

**UNCLASSIFIED**

**Exhibit R-2, RDT&E Budget Item Justification: PB 2024 Navy** **Date:** March 2023

<b>Appropriation/Budget Activity</b> 1319: <i>Research, Development, Test &amp; Evaluation, Navy / BA 7: Operational Systems Development</i>	<b>R-1 Program Element (Number/Name)</b> PE 0303140N / <i>Information Sys Security Program</i>
---	---

COST (\$ in Millions)	Prior Years	FY 2022	FY 2023	FY 2024 Base	FY 2024 OCO	FY 2024 Total	FY 2025	FY 2026	FY 2027	FY 2028	Cost To Complete	Total Cost
Total Program Element	627.045	32.592	33.752	33.390	-	33.390	34.794	35.279	35.664	36.377	Continuing	Continuing
0734: <i>Communications Security R&amp;D</i>	600.137	30.449	31.496	31.089	-	31.089	32.447	32.885	33.222	33.886	Continuing	Continuing
3230: <i>Information Assurance</i>	26.908	2.143	2.256	2.301	-	2.301	2.347	2.394	2.442	2.491	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).

**UNCLASSIFIED**

<b>Exhibit R-2, RDT&amp;E Budget Item Justification:</b> PB 2024 Navy	<b>Date:</b> March 2023
---	-------------------------

<b>Appropriation/Budget Activity</b> 1319: <i>Research, Development, Test &amp; Evaluation, Navy / BA 7: Operational Systems Development</i>	<b>R-1 Program Element (Number/Name)</b> PE 0303140N / <i>Information Sys Security Program</i>
---	---

<b>B. Program Change Summary (\$ in Millions)</b>	<b>FY 2022</b>	<b>FY 2023</b>	<b>FY 2024 Base</b>	<b>FY 2024 OCO</b>	<b>FY 2024 Total</b>
Previous President's Budget	33.311	33.752	34.173	-	34.173
Current President's Budget	32.592	33.752	33.390	-	33.390
Total Adjustments	-0.719	0.000	-0.783	-	-0.783
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-0.003	0.000			
• SBIR/STTR Transfer	-0.716	0.000			
• Rate/Misc Adjustments	0.000	0.000	-0.783	-	-0.783

**Change Summary Explanation**

**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 7.

**SCHEDULE:**

**Navy Cryptography (Crypto):**

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

**Key Management (KM):**

- 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 Development, Integration and Test begins Q4FY23 in accordance with NSA schedule.
- CI-3 Release 1 Development, Integration and Test start shifted from Q2FY23 to Q2FY24 in accordance with NSA schedule.
- CI-3 Release 2 Development, Integration and Test start shifted from Q4FY23 to Q4FY24 in accordance with NSA schedule.

**UNCLASSIFIED**

<b>Exhibit R-2, RDT&amp;E Budget Item Justification:</b> PB 2024 Navy		<b>Date:</b> March 2023
<b>Appropriation/Budget Activity</b> 1319: <i>Research, Development, Test &amp; Evaluation, Navy / BA 7: Operational Systems Development</i>	<b>R-1 Program Element (Number/Name)</b> PE 0303140N / <i>Information Sys Security Program</i>	
<ul style="list-style-type: none"><li>- CI-3 Releases 3-7 Development, Integration and Test will commence 6 months after the prior release starting in Q2FY25.</li><li>- Key Management Infrastructure (KMI) Tech Refresh completion shifted from Q2FY26 to Q1FY27 in accordance with NSA schedule.</li></ul> <p>FUNDING: Overall funding has a net decrease of \$0.362M in subprojects. The most significant funding change is in the Computer Network Defense (CND) program for increasing Continuity of Operations (COOP) development, and Navy Cryptography (Crypto) program for increasing Crypto Modernization (CM) development efforts.</p>		

**UNCLASSIFIED**

<b>Exhibit R-2A, RDT&amp;E Project Justification:</b> PB 2024 Navy										<b>Date:</b> March 2023		
<b>Appropriation/Budget Activity</b> 1319 / 7					<b>R-1 Program Element (Number/Name)</b> PE 0303140N / <i>Information Sys Security Program</i>				<b>Project (Number/Name)</b> 0734 / <i>Communications Security R&amp;D</i>			
<b>COST (\$ in Millions)</b>	<b>Prior Years</b>	<b>FY 2022</b>	<b>FY 2023</b>	<b>FY 2024 Base</b>	<b>FY 2024 OCO</b>	<b>FY 2024 Total</b>	<b>FY 2025</b>	<b>FY 2026</b>	<b>FY 2027</b>	<b>FY 2028</b>	<b>Cost To Complete</b>	<b>Total Cost</b>
0734: <i>Communications Security R&amp;D</i>	600.137	30.449	31.496	31.089	-	31.089	32.447	32.885	33.222	33.886	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.

UNCLASSIFIED

<b>Exhibit R-2A, RDT&amp;E Project Justification:</b> PB 2024 Navy		<b>Date:</b> March 2023
<b>Appropriation/Budget Activity</b> 1319 / 7	<b>R-1 Program Element (Number/Name)</b> PE 0303140N / <i>Information Sys Security Program</i>	<b>Project (Number/Name)</b> 0734 / <i>Communications Security R&amp;D</i>
<p>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&amp;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.</p> <p>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).</p> <p>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.</p> <p>FY24 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, &amp; 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 (INOCSS), and Zero Trust Architecture (ZTA) concepts; (7) assurance technologies, including Key Management (KM) and Public Key Infrastructure (PKI).</p>		

**UNCLASSIFIED**

<b>Exhibit R-2A, RDT&amp;E Project Justification:</b> PB 2024 Navy		<b>Date:</b> March 2023
<b>Appropriation/Budget Activity</b> 1319 / 7	<b>R-1 Program Element (Number/Name)</b> PE 0303140N / <i>Information Sys Security Program</i>	<b>Project (Number/Name)</b> 0734 / <i>Communications Security R&amp;D</i>

**B. Accomplishments/Planned Programs (\$ in Millions, Article Quantities in Each)**

	<b>FY 2022</b>	<b>FY 2023</b>	<b>FY 2024 Base</b>	<b>FY 2024 OCO</b>	<b>FY 2024 Total</b>
<b>Title:</b> Computer Network Defense (CND)	14.465	15.762	16.689	0.000	16.689
<b>Articles:</b>	-	-	-	-	-
<p><b>FY 2023 Plans:</b></p> <ul style="list-style-type: none"> <li>- Continue to manage obsolescence through technical refreshes and capability upgrades to CND subsystems.</li> <li>- 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.</li> <li>- Continue to implement DoD and USCC cybersecurity tools and mandates into ONE-Net and C4I networks.</li> <li>- Continue to provide technical guidance to support CANES deployment of new CND capabilities.</li> <li>- Continue to optimize CND to enable transition to JRSS.</li> <li>- Continue efforts to further virtualize CND capabilities for more effective and cost-efficient deployment of cybersecurity technologies.</li> <li>- Continue to develop, integrate, and test solution to replace and assume acquisition management of NCDOC tactical sensor infrastructure.</li> <li>- Continue the enablement of high assurance infrastructure in support of ZTA.</li> <li>-Commence CND NCDOC Continuity of Operations (COOP) development effort to engineer a live automated failover architecture to maintain resilient NCDOC continuity of operations within the DoDIN-N.</li> <li>-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.</li> </ul> <p><b>FY 2024 Base Plans:</b></p> <ul style="list-style-type: none"> <li>- Continue to manage obsolescence through technical refreshes and capability upgrades to CND subsystems.</li> <li>- 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.</li> <li>- Continue to implement DoD and USCC cybersecurity tools and mandates into ONE-Net and C4I networks.</li> <li>- Continue to provide technical guidance to support CANES deployment of new CND capabilities.</li> <li>- Continue efforts to further virtualize CND capabilities for more effective and cost-efficient deployment of cybersecurity technologies.</li> <li>- Continue to develop, integrate, and test solution to replace and assume acquisition management of NCDOC tactical sensor infrastructure.</li> <li>- Continue the enablement of high assurance infrastructure in support of ZTA.</li> <li>-Continue CND NCDOC Continuity of Operations (COOP) development effort to engineer a live automated failover architecture to maintain resilient NCDOC continuity of operations within the DoDIN-N.</li> </ul>					

**UNCLASSIFIED**

<b>Exhibit R-2A, RDT&amp;E Project Justification:</b> PB 2024 Navy		<b>Date:</b> March 2023
<b>Appropriation/Budget Activity</b> 1319 / 7	<b>R-1 Program Element (Number/Name)</b> PE 0303140N / <i>Information Sys Security Program</i>	<b>Project (Number/Name)</b> 0734 / <i>Communications Security R&amp;D</i>

<b>B. Accomplishments/Planned Programs (\$ in Millions, Article Quantities in Each)</b>	<b>FY 2022</b>	<b>FY 2023</b>	<b>FY 2024 Base</b>	<b>FY 2024 OCO</b>	<b>FY 2024 Total</b>
<p>-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.</p> <p><b>FY 2024 OCO Plans:</b> N/A</p> <p><b>FY 2023 to FY 2024 Increase/Decrease Statement:</b> FY24 increase of \$0.927M supports Cybersecurity Coordination advancements in data correlation and analytics technologies transitioning into Computer Network Defense (CND).</p>					
<p><b>Title:</b> Navy Cryptography (Crypto)</p> <p align="right"><b>Articles:</b></p> <p><b>FY 2023 Plans:</b></p> <ul style="list-style-type: none"> <li>- Continue Advanced Cryptographic Capabilities (ACC) Solutions Development and Product Testing</li> <li>- Continue ACC Deliveries</li> <li>- Commence KGV-11M Deliveries</li> <li>- Continue to provide development and security engineering for modernization of DoN crypto systems and embeddable crypto modernization strategies.</li> <li>- Continue to work with NSA on certification authority and data testing for all crypto modernization efforts.</li> <li>- Continue to investigate impacts of upcoming NSA security enhancements for crypto modernization products.</li> <li>- Continue to enhance and modernize VACM ancillary devices.</li> <li>- Continue to develop Navy strategy and implementation plan to modernize secure voice architectures within Navy networks.</li> </ul> <p><b>FY 2024 Base Plans:</b></p> <ul style="list-style-type: none"> <li>- Continue Advanced Cryptographic Capabilities (ACC) Solutions Development and Product Testing</li> <li>- Continue ACC Deliveries</li> <li>- Continue KGV-11M Deliveries</li> <li>- Continue to provide development and security engineering for modernization of DoN crypto systems and embeddable crypto modernization strategies.</li> <li>- Continue to work with NSA on certification authority and data testing for all crypto modernization efforts.</li> <li>- Continue to investigate impacts of upcoming NSA security enhancements for crypto modernization products.</li> <li>- Continue to enhance and modernize VACM ancillary devices.</li> <li>- Continue to develop Navy strategy and implementation plan to modernize secure voice architectures within Navy networks.</li> </ul>	7.113	6.911	7.316	0.000	7.316
	-	-	-	-	-

**UNCLASSIFIED**

<b>Exhibit R-2A, RDT&amp;E Project Justification:</b> PB 2024 Navy				<b>Date:</b> March 2023	
<b>Appropriation/Budget Activity</b> 1319 / 7		<b>R-1 Program Element (Number/Name)</b> PE 0303140N / <i>Information Sys Security Program</i>		<b>Project (Number/Name)</b> 0734 / <i>Communications Security R&amp;D</i>	
<b>B. Accomplishments/Planned Programs (\$ in Millions, Article Quantities in Each)</b>					
- Initiate Crypto Mod (CM) Solutions Development, Product Testing, and Fielding.					
<b>FY 2024 OCO Plans:</b> N/A					
<b>FY 2023 to FY 2024 Increase/Decrease Statement:</b> FY24 increase of \$0.405M supports Cybersecurity Coordination progressions transitioning into Crypto modernization efforts.					
<b>Title:</b> Key Management (KM)					
<b>Articles:</b>					
	1.026	1.013	1.130	0.000	1.130
	-	-	-	-	-
<b>FY 2023 Plans:</b>					
- Complete the development, engineering and testing of KMI CI-3, Spiral 3 Spin 3 including the integration of iApp within a network environment, which will enhance the accounting for and distribution of Key Management Infrastructure (KMI) key delivery.					
- Begin the development, engineering and testing of KMI CI-3, Spiral 3 Spin 4.					
- Continue migrating Communications Security (COMSEC) Management Workstation (CMWS) and the follow on to Simple Key Loader (SKL) into the KMI environment.					
<b>FY 2024 Base Plans:</b>					
- Begin the development, engineering and testing of Key Management Infrastructure (KMI) CI-3, Release 1.					
- Begin the development, engineering and testing of KMI CI-3, Release 2.					
- Transition development of Capability Increment (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.					
<b>FY 2024 OCO Plans:</b> N/A					
<b>FY 2023 to FY 2024 Increase/Decrease Statement:</b> FY24 increase of \$0.117M is due to beginning development of Next Generation Capabilities to distribute key as part of the Crypto Modernization (CM) effort.					
<b>Title:</b> Public Key Infrastructure (PKI)					
<b>Articles:</b>					
	0.408	0.411	0.462	0.000	0.462
	-	-	-	-	-
<b>FY 2023 Plans:</b>					

**UNCLASSIFIED**

<b>Exhibit R-2A, RDT&amp;E Project Justification:</b> PB 2024 Navy		<b>Date:</b> March 2023
<b>Appropriation/Budget Activity</b> 1319 / 7	<b>R-1 Program Element (Number/Name)</b> PE 0303140N / <i>Information Sys Security Program</i>	<b>Project (Number/Name)</b> 0734 / <i>Communications Security R&amp;D</i>

<b>B. Accomplishments/Planned Programs (\$ in Millions, Article Quantities in Each)</b>	<b>FY 2022</b>	<b>FY 2023</b>	<b>FY 2024 Base</b>	<b>FY 2024 OCO</b>	<b>FY 2024 Total</b>
<p>- 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.</p> <p><b>FY 2024 Base Plans:</b> - 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.</p> <p><b>FY 2024 OCO Plans:</b> N/A</p> <p><b>FY 2023 to FY 2024 Increase/Decrease Statement:</b> FY24 increase of \$0.051M supports Cybersecurity Coordination progressions transitioning into Public Key Infrastructure efforts.</p>					
<p><b>Title:</b> SHARKCAGE</p> <p align="right"><b>Articles:</b></p> <p><b>FY 2023 Plans:</b> - Continue the expansion of other mission requirements (details held at a higher classification) capability within the SHARKCAGE environment. - 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. - Continue the SHARKCAGE contract development efforts required to support emergent cybersecurity threats and to provide enhanced incremental capabilities.</p> <p><b>FY 2024 Base Plans:</b> -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 system units.</p> <p><b>FY 2024 OCO Plans:</b></p>	2.598 -	2.532 -	2.823 -	0.000 -	2.823 -

**UNCLASSIFIED**

<b>Exhibit R-2A, RDT&amp;E Project Justification:</b> PB 2024 Navy				<b>Date:</b> March 2023		
<b>Appropriation/Budget Activity</b> 1319 / 7		<b>R-1 Program Element (Number/Name)</b> PE 0303140N / <i>Information Sys Security Program</i>		<b>Project (Number/Name)</b> 0734 / <i>Communications Security R&amp;D</i>		
<b>B. Accomplishments/Planned Programs (\$ in Millions, Article Quantities in Each)</b>						
		<b>FY 2022</b>	<b>FY 2023</b>	<b>FY 2024 Base</b>	<b>FY 2024 OCO</b>	<b>FY 2024 Total</b>
N/A						
<b>FY 2023 to FY 2024 Increase/Decrease Statement:</b> FY24 increase of \$0.291M due to required architecture and prototype efforts needed to complete Afloat and Ashore system.						
<b>Title:</b> Navy Cyber Situational Awareness (NCSA)		2.387	2.390	2.669	0.000	2.669
		<b>Articles:</b>	-	-	-	-
<b>FY 2023 Plans:</b> - Continue the development of a shared and tailorable Maritime Cyber "Integrated" COP external to Fleet Cyber Command/Commander Tenth Fleet (FCC/C10F) to include all geographic 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. - 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.						
<b>FY 2024 Base Plans:</b> - Continue the development of a shared and tailorable Maritime Cyber "Integrated" COP to FCC/C10F, including all geographic 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.						
<b>FY 2024 OCO Plans:</b> N/A						
<b>FY 2023 to FY 2024 Increase/Decrease Statement:</b> FY24 increase of \$0.279M supports the continued expansion of access to mission critical cyber data and continued development of a shared and tailorable Cyber Common Operations Center (COP).						
<b>Title:</b> Cybersecurity Coordination		2.452	2.477	0.000	0.000	0.000
		<b>Articles:</b>	-	-	-	-

**UNCLASSIFIED**

<b>Exhibit R-2A, RDT&amp;E Project Justification:</b> PB 2024 Navy		<b>Date:</b> March 2023
<b>Appropriation/Budget Activity</b> 1319 / 7	<b>R-1 Program Element (Number/Name)</b> PE 0303140N / <i>Information Sys Security Program</i>	<b>Project (Number/Name)</b> 0734 / <i>Communications Security R&amp;D</i>

<b>B. Accomplishments/Planned Programs (\$ in Millions, Article Quantities in Each)</b>	<b>FY 2022</b>	<b>FY 2023</b>	<b>FY 2024 Base</b>	<b>FY 2024 OCO</b>	<b>FY 2024 Total</b>
<p><b><i>FY 2023 Plans:</i></b></p> <ul style="list-style-type: none"> <li>- Continue coordination and alignment with joint and DCO/NetOps integration efforts such as Joint Information Environment (JIE), National Defense Authorization Act, Joint Cyber Warfighting Architecture (JCWA) Unified Platform/Data and Analytic Framework (DAF) and the Integrated Navy Operations Command and Control System (INOCCS) to ensure Navy architecture requirements for tactical networks are met.</li> <li>- 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.</li> <li>- Continue developing implementation strategies for the incorporation of Zero Trust Architecture (ZTA) concepts into the Navy's tactical C4I cybersecurity environment.</li> <li>- 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.</li> <li>- 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.</li> <li>- 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.</li> <li>- Continue coordination and alignment with JIE (e.g., JRSS, JMS, Tactical Processing Node (TPN) etc.), NDAA 1651/1709 JCWA Unified Platform/DAF and the Integrated Navy Operations Command and Control System (INOCCS) to ensure Navy architecture requirements for tactical networks are met.</li> </ul> <p><b><i>FY 2024 Base Plans:</i></b> N/A</p> <p><b><i>FY 2024 OCO Plans:</i></b> N/A</p> <p><b><i>FY 2023 to FY 2024 Increase/Decrease Statement:</i></b> FY24 decrease due to advancements made through Cybersecurity Coordination efforts now transitioning into Computer Network Defense (CND) and Navy Cryptography (Crypto) programs.</p>					
<b>Accomplishments/Planned Programs Subtotals</b>	30.449	31.496	31.089	0.000	31.089

**UNCLASSIFIED**

<b>Exhibit R-2A, RDT&amp;E Project Justification:</b> PB 2024 Navy		<b>Date:</b> March 2023
<b>Appropriation/Budget Activity</b> 1319 / 7	<b>R-1 Program Element (Number/Name)</b> PE 0303140N / <i>Information Sys Security Program</i>	<b>Project (Number/Name)</b> 0734 / <i>Communications Security R&amp;D</i>

**C. Other Program Funding Summary (\$ in Millions)**

Line Item	FY 2022	FY 2023	FY 2024	FY 2024	FY 2024	FY 2025	FY 2026	FY 2027	FY 2028	Cost To	
			Base	OCO	Total					Complete	Total Cost
• OPN/3415: <i>Info Systems Security Program (ISSP)</i>	145.311	156.034	154.890	-	154.890	151.996	154.781	160.353	161.978	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.

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 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).

**UNCLASSIFIED**

<b>Exhibit R-2A, RDT&amp;E Project Justification:</b> PB 2024 Navy		<b>Date:</b> March 2023
<b>Appropriation/Budget Activity</b> 1319 / 7	<b>R-1 Program Element (Number/Name)</b> PE 0303140N / <i>Information Sys Security Program</i>	<b>Project (Number/Name)</b> 0734 / <i>Communications Security R&amp;D</i>
<p>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 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.</p> <p>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.</p>		

**UNCLASSIFIED**

Exhibit R-3, RDT&E Project Cost Analysis: PB 2024 Navy												Date: March 2023			
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)				FY 2022		FY 2023		FY 2024 Base		FY 2024 OCO		FY 2024 Total			
Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Award Date	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	24.470	3.056	Oct 2021	3.096	Oct 2022	3.055	Oct 2023	-		3.055	Continuing	Continuing	Continuing
Hardware Development	C/CPFF	NIWC PACIFIC : San Diego, CA	8.633	2.268	Oct 2021	2.802	Oct 2022	2.768	Oct 2023	-		2.768	Continuing	Continuing	Continuing
Hardware Development (WR)	WR	NIWC ATLANTIC : Charleston, SC	7.315	0.176	Oct 2021	0.178	Oct 2022	0.176	Oct 2023	-		0.176	Continuing	Continuing	Continuing
Hardware Development	C/CPFF	NIWC ATLANTIC : Charleston, SC	5.890	0.192	Oct 2021	0.195	Oct 2022	0.192	Oct 2023	-		0.192	Continuing	Continuing	Continuing
Software Development (WR)	WR	NIWC PACIFIC : San Diego, CA	52.281	4.646	Oct 2021	4.695	Oct 2022	4.644	Oct 2023	-		4.644	Continuing	Continuing	Continuing
Software Development	C/CPFF	NIWC PACIFIC : San Diego, CA	25.556	3.641	Dec 2021	3.689	Dec 2022	3.639	Dec 2023	-		3.639	Continuing	Continuing	Continuing
Software Development (WR)	WR	NIWC ATLANTIC : Charleston, SC	15.011	2.858	Oct 2021	2.895	Oct 2022	2.857	Oct 2023	-		2.857	Continuing	Continuing	Continuing
Software Development	C/CPFF	NIWC ATLANTIC : Charleston, SC	23.665	3.127	Dec 2021	3.323	Dec 2022	3.278	Dec 2023	-		3.278	Continuing	Continuing	Continuing
Software Development	FFRDC	MITRE : McLean, VA	10.728	0.652	Dec 2021	0.661	Dec 2022	0.936	Dec 2023	-		0.936	Continuing	Continuing	Continuing
Software Development	Various	Various : Various	69.170	0.789	Dec 2021	0.799	Dec 2022	0.984	Dec 2023	-		0.984	Continuing	Continuing	Continuing
Software Development	C/CPFF	BAH : San Diego, CA	15.159	1.652	Jan 2022	1.674	Jan 2023	1.651	Jan 2024	-		1.651	Continuing	Continuing	Continuing
Software Development	FFRDC	GTRI : Atlanta, GA	22.551	0.569	Jan 2022	0.576	Jan 2023	0.285	Jan 2024	-		0.285	Continuing	Continuing	Continuing
Software Development	WR	NSMA : San Diego, CA	7.659	0.650	Oct 2021	0.658	Oct 2022	0.650	Oct 2023	-		0.650	Continuing	Continuing	Continuing
Software Development	WR	NRL : Washington DC	6.146	1.169	Oct 2021	1.184	Oct 2022	0.973	Oct 2023	-		0.973	Continuing	Continuing	Continuing
<b>Subtotal</b>			491.039	25.445		26.425		26.088		-		26.088	Continuing	Continuing	N/A

**UNCLASSIFIED**

Exhibit R-3, RDT&E Project Cost Analysis: PB 2024 Navy												Date: March 2023			
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)				FY 2022		FY 2023		FY 2024 Base		FY 2024 OCO		FY 2024 Total			
Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Cost To Complete	Total Cost	Target Value of Contract
Architecture	WR	Various : Various	6.502	0.123	Oct 2021	0.125	Oct 2022	0.123	Oct 2023	-		0.123	Continuing	Continuing	Continuing
Architecture	WR	NIWC ATLANTIC : Charleston, SC	3.771	0.216	Oct 2021	0.219	Oct 2022	0.216	Oct 2023	-		0.216	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	7.990	0.945	Jan 2022	0.957	Jan 2023	0.944	Jan 2024	-		0.944	Continuing	Continuing	Continuing
Studies & Design	WR	Various : Various	7.768	0.353	Oct 2021	0.358	Oct 2022	0.353	Oct 2023	-		0.353	Continuing	Continuing	Continuing
<b>Subtotal</b>			26.481	1.637		1.659		1.636		-		1.636	Continuing	Continuing	N/A
Test and Evaluation (\$ in Millions)				FY 2022		FY 2023		FY 2024 Base		FY 2024 OCO		FY 2024 Total			
Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Cost To Complete	Total Cost	Target Value of Contract
Developmental Test & Evaluation (DT&E)	WR	NIWC PACIFIC : San Diego, CA	39.694	0.817	Oct 2021	0.828	Oct 2022	0.816	Oct 2023	-		0.816	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	4.784	1.265	Jan 2022	1.282	Jan 2023	1.265	Jan 2024	-		1.265	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	-
<b>Subtotal</b>			48.079	2.082		2.110		2.081		-		2.081	Continuing	Continuing	N/A
Management Services (\$ in Millions)				FY 2022		FY 2023		FY 2024 Base		FY 2024 OCO		FY 2024 Total			
Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Award Date	Cost	Cost To Complete	Total Cost	Target Value of Contract
Program Management	C/CPFF	BAH : San Diego, CA	34.538	1.285	Jan 2022	1.302	Jan 2023	1.284	Jan 2024	-		1.284	Continuing	Continuing	Continuing
<b>Subtotal</b>			34.538	1.285		1.302		1.284		-		1.284	Continuing	Continuing	N/A

**UNCLASSIFIED**

<b>Exhibit R-3, RDT&amp;E Project Cost Analysis:</b> PB 2024 Navy							<b>Date:</b> March 2023				
<b>Appropriation/Budget Activity</b> 1319 / 7			<b>R-1 Program Element (Number/Name)</b> PE 0303140N / Information Sys Security Program				<b>Project (Number/Name)</b> 0734 / Communications Security R&D				
	<b>Prior Years</b>	<b>FY 2022</b>	<b>FY 2023</b>	<b>FY 2024 Base</b>	<b>FY 2024 OCO</b>	<b>FY 2024 Total</b>	<b>Cost To Complete</b>	<b>Total Cost</b>	<b>Target Value of Contract</b>		
<b>Project Cost Totals</b>	600.137	30.449	31.496	31.089	-	31.089	Continuing	Continuing	N/A		

**Remarks**

**UNCLASSIFIED**

**Exhibit R-4, RDT&E Schedule Profile: PB 2024 Navy** **Date:** March 2023

<b>Appropriation/Budget Activity</b> 1319 / 7	<b>R-1 Program Element (Number/Name)</b> PE 0303140N / Information Sys Security Program	<b>Project (Number/Name)</b> 0734 / Communications Security R&D
--	--	--

Computer Network Defense (CND)	FY 2022				FY 2023				FY 2024				FY 2025				FY 2026				FY 2027				FY 2028			
	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q
<b>Development, Integration, and Test</b>																												
CND Inc 2 Dev, Integ, & Test	CND Inc 2 Dev, Integ, & Test																											
<b>Deliveries</b>																												
CND - Inc 2 Deliveries	Inc 2 Deliveries																											

2024PB - 0303140N - 0734

**UNCLASSIFIED**

**Exhibit R-4, RDT&E Schedule Profile: PB 2024 Navy** **Date:** March 2023

<b>Appropriation/Budget Activity</b> 1319 / 7	<b>R-1 Program Element (Number/Name)</b> PE 0303140N / <i>Information Sys Security Program</i>	<b>Project (Number/Name)</b> 0734 / <i>Communications Security R&amp;D</i>
--	---	---

Navy Cryptography (Crypto)	FY 2022				FY 2023				FY 2024				FY 2025				FY 2026				FY 2027				FY 2028			
	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q
<b>Milestones</b>	<div style="display: flex; flex-direction: column; gap: 10px;"> <div style="display: flex; align-items: center;"> <div style="width: 20px; border-bottom: 1px solid black; margin-right: 5px;"></div> <div>ACC 2/3 NSA Fielding Decision</div> </div> <div style="display: flex; align-items: center;"> <div style="width: 20px; border-bottom: 1px solid black; margin-right: 5px;"></div> <div>KGV-11M Full Rate Production</div> </div> <div style="display: flex; align-items: center;"> <div style="width: 20px; border-bottom: 1px solid black; margin-right: 5px;"></div> <div>KGV-11M Initial Operational Capability</div> </div> </div>																											
<b>Development, Integration, and Test</b>	<div style="border: 1px solid black; padding: 2px; display: inline-block; margin-bottom: 5px;">ACC Solutions Development and Product Testing</div>																											
<b>Deliveries</b>	<div style="border: 1px solid black; padding: 2px; display: inline-block; margin-bottom: 5px;">VACM Deliveries</div> <div style="border: 1px solid black; padding: 2px; display: inline-block; margin-bottom: 5px; margin-left: 100px;">KGV-11M Deliveries</div> <div style="border: 1px solid black; padding: 2px; display: inline-block; margin-left: 150px;">ACC Deliveries</div>																											

2024PB - 0303140N - 0734

**UNCLASSIFIED**

**Exhibit R-4, RDT&E Schedule Profile: PB 2024 Navy** **Date:** March 2023

<b>Appropriation/Budget Activity</b> 1319 / 7	<b>R-1 Program Element (Number/Name)</b> PE 0303140N / <i>Information Sys Security Program</i>	<b>Project (Number/Name)</b> 0734 / <i>Communications Security R&amp;D</i>
--	---	---

Key Management (KM)	FY 2022				FY 2023				FY 2024				FY 2025				FY 2026				FY 2027				FY 2028			
	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q
<b>Milestones</b>																												
KMI CI-3 Releases 0-7 Development, Integration, and Test																												
Intermediary Application (iApp) Development and Product Testing																												
<b>Deliveries</b>																												
Key Load Device Deliveries																												
KMI Tech Refresh Deliveries																												

CI-3  
FRPD  
/ FD  
◆

CI-3 Releases 0-7 Development, Integration, and Test

Intermediary Application (iApp)

Key Load Device Deliveries

Tech Refresh Deliveries

2024PB - 0303140N - 0734

**UNCLASSIFIED**

**Exhibit R-4, RDT&E Schedule Profile: PB 2024 Navy** **Date:** March 2023

<b>Appropriation/Budget Activity</b> 1319 / 7	<b>R-1 Program Element (Number/Name)</b> PE 0303140N / <i>Information Sys Security Program</i>	<b>Project (Number/Name)</b> 0734 / <i>Communications Security R&amp;D</i>
--	---	---

Page/Group/Row:	FY 2022				FY 2023				FY 2024				FY 2025				FY 2026				FY 2027				FY 2028			
	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q
<b>SHARKCAGE</b>																												
<b>Development, Integration, and Test SHARKCAGE</b>																												
SHARKCAGE - Transition Dev, Integ, & Test	SHARKCAGE Dev, Integ, & Test																											
<b>Deliveries</b>																												
SHARKCAGE - RDC Deliveries																												
SHARKCAGE - Transition Deliveries	SHARKCAGE Deliveries																											
<b>Navy Cyber Situational Awareness (NCSA)</b>																												
<b>Milestones</b>																												
<b>Development, Integration, and Test NCSA</b>																												
NCSA - Transition Dev, Integ, & Test	NCSA Dev, Integ, & Test																											
<b>Deliveries</b>																												
NCSA - Transition Deliveries	NCSA Deliveries																											

2024PB - 0303140N - 0734

**UNCLASSIFIED**

**Exhibit R-4, RDT&E Schedule Profile: PB 2024 Navy** **Date:** March 2023

<b>Appropriation/Budget Activity</b> 1319 / 7	<b>R-1 Program Element (Number/Name)</b> PE 0303140N / <i>Information Sys Security Program</i>	<b>Project (Number/Name)</b> 0734 / <i>Communications Security R&amp;D</i>
--	---	---

Page/Group/Row	FY 2022				FY 2023				FY 2024				FY 2025				FY 2026				FY 2027				FY 2028			
	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q
<b>Public Key Infrastructure (PKI)</b>																												
Public Key Infrastructure - System Engineering and Development of PKI	System Eng and Dev of PKI																											

2024PB - 0303140N - 0734

**UNCLASSIFIED**

<b>Exhibit R-4A, RDT&amp;E Schedule Details:</b> PB 2024 Navy		<b>Date:</b> March 2023
<b>Appropriation/Budget Activity</b> 1319 / 7	<b>R-1 Program Element (Number/Name)</b> PE 0303140N / <i>Information Sys Security Program</i>	<b>Project (Number/Name)</b> 0734 / <i>Communications Security R&amp;D</i>

Schedule Details

Events by Sub Project	Start		End	
	Quarter	Year	Quarter	Year
<b>Computer Network Defense (CND)</b>				
Development, Integration, and Test: CND Inc 2 Dev, Integ, & Test:	1	2022	4	2028
Deliveries: CND - Inc 2 Deliveries:	1	2022	4	2028
<b>Navy Cryptography (Crypto)</b>				
Milestones: Crypto - ACC 2/3 NSA Fielding Decision	1	2022	1	2022
Milestones: Crypto - KGV-11M Full Rate Production	1	2022	1	2022
Milestones: Crypto - KGV-11M Initial Operational Capability	1	2022	1	2022
Development, Integration, and Test: Crypto - ACC Solutions Development and Product Testing	1	2022	4	2024
Deliveries: Crypto - VACM Deliveries	1	2022	4	2024
Deliveries: Crypto - KGV-11M Deliveries	2	2024	4	2024
Deliveries: Crypto - ACC Deliveries	1	2022	4	2028
<b>Key Management (KM)</b>				
Milestones: KMI CI-3 FRP Decision / FD	2	2024	2	2024
Milestones: KMI CI-3 Releases 0-7 Development, Integration, and Test:	4	2023	4	2028
Milestones: Intermediary Application (iApp) Development and Product Testing:	1	2022	4	2028
Deliveries: Key Load Device Deliveries:	1	2022	4	2028
Deliveries: KMI Tech Refresh Deliveries:	1	2022	4	2028
<b>Page/Group/Row:</b>				
Development, Integration, and Test SHARKCAGE: SHARKCAGE - Transition Dev, Integ, & Test:	1	2022	4	2028
Deliveries: SHARKCAGE - Transition Deliveries:	1	2022	4	2028
Development, Integration, and Test NCSA: NCSA - Transition Dev, Integ, & Test:	1	2022	4	2028

**UNCLASSIFIED**

<b>Exhibit R-4A, RDT&amp;E Schedule Details:</b> PB 2024 Navy		<b>Date:</b> March 2023
<b>Appropriation/Budget Activity</b> 1319 / 7	<b>R-1 Program Element (Number/Name)</b> PE 0303140N / <i>Information Sys Security Program</i>	<b>Project (Number/Name)</b> 0734 / <i>Communications Security R&amp;D</i>

<b>Events by Sub Project</b>	<b>Start</b>		<b>End</b>	
	<b>Quarter</b>	<b>Year</b>	<b>Quarter</b>	<b>Year</b>
Deliveries: NCSA - Transition Deliveries:	1	2022	4	2028
<b><i>Page/Group/Row</i></b>				
Public Key Infrastructure (PKI): Public Key Infrastructure - System Engineering and Development of PKI:	1	2022	4	2028

**UNCLASSIFIED**

<b>Exhibit R-2A, RDT&amp;E Project Justification:</b> PB 2024 Navy										<b>Date:</b> March 2023		
<b>Appropriation/Budget Activity</b> 1319 / 7					<b>R-1 Program Element (Number/Name)</b> PE 0303140N / <i>Information Sys Security Program</i>				<b>Project (Number/Name)</b> 3230 / <i>Information Assurance</i>			
<b>COST (\$ in Millions)</b>	<b>Prior Years</b>	<b>FY 2022</b>	<b>FY 2023</b>	<b>FY 2024 Base</b>	<b>FY 2024 OCO</b>	<b>FY 2024 Total</b>	<b>FY 2025</b>	<b>FY 2026</b>	<b>FY 2027</b>	<b>FY 2028</b>	<b>Cost To Complete</b>	<b>Total Cost</b>
3230: <i>Information Assurance</i>	26.908	2.143	2.256	2.301	-	2.301	2.347	2.394	2.442	2.491	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 interoperability, 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

**UNCLASSIFIED**

<b>Exhibit R-2A, RDT&amp;E Project Justification:</b> PB 2024 Navy		<b>Date:</b> March 2023
<b>Appropriation/Budget Activity</b> 1319 / 7	<b>R-1 Program Element (Number/Name)</b> PE 0303140N / <i>Information Sys Security Program</i>	<b>Project (Number/Name)</b> 3230 / <i>Information Assurance</i>

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)**

	<b>FY 2022</b>	<b>FY 2023</b>	<b>FY 2024 Base</b>	<b>FY 2024 OCO</b>	<b>FY 2024 Total</b>
<b>Title:</b> Information Assurance (IA)	2.143	2.256	2.301	0.000	2.301
<b>Articles:</b>	-	-	-	-	-
<p><b>FY 2023 Plans:</b></p> <ul style="list-style-type: none"> <li>- 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.</li> <li>- 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.</li> <li>- 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).</li> <li>- Continue the development of tools/technology to provide a cloud application trust in its host infrastructure.</li> <li>- 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.</li> <li>- 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.</li> <li>- Continue the development of tools to measure and reduce collateral damage incurred by cyber operations.</li> </ul>					

**UNCLASSIFIED**

<b>Exhibit R-2A, RDT&amp;E Project Justification:</b> PB 2024 Navy		<b>Date:</b> March 2023
<b>Appropriation/Budget Activity</b> 1319 / 7	<b>R-1 Program Element (Number/Name)</b> PE 0303140N / <i>Information Sys Security Program</i>	<b>Project (Number/Name)</b> 3230 / <i>Information Assurance</i>

**B. Accomplishments/Planned Programs (\$ in Millions, Article Quantities in Each)**

	<b>FY 2022</b>	<b>FY 2023</b>	<b>FY 2024 Base</b>	<b>FY 2024 OCO</b>	<b>FY 2024 Total</b>
<p>- Initiate techniques for multimodal sensing, dependency analysis through causal inference, and fusion of active and passive measurements for iterative sensing and reconnaissance.</p> <p>- Initiate 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.</p> <p>- Initiate 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.</p> <p><b>FY 2024 Base Plans:</b></p> <p>- 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.</p> <p>- 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).</p> <p>- 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.</p> <p>- Continue the development of tools/technology to provide a cloud application trust in its host infrastructure.</p> <p>- 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.</p> <p>- 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.</p> <p>- 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.</p>					

**UNCLASSIFIED**

<b>Exhibit R-2A, RDT&amp;E Project Justification:</b> PB 2024 Navy		<b>Date:</b> March 2023
<b>Appropriation/Budget Activity</b> 1319 / 7	<b>R-1 Program Element (Number/Name)</b> PE 0303140N / <i>Information Sys Security Program</i>	<b>Project (Number/Name)</b> 3230 / <i>Information Assurance</i>

<b>B. Accomplishments/Planned Programs (\$ in Millions, Article Quantities in Each)</b>	<b>FY 2022</b>	<b>FY 2023</b>	<b>FY 2024 Base</b>	<b>FY 2024 OCO</b>	<b>FY 2024 Total</b>
<p>- 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.</p> <p>- 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.</p> <p>- 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.</p> <p><b>FY 2024 OCO Plans:</b> N/A</p> <p><b>FY 2023 to FY 2024 Increase/Decrease Statement:</b> FY 2024 increase of \$0.045M due to inflation.</p>					
<b>Accomplishments/Planned Programs Subtotals</b>	2.143	2.256	2.301	0.000	2.301

**C. Other Program Funding Summary (\$ in Millions)**

N/A

**Remarks**

**D. Acquisition Strategy**

N/A

**UNCLASSIFIED**

<b>Exhibit R-3, RDT&amp;E Project Cost Analysis: PB 2024 Navy</b>												<b>Date: March 2023</b>			
<b>Appropriation/Budget Activity</b> 1319 / 7				<b>R-1 Program Element (Number/Name)</b> PE 0303140N / <i>Information Sys Security Program</i>				<b>Project (Number/Name)</b> 3230 / <i>Information Assurance</i>							
<b>Support (\$ in Millions)</b>				<b>FY 2022</b>		<b>FY 2023</b>		<b>FY 2024 Base</b>		<b>FY 2024 OCO</b>		<b>FY 2024 Total</b>			
<b>Cost Category Item</b>	<b>Contract Method &amp; Type</b>	<b>Performing Activity &amp; Location</b>	<b>Prior Years</b>	<b>Cost</b>	<b>Award Date</b>	<b>Cost</b>	<b>Award Date</b>	<b>Cost</b>	<b>Award Date</b>	<b>Cost</b>	<b>Award Date</b>	<b>Cost</b>	<b>Cost To Complete</b>	<b>Total Cost</b>	<b>Target Value of Contract</b>
Development Support	Various	NRL : Washington, DC	26.908	2.143	Nov 2021	2.256	Nov 2022	2.301	Nov 2023	-		2.301	Continuing	Continuing	Continuing
<b>Subtotal</b>			26.908	2.143		2.256		2.301		-		2.301	Continuing	Continuing	N/A
			<b>Prior Years</b>	<b>FY 2022</b>	<b>FY 2023</b>		<b>FY 2024 Base</b>		<b>FY 2024 OCO</b>		<b>FY 2024 Total</b>	<b>Cost To Complete</b>	<b>Total Cost</b>	<b>Target Value of Contract</b>	
<b>Project Cost Totals</b>			26.908	2.143		2.256		2.301		-	2.301	Continuing	Continuing	N/A	
<b>Remarks</b>															

**UNCLASSIFIED**

<b>Exhibit R-4, RDT&amp;E Schedule Profile: PB 2024 Navy</b>		<b>Date:</b> March 2023
<b>Appropriation/Budget Activity</b> 1319 / 7	<b>R-1 Program Element (Number/Name)</b> PE 0303140N / <i>Information Sys Security Program</i>	<b>Project (Number/Name)</b> 3230 / <i>Information Assurance</i>

FY 2022				FY 2023				FY 2024				FY 2025				FY 2026				FY 2027				FY 2028			
1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4

<b>Proj 3230</b>	
Development	

**UNCLASSIFIED**

<b>Exhibit R-4A, RDT&amp;E Schedule Details:</b> PB 2024 Navy		<b>Date:</b> March 2023
<b>Appropriation/Budget Activity</b> 1319 / 7	<b>R-1 Program Element (Number/Name)</b> PE 0303140N / <i>Information Sys Security Program</i>	<b>Project (Number/Name)</b> 3230 / <i>Information Assurance</i>

Schedule Details

Events by Sub Project	Start		End	
	Quarter	Year	Quarter	Year
<b>Proj 3230</b>				
Development	1	2022	4	2028