Exhibit R-2, RDT&E Budget Item Justification: PB 2025 Navy											Date: March 2024	
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 2023**	**FY 2024**	**FY 2025 Base**	**FY 2025 OCO**	**FY 2025 Total**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2029**	**Cost To Complete**	**Total Cost**
Total Program Element	659.637	33.036	33.390	35.339	-	35.339	35.875	36.031	36.257	37.026	Continuing	Continuing
0734: *Communications Security R&D*	630.586	30.848	31.089	33.110	-	33.110	33.481	33.589	33.766	34.483	Continuing	Continuing
3230: *Information Assurance*	29.051	2.188	2.301	2.229	-	2.229	2.394	2.442	2.491	2.543	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 NSS, including other mission requirements (details held at a higher classification), 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 2025 Navy	Date: March 2024
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 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
Previous President's Budget	33.752	33.390	34.794	-	34.794
Current President's Budget	33.036	33.390	35.339	-	35.339
Total Adjustments	-0.716	0.000	0.545	-	0.545
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-0.716	0.000			
• Program Adjustments	0.000	0.000	0.545	-	0.545
• Rate/Misc Adjustments	0.000	0.000	0.000	-	0.000

Change Summary Explanation

FUNDING:
The FY 2025 funding request was increased by $0.545M from previous President's Budget to implement Crypto Modernization 2.

TECHNICAL:

Key Management (KM):
NSA changed methodology from Spirals and Spins to Releases. The KMI program will implement an Agile Development approach that will incorporate the tenets of a Development, Security, and Operations (DevSecOps) development methodology for the continued development of KMI CI-3 capabilities implementing Releases 0 thru 9.

SCHEDULE:

Navy Cryptography (Crypto):

- Shifted KGV-11M deliveries to Q2-Q4 FY24.

Key Management (KM):

Exhibit R-2, RDT&E Budget Item Justification: PB 2025 Navy	Date: March 2024
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*

- CI-3 Full Rate Production Decision (FRPD)/Fielding Decision (FD) shifted from Q1FY24 to Q2FY24 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 Release 0 deployment scheduled for Q1FY24.
- CI-3 Release 1-3 Development and Integration completed Q2FY23
- CI-3 Release 4 Development and Integration scheduled to be complete Q4FY23.
- CI-3 Release 5 Development and Integration scheduled to be complete Q2FY24.
- CI-3 Release 1-5 User Acceptance Testing scheduled to be complete Q3FY24.
- CI-2 Release 1-5 Operational Verification Testing scheduled to complete Q4FY24
- CI-3 Releases 6-9 Development, Integration and Test will commence 6 months after the prior release starting in Q4FY24.
- Key Management Infrastructure (KMI) Tech Refresh completion in Q1FY27 in accordance with NSA schedule.

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy											Date: March 2024	
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 2023**	**FY 2024**	**FY 2025 Base**	**FY 2025 OCO**	**FY 2025 Total**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2029**	**Cost To Complete**	**Total Cost**
0734: *Communications Security R&D*	630.586	30.848	31.089	33.110	-	33.110	33.481	33.589	33.766	34.483	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 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.

Public Key Infrastructure (PKI): The DoD PKI program, under the authority of the Under Secretary of Defense (USD) for Acquisition & Sustainment (USD(A&S)) 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 DoD PKI Increment 2 capabilities so that person and non-person entities can securely access all authorized DoD resources.

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy		Date: March 2024
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. The NCSA software suite includes the Navy Commander's Cyber Dashboard (NCCD), a single view into the platform's cyber readiness, providing better visibility into Information Warfare readiness trends and drivers, as well as current cyber risk to mission; this view is provided by the Readiness Analytics and Visualization Environment (RAVEN) capability. RAVEN is a visualization capability that ingests a variety of readiness and cybersecurity inputs to create visual dashboards. NCSA implements hybrid cloud based modernized Navy Big Data Platform (BDP) instances, including pre-production development and operational instances, that enable data sharing between Navy DCO data and analytics fabric and joint DCO and cyber situational awareness systems as described in the Joint Cyber Warfighting Architecture (JCWA).

FY25 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 other mission requirements (details held at a higher classification), 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 provide 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 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
Title: Computer Network Defense (CND)	15.114	16.689	15.978	0.000	15.978
Articles:	-	-	-	-	-
FY 2024 Plans: - Continue to manage obsolescence through technical refreshes and capability upgrades to CND subsystems.					

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy		Date: March 2024
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 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
- Continue to develop and enhance Navy's portion of other mission requirements (details held at a higher classification) 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 efforts to further virtualize Computer Network Defense (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. - Continue the enablement of high assurance infrastructure in support of Zero Trust Architecture (ZTA). - Continue CND NCDOC Continuity of Operations (COOP) assessment of CND capabilities in an effort to engineer a live automated failover architecture if required or implement fail-over operations with reconfigured CND capability to maintain resilient NCDOC continuity of operations within the DoDIN-N from an alternate site performing command mission essential functions. - Continue Refactor Vulnerability Asset Remediation Manager (VRAM) coding as needed and adapt VRAM to changing technologies utilized by the application, including adequate integration and testing prior to delivery/ production.					
FY 2025 Base Plans: - Continue to manage obsolescence through technical refreshes and capability upgrades to CND subsystems. - Continue to develop and enhance Navy's portion of other mission requirements (details held at a higher classification) and BMD cyber security system of systems within the CND architecture. - 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 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. - Continue the enablement of high assurance infrastructure in support of ZTA. - Continue CND NCDOC Continuity of Operations (COOP) assessment of CND capabilities in an effort to engineer a live automated failover architecture if required or implement fail-over operations with reconfigured					

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy		Date: March 2024
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 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
CND capability to maintain resilient NCDOC continuity of operations within the DoDIN-N from an alternate site performing command mission essential functions. - Continue Refactor VRAM coding as needed, and adapt VRAM to changing technologies utilized by the application, including adequate integration and testing prior to delivery/production. ***FY 2025 OCO Plans:*** N/A ***FY 2024 to FY 2025 Increase/Decrease Statement:*** FY25 decrease ($0.711M) is due to the reduction in capability and architecture upgrades needed to support the classified mission requirements (details held at a higher classification).					
Title: Navy Cryptography (Crypto)	6.911	7.316	11.105	0.000	11.105
Articles:	-	-	-	-	-
FY 2024 Plans: - Continue Advanced Cryptographic Capabilities (ACC) Solutions Development and Product Testing - Continue ACC Wave 2/3 Deliveries and Upgrades - Continue 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 National Security Agency (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). - Continue to develop Navy strategy and implementation plan to modernize secure voice architectures within Navy networks. - Initiate Crypto Mod (CM) 2 Solutions Development, and Fielding Planning. - Continue to support DASN IWAR led COMSEC Steering Board (CSB) ***FY 2025 Base Plans:*** - Complete Advanced Cryptographic Capabilities (ACC) Solutions Development and Product Testing - Complete ACC Deliveries and Upgrades - Continue to provide development and security engineering for modernization of DoN crypto systems and embeddable crypto modernization strategies.					

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy		Date: March 2024
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 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
- 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. - Complete enhancement and modernization of VACM devices. - Continue to develop Navy strategy and implementation plan to modernize secure voice architectures within Navy networks. - Continue Crypto Mod (CM) 2 Solutions Development, Procurement, Product Testing, and Fielding. - Continue to support DASN IWAR led COMSEC Steering Board (CSB) ***FY 2025 OCO Plans:*** N/A ***FY 2024 to FY 2025 Increase/Decrease Statement:*** FY25 increase ($3.789M) is for Crypto Modernization 2 Solutions Development, Procurement, Product Testing, and Fielding.					
Title: Key Management (KM)	1.013	1.130	1.148	0.000	1.148
Articles:	-	-	-	-	-
FY 2024 Plans: - Continue the development and engineering of Key Management Infrastructure (KMI) Capability Increment (CI)-3, Release 4. - Continue development of follow on to Simple Key Loader (SKL) into the KMI environment. - Begin the development, engineering and testing of KMI CI-3, Release 5. - Begin the development, engineering and testing of KMI CI-3, Release 6. - Transition development of CI-2 to CI-3 capabilities into KMI. - Begin development of Next Generation Capabilities to distribute key as part of the Crypto Modernization (CM) effort. - Complete the development, engineering and testing of KMI CI-3, Release 5. ***FY 2025 Base Plans:*** - Complete the development, engineering and testing of KMI CI-3, Release 6. - Continue transition development of CI-2 to CI-3 capabilities into KMI. - Begin the development, engineering and testing of KMI CI-3, Release 7. - Begin the development, engineering and testing of KMI CI-3, Release 8. - Complete development and begin testing of follow on to Simple Key Loader (SKL) into the KMI environment.					

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy		Date: March 2024
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 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
- Continue development of Next Generation Capabilities to distribute key as part of the CM effort. ***FY 2025 OCO Plans:*** N/A ***FY 2024 to FY 2025 Increase/Decrease Statement:*** No significant change from FY24 to FY25.					
Title: SHARKCAGE ***Articles:*** ***FY 2024 Plans:*** - Continue to integrate critical mission requirements (details held at a higher classification) capability within the SHARKCAGE environment to address evolving threats to the warfighter. - Complete the system architecture requirements and prototypes for the SHARKCAGE Afloat and Ashore 2.0 systems respectively. ***FY 2025 Base Plans:*** - Continue to integrate critical mission requirements (details held at a higher classification) capability within the SHARKCAGE 2.0 environment to address evolving threats to the warfighter. -Commence system modifications and capability enhancements for the SHARKCAGE Afloat and Ashore 2.0 system. ***FY 2025 OCO Plans:*** N/A ***FY 2024 to FY 2025 Increase/Decrease Statement:*** FY25 decrease ($1.066M) due to the reduction in critical development efforts required to meet the SHARKCAGE capability enhancements within the 2.0 environment.	2.532 -	2.823 -	1.757 -	0.000 -	1.757 -
Title: Public Key Infrastructure (PKI) ***Articles:*** ***FY 2024 Plans:*** - Continue Navy compliance and compatibility with DoD Public Key Infrastructure (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 for afloat and ashore environments, Common Access Card (CAC) configuration modifications, NIPRNet	0.411 -	0.462 -	0.469 -	0.000 -	0.469 -

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy		Date: March 2024
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 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
Enterprise Alternate Token Systems (NEATS), Non-Person Entity (NPE), and Secret Internet Protocol Router Network (SIPRNet) Token Management System. ***FY 2025 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 2025 OCO Plans:*** N/A ***FY 2024 to FY 2025 Increase/Decrease Statement:*** No significant change from FY24 to FY25.					
Title: Navy Cyber Situational Awareness (NCSA)	2.390	2.669	2.653	0.000	2.653
Articles:	-	-	-	-	-
FY 2024 Plans: - Continue the development of a shared and tailorable Maritime Cyber "Integrated" Common Operational Picture (COP) to Fleet Cyber Command/Commander Tenth Fleet (FCC/C10F), including all geographic Maritime Operations Centers (MOCs) to enable assessments of cyber vulnerabilities, threats, and risks relative to Navy missions. - Continue to expand access to mission critical cyber data to provide actionable information to afloat Commanders to understand and mitigate cyber risk to mission. - Continue to deliver platform readiness metrics at an enterprise view of a unit's cyber posture, which provides better visibility into Information Warfare readiness trends and drivers, and displays current risk to mission execution. ***FY 2025 Base Plans:*** - Continue the development of a shared and tailorable Maritime Cyber "Integrated" Common Operational Picture (COP) to Fleet Cyber Command/Commander Tenth Fleet (FCC/C10F), including all geographic Maritime Operations Centers (MOCs) to enable assessments of cyber vulnerabilities, threats, and risks relative to Navy missions. - Continue to expand access to mission critical cyber data to provide actionable information to afloat Commanders to understand and mitigate cyber risk to mission.					

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy		Date: March 2024
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 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
- Continue to deliver platform readiness metrics at an enterprise view of a unit's cyber posture, which provides better visibility into Information Warfare readiness trends and drivers, and displays current risk to mission execution. ***FY 2025 OCO Plans:*** N/A ***FY 2024 to FY 2025 Increase/Decrease Statement:*** No significant change from FY24 to FY25.					
Title: Cybersecurity Coordination ***Articles:*** ***FY 2024 Plans:*** N/A ***FY 2025 Base Plans:*** N/A ***FY 2025 OCO Plans:*** N/A	2.477 -	0.000 -	0.000 -	0.000 -	0.000 -
Accomplishments/Planned Programs Subtotals	30.848	31.089	33.110	0.000	33.110

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total	FY 2026	FY 2027	FY 2028	FY 2029	Cost To Complete	Total Cost
• OPN/3415: *Info Systems Security Program (ISSP)*	156.034	154.890	162.008	-	162.008	150.681	156.297	157.917	161.267	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 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.

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy		Date: March 2024
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 0734 / *Communications Security R&D*

Navy 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. For Cryptographic Modernization 2 (CM2), Navy has conducted inventory analysis on devices that will be impacted by CM2 requirements and submitted inputs to the FY25 POM. Navy will look towards NSA IDIQ device offering to procure suitable replacements for CM2 impacted devices. The KGV-11M program is Navy led and will replace legacy KGV-11A/C devices use for UHF SATCOM communication with a TD-1271 Terminal.

Key Management (KM): Key Management Infrastructure (KMI) is a NSA-led ACAT I program. It 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 CI-2 followed an agile development strategy, and CI-3 will follow an agile and DevSecOps development strategy. The KMI program will continue to develop alternative architecture implementations for communities within the Navy.

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 (USD) for Acquisition & Sustainment (USD(A&S)) 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. 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 ashore sites and afloat platforms conducting Ballistic Missile Defense (BMD) and other mission requirements (details held at a higher classification).

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 using an iterative, agile software enhancement process in the form of capability drops to address future cyber Situational 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.

Exhibit R-3, RDT&E Project Cost Analysis: PB 2025 Navy			Date: March 2024
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 2023 Cost	FY 2023 Award Date	FY 2024 Cost	FY 2024 Award Date	FY 2025 Base Cost	FY 2025 Base Award Date	FY 2025 OCO Cost	FY 2025 OCO Award Date	FY 2025 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Development (PY)	Various	Various : Various	196.805	0.000		0.000		0.000		-		0.000	0.000	196.805	-
Hardware Development (WR)	WR	NIWC PACIFIC : San Diego, CA	27.526	3.096	Oct 2022	3.055	Oct 2023	3.254	Oct 2024	-		3.254	Continuing	Continuing	Continuing
Hardware Development	C/CPFF	NIWC PACIFIC : San Diego, CA	10.901	2.802	Oct 2022	2.768	Oct 2023	2.948	Oct 2024	-		2.948	Continuing	Continuing	Continuing
Hardware Development (WR)	WR	NIWC ATLANTIC : Charleston, SC	7.491	0.178	Oct 2022	0.176	Oct 2023	0.287	Oct 2024	-		0.287	Continuing	Continuing	Continuing
Hardware Development	C/CPFF	NIWC ATLANTIC : Charleston, SC	6.082	0.195	Oct 2022	0.192	Oct 2023	0.304	Oct 2024	-		0.304	Continuing	Continuing	Continuing
Software Development (WR)	WR	NIWC PACIFIC : San Diego, CA	56.927	4.695	Oct 2022	4.644	Oct 2023	4.946	Oct 2024	-		4.946	Continuing	Continuing	Continuing
Software Development	C/CPFF	NIWC PACIFIC : San Diego, CA	29.197	3.689	Dec 2022	3.639	Dec 2023	3.876	Dec 2024	-		3.876	Continuing	Continuing	Continuing
Software Development (WR)	WR	NIWC ATLANTIC : Charleston, SC	17.869	2.895	Oct 2022	2.857	Oct 2023	3.143	Oct 2024	-		3.143	Continuing	Continuing	Continuing
Software Development	C/CPFF	NIWC ATLANTIC : Charleston, SC	26.792	2.675	Dec 2022	3.278	Dec 2023	3.590	Dec 2024	-		3.590	Continuing	Continuing	Continuing
Software Development	FFRDC	MITRE : McLean, VA	11.380	0.661	Dec 2022	0.936	Dec 2023	1.149	Dec 2024	-		1.149	Continuing	Continuing	Continuing
Software Development	Various	Various : Various	69.959	0.799	Dec 2022	0.984	Dec 2023	1.173	Dec 2024	-		1.173	Continuing	Continuing	Continuing
Software Development	C/CPFF	BAH : San Diego, CA	16.811	1.674	Jan 2023	1.651	Jan 2024	1.458	Jan 2025	-		1.458	Continuing	Continuing	Continuing
Software Development	FFRDC	GTRI : Atlanta, GA	23.120	0.576	Jan 2023	0.285	Jan 2024	0.152	Jan 2025	-		0.152	Continuing	Continuing	Continuing
Software Development	WR	NSMA : San Diego, CA	8.309	0.658	Oct 2022	0.650	Oct 2023	0.692	Oct 2024	-		0.692	Continuing	Continuing	Continuing
Software Development	WR	NRL : Washington DC	7.315	1.184	Oct 2022	0.973	Oct 2023	0.824	Oct 2024	-		0.824	Continuing	Continuing	Continuing
		Subtotal	516.484	25.777		26.088		27.796		-		27.796	Continuing	Continuing	N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2025 Navy			Date: March 2024
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 2023 Cost	FY 2023 Award Date	FY 2024 Cost	FY 2024 Award Date	FY 2025 Base Cost	FY 2025 Base Award Date	FY 2025 OCO Cost	FY 2025 OCO Award Date	FY 2025 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Architecture	WR	Various : Various	6.625	0.125	Oct 2022	0.123	Oct 2023	0.120	Oct 2024	-		0.120	Continuing	Continuing	Continuing
Architecture	WR	NIWC ATLANTIC : Charleston, SC	3.987	0.219	Oct 2022	0.216	Oct 2023	0.230	Oct 2024	-		0.230	Continuing	Continuing	Continuing
Architecture	WR	NIWC PACIFIC : San Diego, CA	0.450	0.000		0.000		0.000		-		0.000	0.000	0.450	-
Requirements Analysis	C/CPFF	BAH : San Diego, CA	8.935	0.957	Jan 2023	0.944	Jan 2024	1.005	Jan 2025	-		1.005	Continuing	Continuing	Continuing
Studies & Design	WR	Various : Various	8.121	0.358	Oct 2022	0.353	Oct 2023	0.376	Oct 2024	-		0.376	Continuing	Continuing	Continuing
		Subtotal	28.118	1.659		1.636		1.731		-		1.731	Continuing	Continuing	N/A

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2023 Cost	FY 2023 Award Date	FY 2024 Cost	FY 2024 Award Date	FY 2025 Base Cost	FY 2025 Base Award Date	FY 2025 OCO Cost	FY 2025 OCO Award Date	FY 2025 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Developmental Test & Evaluation (DT&E)	WR	NIWC PACIFIC : San Diego, CA	40.511	0.828	Oct 2022	0.816	Oct 2023	0.869	Oct 2024	-		0.869	Continuing	Continuing	Continuing
Prior Year Developmental Test & Evaluation Not Funded FYDP (PYDT&E)	WR	COTF : Norfolk, VA	3.367	0.000		0.000		0.000		-		0.000	0.000	3.367	-
Developmental Test & Evaluation (DT&E)	C/CPFF	BAH : San Diego, CA	6.049	1.282	Jan 2023	1.265	Jan 2024	1.347	Jan 2025	-		1.347	Continuing	Continuing	Continuing
Prior Year Developmental Test & Evaluation Not Funded FYDP (PYDT&E)	WR	NIWC ATLANTIC : Charleston, SC	0.234	0.000		0.000		0.000		-		0.000	0.000	0.234	-
		Subtotal	50.161	2.110		2.081		2.216		-		2.216	Continuing	Continuing	N/A

Management Services ($ in Millions)

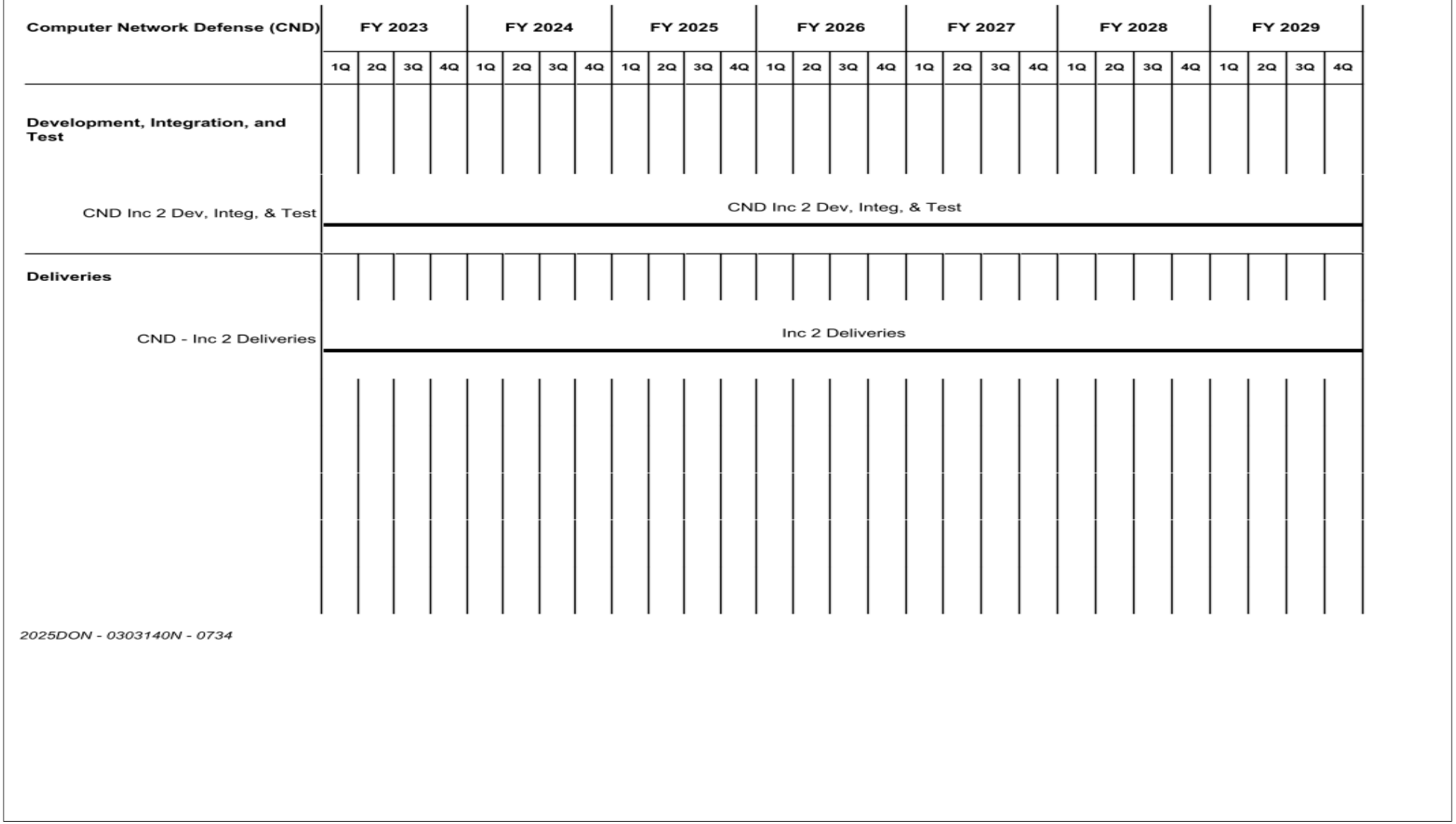
Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2023 Cost	FY 2023 Award Date	FY 2024 Cost	FY 2024 Award Date	FY 2025 Base Cost	FY 2025 Base Award Date	FY 2025 OCO Cost	FY 2025 OCO Award Date	FY 2025 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Program Management	C/CPFF	BAH : San Diego, CA	35.823	1.302	Jan 2023	1.284	Jan 2024	1.367	Jan 2025	-		1.367	Continuing	Continuing	Continuing
		Subtotal	35.823	1.302		1.284		1.367		-		1.367	Continuing	Continuing	N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2025 Navy			Date: March 2024
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 2023		FY 2024		FY 2025 Base		FY 2025 OCO		FY 2025 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	630.586	30.848		31.089		33.110		-		33.110	Continuing	Continuing	N/A

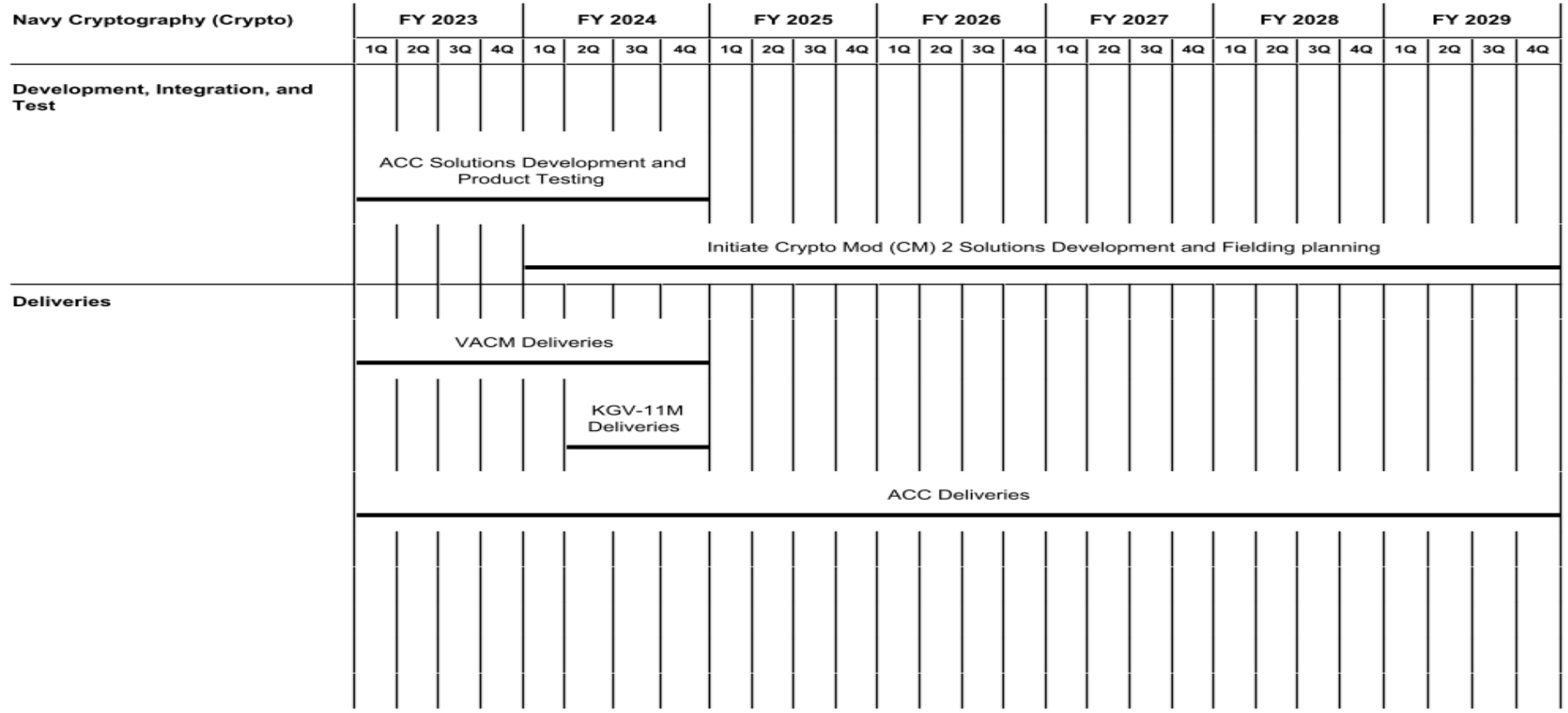
Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2025 Navy		Date: March 2024
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*



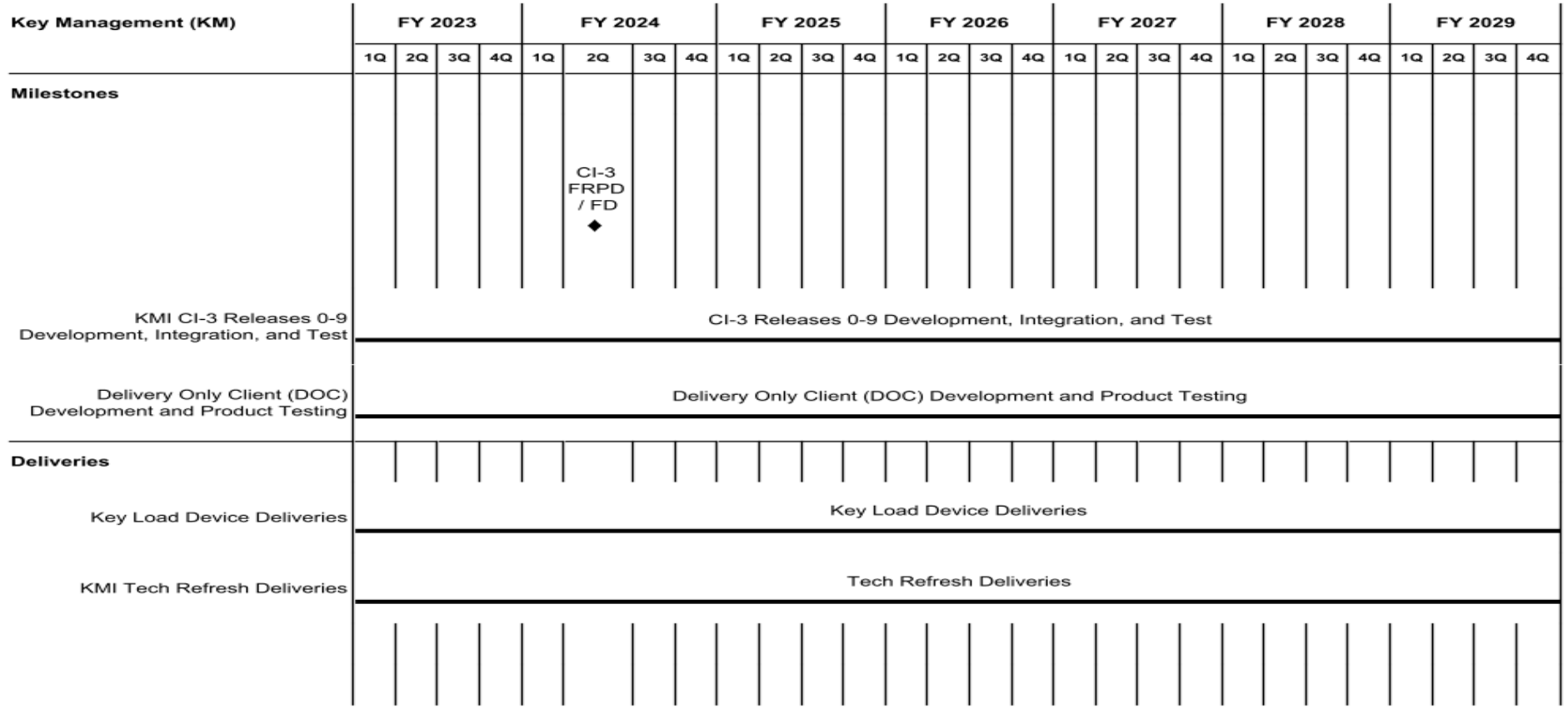
2025DON - 0303140N - 0734

Exhibit R-4, RDT&E Schedule Profile: PB 2025 Navy		Date: March 2024
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*



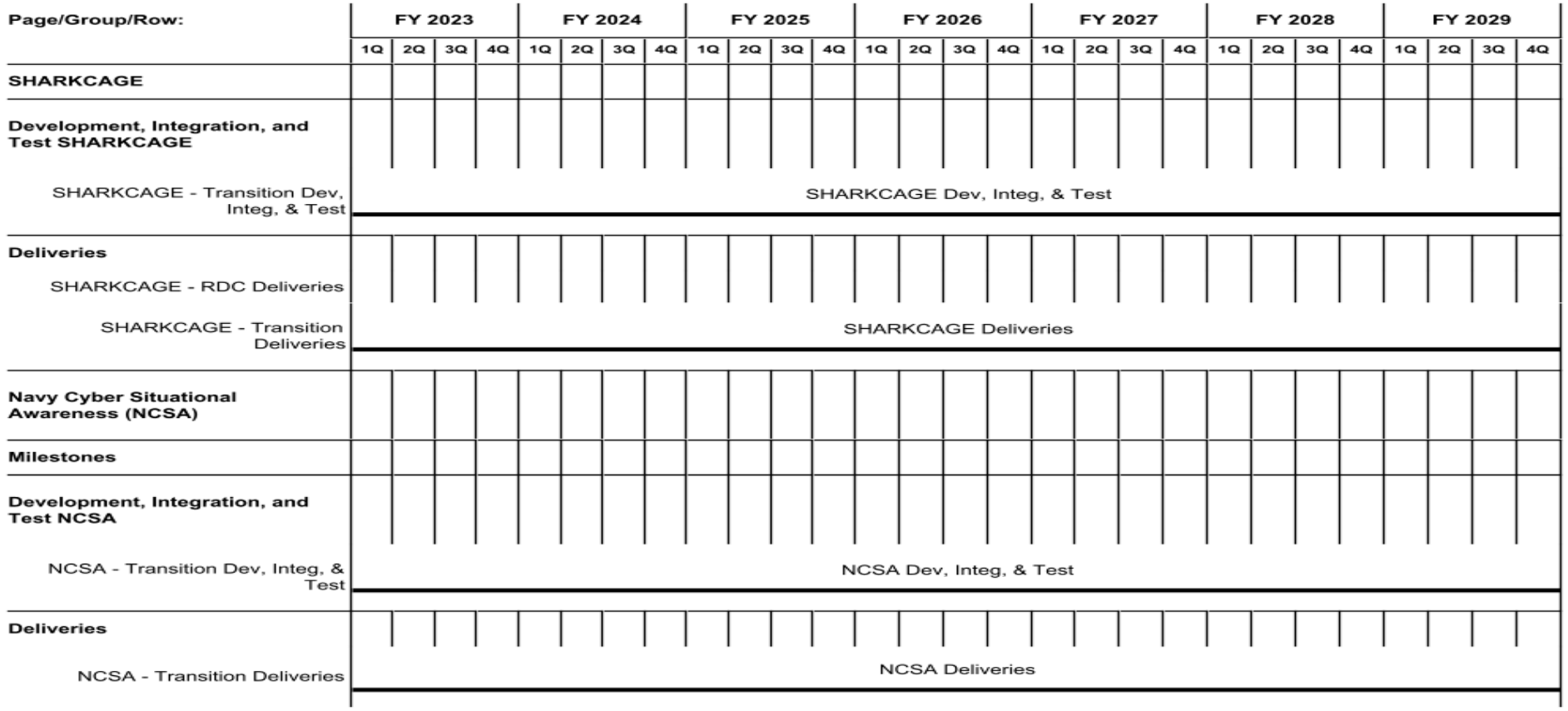
2025DON - 0303140N - 0734

Exhibit R-4, RDT&E Schedule Profile: PB 2025 Navy		Date: March 2024
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*



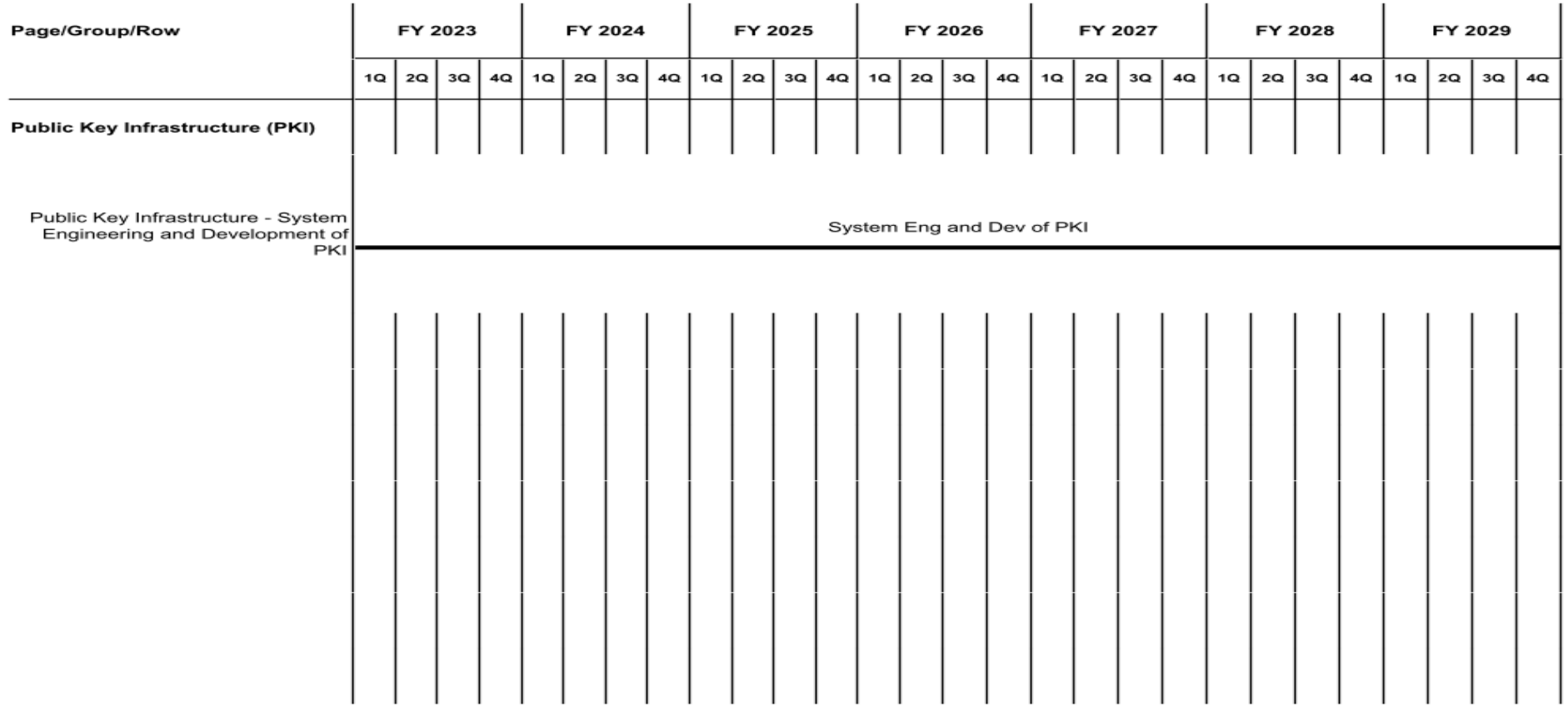
2025DON - 0303140N - 0734

Exhibit R-4, RDT&E Schedule Profile: PB 2025 Navy		Date: March 2024
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*



2025DON - 0303140N - 0734

Exhibit R-4, RDT&E Schedule Profile: PB 2025 Navy		Date: March 2024
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*



2025DON - 0303140N - 0734

Exhibit R-4A, RDT&E Schedule Details: PB 2025 Navy		Date: March 2024
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 Inc 2 Dev, Integ, & Test:	1	2023	4	2029
Deliveries: CND - Inc 2 Deliveries:	1	2023	4	2029
Navy Cryptography (Crypto)				
Development, Integration, and Test: Crypto - ACC Solutions Development and Product Testing	1	2023	4	2024
Development, Integration, and Test: Crypto - Initiate Crypto Mod (CM) 2 Solutions Development and Fielding planning	1	2024	4	2029
Deliveries: Crypto - VACM Deliveries	1	2023	4	2024
Deliveries: Crypto - KGV-11M Deliveries	2	2024	4	2024
Deliveries: Crypto - ACC Deliveries	1	2023	4	2029
Key Management (KM)				
Milestones: KMI CI-3 FRP Decision / FD	2	2024	2	2024
Milestones: KMI CI-3 Releases 0-9 Development, Integration, and Test:	1	2023	4	2029
Milestones: Delivery Only Client (DOC) Development and Product Testing:	1	2023	4	2029
Deliveries: Key Load Device Deliveries:	1	2023	4	2029
Deliveries: KMI Tech Refresh Deliveries:	1	2023	4	2029
Page/Group/Row:				
Development, Integration, and Test SHARKCAGE: SHARKCAGE - Transition Dev, Integ, & Test:	1	2023	4	2029
Deliveries: SHARKCAGE - Transition Deliveries:	1	2023	4	2029
Development, Integration, and Test NCSA: NCSA - Transition Dev, Integ, & Test:	1	2023	4	2029
Deliveries: NCSA - Transition Deliveries:	1	2023	4	2029

Exhibit R-4A, RDT&E Schedule Details: PB 2025 Navy		Date: March 2024
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**
Page/Group/Row				
Public Key Infrastructure (PKI): Public Key Infrastructure - System Engineering and Development of PKI:	1	2023	4	2029

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy										Date: March 2024		
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 2023**	**FY 2024**	**FY 2025 Base**	**FY 2025 OCO**	**FY 2025 Total**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2029**	**Cost To Complete**	**Total Cost**
3230: *Information Assurance*	29.051	2.188	2.301	2.229	-	2.229	2.394	2.442	2.491	2.543	Continuing	Continuing
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 2025 Navy		Date: March 2024
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 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
Title: Information Assurance (IA)	2.188	2.301	2.229	0.000	2.229
Articles:	-	-	-	-	-
FY 2024 Plans: - Complete 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. - Complete 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). - 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/technology to provide a cloud application trust in its host infrastructure. - Continue to 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. - Continue 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.					

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy		Date: March 2024
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 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
- Continue 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. - Continue the development of tools to covertly embed sensitive message traffic for resilient cyber and intelligence operations. This includes implementing techniques for altering network protocol parameters in situ, as well as modifying the timing, delay, and delivery of network packets. This further includes techniques to quantify and limit unwanted information leakage to adversaries. - Continue the development of scalable tools to assure a wide array of naval systems that implement machine learning and deep learning. This includes developer-friendly tools to automate the identification of hazards and faults during the design and development of systems, which process text, image, voice, video, signals, and cyber communications. - Initiate the development and agile transition of enhanced communication networks to improve information infrastructure protection between the Navy and its commercial partners. This includes cryptographic high value product prototypes, traffic security measures, identity and cryptographic certificate enhancements, and resilience against exfiltration attacks.					
FY 2025 Base Plans: - 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/technology to provide a cloud application trust in its host infrastructure. This includes 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. - Continue the development of tools to measure and reduce collateral damage incurred by cyber operations. This includes techniques for multimodal sensing, dependency analysis through causal inference, and fusion of active and passive measurements for iterative sensing and reconnaissance. - Continue the development and agile transition of enhanced communication networks to improve information infrastructure protection between the Navy and its commercial partners. This includes cryptographic high value product prototypes, traffic security measures, identity and cryptographic certificate enhancements, and resilience against exfiltration attacks. - Complete the development of tools to covertly embed sensitive message traffic for resilient cyber and intelligence operations. This includes techniques for altering network protocol parameters in situ, as well as					

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy		Date: March 2024
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 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
modifying the timing, delay, and delivery of network packets. This further includes techniques to quantify and limit unwanted information leakage to adversaries. - Complete the development of scalable tools to assure a wide array of naval systems that implement machine learning and deep learning. This includes developer-friendly tools to automate the identification of hazards and faults during the design and development of systems, which process text, image, voice, video, signals, and cyber communications. - Complete the development of tools/technologies that enable scalable, secure device-to-device tactical communications. This includes fine-grained access controls and fully decentralized authorization and enforcement of security policies that enables a self-organizing distributed network in disconnected environments. - Initiate development of high-assurance tools for programmable hardware. This includes real-time monitors for Field Programmable Gate Arrays (FPGA) and other programmable fabrics, and novel fuzzing techniques that can take advantage of structural knowledge of system-on-chips and other component-based design to automate vulnerability discovery. ***FY 2025 OCO Plans:*** N/A ***FY 2024 to FY 2025 Increase/Decrease Statement:*** No significant funding change from FY 2024 to FY 2025.					
Accomplishments/Planned Programs Subtotals	2.188	2.301	2.229	0.000	2.229

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2025 Navy			Date: March 2024
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 2023 Cost	FY 2023 Award Date	FY 2024 Cost	FY 2024 Award Date	FY 2025 Base Cost	FY 2025 Base Award Date	FY 2025 OCO Cost	FY 2025 OCO Award Date	FY 2025 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Development Support	Various	NRL : Washington, DC	29.051	2.188	Nov 2022	2.301	Nov 2023	2.229	Nov 2024	-		2.229	Continuing	Continuing	Continuing
		Subtotal	29.051	2.188		2.301		2.229		-		2.229	Continuing	Continuing	N/A

	Prior Years	FY 2023		FY 2024		FY 2025 Base		FY 2025 OCO		FY 2025 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	29.051	2.188		2.301		2.229		-		2.229	Continuing	Continuing	N/A

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2025 Navy		Date: March 2024
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 3230 / *Information Assurance*

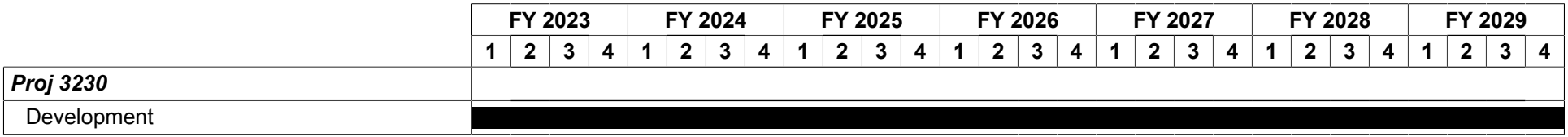


Exhibit R-4A, RDT&E Schedule Details: PB 2025 Navy		Date: March 2024
Appropriation/Budget Activity 1319 / 7	**R-1 Program Element (Number/Name)** PE 0303140N / *Information Sys Security Program*	**Project (Number/Name)** 3230 / *Information Assurance*

Schedule Details

	Start		End	
Events by Sub Project	**Quarter**	**Year**	**Quarter**	**Year**
Proj 3230				
Development	1	2023	4	2029