to develop Task Force Cyber Awakening (TFCA), specifically Navy Cyber Situational Awareness (NCSA) and Operation Rolling Tide (ORT)/Cyber Remediation initiatives. Funding provided additional capabilities within the Navy's Computer Network Defense (CND) program in order to accelerate advanced cybersecurity initiatives to achieve improved network defense and security wholeness. Additional capabilities included network vulnerability remediation, security compliance reporting, mapping of Navy networks in order to automate real time cybersecurity capabilities critical to the warfighter and to support Command and Control (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. 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 afloat platforms. Continued to develop new capabilities for the Navy's C2 architecture and provide 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 mandates into ONE-Net and Command, Control, Communications, Computers and Intelligence (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) and Continuous Monitoring Risk Score (CMRS) capabilities. Continued to develop and implement an optimal technical and governance solution for interception of outbound encrypted traffic. Continued integration and testing of Secure Socket Layer (SSL) intercept to achieve compliance with DISA firewall security guidance. Furthered efforts to virtualize CND capabilities and consolidate cybersecurity services in the ONE-Net environment. Continued analysis to replace and assume acquisition management of

Exhibit R-2A, RDT&E Project Justification: FY 2018 Navy		Date: May 2017
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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total
Navy Cyber Defense Operations Command's (NCDOC) tactical sensor infrastructure. Continued to support Fleet Cyber Command / Commander Tenth Fleet's (FCC/C10F) NCSA efforts by deploying integrated tools at the C10F Maritime Operations Center (MOC) to support C2 of the communications systems. Continue to develop Joint Capability Technology Demonstration (JCTD) Virtual Secure Enclave (VSE) to segment networks and adaptively manage operational risks. ***FY 2017 Plans:*** Continue to develop Navy's portion of the Nuclear Command, Control, and Communications, Navy (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. Non-classified Internet Protocol (IP) Router Network (NIPRNet), Secret Internet Protocol Router Network (SIPRNet), C4I, Combat Systems, Hull Mechanical & Electrical (HM&E), etc.). Additionally, funding was 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 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 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 2018 Base Plans:*** SHARKCAGE and NCSA development efforts previously budgeted under CND have been broken out for greater visibility into cybersecurity.					

Exhibit R-2A, RDT&E Project Justification: FY 2018 Navy		Date: May 2017
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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total
Continue to develop Navy's portion of the NC3-N and BMD cyber security system of systems within the CND architecture. 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 enhancing the VRAM tool per FCC/C10F and Naval Information Forces (NAVIFOR) requirements, to include Security Technical Implementation Guides (STIG) Reporting Integration, web services to share data between VRAM, cyber readiness databases and mission support systems to improve DoD cyber readiness. Continue to evaluate needs derived from stakeholders and the CCSG, and correspondingly develop, update, and integrate CND suites. Continue to implement DoD and USCC cybersecurity tools and mandates into ONE-Net and C4I networks. Continue to provide technical guidance to support CANES deployment of new CND capabilities. Begin to optimize CND suite for alignment with Joint Regional Security Stack (JRSS), including the transition of some capabilities from the CND suite into JRSS. Continue efforts to further virtualize CND capabilities for more effective and cost-efficient deployment of cybersecurity technologies. Continue to develop, integrate, and test solution to replace and assume acquisition management of NCDOC's tactical sensor infrastructure. Begin development and alignment to Navy's Insider Threat program to identify possible insider threats across multiple enclaves in order to fulfill the Presidential, DoD, and Department of Navy (DoN) directives. ***FY 2018 OCO Plans:*** N/A					
Title: Navy Cryptography (Crypto)	5.414	7.642	11.912	0.000	11.912
Articles:	-	-	-	-	-
FY 2016 Accomplishments: Completed Transmission Security (TRANSEC) studies and analysis, delivered Analysis of Alternatives (AoA) replacement products, initiated development efforts to modernize legacy devices, and initiated developmental testing. Continued to provide development and security engineering for modernization of Department of the Navy (DoN) crypto systems and embeddable crypto modernization strategies. Continued to work with National Security Agency (NSA) on certification authority, acquisition authority and data testing for all crypto modernization efforts. Continued to investigate impacts of upcoming NSA security enhancements for crypto modernization products. Initiated Advanced Cryptographic Capabilities (ACC) solutions development and testing across multiple products. Achieved VINSON/Advanced Narrowband Digital Voice Terminal (VACM) Full Rate					

Exhibit R-2A, RDT&E Project Justification: FY 2018 Navy		Date: May 2017
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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total
Production (FRP) decision. Achieved VACM Initial Operational Capability (IOC). Continued modernization of VACM ancillary devices. ***FY 2017 Plans:*** Accelerate TRANSEC replacement product development and continue developmental testing. Continue to provide development and security engineering for modernization of DoN crypto systems and embeddable crypto modernization strategies. Continue to work with NSA on 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 solutions 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 2018 Base Plans:*** Increase in FY18 will modernize common software for Transmission Security (TRANSEC), including the KGV-11M crypto core, based on the THORNTON TRANSEC Algorithm Modernization (TTAM). Specification algorithm modernization is mandated by Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510 to meet mandated NSA cease key dates. The TRANSEC algorithm modernization mandate protects critical UHF circuits from unauthorized access, spoofing, and denial of service. Complete contract award for development of KGV-11M TRANSEC End Cryptographic Units (ECU). Develop a transition plan for TRANSEC and ACC-based devices to support crypto modernization. Continue TRANSEC replacement product development and continue developmental testing, focusing on the KGV-11M device. Continue to provide development and security engineering for modernization of DoN crypto systems and embeddable crypto modernization strategies. Continue to work with NSA on 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 solutions development and testing across multiple products. Conduct test and evaluation on new software capabilities for crypto modernization products. Continue modernization of VACM ancillary devices. Continue to develop Navy strategy and implementation plan to modernize secure voice architectures within Navy networks. ***FY 2018 OCO Plans:*** N/A					
Title: Key Management (KM)	2.229	2.363	2.230	0.000	2.230
Articles:	-	-	-	-	-
FY 2016 Accomplishments:					

Exhibit R-2A, RDT&E Project Justification: FY 2018 Navy		Date: May 2017
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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total
Continued Key Management Infrastructure (KMI) Capability Increment (CI)-2 Spiral 2/Spin 2 verification testing to include vendor Development Testing (DT) and Operational Assessment (OA). Completed Spiral 2/Spin 3 capability engineering and development. Continued to define capability requirements for KMI CI-3 and KMI Tech Refresh. Continued migrating Communications Security (COMSEC) Management Workstation (CMWS) and the follow on to Simple Key Loader (SKL) into the KMI environment. Continued the development, engineering, and testing of the Intermediary Application (iApp) which enhances the accounting for and distribution of KMI key delivery. ***FY 2017 Plans:*** Achieve KMI CI-2 Spiral 2/Spin 2 fielding Decision (FD). Continue verification testing to include vendor DT and OA in support of KMI CI-2 Spiral 2/Spin 3. Continue to define capability requirements for KMI CI-3. Continue migrating CMWS and the follow on to SKL into the KMI environment. Continue the development, engineering, and testing of iApp, which will enhance the accounting for and distribution of KMI key delivery. Complete the development, engineering and testing of KMI Tech Refresh. ***FY 2018 Base Plans:*** Achieve Full Operational Test & Evaluation (FOT&E) and Full Deployment Decision (FDD) for KMI Spiral 2. Continue migrating COMSEC CMWS and the follow on to SKL into the KMI environment. Initiate the development, engineering, and testing of KMI CI-3, including the integration of the iApp within a network environment, which will enhance the accounting for and distribution of KMI key delivery. ***FY 2018 OCO Plans:*** N/A					
Title: Public Key Infrastructure (PKI)	0.354	0.350	0.360	0.000	0.360
Articles:	-	-	-	-	-
FY 2016 Accomplishments: Continued Navy compliance and compatibility with Department of Defense (DoD) Public Key Infrastructure (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 the Non-classified Internet Protocol Router Network (NIPRNet) Enterprise Alternate Token System (NEATS), and continue researching tools to support certificates for Non-Person Entity (NPE). Continued researching and testing PKI authentication capabilities to support mobile devices, Identity and Access Management (IdAM) in tactical/austere environments,					

Exhibit R-2A, RDT&E Project Justification: FY 2018 Navy		Date: May 2017
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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total
increased information security and began Real-time Automated Personnel Identification System (RAPIDS) Operating Systems (OS) testing. ***FY 2017 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 2018 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 2018 OCO Plans:*** N/A					
Title: SHARKCAGE ***Articles:*** ***FY 2016 Accomplishments:*** N/A ***FY 2017 Plans:*** N/A ***FY 2018 Base Plans:*** SHARKCAGE development efforts were previously budgeted under Computer Network Defense (CND); funding broken out for greater visibility into cybersecurity. Increase in FY18 will accelerate SHARKCAGE development efforts to provide Defensive Cyber Operations (DCO) forces with the ability to detect adversary activities and analyze cyber attacks against Navy networks via protected, isolated networks, and integrate intelligence and Navy data to assess potential cyber threats. SHARKCAGE will provide the capability to analyze active cyber threats and take actions to contain/stop threat activities. The data that is collected and analyzed via SHARKCAGE is presented and visualized via the Navy Cyber Situational Awareness (NCSA) capability. Continue development of SHARKCAGE DCO enclave to	0.000 -	0.000 -	8.973 -	0.000 -	8.973 -

Exhibit R-2A, RDT&E Project Justification: FY 2018 Navy		Date: May 2017
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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total
address new requirements from the fleet in light of emerging threats in the tactical environment. Development efforts include network taps, sensors, and analytic toolsets for passively monitoring multiple Navy shore and afloat networks and enclaves (e.g., Command, Control, Communications, Computers and Intelligence (C4I) networks, Combat Systems (CS), Hull, Mechanical, and Electrical (HM&E), etc.) to detect and assess cyber threats across multiple security enclaves. Continue development of event collection and analysis components for shore sensor nodes and afloat flyaway kits for deployed Cyber Protection Teams (CPT). ***FY 2018 OCO Plans:*** N/A					
Title: Navy Cyber Situational Awareness (NCSA) ***Articles:*** ***FY 2016 Accomplishments:*** N/A ***FY 2017 Plans:*** N/A ***FY 2018 Base Plans:*** Navy Cyber Situational Awareness (NCSA) development efforts were previously budgeted under Computer Network Defense (CND); funding broken out for greater visibility into cybersecurity. Increase in FY18 will accelerate NCSA development activities that provide Navy forces near real-time cyber risk and readiness information of Navy networks and their associated mission impacts across the Navy enterprise as an enabler of assured Command and Control (C2). NCSA receives cyber threat analysis from SHARKCAGE. As a result, operational level of war cyber situational awareness will be provided to Fleet Cyber Command (FCC) and Navy Geographic Maritime Operations Centers (MOC) through visualization capabilities via web-accessible cyber Common Operational Pictures (COP) established through the correlation of relevant cyber data sources; combining asset data, baseline configuration data, event data, and real-time threat data critical for defending Navy networks and Navy network infrastructure. Continue development and maturation of NCSA capabilities to address new requirements from the fleet in light of emerging threats in the tactical environment. Development efforts will include the integration of all-source intelligence with Navy maritime data to enable early threat detection, and assessment of adversary activities and capabilities, intent, and access to critical Navy networks. NCSA development efforts will provide a shared and tailorable Maritime Cyber "Integrated" COP external to FCC/C10F beginning with Commander, Pacific Fleet (COMPACFLT) MOC to enable assessments	0.000 -	0.000 -	7.840 -	0.000 -	7.840 -

Exhibit R-2A, RDT&E Project Justification: FY 2018 Navy		Date: May 2017
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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total
of cyber vulnerabilities, threats, and risks relative to Ballistic Missile Defense (BMD) and Nuclear Command, Control, and Communications, Navy (NC3-N) missions. NCSA's maturation will provide for monitoring of relevant and current Navy networks providing near real-time visualization and analytics of the cyberspace domain. ***FY 2018 OCO Plans:*** N/A					
Title: Cybersecurity Services	2.084	2.442	2.500	0.000	2.500
Articles:	-	-	-	-	-
FY 2016 Accomplishments: Continued to provide security systems engineering support for the development of Department of Defense (DoD) and Department of the Navy (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 System 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 of the Continental United States (OCONUS) networks. Continued to provide cybersecurity risk analysis and recommended risk mitigation strategies for Navy critical networks and Command, Control, Communications, Computers and Intelligence (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 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 2017 Plans:*** Begin coordination with Joint Information Environment (JIE) (e.g., Joint Regional Security Stack (JRSS), Joint Management System (JMS), etc.) 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					

Exhibit R-2A, RDT&E Project Justification: FY 2018 Navy		Date: May 2017
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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total
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 2018 Base Plans:*** Continue coordination and alignment with JIE (e.g., JRSS, JMS, etc.) 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 2018 OCO Plans:*** N/A					
Accomplishments/Planned Programs Subtotals	27.371	36.987	47.854	0.000	47.854

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
• OPN/3415: *Info Sys Security Program (ISSP)*	126.237	85.694	89.663	-	89.663	128.177	155.401	166.705	165.946	Continuing	Continuing

Remarks

D. Acquisition Strategy

Computer Network Defense (CND): The CND Acquisition Category (ACAT) IVT program is a layered protection strategy, which militarizes Commercial Off-The-Shelf (COTS) and integrates Government Off-The-Shelf (GOTS) hardware and software products that collectively provide an effective network security infrastructure. The rapid advancement of cyber technology requires an efficient process for updating CND tools deployed to afloat and shore platforms. Recognizing the need for future

Exhibit R-2A, RDT&E Project Justification: FY 2018 Navy		Date: May 2017
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*

CND capability improvements, the CND program 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 mandate by Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510 as well as the National Security Agency (NSA) planned decertification, which improves the Navy's cyber defense posture. For Advanced Cryptographic Capability (ACC) the acquisition strategy will follow the NSA direction on mandated software upgrades. The planned KGV-11M program will be led by the Navy.

Key Management (KM): Key Management Infrastructure (KMI) is a NSA-led 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 the Intermediary Application (iApp) as a KM solution.

Public Key Infrastructure (PKI): Department of Defense (DoD) PKI is an ACAT I program jointly led by the NSA and the Defense Information Systems Agency (DISA). The Under Secretary of Defense for Acquisition, Technology and Logistics (USD AT&L) is 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), Outside the Continental United States (OCONUS) networks and other excepted networks.

SHARKCAGE: The planned SHARKCAGE Rapid Deployment Capability (RDC) effort will integrate COTS and GOTS hardware and software products to monitor multiple Navy networks and enclaves to detect, analyze, and assess threats. SHARKCAGE will provide Navy Cyber Defense Operations Command (NCDOC), Navy Information Operations Centers (NIOC), Fleet Cyber Command/Commander Tenth Fleet (FCC/C10F), Cyber Protection Teams (CPT), and other Computer Network Defense (CND) deployers with a global Defensive Cyberspace Operations (DCO) enclave to monitor the Naval Networking Environment (NNE) and maritime Navy networks, including Navy shore sites and afloat platforms conducting Ballistic Missile Defense (BMD) and Nuclear Command, Control, and Communications, Navy (NC3-N) missions.

Navy Cyber Situational Awareness (NCSA): The planned NCSA RDC effort will integrate COTS and GOTS hardware and software products to provide visualization of Navy networks and enclaves to analyze and assess mission threats. NCSA will be implemented via an evolutionary acquisition approach using an iterative, agile software enhancement process in the form of capability drops to address future cyber Situation Awareness (SA) capabilities and improvements required by fleet warfighters. These government-led agile software enhancements will be documented and managed through a requirements governance board process.

Cybersecurity Services: Cybersecurity Services is a Navy project, which develops cyber architecture and provides security engineering for the DoD and Department of the Navy (DoN) cybersecurity interests based on the requirements prioritized by FCC/C10F. Cybersecurity Services transitions new technologies to address current Navy cybersecurity challenges.

E. Performance Metrics

Computer Network Defense (CND):

Exhibit R-2A, RDT&E Project Justification: FY 2018 Navy		Date: May 2017
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*

* 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.

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 Naval Information Forces (NAVIFOR) 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 requirements 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 two legacy cryptographic devices with one modern device, where possible, identify, and implement modern small form factor, multi-channel cryptography devices.

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.
* Incorporate 100% of the Communication Security (COMSEC) Manager Workstation (CMWS) requirements into the iApp baseline to meet KMI Capability Increment (CI)-2 and KMI CI-3 capabilities.

Public Key Infrastructure (PKI):
* Provide integration support to ensure Navy networks and programs of record comply with Department of Defense (DoD) PKI requirements on Non-classified Internet Protocol Router Network (NIPRNet) and Secret Internet Protocol Router Network (SIPRNet), per DoD Instruction 8520.02.
* Ensure 100% interoperability with DoD and Federal partners by researching and evaluating enhanced cryptographic algorithms and DoD PKI certificate changes.

SHARKCAGE:
* Deliver a global Defensive Cyberspace Operations (DCO) enclave that conducts monitoring and analysis of network traffic and event data to detect, correlate, and assess cyber threats to the Naval Networking Environment (NNE).
* Continue to develop and enhance SHARKCAGE capabilities in order to meet the Navy Cyber Situational Awareness Urgent Operational Need (UON) as defined by Fleet Cyber Command/Commander Tenth Fleet (FCC/C10F).

Exhibit R-2A, RDT&E Project Justification: FY 2018 Navy		Date: May 2017
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*

Navy Cyber Situational Awareness (NCSA):
* Deliver a maritime Cyber Common Operational Picture (COP) tailored to a fleet Maritime Operations Center (MOC) area of responsibility to provide operational impacts based on cyber events.
* Continue to develop and enhance NCSA capabilities in order to meet the NCSA UON as defined by FCC/C10F.

Cybersecurity Services:
* Ensure 100% interoperability and application of commercial standards compliance for ISSP products by researching and conducting selective evaluations, integrating and testing COTS/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: FY 2018 Navy		Date: May 2017
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 2016 Cost	FY 2016 Award Date	FY 2017 Cost	FY 2017 Award Date	FY 2018 Base Cost	FY 2018 Base Award Date	FY 2018 OCO Cost	FY 2018 OCO Award Date	FY 2018 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Hardware Development (WR)	WR	SSC PAC : San Diego, CA	8.975	1.001	Oct 2015	2.232	Oct 2016	2.953	Oct 2017	-		2.953	Continuing	Continuing	Continuing
Hardware Development	C/CPFF	SSC PAC : San Diego, CA	2.254	0.562	Dec 2015	0.560	Dec 2016	0.869	Dec 2017	-		0.869	Continuing	Continuing	Continuing
Hardware Development (WR)	WR	SSC LANT : Charleston, SC	4.605	0.200	Oct 2015	0.269	Oct 2016	0.570	Oct 2017	-		0.570	Continuing	Continuing	Continuing
Hardware Development	C/CPFF	SSC LANT : Charleston, SC	1.055	0.200	Dec 2015	0.504	Dec 2016	1.068	Dec 2017	-		1.068	Continuing	Continuing	Continuing
Hardware Development	FFRDC	GTRI : Atlanta, GA	0.000	0.000		3.776	Jan 2017	4.992	Jan 2018	-		4.992	Continuing	Continuing	Continuing
Hardware Development	Various	Various : Various	185.257	0.416	Oct 2015	0.000		0.000		-		0.000	0.000	185.673	-
Software Development (WR)	WR	SSC PAC : San Diego, CA	12.049	6.149	Oct 2015	6.533	Oct 2016	9.781	Oct 2017	-		9.781	Continuing	Continuing	Continuing
Software Development	C/CPFF	SSC PAC : San Diego, CA	3.295	0.400	Dec 2015	4.011	Dec 2016	5.610	Dec 2017	-		5.610	Continuing	Continuing	Continuing
Software Development (WR)	WR	SSC LANT : Charleston, SC	3.550	0.709	Oct 2015	2.253	Oct 2016	2.232	Oct 2017	-		2.232	Continuing	Continuing	Continuing
Software Development	C/CPFF	SSC LANT : Charleston, SC	3.102	2.247	Dec 2015	3.956	Dec 2016	4.138	Dec 2017	-		4.138	Continuing	Continuing	Continuing
Software Development	FFRDC	MITRE : McLean, VA	0.000	1.371	Nov 2015	1.451	Dec 2016	2.022	Dec 2017	-		2.022	Continuing	Continuing	Continuing
Software Development	Various	Various : Various	66.200	0.537	Dec 2015	0.251	Dec 2016	0.532	Dec 2017	-		0.532	Continuing	Continuing	Continuing
Software Development	C/CPFF	BAH : San Diego, CA	0.000	3.187	Dec 2015	2.539	Jan 2017	2.801	Jan 2018	-		2.801	Continuing	Continuing	Continuing
Software Development	FFRDC	GTRI : Atlanta, GA	1.442	4.786	Feb 2016	2.593	Jan 2017	2.881	Jan 2018	-		2.881	Continuing	Continuing	Continuing
Software Development	WR	NSMA : San Diego, CA	0.000	0.805	Mar 2016	1.308	Dec 2016	1.631	Dec 2017	-		1.631	Continuing	Continuing	Continuing
Software Development	WR	NRL : Washington DC	0.000	1.260	Nov 2015	0.895	Dec 2016	0.903	Dec 2017	-		0.903	Continuing	Continuing	Continuing
Software Development	MIPR	NSA : Fort Meade, MD	0.000	1.301	Feb 2016	0.000		0.000		-		0.000	0.000	1.301	-
		Subtotal	291.784	25.131		33.131		42.983		-		42.983	-	-	-

Exhibit R-3, RDT&E Project Cost Analysis: FY 2018 Navy			Date: May 2017
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 2016 Cost	FY 2016 Award Date	FY 2017 Cost	FY 2017 Award Date	FY 2018 Base Cost	FY 2018 Base Award Date	FY 2018 OCO Cost	FY 2018 OCO Award Date	FY 2018 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Architecture	WR	Various : Various	5.357	0.060	Oct 2015	0.246	Oct 2016	0.248	Oct 2017	-		0.248	Continuing	Continuing	Continuing
Architecture	WR	SSC LANT : Charleston, SC	1.246	0.325	Oct 2015	0.458	Oct 2016	0.473	Oct 2017	-		0.473	Continuing	Continuing	Continuing
Studies & Design	WR	Various : Various	5.909	0.150	Jul 2016	0.196	Oct 2016	0.415	Oct 2017	-		0.415	Continuing	Continuing	Continuing
Requirements Analysis	C/CPFF	BAH : San Diego, CA	5.494	0.157	Dec 2015	0.196	Oct 2016	0.416	Oct 2017	-		0.416	0.000	6.263	-
Systems Engineering	Various	Various : Various	3.044	0.000		0.000		0.000		-		0.000	0.000	3.044	-
		Subtotal	21.050	0.692		1.096		1.552		-		1.552	-	-	-

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2016 Cost	FY 2016 Award Date	FY 2017 Cost	FY 2017 Award Date	FY 2018 Base Cost	FY 2018 Base Award Date	FY 2018 OCO Cost	FY 2018 OCO Award Date	FY 2018 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
System DT&E	WR	SSC PAC : San Diego, CA	37.375	0.260	Nov 2015	0.330	Oct 2016	0.333	Oct 2017	-		0.333	Continuing	Continuing	Continuing
System DT&E	WR	COTF : Norfolk, VA	0.837	0.000		0.470	Dec 2016	0.729	Dec 2017	-		0.729	Continuing	Continuing	Continuing
System DT&E	C/CPFF	BAH : San Diego, CA	0.000	0.510	Dec 2015	0.850	Dec 2016	0.858	Dec 2017	-		0.858	Continuing	Continuing	Continuing
		Subtotal	38.212	0.770		1.650		1.920		-		1.920	-	-	-

Management Services ($ in Millions)

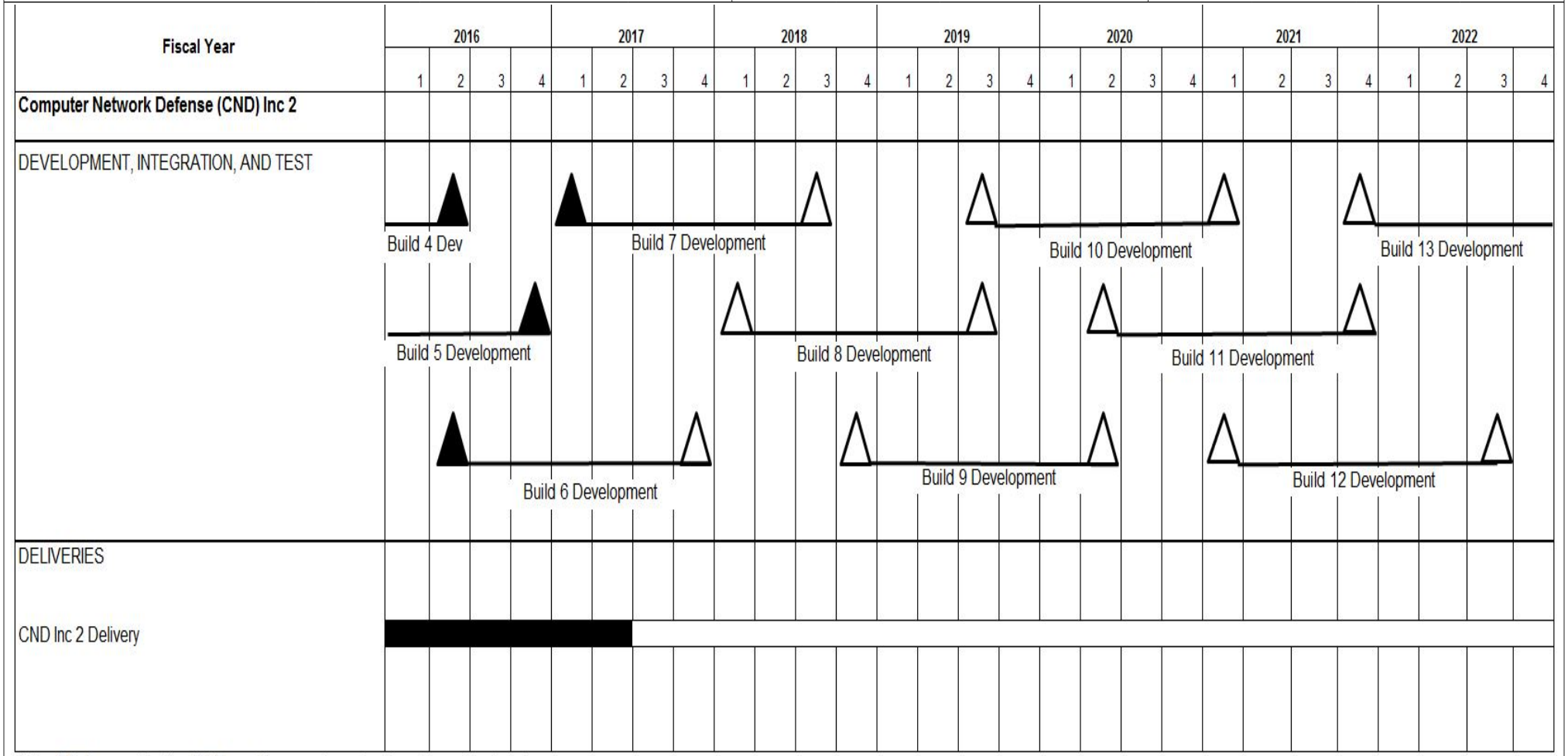
Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2016 Cost	FY 2016 Award Date	FY 2017 Cost	FY 2017 Award Date	FY 2018 Base Cost	FY 2018 Base Award Date	FY 2018 OCO Cost	FY 2018 OCO Award Date	FY 2018 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Program Management	C/CPFF	BAH : San Diego, CA	27.497	0.778	Dec 2015	1.110	Dec 2016	1.399	Dec 2017	-		1.399	Continuing	Continuing	Continuing
Travel	WR	SPAWAR : San Diego, CA	0.187	0.000		0.000		0.000		-		0.000	0.000	0.187	-
		Subtotal	27.684	0.778		1.110		1.399		-		1.399	-	-	-

Exhibit R-3, RDT&E Project Cost Analysis: FY 2018 Navy			Date: May 2017
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 2016		FY 2017		FY 2018 Base		FY 2018 OCO		FY 2018 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	378.730	27.371		36.987		47.854		-		47.854	-	-	-

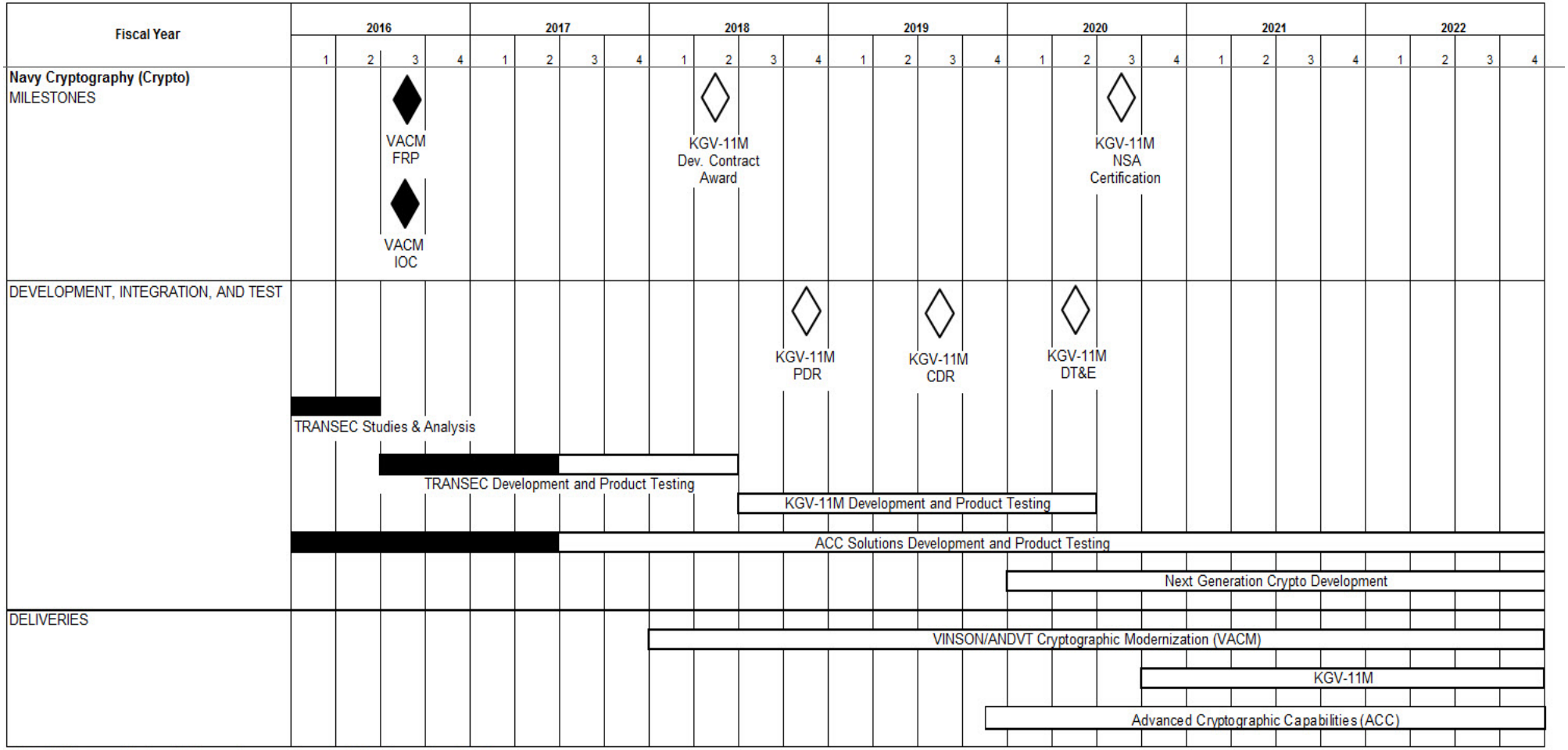
Remarks

Exhibit R-4, RDT&E Schedule Profile: FY 2018 Navy		Date: May 2017
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*



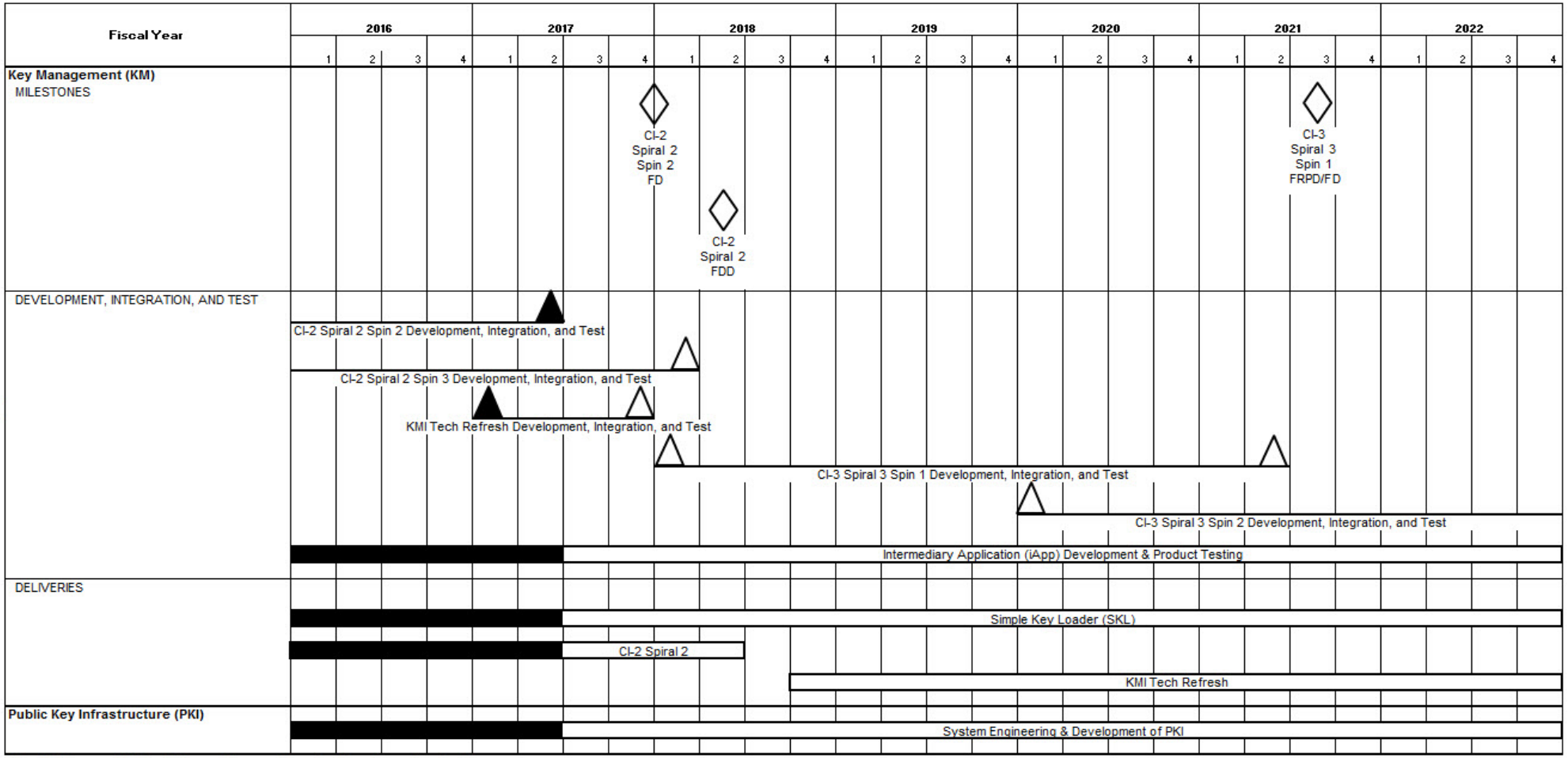
Note 1: Reference Section B Change Summary for schedule notes and explanations

Exhibit R-4, RDT&E Schedule Profile: FY 2018 Navy		Date: May 2017
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*



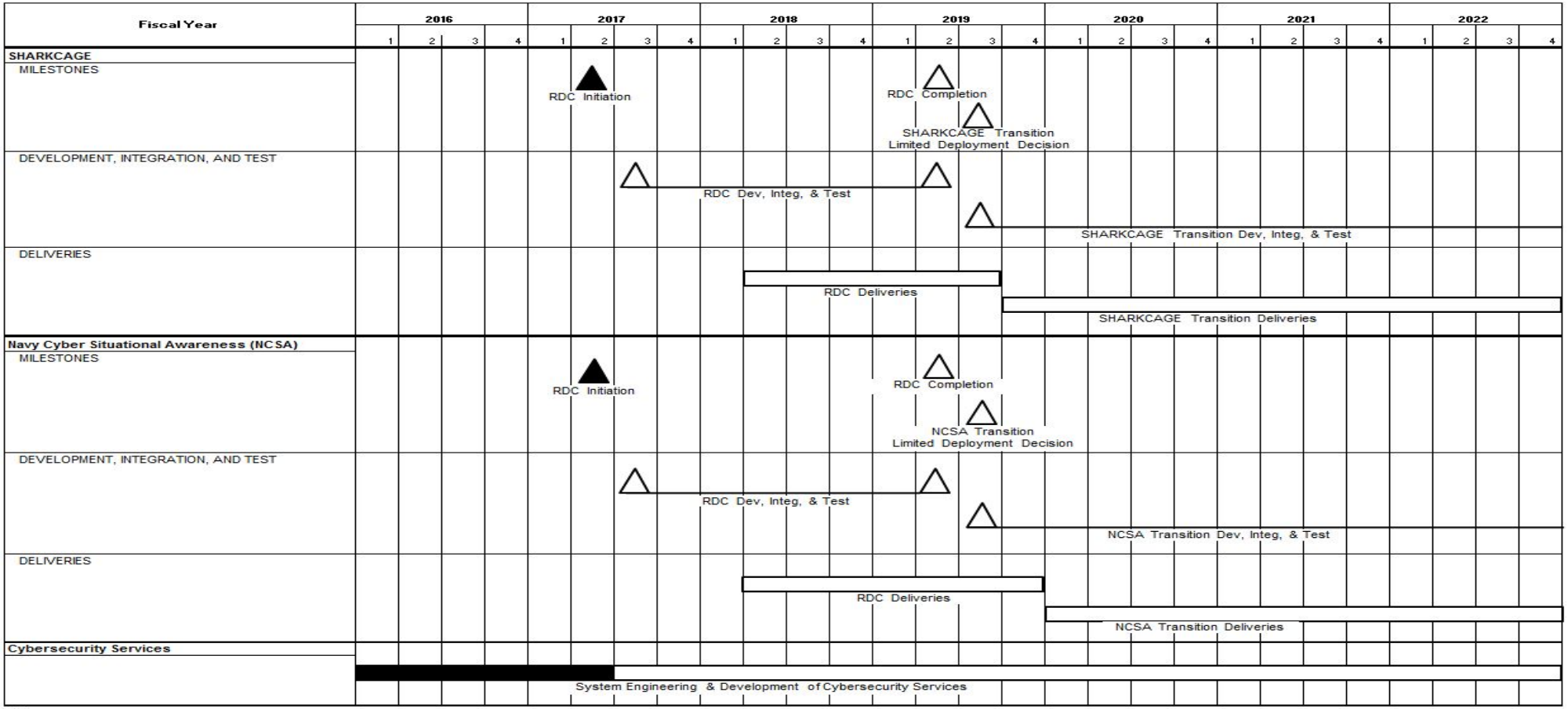
Note 1: Reference Section B Change Summary for schedule notes and explanations

Exhibit R-4, RDT&E Schedule Profile: FY 2018 Navy		Date: May 2017
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: FY 2018 Navy		Date: May 2017
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*



Notes:
1. SHARKCAGE and NCSA are planned Rapid Deployment Capability's (RDC). An RDC is the Navy's implementation of the Department of Defense (DoD) 5000 defined "Accelerated Acquisition Program." It provides the ability to react immediately to a newly discovered enemy threat(s) or potential enemy threat(s) through tailored procedures, to allow for fielding of mature capabilities based on Commercial Off-The-Shelf (COTS) and Non-Developmental Item (NDI) products within a 2 year period. At the end of that period, SHARKCAGE and NCSA are planning to transition to respective ACAT programs.
2. RDC Initiation milestone provides the authority to procure and field RDC units.
3. SHARKCAGE and NCSA were previously budgeted under Computer Network Defense (CND); broken out separately for greater visibility into cybersecurity.

Exhibit R-4A, RDT&E Schedule Details: FY 2018 Navy		Date: May 2017
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 4 Dev, Integ, & Test	1	2016	2	2016
CND - Build 5 Dev, Integ, & Test	1	2016	4	2016
CND - Build 6 Dev, Integ, & Test	2	2016	4	2017
CND - Build 7 Dev, Integ, & Test	1	2017	3	2018
CND - Build 8 Dev, Integ, & Test	1	2018	3	2019
CND - Build 9 Dev, Integ, & Test	4	2018	2	2020
CND - Build 10 Dev, Integ, & Test	3	2019	1	2021
CND - Build 11 Dev, Integ, & Test	2	2020	4	2021
CND - Build 12 Dev, Integ, & Test	1	2021	3	2022
CND - Build 13 Dev, Integ, & Test	4	2021	4	2022
CND - Inc 2 Deliveries	1	2016	4	2022
Crypto - VACM Full Rate Production (FRP) Decision	3	2016	3	2016
Crypto - VACM Initial Operational Capability (IOC)	3	2016	3	2016
Crypto - TRANSEC Studies & Analysis	1	2016	2	2016
Crypto - TRANSEC Development and Product Testing	3	2016	2	2018
Crypto - KGV-11M Development and Product Testing	3	2018	2	2020
Crypto - ACC Solutions Development and Product Testing	1	2016	4	2022
Crypto - Next Generation Crypto Development	1	2020	4	2022
Crypto - KGV-11M Development Contract Award	2	2018	2	2018
Crypto - KGV-11M PDR	4	2018	4	2018
Crypto - KGV-11M CDR	3	2019	3	2019

Exhibit R-4A, RDT&E Schedule Details: FY 2018 Navy		Date: May 2017
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 - KGV-11M DT&E	2	2020	2	2020
Crypto - KGV-11M NSA Certification	3	2020	3	2020
Crypto - VACM Deliveries	1	2018	4	2022
Crypto - KGV-11M Deliveries	4	2020	4	2022
Crypto - ACC Deliveries	4	2019	4	2022
Key Management - KMI CI-2 Spiral 2 Spin 2 Development, Integration, and Test	1	2016	2	2017
Key Management - KMI CI-2 Spiral 2 Spin 3 Development, Integration, and Test	1	2016	1	2018
Key Management - KMI Tech Refresh Development, Integration, and Test	1	2017	4	2017
Key Management - KMI CI-3 Spiral 3 Spin 1 Development, Integration, and Test	1	2018	2	2021
Key Management - KMI CI-3 Spiral 3 Spin 2 Development, Integration, and Test	1	2020	4	2022
Key Management - Intermediary Application (iApp) Development and Product Testing	1	2016	4	2022
Key Management - KMI CI-2 Spiral 2 Spin 2 Fielding Decision (FD)	4	2017	4	2017
Key Management - KMI CI-2 Spiral 2 Full Deployment Decision (FDD)	2	2018	2	2018
Key Management - KMI CI-3 Spiral 3 Spin 1 FRP Decision / FD	3	2021	3	2021
Key Management - Simple Key Loader (SKL) Deliveries	1	2016	4	2022
Key Management - KMI CI-2 Spiral 2 Deliveries	1	2016	2	2018
Key Management - KMI Tech Refresh Deliveries	4	2018	4	2022
Public Key Infrastructure - System Engineering and Development of PKI	1	2016	4	2022
SHARKCAGE - RDC Initiation	2	2017	2	2017
SHARKCAGE - RDC Dev, Integ, & Test	3	2017	2	2019
SHARKCAGE - RDC Deliveries	2	2018	3	2019
SHARKCAGE - RDC Completion	2	2019	2	2019
SHARKCAGE - SHARKCAGE Transition Limited Deployment Decision	3	2019	3	2019
SHARKCAGE - SHARKCAGE Transition Dev, Integ, & Test	3	2019	4	2022
SHARKCAGE - SHARKCAGE Transition Deliveries	4	2019	4	2022

Exhibit R-4A, RDT&E Schedule Details: FY 2018 Navy		Date: May 2017
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**
NCSA - RDC Initiation	2	2017	2	2017
NCSA - RDC Dev, Integ, & Test	3	2017	2	2019
NCSA - RDC Deliveries	2	2018	4	2019
NCSA - RDC Completion	2	2019	2	2019
NCSA - NCSA Transition Limited Deployment Decision	3	2019	3	2019
NCSA - NCSA Transition Dev, Integ, & Test	3	2019	4	2022
NCSA - NCSA Transition Deliveries	1	2020	4	2022
Cybersecurity - Systems Engineering & Development of Cybersecurity Services	1	2016	4	2022

Exhibit R-2A, RDT&E Project Justification: FY 2018 Navy											Date: May 2017	
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 2016**	**FY 2017**	**FY 2018 Base**	**FY 2018 OCO**	**FY 2018 Total**	**FY 2019**	**FY 2020**	**FY 2021**	**FY 2022**	**Cost To Complete**	**Total Cost**
3230: *Information Assurance*	14.376	2.120	1.523	2.415	-	2.415	2.390	2.230	2.274	2.318	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. The Information Systems Security Program (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 of 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 Committee; 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. This program will also initiate requirements definition for secure

coalition data exchange and interoperation among security levels and classifications, and ensure approaches address various security level technologies as well as emerging architectural methods of providing interoperability across different security levels. IA will 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, Department of Defense (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. Additionally, 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.

The increase in FY18 supports investment in efforts to improve effectiveness of cyber defenses and critical infrastructure protection and adequately fund continuing efforts from FY17.

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total
Title: Information Assurance (IA)	2.120	1.523	2.415	0.000	2.415
Articles:	-	-	-	-	-
Description: The increase in FY18 supports investment in efforts to improve effectiveness of cyber defenses and critical infrastructure protection and adequately fund continuing efforts from FY17.					
FY 2016 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. Continued the development of new sensing and instrumentation technology to measure the effectiveness of network security technology. Continued the development of technology to provide prediction/early warning sensing of impending attacks based on network traffic and user behavior. Continued the development of critical cryptographic technology to support Navy unique platforms and requirements such as Unmanned Aircraft Systems (UASs) (e.g., Unmanned Aerial Vehicles (UAVs), Unmanned Underwater Vehicles (UUV)) ensuring the technology addresses the limited size, weight and power issues, and					

Exhibit R-2A, RDT&E Project Justification: FY 2018 Navy		Date: May 2017
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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total
multiple data classification processing requirements, while as providing on-the-fly programmability of mission data and key material to support various missions such as Communications Security (COMSEC), Electronic Intelligence (ELINT), Signals Intelligence (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 Department of Defense (DoD) requirements. Completed 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. Completed the development of a security framework for mobile communication devices. Addressed the security issues associated with bring-your-own-device/bring-your-own-application, such as to support the integration of phone and tablet devices. Initiated 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 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. 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.					

Exhibit R-2A, RDT&E Project Justification: FY 2018 Navy		Date: May 2017
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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total
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 2018 Base Plans: 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. Continue 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 while maintaining continuity of operations and access to critical data. Complete 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 and train sensors to address predicted threat to reduce the threat to engage cycle. Complete 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 based on successful technology demonstration.					

Exhibit R-2A, RDT&E Project Justification: FY 2018 Navy		Date: May 2017
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 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total
Complete 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. Initiate the development of new technology to support asset criticality and management to improve effectiveness of cyber defenses in support of mission execution, focusing on threats and attack propagation through the network. Initiate the development of a new generation of cross-domain technology that focuses on critical infrastructure protection while protecting against sophisticated nation state attacks and exfiltration, while supporting new data models and formats for emerging Navy networks. ***FY 2018 OCO Plans:*** N/A					
Accomplishments/Planned Programs Subtotals	2.120	1.523	2.415	0.000	2.415

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.