Exhibit R-2, RDT&E Budget Item Justification: PB 2019 Navy											Date: February 2018	
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 2017**	**FY 2018**	**FY 2019 Base**	**FY 2019 OCO**	**FY 2019 Total**	**FY 2020**	**FY 2021**	**FY 2022**	**FY 2023**	**Cost To Complete**	**Total Cost**
Total Program Element	422.597	32.708	50.269	44.228	-	44.228	44.823	38.742	33.577	36.649	Continuing	Continuing
0734: *Communications Security R&D*	406.101	31.185	47.854	41.954	-	41.954	42.690	36.563	31.358	34.381	Continuing	Continuing
3230: *Information Assurance*	16.496	1.523	2.415	2.274	-	2.274	2.133	2.179	2.219	2.268	Continuing	Continuing

A. Mission Description and Budget Item Justification

The Information Systems Security Program (ISSP) ensures the protection of Navy and Navy hosted joint telecommunication and Information Technology (IT) systems from cyber exploitation and attack. The ISSP extends cybersecurity to ensure confidentiality, integrity, and availability of these systems and content processed, stored, or transmitted therein by performing the acquisition, modernization and sustainment of cybersecurity platforms and systems; cyberspace operations include both defensive and offensive measures, which preserve the ability to protect data, networks, net-centric capabilities, and other designated systems while projecting power by the application of force in or through cyberspace. The ISSP includes the protection of the Navy's National Security Systems (NSS). The ISSP must be rapid, predictive, adaptive, and tightly coupled to cyberspace technology. The ISSP provides cybersecurity systems and infrastructure 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 National Security Systems (NSS), 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 for the Navy's Computer Network Defense (CND) service provider that accelerates the Navy's ability to prevent, constrain, and mitigate cyber attacks and critical vulnerabilities; (3) Navy Cyber Situational Awareness (NCSA) technologies that provides the operational context for cyber threat intelligence and Situational Awareness (SA), from external boundaries to tactical edge infrastructures; (4) assurance of the Navy's Cryptography (Crypto) telecommunications infrastructure and the wireless spectrum; (5) sensing cyber threats across all Navy shore and afloat networks to expand the capabilities 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 Key Management (KM) and Public Key Infrastructure (PKI).

Exhibit R-2, RDT&E Budget Item Justification: PB 2019 Navy					Date: February 2018
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 2017**	**FY 2018**	**FY 2019 Base**	**FY 2019 OCO**	**FY 2019 Total**
Previous President's Budget	38.510	50.269	53.013	-	53.013
Current President's Budget	32.708	50.269	44.228	-	44.228
Total Adjustments	-5.802	0.000	-8.785	-	-8.785
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-0.549	0.000			
• Program Adjustments	0.000	0.000	-8.202	-	-8.202
• Rate/Misc Adjustments	0.000	0.000	-0.583	-	-0.583
• Congressional General Reductions Adjustments	-0.053	-	-	-	-
• Congressional Directed Reductions Adjustments	-5.200	-	-	-	-

Change Summary Explanation

The FY 2019 funding request was reduced by $0.704 million to account for the availability of prior year execution balances.

TECHNICAL: N/A

SCHEDULE:

Computer Network Defense (CND):
- Added Build 14 Development milestone. Starts in 3QFY22.

Navy Cryptography (Crypto):
- VINSON/Advanced Narrowband Digital Voice Terminal (ANDVT) Cryptographic Modernization (VACM) deliveries shifted from 1QFY18 to 2QFY18 in accordance with the United States Air Force (USAF) schedule.
- Advanced Cryptographic Capability (ACC) Fielding Decision added to Q4FY18 in accordance with the National Security Agency (NSA) schedule.
- KGV-11M Preliminary Design Review (PDR) shifted from 4QFY18 to 1QFY19, in accordance with the schedule.
- KGV-11M Development Test and Evaluation (DT&E) shifted from 2QFY20 to 1QFY20, in accordance with the schedule.

Exhibit R-2, RDT&E Budget Item Justification: PB 2019 Navy	Date: February 2018
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*

Key Management (KM):
- Capability Increment (CI)-2 Spiral 2 Spin 3 Development, Integration and Test shifted from Q1FY18 to Q3FY17.
- CI-2 Spiral 2 Deliveries shifted from Q2FY18 to Q1FY18.

SHARKCAGE & Navy Cyber Situational Awareness (NCSA):
- SHARKCAGE and NCSA are Rapid Deployment Capability (RDC) efforts. 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 Acquisition Category (ACAT) programs.
- SHARKCAHE & NCSA RDC Delivery completion shifted from 4QFY19 to 3QFY19.
- SHARKCAGE & NCSA Transition Deliveries start shifted from 1QFY20 to 4QFY19.

FUNDING:

Navy Cryptography (Crypto):
- FY19 increase is for continued development of Advanced Cryptographic Capabilities (ACC) security software of various Communications Security (COMSEC) devices and compatibility of cryptographic devices capable of receiving software updates.

Key Management (KM):
- FY19 decrease aligns to the completion of CI-2 Spiral 2/Spin 3.

SHARKCAGE:
- FY19 decrease reflects a realignment within SHARKCAGE from Research, Development, Test and Evaluation (RDTE) to Other Procurement, Navy (OPN) and Operations and Maintenance, Navy (OMN) based on program requirements shifting from development to procurement, integration and sustainment.

Exhibit R-2A, RDT&E Project Justification: PB 2019 Navy											Date: February 2018	
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 2017**	**FY 2018**	**FY 2019 Base**	**FY 2019 OCO**	**FY 2019 Total**	**FY 2020**	**FY 2021**	**FY 2022**	**FY 2023**	**Cost To Complete**	**Total Cost**
0734: *Communications Security R&D*	406.101	31.185	47.854	41.954	-	41.954	42.690	36.563	31.358	34.381	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 (DoD) 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 development, design and application integration 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 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, 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 networks 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: PB 2019 Navy		Date: February 2018
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 suites. 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 which is 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.

FY19 will focus 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 (NSS), 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 help the Navy's ability to prevent, constrain, and mitigate cyber attacks and critical vulnerabilities; (3) Navy Cyber Situational Awareness (NCSA) technologies that provides the operational context for cyber threat intelligence and Situational Awareness (SA), 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 expand the capabilities 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).

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total
Title: Computer Network Defense (CND)	21.358	14.039	13.160	0.000	13.160
Articles:	-	-	-	-	-
FY 2018 Plans: SHARKCAGE and Navy Cyber Situational Awareness (NCSA) development efforts previously budgeted under CND have been broken out for greater visibility into cybersecurity.					

Exhibit R-2A, RDT&E Project Justification: PB 2019 Navy		Date: February 2018
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 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total
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 within the Computer Network Defense (CND) architecture. Continue to develop, integrate, and test CND Inc 2 Builds, Defense-in-Depth (DiD), and Situational Awareness (SA) technologies for knowledge-empowered CND operations for shore sites and afloat platforms within Navy's Outside Continental United States (OCONUS) Navy Enterprise Network (ONE-Net) and Command, Control, Communication, Computers and Intelligence (C4I) networks to achieve improved network defense and security wholeness. Continue enhancing the Vulnerability Remediation Asset Manager (VRAM) tool per Fleet Cyber Command / Commander Tenth Fleet (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 Department of Defense (DoD) cyber readiness. Continue to evaluate needs derived from stakeholders and the CND Capabilities Steering Group (CCSG), and correspondingly develop, update, and integrate CND suites. Continue to implement DoD and United States Cyber Command (USCC) cybersecurity tools and mandates into ONE-Net and C4I networks. Continue to provide technical guidance to support Consolidated Afloat Network and Enterprise Services (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 Navy Cyber Defense Operations Command's (NCDOC) 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 2019 Base 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 within the CND architecture. Continue to develop, integrate, and test Computer Network Defense (CND) Inc 2 Builds, Defense-in-Depth (DiD), and Situational Awareness (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 Vulnerability Remediation Asset Manager (VRAM) tool, to include 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 CND Capabilities Steering Group (CCSG), and correspondingly develop, update, and integrate CND suites. Continue to implement DoD and United States Cyber Command (USCC) cybersecurity tools and mandates					

Exhibit R-2A, RDT&E Project Justification: PB 2019 Navy		Date: February 2018
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 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total
into ONE-Net and C4I networks. Continue to provide technical guidance to support CANES deployment of new CND capabilities. Continue to optimize CND suite for alignment with 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. Continue 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 DoN directives. ***FY 2019 OCO Plans:*** N/A ***FY 2018 to FY 2019 Increase/Decrease Statement:*** No significant changes from FY18 to FY19					
Title: Navy Cryptography (Crypto)	4.672	11.912	13.565	0.000	13.565
Articles:	-	-	-	-	-
FY 2018 Plans: FY18 increase 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 National Security Agency (NSA) cease key dates. The TRANSEC algorithm modernization mandate protects critical Ultra High Frequency (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 Advanced Cryptographic Capabilities (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 Department of the Navy (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 VINSON/Advanced Narrowband Digital Voice Terminal (ANDVT) Cryptographic Modernization (VACM) ancillary devices. Continue					

Exhibit R-2A, RDT&E Project Justification: PB 2019 Navy		Date: February 2018
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 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total
to develop Navy strategy and implementation plan to modernize secure voice architectures within Navy networks. ***FY 2019 Base Plans:*** FY19 increase is for continued development of Advanced Cryptographic Capabilities (ACC) security software of various Communications Security (COMSEC) devices and compatibility of cryptographic devices capable of receiving software updates. Continue developing a transition plan for Transmission Security (TRANSEC) and Advanced Cryptographic Capabilities (ACC) for crypto modernization. Continue KGV-11M product development and continue developmental testing. Complete KGV-11M Preliminary Design Review (PDR). Complete KGV-11M Critical Design Review (CDR). 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 and data testing for all crypto modernization efforts. Continue to investigate impacts of upcoming NSA security enhancements for crypto modernization products. Continue to enhance and modernize VINSON/Advanced Narrowband Digital Voice Terminal (ANDVT) Cryptographic Modernization (VACM) ancillary devices. Continue to develop Navy strategy and implementation plan to modernize secure voice architectures within Navy networks. ***FY 2019 OCO Plans:*** N/A ***FY 2018 to FY 2019 Increase/Decrease Statement:*** FY19 increase is for continued development of Advanced Cryptographic Capabilities (ACC) security software of various Communications Security (COMSEC) devices and compatibility of cryptographic devices capable of receiving software updates.					
Title: Key Management (KM)	2.363	2.230	0.823	0.000	0.823
Articles:	-	-	-	-	-
FY 2018 Plans: Achieve Full Operational Test & Evaluation (FOT&E) and Full Deployment Decision (FDD) for Key Management Infrastructure (KMI) Spiral 2. Continue migrating Continue migrating Communications Security (COMSEC) Management Workstation (CMWS) and the follow on to Simple Key Loader (SKL) into the KMI environment. Initiate the development, engineering, and testing of KMI Capability Increment (CI)-3, including the integration					

Exhibit R-2A, RDT&E Project Justification: PB 2019 Navy		Date: February 2018
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 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total
of the Intermediary Application (iApp) within a network environment, which will enhance the accounting for and distribution of KMI key delivery. ***FY 2019 Base Plans:*** Continue migrating COMSEC CMWS and the follow on to SKL into the KMI environment. Continue the development, engineering and testing of KMI CI-3, including the integration of iApp within a network environment, which will enhance the accounting for and distribution of KMI key delivery. ***FY 2019 OCO Plans:*** N/A ***FY 2018 to FY 2019 Increase/Decrease Statement:*** FY19 decrease aligns to the completion of Capability Increment (CI)-2 Spiral 2/Spin 3.					
Title: Public Key Infrastructure (PKI)	0.350	0.360	0.366	0.000	0.366
Articles:	-	-	-	-	-
FY 2018 Plans: Continue 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) and other encryption methodologies, Navy Certificate Validation Infrastructure (NCVI), Common Access Card (CAC), Alternate Logon Token (ALT), and Alternate Logon Token (SIPRNet) Token. Continue research, test and evaluation of Non-classified Internet Protocol Router Network (NIPRNet) Enterprise Alternate Token System (NEATS), Non-Person Entity (NPE), PKI authentication capabilities to support mobile devices, Identity and Access Management (IdAM) technologies, and Real-time Automated Personnel Identification System (RAPIDS) Operating Systems (OS). ***FY 2019 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 2019 OCO Plans:*** N/A ***FY 2018 to FY 2019 Increase/Decrease Statement:***					

Exhibit R-2A, RDT&E Project Justification: PB 2019 Navy		Date: February 2018
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 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total
No significant changes from FY18 to FY19					
Title: SHARKCAGE	0.000	8.973	5.322	0.000	5.322
Articles:	-	-	-	-	-

FY 2018 Plans:
SHARKCAGE development efforts were previously budgeted under Computer Network Defense (CND); funding broken out for greater visibility into cybersecurity.

FY18 funds 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 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 2019 Base Plans:
Continue development of SHARKCAGE DCO enclave to address 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., C4I networks, CS, 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 CPT.

FY 2019 OCO Plans:
N/A

FY 2018 to FY 2019 Increase/Decrease Statement:

Exhibit R-2A, RDT&E Project Justification: PB 2019 Navy		Date: February 2018
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 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total
FY19 decrease reflects a realignment within SHARKCAGE from Research, Development, Test and Evaluation (RDTE) to Other Procurement, Navy (OPN) and Operations and Maintenance, Navy (OMN) based on program requirements shifting from development to procurement, integration and sustainment.					
Title: Navy Cyber Situational Awareness (NCSA)	0.000	7.840	6.356	0.000	6.356
Articles:	-	-	-	-	-
FY 2018 Plans: Navy Cyber Situational Awareness (NCSA) development efforts were previously budgeted under Computer Network Defense (CND); funding broken out for greater visibility into cybersecurity. FY18 funds 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/Commander Tenth Fleet (C10F) beginning with Commander, Pacific Fleet (COMPACFLT) MOC to enable assessments 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 2019 Base Plans:*** Continue 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. Continue the development of a shared and tailorable Maritime Cyber "Integrated" COP external to FCC/C10F beginning with COMPACFLT MOC to enable assessments of cyber vulnerabilities, threats, and risks relative to BMD and NC3-					

Exhibit R-2A, RDT&E Project Justification: PB 2019 Navy		Date: February 2018
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 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total
N missions. NCSA maturation will provide for monitoring of relevant and current Navy networks providing near real-time visualization and analytics of the cyberspace domain. ***FY 2019 OCO Plans:*** N/A ***FY 2018 to FY 2019 Increase/Decrease Statement:*** FY19 decrease reflects a realignment within NCSA from Research, Development, Test and Evaluation (RDTE) to Operations and Maintenance, Navy (OMN) based on program requirements.					
Title: Cybersecurity Services	2.442	2.500	2.362	0.000	2.362
Articles:	-	-	-	-	-
FY 2018 Plans: Continue coordination and alignment 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 Department of Defense (DoD) and Department of Navy (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 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. Continue to provide cybersecurity risk analysis and recommended risk mitigation strategies for Navy critical networks and Command, Control, Communication, Computers, & Intelligence (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 2019 Base Plans:*** Continue coordination and alignment with JIE (e.g., JRSS, JMS, Tactical Processing Node (TPN) 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					

Exhibit R-2A, RDT&E Project Justification: PB 2019 Navy		Date: February 2018
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 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total
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 2019 OCO Plans:*** N/A ***FY 2018 to FY 2019 Increase/Decrease Statement:*** No significant changes from FY18 to FY19					
Accomplishments/Planned Programs Subtotals	31.185	47.854	41.954	0.000	41.954

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total	FY 2020	FY 2021	FY 2022	FY 2023	Cost To Complete	Total Cost
• OPN/3415: *Info Sys Security Program (ISSP)*	92.454	89.663	153.526	-	153.526	169.790	167.008	164.884	171.918	Continuing	Continuing

Remarks

D. Acquisition Strategy

Computer Network Defense (CND): The CND Acquisition Category (ACAT) IVM 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 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.

Exhibit R-2A, RDT&E Project Justification: PB 2019 Navy		Date: February 2018
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*

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 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 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 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 Fleet Cyber Command/Commander Tenth Fleet (FCC/C10F). Cybersecurity Services transitions new technologies to address current Navy cybersecurity challenges.

E. Performance Metrics

Computer Network Defense (CND):
* Provide the ability to protect from, react to, and restore operations after an intrusion or other catastrophic event through validated contingency plans for 100% of CND systems.
* Develop dynamic security defense capabilities, based on the CND posture as an active response to threat attack sensors and vulnerability indications to provide adequate defenses against subversive acts of trusted people and systems, both internal and external, by integration of anomaly-based detection solutions into the design solutions for 100% of authorized Navy enclaves.
* Defend against the unauthorized use of a host or application, particularly operating systems, by development and/or integration of host-based intrusion prevention system design solutions for 100% of authorized Navy enclaves.

Navy Cryptography (Crypto):

Exhibit R-2A, RDT&E Project Justification: PB 2019 Navy		Date: February 2018
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*

* 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).

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 Information Systems Security Program (ISSP) products by researching and conducting selective evaluations, integrating and testing Commercial Off-The-Shelf (COTS)/Non-Developmental Item cybersecurity products. Evaluation may include

Exhibit R-2A, RDT&E Project Justification: PB 2019 Navy		Date: February 2018
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*

defensible network boundary capabilities such as firewalls, secure routers and switches, guards, Virtual Private Networks (VPN), and network Intrusion Prevention Systems (IPS).

* Provide 100% of the services delineated in OPNAVINST 5239.1C by serving as the Navy's cybersecurity technical lead by developing cybersecurity risk analysis and recommended risk mitigation strategies for critical Navy networks and Command, Control, Communications, Computers, and Intelligence (C4I) systems.
* Coordinate cybersecurity activities across the Navy Enterprise via the Cybersecurity Trusted Architecture (TA) to measure effectiveness of Navy networks. Ensure the security design and integration of Computer Adaptive Network Defense-in-Depth (CANDiD) products and services and that they are 100% interoperable and operationally acceptable across the Navy for major initiatives such as the future afloat, ashore, and Outside the Continental United States (OCONUS) networks.

Exhibit R-3, RDT&E Project Cost Analysis: PB 2019 Navy		Date: February 2018
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 2017 Cost	FY 2017 Award Date	FY 2018 Cost	FY 2018 Award Date	FY 2019 Base Cost	FY 2019 Base Award Date	FY 2019 OCO Cost	FY 2019 OCO Award Date	FY 2019 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Hardware Development (WR)	WR	SSC PAC : San Diego, CA	9.976	2.232	Oct 2016	2.953	Oct 2017	2.750	Oct 2018	-		2.750	Continuing	Continuing	Continuing
Hardware Development	C/CPFF	SSC PAC : San Diego, CA	2.816	0.560	Dec 2016	0.869	Dec 2017	0.809	Dec 2018	-		0.809	Continuing	Continuing	Continuing
Hardware Development (WR)	WR	SSC LANT : Charleston, SC	4.805	0.269	Oct 2016	0.570	Oct 2017	0.531	Oct 2018	-		0.531	Continuing	Continuing	Continuing
Hardware Development	C/CPFF	SSC LANT : Charleston, SC	1.255	0.504	Jan 2017	1.068	Jan 2018	0.995	Jan 2019	-		0.995	Continuing	Continuing	Continuing
Software Development (WR)	WR	SSC PAC : San Diego, CA	18.198	5.520	Oct 2016	9.781	Oct 2017	7.746	Oct 2018	-		7.746	Continuing	Continuing	Continuing
Software Development	C/CPFF	SSC PAC : San Diego, CA	3.695	2.998	Dec 2016	5.610	Dec 2017	5.040	Dec 2018	-		5.040	Continuing	Continuing	Continuing
Software Development (WR)	WR	SSC LANT : Charleston, SC	4.259	2.253	Oct 2016	2.232	Oct 2017	2.079	Oct 2018	-		2.079	Continuing	Continuing	Continuing
Software Development	C/CPFF	SSC LANT : Charleston, SC	5.349	3.956	Jan 2017	4.138	Jan 2018	3.854	Jan 2019	-		3.854	Continuing	Continuing	Continuing
Software Development	FFRDC	MITRE : McLean, VA	1.371	1.451	Dec 2016	2.022	Dec 2017	1.883	Dec 2018	-		1.883	Continuing	Continuing	Continuing
Software Development	Various	Various : Various	66.737	0.251	Dec 2016	0.532	Dec 2017	0.495	Dec 2018	-		0.495	Continuing	Continuing	Continuing
Software Development	C/CPFF	BAH : San Diego, CA	3.187	2.539	Jan 2017	2.801	Jan 2018	2.609	Jan 2019	-		2.609	Continuing	Continuing	Continuing
Software Development	FFRDC	GTRI : Atlanta, GA	6.228	2.593	Jan 2017	7.873	Jan 2018	6.266	Jan 2019	-		6.266	Continuing	Continuing	Continuing
Software Development	WR	NSMA : San Diego, CA	0.805	1.308	Dec 2016	1.631	Dec 2017	1.519	Oct 2018	-		1.519	Continuing	Continuing	Continuing
Software Development	WR	NRL : Washington DC	1.260	0.895	Dec 2016	0.903	Dec 2017	0.841	Oct 2018	-		0.841	Continuing	Continuing	Continuing
Development (PY)	Various	Various : Various	190.205	0.000		0.000		0.000		-		0.000	0.000	190.205	-
		Subtotal	320.146	27.329		42.983		37.417		-		37.417	Continuing	Continuing	N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2019 Navy		Date: February 2018
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 2017 Cost	FY 2017 Award Date	FY 2018 Cost	FY 2018 Award Date	FY 2019 Base Cost	FY 2019 Base Award Date	FY 2019 OCO Cost	FY 2019 OCO Award Date	FY 2019 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Architecture	WR	Various : Various	5.417	0.246	Oct 2016	0.248	Oct 2017	0.231	Oct 2018	-		0.231	Continuing	Continuing	Continuing
Architecture	WR	SSC LANT : Charleston, SC	1.571	0.458	Oct 2016	0.473	Oct 2017	0.441	Oct 2018	-		0.441	Continuing	Continuing	Continuing
Studies & Design	WR	Various : Various	6.059	0.196	Oct 2016	0.415	Oct 2017	0.387	Oct 2018	-		0.387	Continuing	Continuing	Continuing
Requirements Analysis	C/CPFF	BAH : San Diego, CA	5.651	0.196	Oct 2016	0.416	Jan 2018	0.387	Jan 2019	-		0.387	Continuing	Continuing	Continuing
		Subtotal	18.698	1.096		1.552		1.446		-		1.446	Continuing	Continuing	N/A

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2017 Cost	FY 2017 Award Date	FY 2018 Cost	FY 2018 Award Date	FY 2019 Base Cost	FY 2019 Base Award Date	FY 2019 OCO Cost	FY 2019 OCO Award Date	FY 2019 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
System DT&E	WR	SSC PAC : San Diego, CA	37.635	0.330	Oct 2016	0.333	Oct 2017	0.310	Oct 2018	-		0.310	Continuing	Continuing	Continuing
System DT&E	WR	COTF : Norfolk, VA	0.837	0.470	Dec 2016	0.729	Dec 2017	0.679	Dec 2018	-		0.679	Continuing	Continuing	Continuing
System DT&E	C/CPFF	BAH : San Diego, CA	0.510	0.850	Dec 2016	0.858	Jan 2018	0.799	Jan 2019	-		0.799	Continuing	Continuing	Continuing
		Subtotal	38.982	1.650		1.920		1.788		-		1.788	Continuing	Continuing	N/A

Management Services ($ in Millions)

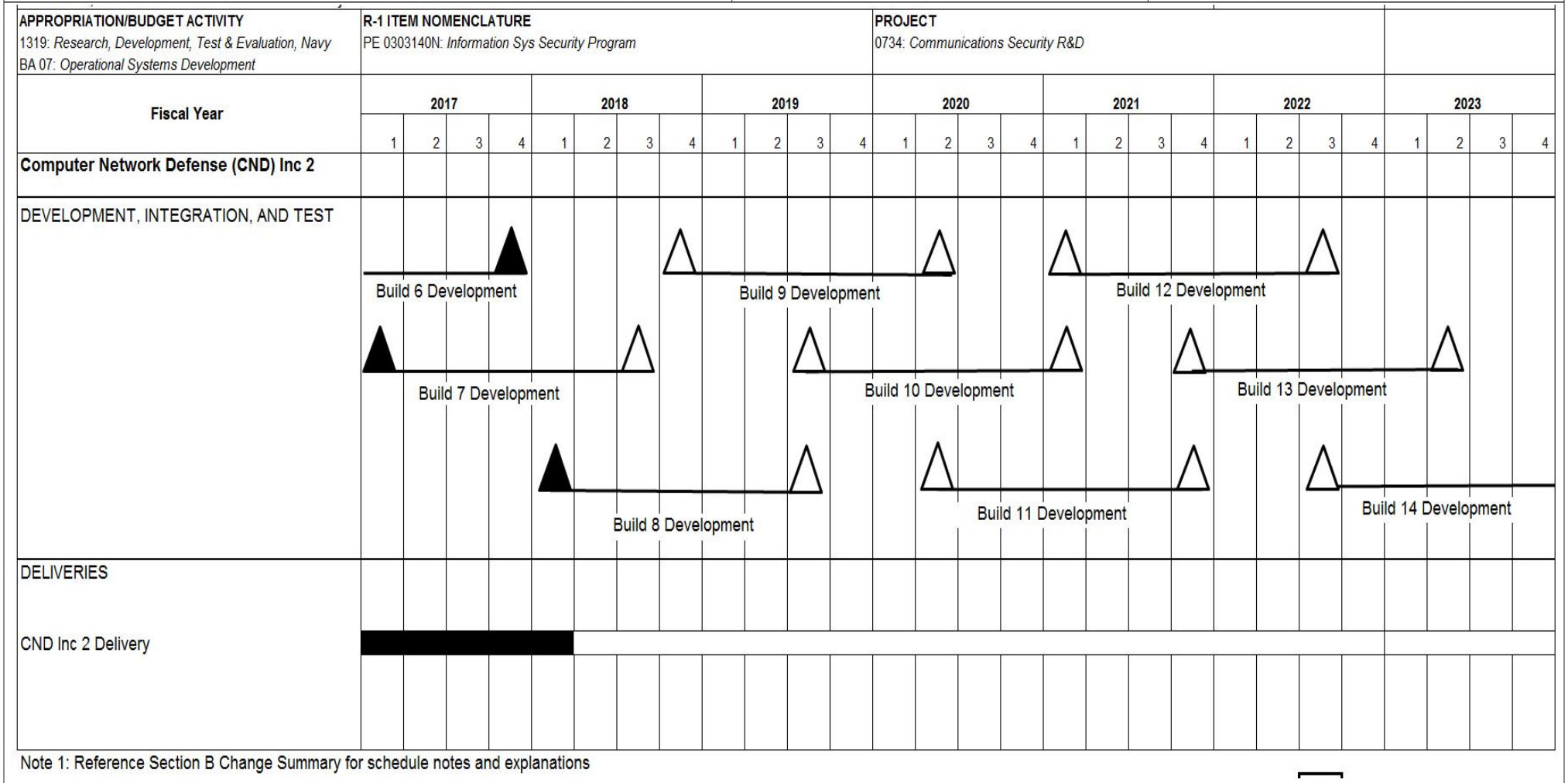
Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2017 Cost	FY 2017 Award Date	FY 2018 Cost	FY 2018 Award Date	FY 2019 Base Cost	FY 2019 Base Award Date	FY 2019 OCO Cost	FY 2019 OCO Award Date	FY 2019 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Program Management	C/CPFF	BAH : San Diego, CA	28.275	1.110	Dec 2016	1.399	Jan 2018	1.303	Jan 2019	-		1.303	0.000	32.087	-
		Subtotal	28.275	1.110		1.399		1.303		-		1.303	0.000	32.087	N/A

	Prior Years	FY 2017 Cost	FY 2017 Award Date	FY 2018 Cost	FY 2018 Award Date	FY 2019 Base Cost	FY 2019 Base Award Date	FY 2019 OCO Cost	FY 2019 OCO Award Date	FY 2019 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	406.101	31.185		47.854		41.954		-		41.954	Continuing	Continuing	N/A

Remarks

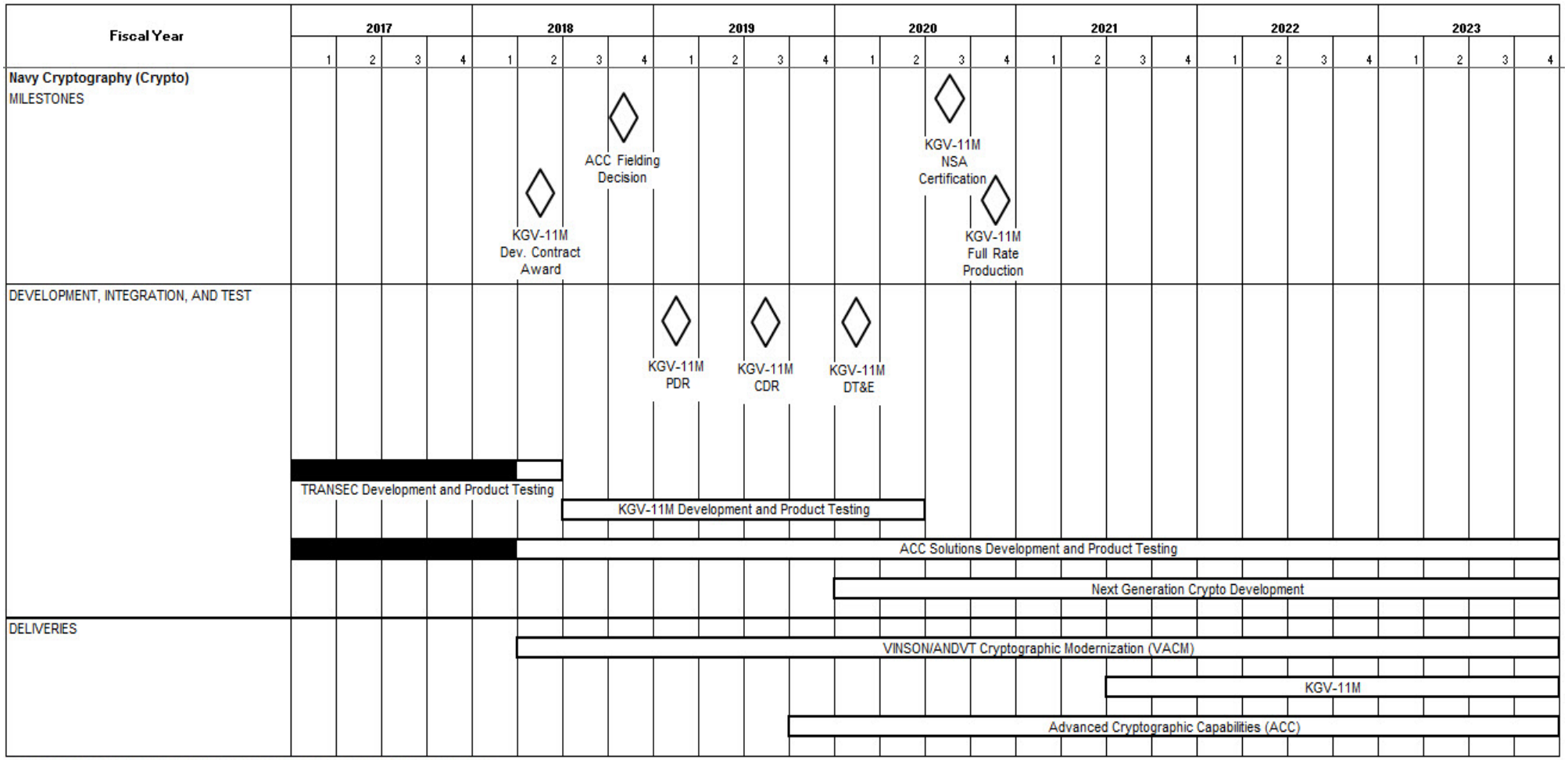
Exhibit R-4, RDT&E Schedule Profile: PB 2019 Navy		Date: February 2018
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*

APPROPRIATION/BUDGET ACTIVITY	R-1 ITEM NOMENCLATURE	PROJECT
1319: *Research, Development, Test & Evaluation, Navy* BA 07: *Operational Systems Development*	PE 0303140N: *Information Sys Security Program*	0734: *Communications Security R&D*



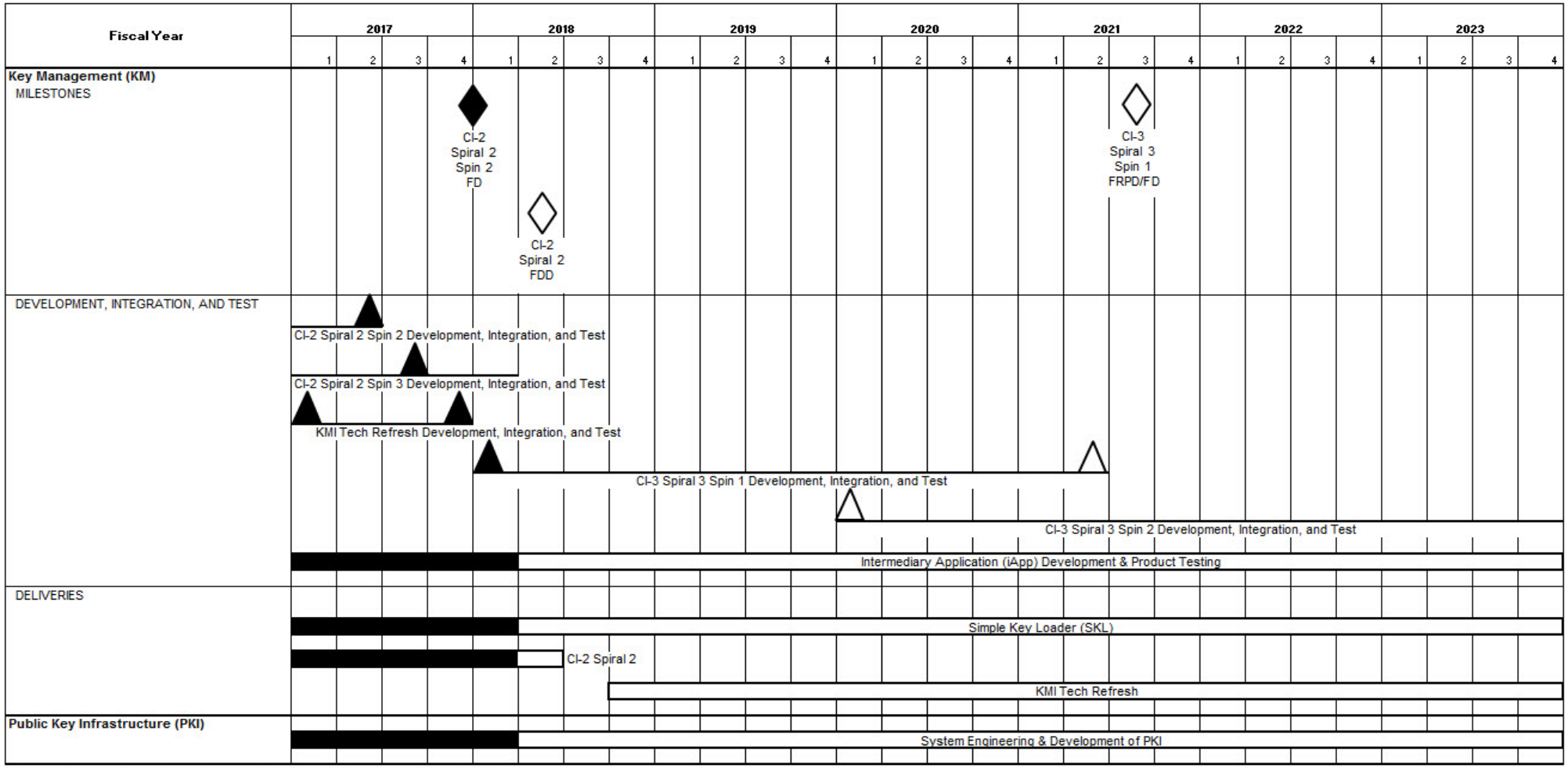
Note 1: Reference Section B Change Summary for schedule notes and explanations

Exhibit R-4, RDT&E Schedule Profile: PB 2019 Navy		Date: February 2018
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*



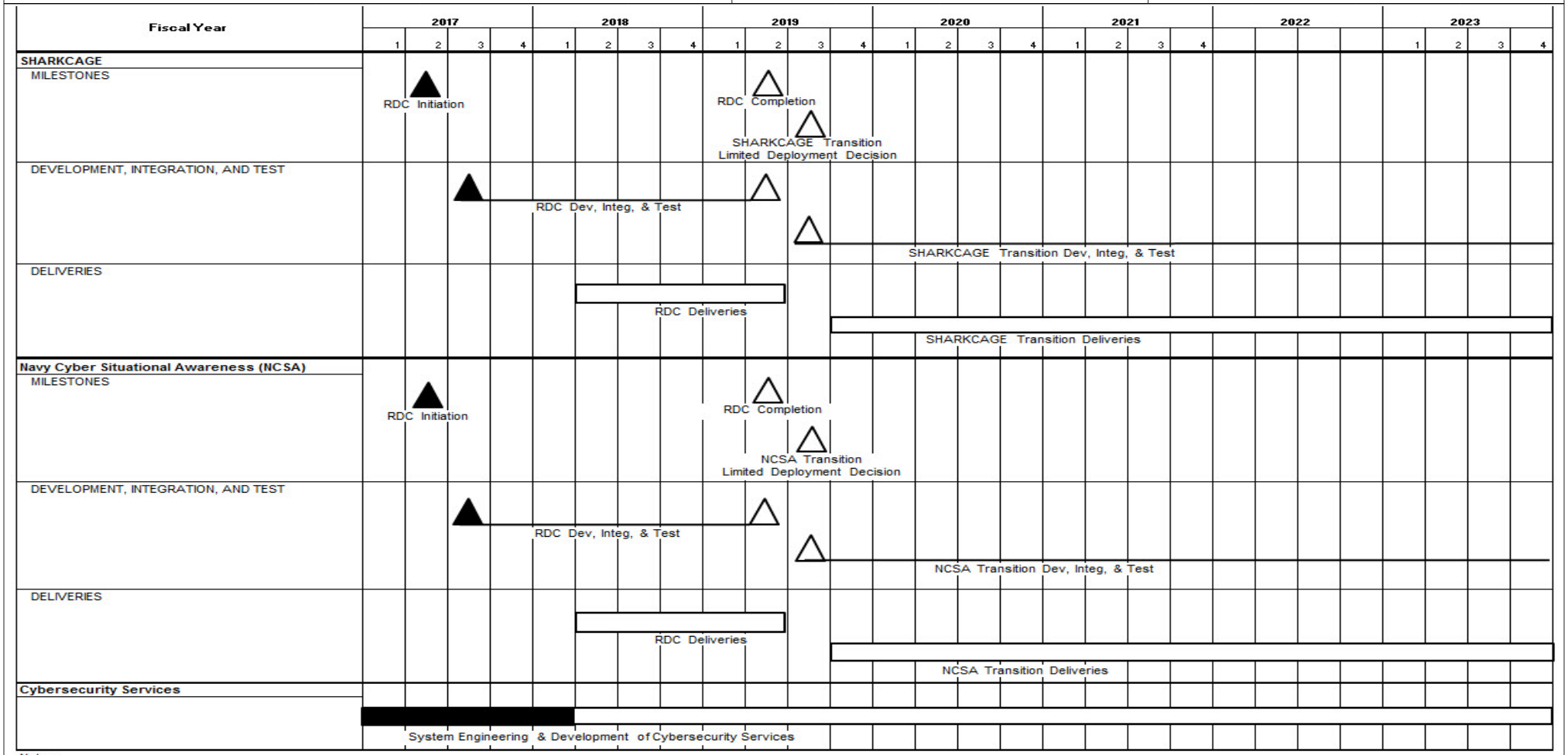
Note 1: Reference Section B Change Summary for schedule notes and explanations

Exhibit R-4, RDT&E Schedule Profile: PB 2019 Navy		Date: February 2018
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 2019 Navy		Date: February 2018
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. Reference Section B Change Summary for schedule notes and explanations

Exhibit R-4A, RDT&E Schedule Details: PB 2019 Navy		Date: February 2018
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				
Computer Network Defense (CND) - Build 6 Dev, Integ, & Test	1	2017	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	2	2023
CND - Build 14 Dev, Integ, & Test	3	2022	4	2023
CND - Inc 2 Deliveries	1	2017	4	2023
Crypto - TRANSEC Development and Product Testing	1	2017	2	2018
Crypto - KGV-11M Development and Product Testing	3	2018	2	2020
Crypto - ACC Solutions Development and Product Testing	1	2017	4	2023
Crypto - Next Generation Crypto Development	1	2020	4	2023
Crypto - KGV-11M Development Contract Award	2	2018	2	2018
Crypto - ACC Fielding Decision (FD)	4	2018	4	2018
Crypto - KGV-11M PDR	1	2019	1	2019
Crypto - KGV-11M CDR	3	2019	3	2019
Crypto - KGV-11M DT&E	1	2020	1	2020
Crypto - KGV-11M NSA Certification	3	2020	3	2020
Crypto - VACM Deliveries	2	2018	4	2023

Exhibit R-4A, RDT&E Schedule Details: PB 2019 Navy		Date: February 2018
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 Deliveries	4	2020	4	2023
Crypto - ACC Deliveries	4	2019	4	2023
Key Management - KMI CI-2 Spiral 2 Spin 2 Development, Integration, and Test	1	2017	2	2017
Key Management - KMI CI-2 Spiral 2 Spin 3 Development, Integration, and Test	1	2017	3	2017
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	2023
Key Management - Intermediary Application (iApp) Development and Product Testing	1	2017	4	2023
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	2017	4	2023
Key Management - KMI CI-2 Spiral 2 Deliveries	1	2017	1	2018
Key Management - KMI Tech Refresh Deliveries	4	2018	4	2023
Public Key Infrastructure - System Engineering and Development of PKI	1	2017	4	2023
SHARKCAGE - RDC Initiation	2	2017	2	2017
SHARKCAGE - RDC Dev, Integ, & Test	3	2017	2	2019
SHARKCAGE - RDC Deliveries	2	2018	2	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	2023
SHARKCAGE - SHARKCAGE Transition Deliveries	4	2019	4	2023
Navy Cyber Situational Awareness (NCSA) - RDC Initiation	2	2017	2	2017
NCSA - RDC Dev, Integ, & Test	3	2017	2	2019
NCSA - RDC Deliveries	2	2018	2	2019

Exhibit R-4A, RDT&E Schedule Details: PB 2019 Navy		Date: February 2018
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 Completion	2	2019	2	2019
NCSA - NCSA Transition Limited Deployment Decision	3	2019	3	2019
NCSA - NCSA Transition Dev, Integ, & Test	3	2019	4	2023
NCSA - NCSA Transition Deliveries	4	2019	4	2023
Cybersecurity Services - Systems Engineering & Development of Cybersecurity Services	1	2017	4	2023

Exhibit R-2A, RDT&E Project Justification: PB 2019 Navy			Date: February 2018
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 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total	FY 2020	FY 2021	FY 2022	FY 2023	Cost To Complete	Total Cost
3230: *Information Assurance*	16.496	1.523	2.415	2.274	-	2.274	2.133	2.179	2.219	2.268	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

Exhibit R-2A, RDT&E Project Justification: PB 2019 Navy		Date: February 2018
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 3230 / *Information Assurance*

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.

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total
Title: Information Assurance (IA)	1.523	2.415	2.274	0.000	2.274
Articles:	-	-	-	-	-
FY 2018 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 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. 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					

Exhibit R-2A, RDT&E Project Justification: PB 2019 Navy		Date: February 2018
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 2017	FY 2018	FY 2019 Base	FY 2019 OCO	FY 2019 Total
sophisticated nation state attacks and exfiltration, while supporting new data models and formats for emerging Navy networks. ***FY 2019 Base Plans:*** Continue the development of a new techniques/technology for discovering adversarial presence in Navy/ DoD networks, especially for 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. Continue systems security engineering, certification and accreditation support for high-confidence, high criticality naval information systems and ensure certification and accreditation approaches are consistent with Navy and DoD requirements. Continue 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. Continue 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. Initiate the development of intelligent security components and infrastructure capable of protecting the DON's critical cyber assets through intelligent, autonomous self-diagnostics, automated damage assessment, and self-healing capabilities. Initiate the development of a framework to systematically identify optimal and pertinent features of cyber behavior data in order to detect anomalies. Anomalies stemming from malicious cyber activity (e.g., intrusions, denial of service, malware) will be identified, as well as the development of metrics indicating the health and security posture of the cyber resources. Initiate the development of algorithms that automatically identify the feature space and select the optimal feature set from the given cyber data, the network traffic, and the interconnectivity of the cyber resources. ***FY 2019 OCO Plans:*** N/A ***FY 2018 to FY 2019 Increase/Decrease Statement:*** Decrease from FY18/19 is due to various efficiency and inflation rate adjustments.					
Accomplishments/Planned Programs Subtotals	1.523	2.415	2.274	0.000	2.274

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

Exhibit R-2A, RDT&E Project Justification: PB 2019 Navy		Date: February 2018
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 3230 / *Information Assurance*

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 2019 Navy		Date: February 2018
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 2017 Cost	FY 2017 Award Date	FY 2018 Cost	FY 2018 Award Date	FY 2019 Base Cost	FY 2019 Base Award Date	FY 2019 OCO Cost	FY 2019 OCO Award Date	FY 2019 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Development Support	Various	NRL : Washington, DC	16.496	1.523	Nov 2016	2.415	Nov 2017	2.274	Nov 2018	-		2.274	Continuing	Continuing	Continuing
		Subtotal	16.496	1.523		2.415		2.274		-		2.274	Continuing	Continuing	N/A

	Prior Years	FY 2017		FY 2018		FY 2019 Base		FY 2019 OCO		FY 2019 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	16.496	1.523		2.415		2.274		-		2.274	Continuing	Continuing	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2019 Navy		Date: February 2018
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 3230 / *Information Assurance*

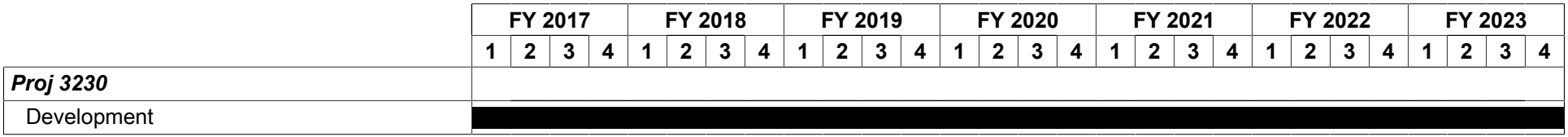


Exhibit R-4A, RDT&E Schedule Details: PB 2019 Navy		Date: February 2018
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 3230 / *Information Assurance*

Schedule Details

	Start		End	
Events by Sub Project	**Quarter**	**Year**	**Quarter**	**Year**
Proj 3230				
Development	1	2017	4	2023