Exhibit R-2, RDT&E Budget Item Justification: PB 2022 Navy												Date: May 2021
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 2020**	**FY 2021**	**FY 2022 Base**	**FY 2022 OCO**	**FY 2022 Total**	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**Cost To Complete**	**Total Cost**
Total Program Element	547.963	43.866	38.814	33.311	-	33.311	-	-	-	-	-	-
0734: *Communications Security R&D*	525.273	38.894	36.644	31.102	-	31.102	-	-	-	-	-	-
3230: *Information Assurance*	22.690	2.076	2.170	2.209	-	2.209	-	-	-	-	-	-
9999: *Congressional Adds*	0.000	2.896	0.000	0.000	-	0.000	-	-	-	-	-	-

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 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 ashore 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 ashore 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) 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); (7) assurance technologies, including Key Management (KM) and Public Key Infrastructure (PKI).

Exhibit R-2, RDT&E Budget Item Justification: PB 2022 Navy	Date: May 2021
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 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total
Previous President's Budget	44.853	39.094	33.888	-	33.888
Current President's Budget	43.866	38.814	33.311	-	33.311
Total Adjustments	-0.987	-0.280	-0.577	-	-0.577
• Congressional General Reductions	-	-0.280			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-0.988	0.000			
• Program Adjustments	0.000	0.000	-0.288	-	-0.288
• Rate/Misc Adjustments	0.001	0.000	-0.289	-	-0.289

Congressional Add Details ($ in Millions, and Includes General Reductions)	FY 2020	FY 2021
Project: 9999: *Congressional Adds*		
Congressional Add: *High assurance infrastructure in defense systems*	2.896	0.000
Congressional Add Subtotals for Project: 9999	2.896	0.000
Congressional Add Totals for all Projects	2.896	0.000

Change Summary Explanation

TECHNICAL:

Key Management (KM):
- Capability Increment (CI)-2 Spiral 2 Full Deployment Decision (FDD) renamed to CI-2 Maintenance Revision (MR)-2 Milestone FDD.

SCHEDULE:

Navy Cryptography (Crypto):
- All KGV-11M milestones shifted due to change in developmental contract award schedule; no impact to programmatic schedule.
- Advanced Cryptographic Capability (ACC) schedule updates are a result of a change in NSA software release date.
- KGV-11M Development and Product Testing extended into 1QFY21 (extension due to COVID-19 schedule delays).
- Added KGV-11M TRR 2QFY20.

- ACC Deliveries did not start in 4QFY19 due to an NSA schedule slip. NSA fielding decision was received March 2020. Shifted ACC Deliveries to start in 3QFY20.

Key Management (KM):
- CI-3 Spiral 3 Spin 1 Milestone Full Rate Production Decision (FRPD)/Fielding Decision (FD) shifted from Q1FY23 to Q4FY25 in accordance with NSA schedule. NSA reassessed the Technical Requirements Package to include CI-3 as a result of Department of Defense Chief Information Officer (DODCIO) guidance to address Tier 1 updates in CI-3, resulting in additional scheduling delays.
- CI-3 Spiral 3 Spin 1 Development, Integration and Test completion shifted from Q2FY21 to Q4FY21 in accordance with NSA schedule
- CI-3 Spiral 3 Spin 2 Development, Integration and Test start shifted from Q1FY21 to Q3FY21 in accordance with NSA schedule.
- Key Management Infrastructure (KMI) Tech Refresh initial delivery shifted from Q1FY21 to Q3FY21 in accordance with NSA schedule.
- Key Management Infrastructure (KMI) Tech Refresh completion shifted from Q4FY25 to Q2FY26 in accordance with NSA schedule.

FUNDING:

SHARKCAGE (-$4.108M):
- FY22 decrease is due to the maturity of the current SHARKCAGE COTS/GOTS capabilities that are integrated together to support the POR system.

Navy Cyber Situational Awareness (NCSA) (-$1.598M):
FY22 decrease is due to the reduction of new data feed ingestion resulting in less development and also a shift of effort to maintaining current data feeds and incremental improvements to the existing baseline using Operations and Maintenance, Navy (OM,N).

Exhibit R-2A, RDT&E Project Justification: PB 2022 Navy											Date: May 2021	
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 2020**	**FY 2021**	**FY 2022 Base**	**FY 2022 OCO**	**FY 2022 Total**	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**Cost To Complete**	**Total Cost**
0734: *Communications Security R&D*	525.273	38.894	36.644	31.102	-	31.102	-	-	-	-	-	-
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 in order to meet mandated National Security Agency (NSA) cease key dates for modernized encryption. Advanced Cryptographic Capabilities (ACC) will provide NSA mandated cryptographic security software modernization of various communications security devices by cease key dates (details held at a higher classification).

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 ashore non-Navy Marine Corps Intranet (NMCI) networks and institutionalizes Identity, Credential and Access Management (ICAM) so that person and non-person entities can securely access all authorized DoD resources.

Exhibit R-2A, RDT&E Project Justification: PB 2022 Navy		Date: May 2021
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 the U.S. Navy's Defensive Cyberspace Operations (DCO) analysis enclave and means to achieve cyberspace detection-in-depth for maritime forces afloat and ashore. SHARKCAGE is the mechanism by which units, groups, and fleets will gain an attack sensing and warning (AS&W) capability and how Commander, Task Force 1020/Navy Cyber Defense Operations Command (NCDOC) will achieve unity of effort and economy of force across the Navy's DCO forces. SHARKCAGE is a Navy-specific platform to complement where existing and future theater, joint, and national capabilities are insufficient for detection of adversary activities onboard maritime warfighting platforms that are located at the tactical-edge and distributed across the globe.

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 develops 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.

FY22 will focus on efforts that address the risk management of cyberspace, which provides capabilities to identify, 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 ashore 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 ashore 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) 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), the Integrated Navy Operations Command and Control System (INOCCS), and Zero Trust Architecture (ZTA) concepts; (7) assurance technologies, including Key Management (KM) and Public Key Infrastructure (PKI).

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total
Title: Computer Network Defense (CND)	13.213	14.908	15.118	0.000	15.118
Articles:	-	-	-	-	-
FY 2021 Plans:					

Exhibit R-2A, RDT&E Project Justification: PB 2022 Navy		Date: May 2021
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 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total
- FY21 increase is due to Vulnerability Asset Remediation Manager (VRAM) 3.0 development efforts to replace VRAM 2.0 end-of-life, and development work to optimize VRAM for the cloud environment. - Begin major CND security operation workstation upgrades, upgrades to Load Balancers, addressing endpoint security gaps in the CND Architecture and updates to the Detonation Malware Analysis Capability at NCDOC. - Continue CND Virtual Hosting Environment (VTE), operating systems and endpoint security assessments and upgrades, and enhance security of the network. - Complete VTE hardware and software upgrades and enhancements including remote replication and hosting of critical endpoint security management servers. - Complete cybersecurity enhancements of VRAM to improve Department of Defense (DoD) cyber readiness and upgrade to VRAM 3.0 with improved capabilities and complete new graphical user interface (GUI) in response to urgent Operation Orders (OPRDs) and Tasking Orders (TASKORDs), and begin migration to cloud environment. - Continue to develop and enhance Navy's portion of the NC3-N and Ballistic Missile Defense (BMD) cyber security system of systems within the CND architecture. - Continue to implement DoD and United States Cyber Command (USCC) cybersecurity tools and mandates into Outside Continental United States (OCONUS) Navy Enterprise Network (ONE-Net) and Command, Control, Communication, Computers, & Intelligence (C4I)networks. - Continue to provide technical guidance to support CANES deployment of new CND capabilities. - Continue to optimize CND suite to enable transition to Joint Regional Security Stack (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 tactical sensor infrastructure. - Complete prototyping assessments for high assurance infrastructure in support of Zero Trust Architecture (ZTA).					
FY 2022 Base Plans: - Complete major CND security operation workstation upgrades, upgrades to Load Balancers, addressing endpoint security gaps in the CND Architecture and updates to the Detonation Malware Analysis Capability at NCDOC. - Continue to manage obsolescence through technical refreshes and capability upgrades to CND subsystems. - Continue to develop and enhance Navy's portion of the NC3-N and BMD cyber security system of systems within the CND architecture.					

Exhibit R-2A, RDT&E Project Justification: PB 2022 Navy		Date: May 2021
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 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total
- 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. - Continue to optimize CND to enable transition to 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 tactical sensor infrastructure. -Begin fielding high assurance infrastructure in support of ZTA. ***FY 2022 OCO Plans:*** N/A ***FY 2021 to FY 2022 Increase/Decrease Statement:*** No significant changes from FY21 to FY22; funding increased for inflation.					
Title: Navy Cryptography (Crypto)	10.608	7.198	7.113	0.000	7.113
Articles:	-	-	-	-	-
FY 2021 Plans: -FY21 decrease is due to the completion of a three-year development effort of KGV-11M End Cryptographic Units (ECU). - Continue Advanced Cryptographic Capabilities (ACC) Solutions Development and Product Testing - Continue ACC Deliveries - Complete KGV-11M National Security Agency (NSA) Certification to initiate the Full Rate Production (FRP) for KGV-11M. - Continue to provide development and security engineering for modernization of Department of Navy (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 2022 Base Plans:*** - Continue Advanced Cryptographic Capabilities (ACC) Solutions Development and Product Testing					

Exhibit R-2A, RDT&E Project Justification: PB 2022 Navy		Date: May 2021
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 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total
- Continue ACC Deliveries - Commence KGV-11M Deliveries - 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 VACM ancillary devices. - Continue to develop Navy strategy and implementation plan to modernize secure voice architectures within Navy networks. ***FY 2022 OCO Plans:*** N/A ***FY 2021 to FY 2022 Increase/Decrease Statement:*** No significant changes from FY21 to FY22.					
Title: Key Management (KM)	0.786	1.010	1.026	0.000	1.026
Articles:	-	-	-	-	-
FY 2021 Plans: - FY21 increase aligns to the initial development of Capability Increment (CI)-3 Spiral 3 Spin 2 Development, Integration and Testing. - Begin the development, engineering and testing of Key Management Infrastructure (KMI) CI-3, Spiral 3 Spin 2. - Continue migrating Communications Security (COMSEC) Management Workstation (CMWS) and the follow on to Simple Key Loader (SKL) into the KMI environment. - Complete the development, engineering and testing of KMI CI-3, Spiral 3 Spin 1 including the integration of iApp within a network environment, which will enhance the accounting for and distribution of KMI key delivery. ***FY 2022 Base Plans:*** - Continue the development, engineering and testing of KMI CI-3, Spiral 3 Spin 2. - Continue migrating COMSEC CMWS and the follow on to SKL into the KMI environment. ***FY 2022 OCO Plans:*** N/A ***FY 2021 to FY 2022 Increase/Decrease Statement:***					

Exhibit R-2A, RDT&E Project Justification: PB 2022 Navy		Date: May 2021
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 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total
No significant changes from FY21 to FY22; funding increase to account for inflation.					
Title: SHARKCAGE	6.658	6.706	2.598	0.000	2.598
Articles:	-	-	-	-	-
FY 2021 Plans: - Continue the expansion of the Nuclear Command, Control, and Communications, Navy (NC3-N) mission's capability within the SHARKCAGE environment (details held at a higher classification). - Continue the enhancement of capabilities to the SHARKCAGE Defensive Cyberspace Operations (DCO) enclave to address additional fleet requirements as the emerging threats evolve. Development efforts include network taps, sensors, and analytic toolsets for passively monitoring multiple Navy ashore and afloat networks and enclaves. - Continue the expansion of the development of analysis components and event collection activities for ashore nodes and afloat units for the deployed Cyber Protection Teams (CPT) community.					
FY 2022 Base Plans: - Continue the expansion of the NC3-N mission's capability within the SHARKCAGE environment (details held at a higher classification). - Continue the enhancement of capabilities to the SHARKCAGE DCO enclave to address additional fleet requirements as the emerging threats evolve. Integration efforts include network taps, sensors, and analytic toolsets for passively monitoring multiple Navy ashore and afloat networks and enclaves. -Commence SHARKCAGE Program of Record (POR) Development Contract Award.					
FY 2022 OCO Plans: N/A					
FY 2021 to FY 2022 Increase/Decrease Statement: FY22 decrease is due to maturity of the current SHARKCAGE Commercial off the Shelf/Government off the Shelf (COTS/GOTS) capabilities that are integrated together to support the POR system.					
Title: Public Key Infrastructure (PKI)	0.365	0.402	0.408	0.000	0.408
Articles:	-	-	-	-	-
FY 2021 Plans: - Continue Navy compliance and compatibility with Department of Defense (DoD) PKI implementation, cryptographic algorithms and development efforts, to include Computer Network Defense (CND), enhanced algorithms and other encryption methodologies, Navy Certificate Validation Infrastructure (NCVI) enhancements					

Exhibit R-2A, RDT&E Project Justification: PB 2022 Navy		Date: May 2021
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 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total
for afloat and ashore environments, Common Access Card (CAC) configuration modifications, Network (NIPRNet) Enterprise Alternate Token System (NEATS), Non-Person Entity (NPE), and Secret Internet Protocol Router Network (SIPRNet) Token Management System. ***FY 2022 Base Plans:*** - Continue Navy compliance and compatibility with DoD PKI implementation, cryptographic algorithms and development efforts, to include CND, enhanced algorithms and other encryption methodologies, NCVI enhancements for afloat and ashore environments, CAC configuration modifications, NEATS, NPE, and SIPRNet Token Management System. ***FY 2022 OCO Plans:*** N/A ***FY 2021 to FY 2022 Increase/Decrease Statement:*** No significant changes from FY21 to FY22; funding increased for inflation.					
Title: Navy Cyber Situational Awareness (NCSA)	4.923	3.985	2.387	0.000	2.387
Articles:	-	-	-	-	-
FY 2021 Plans: - FY21 decrease reflects a realignment within NCSA from Research, Development, Test and Evaluation (RDT&E) to Operations and Maintenance, Navy (OM,N) due to a change in engineering and fielding strategy to be a predominantly software solution hosted by other planned Defensive Cyberspace Operations/ Network Operations (DCO/NETOPS) systems. - Shift engineering strategy to be a predominantly software solution providing monitoring of relevant Navy networks providing near real-time visualization and analytics of the cyberspace domain in Navy mission context. - Continue the development of a shared and tailorable Maritime Cyber "Integrated" Cyber Common Operations Center (COP) external to Fleet Cyber Command/Commander Tenth Fleet (FCC/C10F) to include all geographic Maritime Operations Center (MOCs) to enable assessments of cyber vulnerabilities, threats, and risks relative to Navy missions. - NCSA maturation will provide monitoring of relevant and current Navy networks providing near real-time visualization and analytics of the cyberspace domain. ***FY 2022 Base Plans:***					

Exhibit R-2A, RDT&E Project Justification: PB 2022 Navy		Date: May 2021
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 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total
- Continue the development of a shared and tailorable Maritime Cyber "Integrated" COP external to FCC/C10F to include all geographic MOCs to enable assessments of cyber vulnerabilities, threats, and risks relative to Navy missions. - Expand access to mission critical cyber data to provide actionable information to afloat Commanders to understand and mitigate cyber risk to mission. ***FY 2022 OCO Plans:*** N/A ***FY 2021 to FY 2022 Increase/Decrease Statement:*** FY22 decrease is due to the reduction of new data feed ingestion resulting in less development and also a shift of effort to maintaining current data feeds and incremental capability improvements to the existing baseline using Operations and Maintenance, Navy (OM,N).					
Title: Cybersecurity Coordination	2.341	2.435	2.452	0.000	2.452
Articles:	-	-	-	-	-
FY 2021 Plans: - Continue coordination and alignment with Joint Information Environment (JIE) (e.g., JRSS, JMS, Tactical Processing Node (TPN) etc.) and the Integrated Navy Operations Command and Control System (INOCCS) 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. - Develop implementation strategies for the incorporation of Zero Trust Architecture (ZTA) concepts into the Navy's tactical Command, Control, Communication, Computers, & Intelligence (C4I) cybersecurity environment. - 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 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.					

Exhibit R-2A, RDT&E Project Justification: PB 2022 Navy		Date: May 2021
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 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total
- 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 2022 Base Plans:*** - Continue coordination and alignment with JIE (e.g., JRSS, JMS, Tactical Processing Node (TPN) etc.) and the Integrated Navy Operations Command and Control System (INOCCS) 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 developing implementation strategies for the incorporation of Zero Trust Architecture (ZTA) concepts into the Navy's tactical C4I cybersecurity environment. - 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 2022 OCO Plans:*** N/A ***FY 2021 to FY 2022 Increase/Decrease Statement:*** No significant changes from FY21 to FY22; funding increased for inflation.					
Accomplishments/Planned Programs Subtotals	38.894	36.644	31.102	0.000	31.102

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total	FY 2023	FY 2024	FY 2025	FY 2026	Cost To Complete	Total Cost
• OPN/3415: *Info Systems Security Program (ISSP)*	166.540	157.551	146.879	-	146.879	-	-	-	-	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2022 Navy		Date: May 2021
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total	FY 2023	FY 2024	FY 2025	FY 2026	Cost To Complete	Total Cost

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 ashore platforms. Recognizing the need for future CND capability improvements, the CND program implements an evolutionary acquisition strategy that continuously modernizes and refreshes end-of-life/end-of-service capabilities to ensure the latest cybersecurity tools are protecting the Navy's tactical networks.

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 KGV-11M program is being 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: SHARKCAGE is transitioning from Rapid Deployment Capability (RDC) to Program of Record and will leverage COTS software and hardware configured to existing Navy networks and enclaves to detect, analyze, and assess cyber threats. In FY22, SHARKCAGE will commence a single award contract and 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 ashore 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 Deliberate Acquisition Activities will continue to 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

Exhibit R-2A, RDT&E Project Justification: PB 2022 Navy		Date: May 2021
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*

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.

Exhibit R-3, RDT&E Project Cost Analysis: PB 2022 Navy			Date: May 2021
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 2020 Cost	FY 2020 Award Date	FY 2021 Cost	FY 2021 Award Date	FY 2022 Base Cost	FY 2022 Base Award Date	FY 2022 OCO Cost	FY 2022 OCO Award Date	FY 2022 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Development (PY)	Various	Various : Various	190.205	0.000		0.000		0.000		-		0.000	-	-	-
Hardware Development (WR)	WR	NIWC PACIFIC : San Diego, CA	17.911	2.641	Oct 2019	3.918	Oct 2020	3.056	Oct 2021	-		3.056	-	-	-
Hardware Development	C/CPFF	NIWC PACIFIC : San Diego, CA	5.054	0.777	Dec 2019	2.802	Dec 2020	2.768	Oct 2021	-		2.768	-	-	-
Hardware Development (WR)	WR	NIWC ATLANTIC : Charleston, SC	6.175	0.510	Oct 2019	0.630	Oct 2020	0.176	Oct 2021	-		0.176	-	-	-
Hardware Development	C/CPFF	NIWC ATLANTIC : Charleston, SC	3.822	0.956	Jan 2020	1.112	Jan 2021	0.192	Oct 2021	-		0.192	-	-	-
Hardware Development	C/CPIF	Viasat : San Diego, CA	3.500	3.100	Apr 2020	0.000		0.000		-		0.000	-	-	-
Software Development (WR)	WR	NIWC PACIFIC : San Diego, CA	40.293	6.460	Oct 2019	6.202	Oct 2020	4.646	Oct 2021	-		4.646	-	-	-
Software Development	C/CPFF	NIWC PACIFIC : San Diego, CA	17.343	4.421	Dec 2019	3.792	Dec 2020	3.641	Dec 2021	-		3.641	-	-	-
Software Development (WR)	WR	NIWC ATLANTIC : Charleston, SC	10.823	1.997	Oct 2019	2.191	Oct 2020	2.858	Oct 2021	-		2.858	-	-	-
Software Development	C/CPFF	NIWC ATLANTIC : Charleston, SC	17.297	3.701	Jan 2020	2.667	Jan 2021	3.280	Dec 2021	-		3.280	-	-	-
Software Development	FFRDC	MITRE : McLean, VA	6.727	1.808	Dec 2019	2.193	Dec 2020	0.652	Dec 2021	-		0.652	-	-	-
Software Development	Various	Various : Various	68.015	0.475	Dec 2019	0.680	Dec 2020	0.789	Dec 2021	-		0.789	-	-	-
Software Development	C/CPFF	BAH : San Diego, CA	11.136	2.506	Jan 2020	1.517	Jan 2021	1.652	Jan 2022	-		1.652	-	-	-
Software Development	FFRDC	GTRI : Atlanta, GA	18.591	2.917	Jan 2020	1.043	Jan 2021	0.569	Jan 2022	-		0.569	-	-	-
Software Development	WR	NSMA : San Diego, CA	5.263	1.459	Oct 2019	0.937	Oct 2020	0.650	Oct 2021	-		0.650	-	-	-
Software Development	WR	NRL : Washington DC	3.899	0.808	Oct 2019	1.439	Oct 2020	1.169	Oct 2021	-		1.169	-	-	-
		Subtotal	426.054	34.536		31.123		26.098		-		26.098	-	-	N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2022 Navy			Date: May 2021
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 2020 Cost	FY 2020 Award Date	FY 2021 Cost	FY 2021 Award Date	FY 2022 Base Cost	FY 2022 Base Award Date	FY 2022 OCO Cost	FY 2022 OCO Award Date	FY 2022 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Architecture	WR	Various : Various	6.142	0.222	Oct 2019	0.138	Oct 2020	0.123	Oct 2021	-		0.123	-	-	-
Architecture	WR	NIWC ATLANTIC : Charleston, SC	2.943	0.424	Oct 2019	0.404	Oct 2020	0.216	Oct 2021	-		0.216	-	-	-
Architecture	WR	NIWC PACIFIC : San Diego, CA	0.000	0.000		0.450	Oct 2020	0.000		-		0.000	-	-	-
Requirements Analysis	C/CPFF	BAH : San Diego, CA	6.650	0.372	Jan 2020	0.968	Jan 2021	0.945	Jan 2022	-		0.945	-	-	-
Studies & Design	WR	Various : Various	7.057	0.372	Oct 2019	0.339	Oct 2020	0.353	Oct 2021	-		0.353	-	-	-
		Subtotal	22.792	1.390		2.299		1.637		-		1.637	-	-	N/A

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2020 Cost	FY 2020 Award Date	FY 2021 Cost	FY 2021 Award Date	FY 2022 Base Cost	FY 2022 Base Award Date	FY 2022 OCO Cost	FY 2022 OCO Award Date	FY 2022 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
System DT&E	WR	NIWC PACIFIC : San Diego, CA	38.608	0.298	Oct 2019	0.788	Oct 2020	0.817	Oct 2021	-		0.817	-	-	-
System DT&E	WR	COTF : Norfolk, VA	2.715	0.652	Dec 2019	0.000		0.000		-		0.000	-	-	-
System DT&E	C/CPFF	BAH : San Diego, CA	3.017	0.767	Jan 2020	1.000	Jan 2021	1.265	Jan 2022	-		1.265	-	-	-
System DT&E	WR	NIWC ATLANTIC : Charleston, SC	0.000	0.000		0.234	Oct 2020	0.000		-		0.000	-	-	-
		Subtotal	44.340	1.717		2.022		2.082		-		2.082	-	-	N/A

Management Services ($ in Millions)

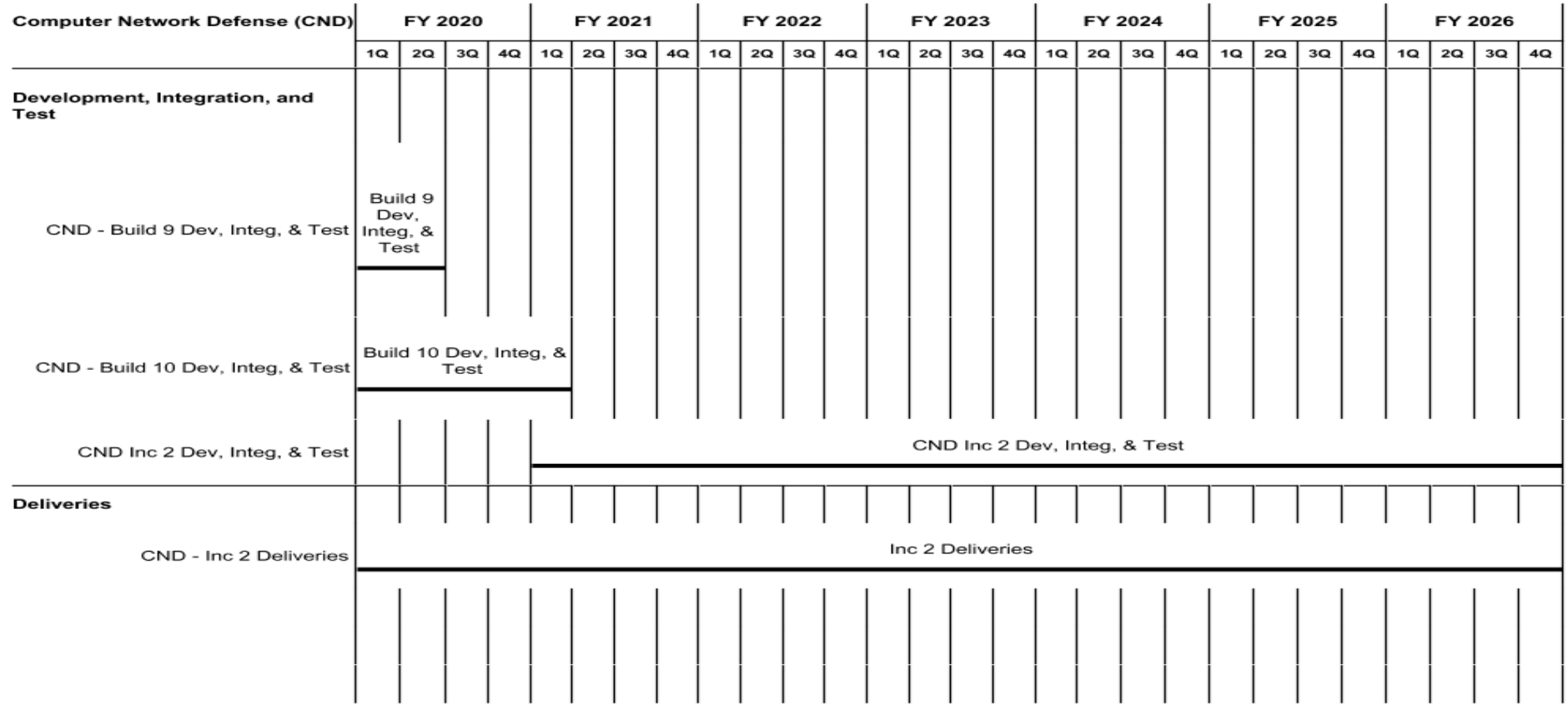
Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2020 Cost	FY 2020 Award Date	FY 2021 Cost	FY 2021 Award Date	FY 2022 Base Cost	FY 2022 Base Award Date	FY 2022 OCO Cost	FY 2022 OCO Award Date	FY 2022 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Program Management	C/CPFF	BAH : San Diego, CA	32.087	1.251	Jan 2020	1.200	Jan 2021	1.285	Jan 2022	-		1.285	-	-	-
		Subtotal	32.087	1.251		1.200		1.285		-		1.285	-	-	N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2022 Navy			Date: May 2021
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 2020		FY 2021		FY 2022 Base		FY 2022 OCO		FY 2022 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	525.273	38.894		36.644		31.102		-		31.102	-	-	N/A

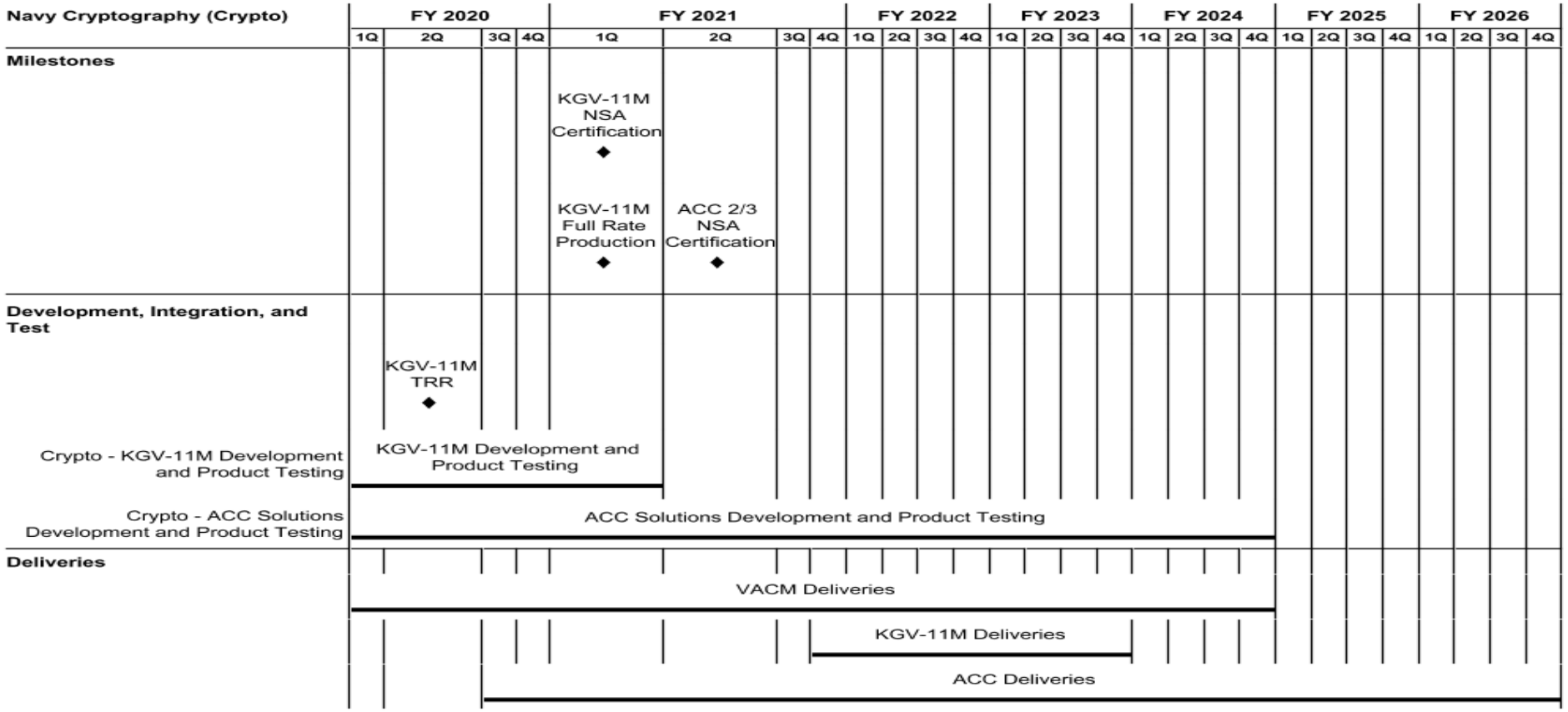
Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2022 Navy		Date: May 2021
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*



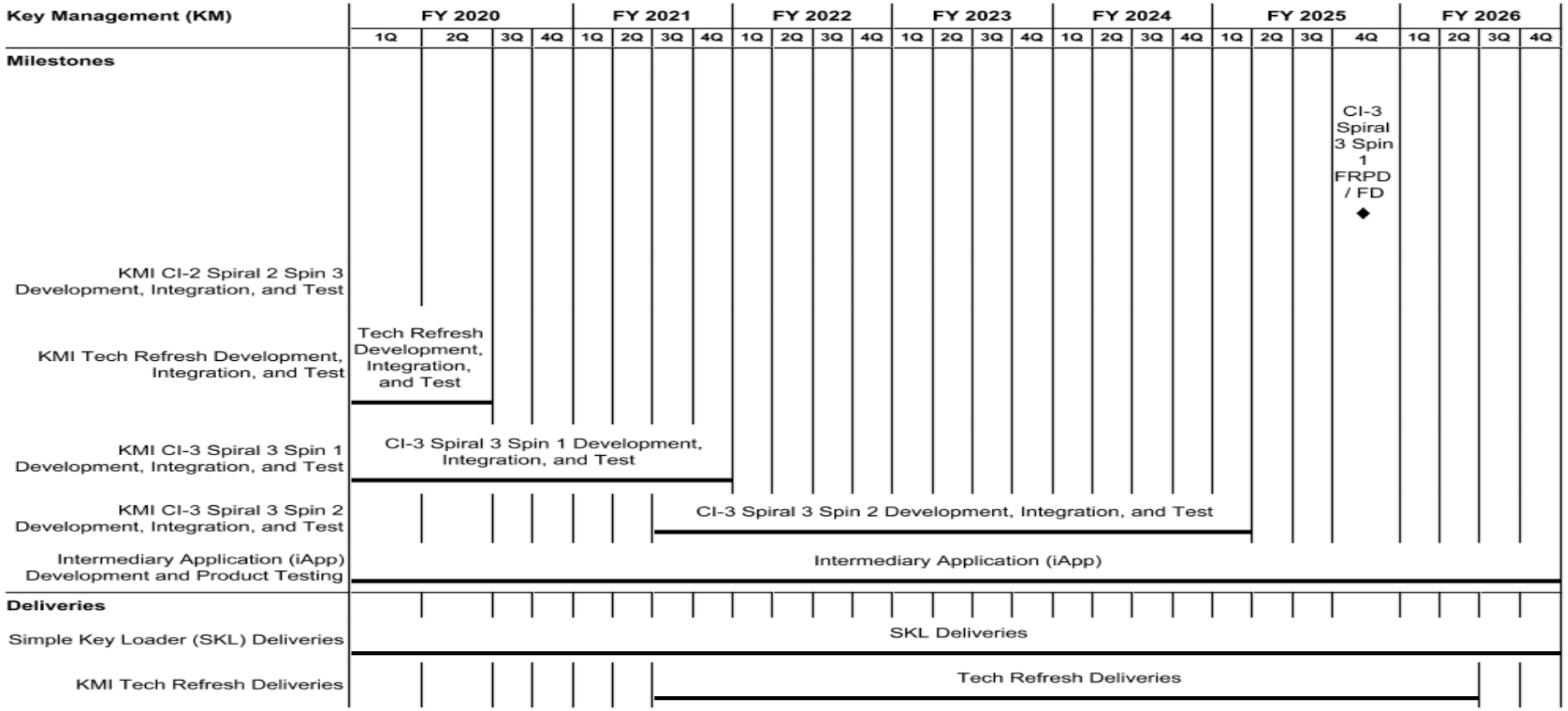
2022PB - 0303140N - 0734

Exhibit R-4, RDT&E Schedule Profile: PB 2022 Navy		Date: May 2021
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*



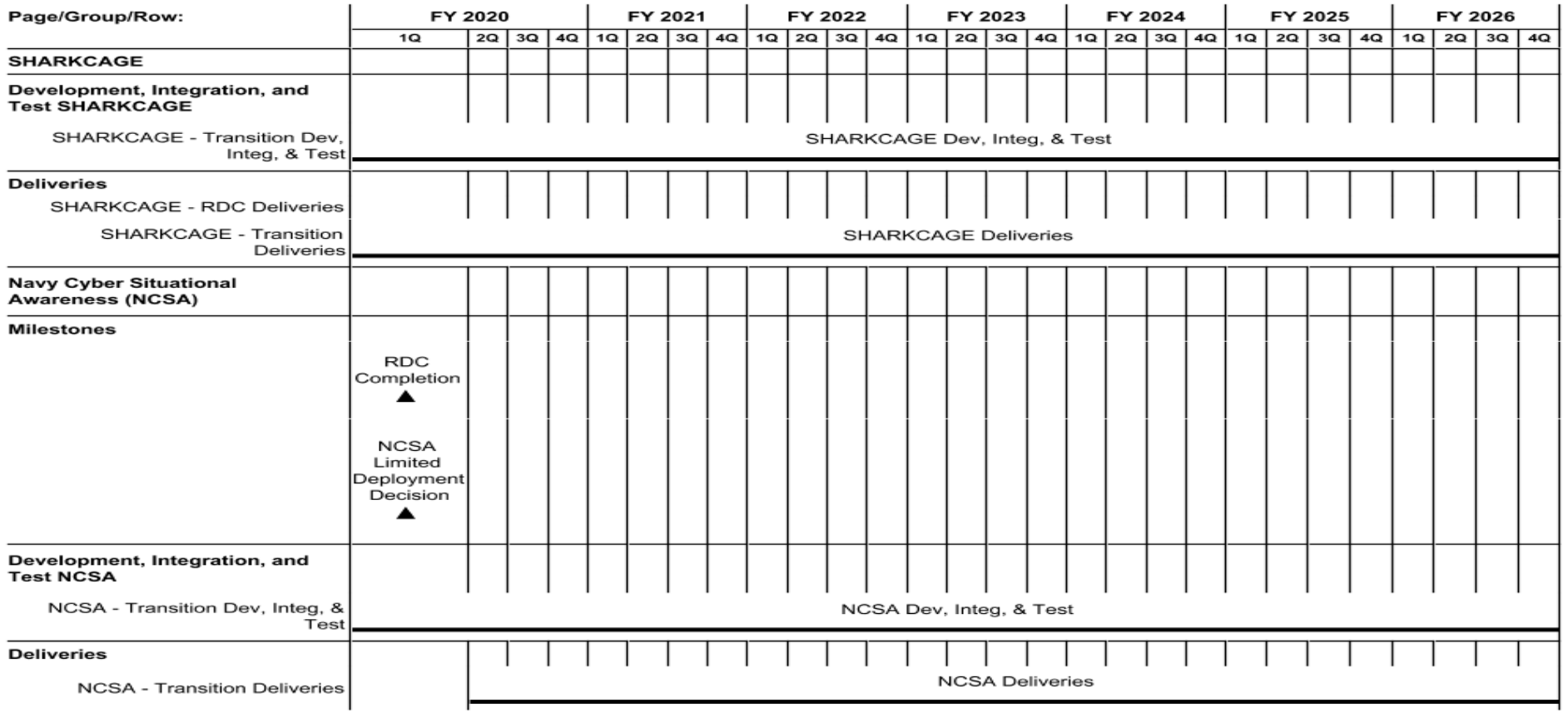
2022PB - 0303140N - 0734

Exhibit R-4, RDT&E Schedule Profile: PB 2022 Navy		Date: May 2021
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*



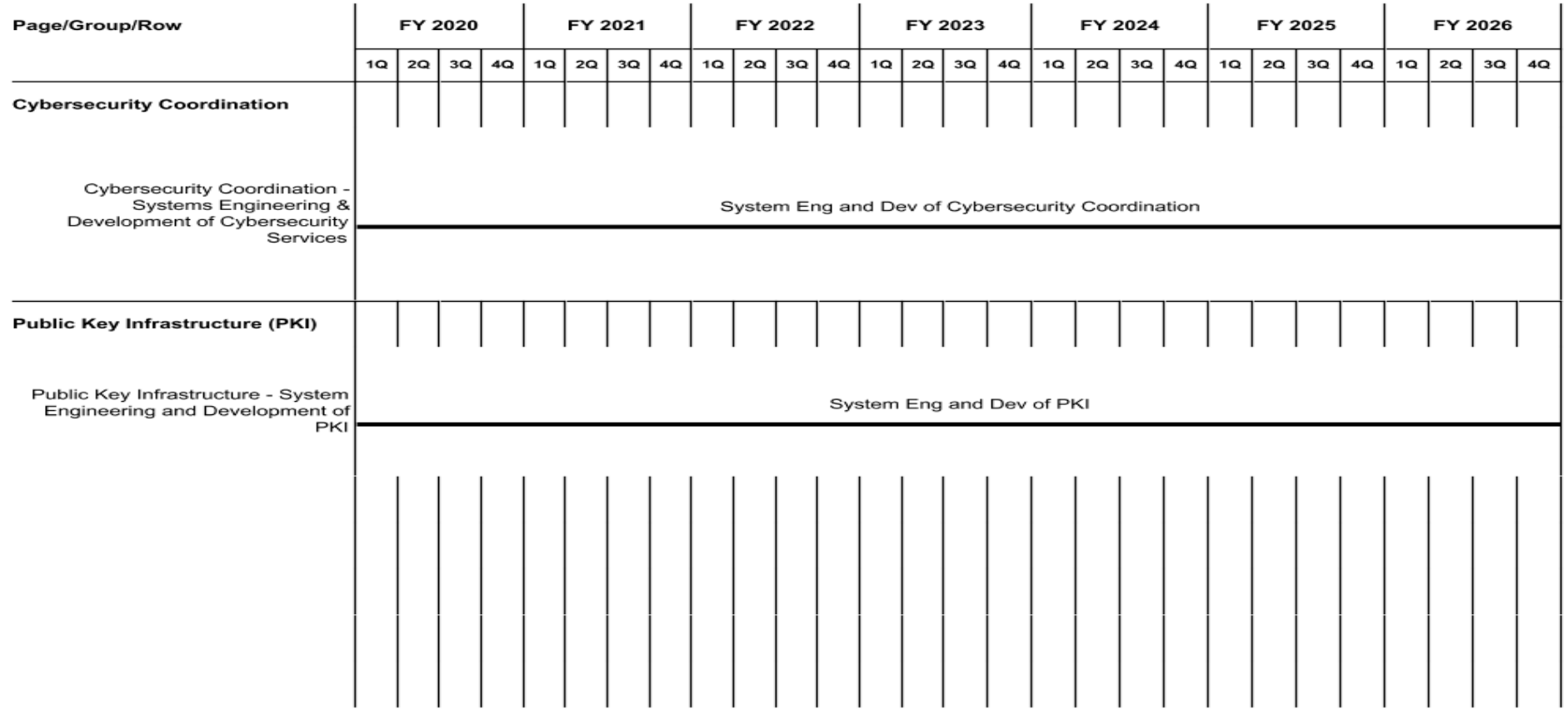
2022PB - 0303140N - 0734

Exhibit R-4, RDT&E Schedule Profile: PB 2022 Navy		Date: May 2021
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*



2022PB - 0303140N - 0734

Exhibit R-4, RDT&E Schedule Profile: PB 2022 Navy		Date: May 2021
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*



2022PB - 0303140N - 0734

Exhibit R-4A, RDT&E Schedule Details: PB 2022 Navy		Date: May 2021
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**
Computer Network Defense (CND)				
Development, Integration, and Test: CND - Build 9 Dev, Integ, & Test:	1	2020	2	2020
Development, Integration, and Test: CND - Build 10 Dev, Integ, & Test:	1	2020	1	2021
Development, Integration, and Test: CND Inc 2 Dev, Integ, & Test:	1	2021	4	2022
Deliveries: CND - Inc 2 Deliveries:	1	2020	4	2022
Navy Cryptography (Crypto)				
Milestones: Crypto - KGV-11M NSA Certification	1	2021	1	2021
Milestones: Crypto - KGV-11M Full Rate Production	1	2021	1	2021
Milestones: Crypto - ACC 2/3 NSA Certification	2	2021	2	2021
Development, Integration, and Test: Crypto - KGV-11M TRR	2	2020	2	2020
Development, Integration, and Test: Crypto - KGV-11M Development and Product Testing:	1	2020	1	2021
Development, Integration, and Test: Crypto - ACC Solutions Development and Product Testing:	1	2020	4	2022
Deliveries: Crypto - VACM Deliveries	1	2020	4	2022
Deliveries: Crypto - KGV-11M Deliveries	4	2021	4	2022
Deliveries: Crypto - ACC Deliveries	3	2020	4	2022
Key Management (KM)				
Milestones: KMI Tech Refresh Development, Integration, and Test:	1	2020	2	2020
Milestones: KMI CI-3 Spiral 3 Spin 1 Development, Integration, and Test:	1	2020	4	2021
Milestones: KMI CI-3 Spiral 3 Spin 2 Development, Integration, and Test:	3	2021	4	2022
Milestones: Intermediary Application (iApp) Development and Product Testing:	1	2020	4	2022
Deliveries: Simple Key Loader (SKL) Deliveries:	1	2020	4	2022

Exhibit R-4A, RDT&E Schedule Details: PB 2022 Navy		Date: May 2021
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**
Deliveries: KMI Tech Refresh Deliveries:	3	2021	4	2022
Page/Group/Row:				
Development, Integration, and Test SHARKCAGE: SHARKCAGE - Transition Dev, Integ, & Test:	1	2020	4	2022
Deliveries: SHARKCAGE - Transition Deliveries:	1	2020	4	2022
Milestones: NCSA - RDC Completion	1	2020	1	2020
Milestones: NCSA - NCSA Transition Limited Deployment Decision	1	2020	1	2020
Development, Integration, and Test NCSA: NCSA - Transition Dev, Integ, & Test:	1	2020	4	2022
Deliveries: NCSA - Transition Deliveries:	2	2020	4	2022
Page/Group/Row				
Cybersecurity Coordination: Cybersecurity Coordination - Systems Engineering & Development of Cybersecurity Services:	1	2020	4	2022
Public Key Infrastructure (PKI): Public Key Infrastructure - System Engineering and Development of PKI:	1	2020	4	2022

Exhibit R-2A, RDT&E Project Justification: PB 2022 Navy												Date: May 2021
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 2020**	**FY 2021**	**FY 2022 Base**	**FY 2022 OCO**	**FY 2022 Total**	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**Cost To Complete**	**Total Cost**
3230: *Information Assurance*	22.690	2.076	2.170	2.209	-	2.209	-	-	-	-	-	-
Quantity of RDT&E Articles		-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

The goal of the Information Systems Security Program (ISSP) is to ensure the continued protection of Navy and joint information and information systems from hostile exploitation and attack. The 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 the protection of Information Systems, including weapons systems. 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, as well as developing information assurance technology and systems that are resilient and survivable in the face of adversarial attacks. Features that are critical in supporting the Navy's concept of Distributed Maritime Operations (DMO).

The rapid rate of change in the underlying commercial and government information infrastructures makes the provision of security an increasingly complex and dynamic problem. Information Assurance (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

Exhibit R-2A, RDT&E Project Justification: PB 2022 Navy		Date: May 2021
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 3230 / *Information Assurance*

configurations of network security components to implement changes in real time or near real time. 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 Information Assurance (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 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total
Title: Information Assurance (IA)	2.076	2.170	2.209	0.000	2.209
Articles:	-	-	-	-	-
FY 2021 Plans: - Complete 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. - Ensure technology meets low-latency requirements of interconnecting naval systems. - Complete 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. - Complete 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. - Continue 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. - 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 tools to automatically analyze and reverse engineer malware of unknown provenance at scale. This includes rapid prototyping and fielding of novel digital content inspection mechanisms					

Exhibit R-2A, RDT&E Project Justification: PB 2022 Navy		Date: May 2021
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 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total
that identify indicators of compromise and generate tailored defensive countermeasures to emerging cyber threats. - Initiate the development of new cyber tools/technology to provide dynamic maneuvering/moving target defense of critical naval assets to reduce the attack surface and obviate vulnerabilities prior to exploitation. This includes addressing protocols, input/output resources and stacks, and system software; with emphasis on advanced persistent threats (APTs). ***FY 2022 Base Plans:*** - Complete the development of intelligent security components and infrastructure capable of protecting Navy critical cyber assets through intelligent, autonomous self-diagnostics, automated damage assessment, and self-healing capabilities. - 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 tools to automatically analyze and reverse engineer malware of unknown provenance at scale. This includes rapid prototyping and fielding of novel digital content inspection mechanisms that identify indicators of compromise and generate tailored defensive countermeasures to emerging cyber threats. - Continue the development of new cyber tools/technology to provide dynamic maneuvering/moving target defense of critical naval assets to reduce the attack surface and obviate vulnerabilities prior to exploitation. This includes addressing protocols, input/output resources and stacks, and system software; with emphasis on Advanced Persistent Threats (APTs). - Initiate the development of tools/technology to provide a cloud application trust in its host infrastructure. Address SDN-based traffic protection amongst containers deployed on low-trust providers and provide attestation to verify its host complies with a stated network security policy. - Initiate the development of tools/technologies that enable scalable, secure device to device tactical communications. This includes addressing fine grained access controls and fully decentralized authorization and enforcement of security policies that enables a self-organizing distributed network in disconnected environments. - Initiate the development of tools to measure and reduce collateral damage incurred by cyber operations. Implement techniques for multimodal sensing, dependency analysis through causal inference, and fusion of active and passive measurements for iterative sensing and reconnaissance. ***FY 2022 OCO Plans:***					

Exhibit R-2A, RDT&E Project Justification: PB 2022 Navy		Date: May 2021
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 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total
N/A ***FY 2021 to FY 2022 Increase/Decrease Statement:*** No significant changes from FY21 to FY22.					
Accomplishments/Planned Programs Subtotals	2.076	2.170	2.209	0.000	2.209

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2022 Navy			Date: May 2021
Appropriation/Budget Activity 1319 / 7	R-1 Program Element (Number/Name) PE 0303140N / *Information Sys Security Program*	Project (Number/Name) 3230 / *Information Assurance*	

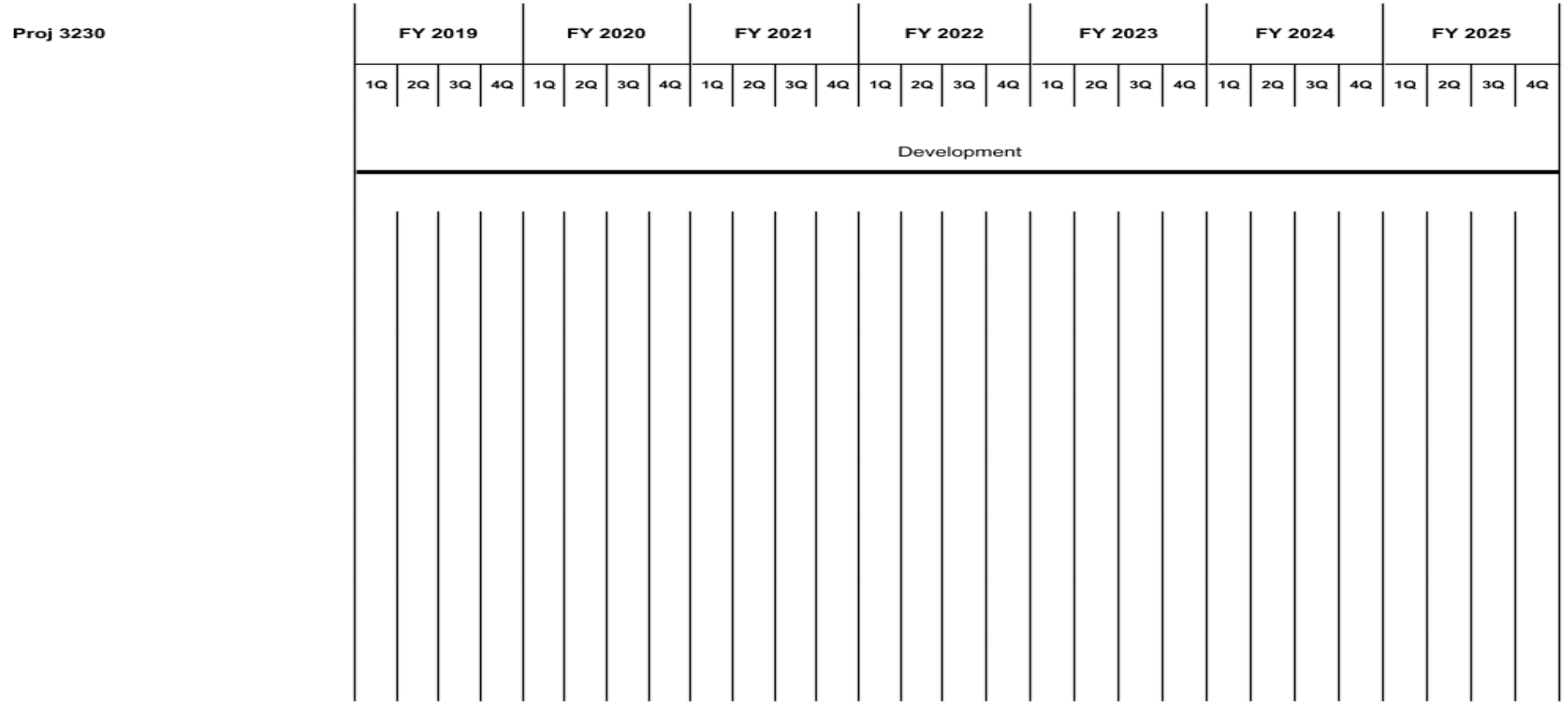
Support ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2020 Cost	FY 2020 Award Date	FY 2021 Cost	FY 2021 Award Date	FY 2022 Base Cost	FY 2022 Base Award Date	FY 2022 OCO Cost	FY 2022 OCO Award Date	FY 2022 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Development Support	Various	NRL : Washington, DC	22.690	2.076	Nov 2019	2.170	Nov 2020	2.209	Nov 2021	-		2.209	-	-	-
		Subtotal	22.690	2.076		2.170		2.209		-		2.209	-	-	N/A

	Prior Years	FY 2020		FY 2021		FY 2022 Base		FY 2022 OCO		FY 2022 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	22.690	2.076		2.170		2.209		-		2.209	-	-	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2022 Navy		Date: May 2021
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 3230 / *Information Assurance*



2021OSD - 0303140N - 3230

Exhibit R-4A, RDT&E Schedule Details: PB 2022 Navy		Date: May 2021
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	2020	4	2022

Exhibit R-2A, RDT&E Project Justification: PB 2022 Navy												Date: May 2021
Appropriation/Budget Activity 1319 / 7					R-1 Program Element (Number/Name) PE 0303140N / *Information Sys Security Program*				Project (Number/Name) 9999 / *Congressional Adds*			
COST ($ in Millions)	**Prior Years**	**FY 2020**	**FY 2021**	**FY 2022 Base**	**FY 2022 OCO**	**FY 2022 Total**	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**Cost To Complete**	**Total Cost**
9999: *Congressional Adds*	0.000	2.896	0.000	0.000	-	0.000	-	-	-	-	-	-
Quantity of RDT&E Articles		-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

The goal of the Information Systems Security Program (ISSP) is to ensure the continued protection of Navy and joint information and information systems from hostile exploitation and attack. The 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 the protection of Information Systems, including weapons systems. 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, as well as developing information assurance technology and systems that are resilient and survivable in the face of adversarial attacks. Features that are critical in supporting the Navy's concept of Distributed Maritime Operations (DMO). 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 included funds for advanced technology development, test and evaluation of naval information systems security based on leading edge technologies that improved information assurance (e.g., situational awareness and information infrastructure protection) across all command echelons to tactical units afloat and war fighters ashore. This effort provided 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 provided 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 also developed 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 developed common architectural frameworks that facilitated integration of network security capabilities, enabled effective seamless interoperation, and contributed to a common consistent picture of the networked environment with respect to information assurance and security. This effort addressed 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 also initiated 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 included the architectural definition of situational awareness and visualization capabilities to support active computer network defense and support underlying data mining and correlation tools, and addressed 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 also initiated requirements definition for secure coalition data exchange and interoperation among security levels and classifications, and ensured approaches address various security level technologies as well as emerging architectural

Exhibit R-2A, RDT&E Project Justification: PB 2022 Navy		Date: May 2021
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 9999 / *Congressional Adds*

methods of providing interoperability across different security levels. IA examined multi-level aware applications and technologies including databases, web browsers, routers/switches, etc. Efforts also initiated 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 ensured the architectures evolved to provide proper protection as technology, Department of Defense (DoD) missions, and threats continuously evolved. 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 initiated 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 provided 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)	FY 2020	FY 2021
Congressional Add: High assurance infrastructure in defense systems	2.896	0.000
FY 2020 Accomplishments: N/A		
FY 2021 Plans: N/A		
Congressional Adds Subtotals	2.896	0.000

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2022 Navy		Date: May 2021
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 9999 / *Congressional Adds*

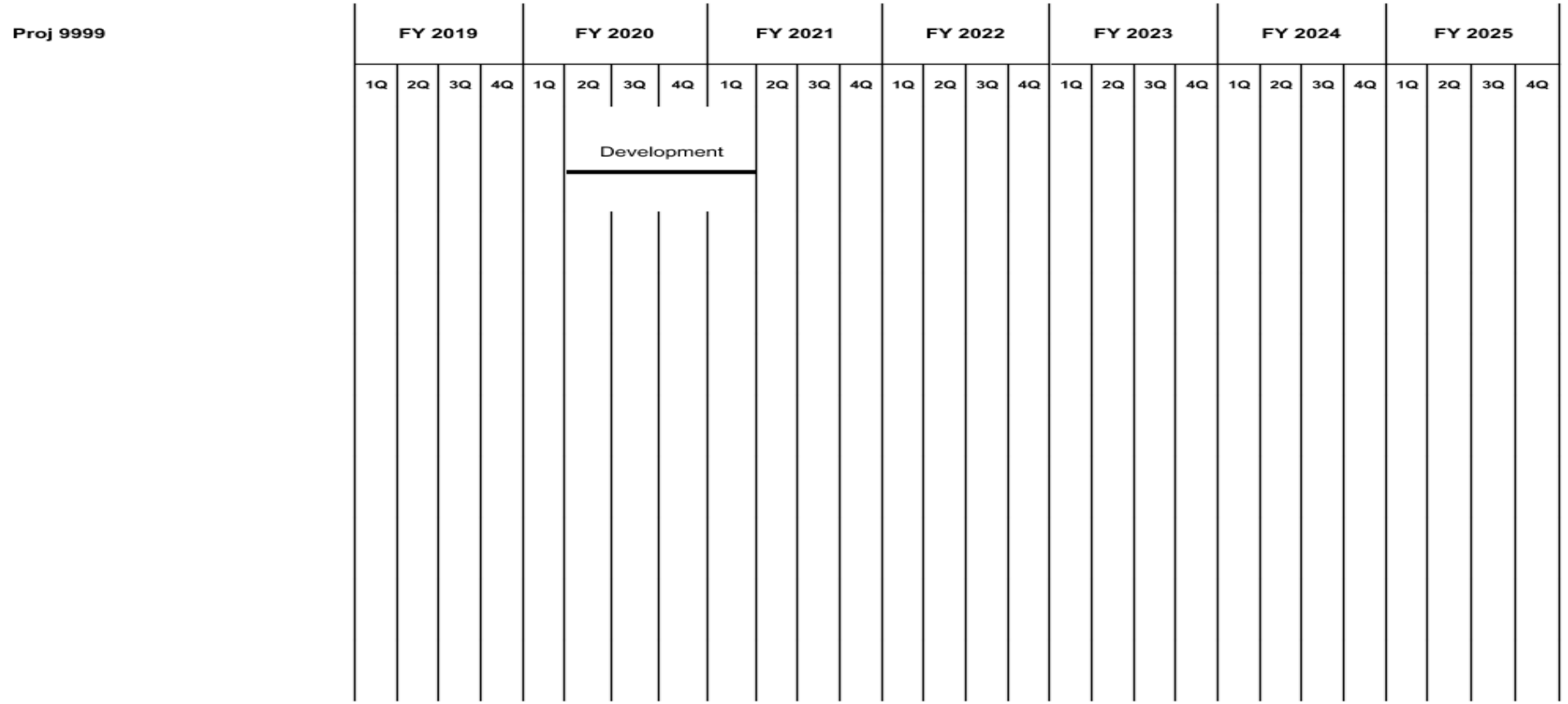
Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2020 Cost	FY 2020 Award Date	FY 2021 Cost	FY 2021 Award Date	FY 2022 Base Cost	FY 2022 Base Award Date	FY 2022 OCO Cost	FY 2022 OCO Award Date	FY 2022 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Software Development	WR	NIWC ATLANTIC : Charleston, SC	0.000	2.896	Jan 2020	0.000		0.000		-		0.000	-	-	-
		Subtotal	0.000	2.896		0.000		0.000		-		0.000	-	-	N/A

	Prior Years	FY 2020		FY 2021		FY 2022 Base		FY 2022 OCO		FY 2022 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	0.000	2.896		0.000		0.000		-		0.000	-	-	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2022 Navy		Date: May 2021
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 9999 / *Congressional Adds*



2021PB - 0303140N - 9999

Exhibit R-4A, RDT&E Schedule Details: PB 2022 Navy		Date: May 2021
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 9999 / *Congressional Adds*

Schedule Details

	Start		End	
Events by Sub Project	**Quarter**	**Year**	**Quarter**	**Year**
Proj 9999				
Development	2	2020	1	2021