Exhibit R-2, RDT&E Budget Item Justification: PB 2021 Navy	Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
Total Program Element	0.000	1.682	2.645	2.310	-	2.310	2.676	2.568	2.536	2.586	Continuing	Continuing
3442: *Insider Threat*	0.000	1.682	2.645	2.310	-	2.310	2.676	2.568	2.536	2.586	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 deter, detect, and respond to the threat from witting and unwitting insiders. The Personnel Risk Indicator Detection Enterprise (PRIDE) is the materiel solution required to support the CITC mission, and it will consist of two parts: (1) User Activity Monitoring (UAM), which will monitor user activity on Navy networks, and (2) an Integrated Tool Suite (ITS), which will provide the Information Technology platform for the analytic and response capabilities. The PRIDE system will provide the technology required by the Department of the Navy Insider Threat 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, integrate, and perform testing and evaluation of this capability.

B. Program Change Summary ($ in Millions)	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
Previous President's Budget	1.682	2.645	2.500	-	2.500
Current President's Budget	1.682	2.645	2.310	-	2.310
Total Adjustments	0.000	0.000	-0.190	-	-0.190
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Program Adjustments	0.000	0.000	-0.190	-	-0.190

Change Summary Explanation

The FY2021 funding request was reduced by $0.208M to account for the availability of prior year execution balances.

Exhibit R-2A, RDT&E Project Justification: PB 2021 Navy			Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
3442: *Insider Threat*	0.000	1.682	2.645	2.310	-	2.310	2.676	2.568	2.536	2.586	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 deter, detect, and respond to the threat from witting and unwitting insiders. The Personnel Risk Indicator Detection Enterprise (PRIDE) is the materiel solution required to support the CITC mission, and it will consist of two parts: (1) User Activity Monitoring (UAM), which will monitor user activity on Navy networks, and (2) an Integrated Tool Suite (ITS), which will provide the Information Technology platform for the analytic and response capabilities. The PRIDE system will provide the technology required by the Department of the Navy Insider Threat 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, integrate, and perform testing and evaluation of this capability.

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
Title: Counter Insider Threat Capability (CITC)	1.682	2.645	2.310	0.000	2.310
Articles:	-	-	-	-	-
FY 2020 Plans: - Develop and integrate the new capability to identify a specific type of person, as required by the Counter Insider Threat Capability (CITC) Mission. - Continue to research and design a Hub to receive, analyze and appropriately report data from User Activity Monitoring (UAM), Random Polygraph program, Law Enforcement, Counter Intelligence, Travel/Border data, Hotline tips, Identity Matching Engine for Security and Analysis (IMESA), Inspector General (IG) and others. - Expand the UAM tool into the software baselines of Navy Secret Internet Protocol Router Network (SIPRnet), including Consolidated Afloat Networks and Enterprise Services (CANES), Navy Marine Corps Intranet (NMCI), Outside the Continental United States (OCONUS) Navy Enterprise Network (ONE-Net), and additional Joint Worldwide Intelligence Communications System (JWICS) domains. - Perform developmental testing of the Integrated Tool Suite (ITS) and afloat UAM installations. - Evaluate Defense Information Systems Agency' (DISA) Big Data Platform (BDP) and Defense Security Services (DSS) Federal Vetting Enterprise (FVE) solutions as potential replacements for the commercial ITS in future increments of the Personnel Risk Indicator Detection Enterprise (PRIDE). - Investigate commercial cloud environments for future increments of PRIDE capability on SIPRnet.					
FY 2021 Base Plans:					

Exhibit R-2A, RDT&E Project Justification: PB 2021 Navy		Date: February 2020
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 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
- Complete UAM tool integration into the software baselines of SIPRnet including CANES, NMCI, OCONUS ONE-Net, and additional JWICS domains. - Continue efforts to expand the UAM tool into the software baselines of additional Navy networks including additional JWICS domains and additional SIPRnet networks. - Continue evaluation of alternate technologies for future increments of UAM and ITS capability including proof of concept for DISA BPD and/or DCS FVE. - Perform testing and evaluation of UAM capability on SIPRnet. - Perform integration of additional data feeds to the ITS. - Investigate commercial cloud environments for future increments of PRIDE capability on Non-classified Internet Protocol Router System (NIPRnet). ***FY 2021 OCO Plans:*** N/A ***FY 2020 to FY 2021 Increase/Decrease Statement:*** No significant changes from FY20 to FY21.					
Accomplishments/Planned Programs Subtotals	1.682	2.645	2.310	0.000	2.310

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
• OPN/8106: *Command Support Equipment/Insider Threat*	1.707	0.000	0.000	-	0.000	0.000	0.000	0.000	0.000	0.000	2.707
• OPN/3415: *Info Systems Security Program (ISSP)*	0.000	2.619	0.000	-	0.000	0.000	0.000	0.000	0.000	0.000	2.619

Remarks

D. Acquisition Strategy

N/A