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 6: *RDT&E Management Support*	**R-1 Program Element (Number/Name)** PE 0305327N *I Insider Threat*

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	0.000	2.315	2.246	2.920	-	2.920	2.798	2.657	2.710	2.766	Continuing	Continuing
3442: *Insider Threat*	0.000	2.315	2.246	2.920	-	2.920	2.798	2.657	2.710	2.766	Continuing	Continuing

A. Mission Description and Budget Item Justification

Executive Order 13587 and the National Insider Threat Policy mandate all United States Government departments and agencies to implement insider threat programs that monitor user activity on all classified networks and provide an insider threat analytical and response capability. The Counter Insider Threat Capability (CITC) is the Department of the Navy's implementation of this requirement. CITC's mission is to prevent, deter, detect, and respond to the threat from witting and unwitting insiders. The Platform for Risk Evaluation and Engagement to Neutralize Threat (PREVENT) is the materiel solution required to support the CITC mission, and consists of two parts: (1) User Activity Monitoring (UAM), which monitors user activity on classified Navy networks, and (2) an Integrated Tool Suite (ITS), which provides the Information Technology platform for the analytic and response capabilities. The PREVENT system provides the technology required by the Navy Insider Threat Analytic Hub to comply with the National mandates and to protect Navy data, equipment, and personnel from insider threats. RDT&E,N funding is required to develop future, long-term, capability; integrate; and perform testing and evaluation of this capability.

B. Program Change Summary ($ in Millions)	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
Previous President's Budget	2.315	2.246	2.994	-	2.994
Current President's Budget	2.315	2.246	2.920	-	2.920
Total Adjustments	0.000	0.000	-0.074	-	-0.074
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Program Adjustments	0.000	0.000	-0.074	-	-0.074

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy			Date: March 2024
Appropriation/Budget Activity 1319 / 6	R-1 Program Element (Number/Name) PE 0305327N / *Insider Threat*	Project (Number/Name) 3442 / *Insider Threat*	

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
3442: *Insider Threat*	0.000	2.315	2.246	2.920	-	2.920	2.798	2.657	2.710	2.766	Continuing	Continuing
Quantity of RDT&E Articles		-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

Executive Order 13587 and the National Insider Threat Policy mandate all United States Government departments and agencies to implement insider threat programs that monitor user activity on all classified networks and provide an insider threat analytical and response capability. The Counter Insider Threat Capability (CITC) is the Department of the Navy's implementation of this requirement. CITC's mission is to prevent, deter, detect, and respond to the threat from witting and unwitting insiders. The Platform for Risk Evaluation and Engagement to Neutralize Threat (PREVENT) is the materiel solution required to support the CITC mission, and consists of two parts: (1) User Activity Monitoring (UAM), which monitors user activity on classified Navy networks, and (2) an Integrated Tool Suite (ITS), which provides the Information Technology platform for the analytic and response capabilities. The PREVENT system provides the technology required by the Navy Insider Threat Analytic Hub to comply with the National mandates and to protect Navy data, equipment, and personnel from insider threats. RDT&E,N funding is required to develop future, long-term, capability; integrate; and perform testing and evaluation of this capability.

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
Title: Counter Insider Threat Capability (CITC)	2.315	2.246	2.920	0.000	2.920
Articles:	-	-	-	-	-
FY 2024 Plans: - Initiate testing and development of long-term UAM and ITS capability on JWICS and SIPRNet. - Initiate testing of Integrated Tool Suite (ITS) major upgrades to current ITS solution. - Initiate research of Cross Domain Solution (CDS) for Integrated Tool Suite (ITS) data between Secret Internet Protocol Router Network (SIPRNet), Joint Worldwide Intelligence Communications System (JWICS), and Non-classified Internet Protocol (IP) Router Network (NIPRNet) and begin testing and evaluation efforts. - Continue testing of UAM major upgrades to current UAM solution including testing across multiple networks with existing UAM capabilities and cloud environment. - Continue testing, evaluation, and integration efforts on Secret Internet Protocol Router Network (SIPRNet) afloat networks (CANES). - Continue research, development, and integration of enhanced testing environment into Navy networks to measure health of UAM system including policy performance and network impacts. - Continue reassessment and reaccreditation of PREVENT capability.					
FY 2025 Base Plans: - Continue testing of ITS major upgrades to current ITS solution.					

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy		Date: March 2024
Appropriation/Budget Activity 1319 / 6	**R-1 Program Element (Number/Name)** PE 0305327N / *Insider Threat*	**Project (Number/Name)** 3442 / *Insider Threat*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
- Continue testing of UAM major upgrades to current UAM solution including testing across multiple networks with existing UAM capabilities and cloud environment. - Continue testing, evaluation, and integration efforts on SIPRNet afloat networks (CANES). - Continue research, development, and integration of enhanced testing environment into Navy networks to measure health of UAM system including policy performance and network impacts. - Continue reassessment and reaccreditation of Platform for Risk Evaluation and Engagement to Neutralize Threat (PREVENT) capability. - Continue research of Cross Domain Solution (CDS)for Integrated Tool Suite (ITS) data between Secret Internet Protocol Router Network (SIPRNet), Joint Worldwide Intelligence Communications System (JWICS), and Non-classified Internet Protocol (IP) Router Network (NIPRNet) and begin testing and evaluation efforts. - Continue testing and development of long-term UAM and ITS capabilities on JWICS and SIPRNet. - Initiate investigating commercial cloud environments and User Activity Monitoring (UAM) capabilities for future increments of PREVENT capability including alternative technologies and existing solutions including Big Data Platform (BDP). - Initiate testing and integration of UAM and ITS expansion across Navy networks. ***FY 2025 OCO Plans:*** N/A ***FY 2024 to FY 2025 Increase/Decrease Statement:*** The FY24 to FY25 increase of $0.674M is attributed to the long term development of future Integrated Tool Suite (ITS) and User Activity Monitoring (UAM) capabilities, testing and integration of future upgrades to ITS and UAM current solutions, continued expansion and testing of UAM capability across additional classified networks, test and evaluation of a Cross Domain Solution (CDS), continued research into commercial cloud environments, continued research into alternative technologies and existing solutions, reassessment and reaccreditation efforts for UAM and ITS systems, and research and development of long term UAM capability utilizing insider threat Subject-Matter Experts (SMEs).					
Accomplishments/Planned Programs Subtotals	2.315	2.246	2.920	0.000	2.920

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

Exhibit R-2A, RDT&E Project Justification: PB 2025 Navy		Date: March 2024
Appropriation/Budget Activity 1319 / 6	**R-1 Program Element (Number/Name)** PE 0305327N / *Insider Threat*	**Project (Number/Name)** 3442 / *Insider Threat*

D. Acquisition Strategy

CITC employs a flexible acquisition strategy based on the IT Box model to incrementally deliver capability that is responsive to rapidly evolving requirements, priorities, and technology. Requirements for each capability increment are derived from the Platform for Risk Evaluation and Engagement to Neutralize Threat (PREVENT) Information Systems Capability Development Document (IS-CDD) via Capability Drops (CDs) and approved by the CITC Requirements Governance Board (RBG). CD-1 defined the initial capability set to achieve Initial Operational Capability (IOC) by rapidly fielding existing Commercial-Off-The-Shelf (COTS) tools using Middle Tier of Acquisition (MTA) authority. CD-1 was successfully fielded and achieved Initial Operational Capability (IOC) in February 2022. Capability Drop-2 (CD-2), approved by the CITC Requirements Governance Board (RGB) in September 2022, expands upon CD-1 by delivering enhanced case management capabilities and additional Integrated Tool Suite (ITS) data sources.

Under Middle Tier of Acquisition (MTA) authority, CITC met the MTA fielding requirements by successfully fielding CD-1. Currently, the program is in the process of closing out the MTA period and transition to an Abbreviated Acquisition Program (AAP). An AAP provides CITC with the most flexibility to sustain the existing capability and deliver incremental capability enhancements based on existing and/or new requirements. CITC will continue to deliver via Capability Drops (CDs) based on the existing Platform for Risk Evaluation and Engagement to Neutralize Threat (PREVENT) Information Systems Capability Development Document (IS-CDD).