Exhibit R-2, RDT&E Budget Item Justification: PB 2020 Navy											Date: March 2019	
Appropriation/Budget Activity 1319: *Research, Development, Test & Evaluation, Navy* / BA 6: *RDT&E Management Support*					R-1 Program Element (Number/Name) PE 0305327N / *Insider Threat*							
COST ($ in Millions)	**Prior Years**	**FY 2018**	**FY 2019**	**FY 2020 Base**	**FY 2020 OCO**	**FY 2020 Total**	**FY 2021**	**FY 2022**	**FY 2023**	**FY 2024**	**Cost To Complete**	**Total Cost**
Total Program Element	0.000	0.000	1.682	2.645	-	2.645	2.500	2.532	2.465	2.515	Continuing	Continuing
3442: *Insider Threat*	0.000	0.000	1.682	2.645	-	2.645	2.500	2.532	2.465	2.515	Continuing	Continuing

A. Mission Description and Budget Item Justification

The Navy Counter Insider Threat Capability (CITC) meets National, Department of Defense (DoD) and Department of the Navy (DoN) direction to deter, detect, and mitigate the threat from witting and unwitting insiders. Counter Insider Threat program accomplishes these objectives by monitoring users' computers and network activities, fusing that information with security risk data from multiple other sources, and providing the fused information to analysts for threat identification and initial response action. All agencies that manage classified networks are required to establish an Insider Threat program consisting of User Activity Monitoring (UAM) and an Analytical Hub. As a Presidential Directive, Navy will come under increased Congressional scrutiny if Insider Threat does not maintain funding.

Navy currently does not fully meet CITC requirements. As the CITC Mission requires Navy to establish a new capability to identify a specific type of person, as defined above, RDT&E,N funding is required to appropriately develop and integrate this capability effectively.

B. Program Change Summary ($ in Millions)	FY 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total
Previous President's Budget	0.000	1.682	2.680	-	2.680
Current President's Budget	0.000	1.682	2.645	-	2.645
Total Adjustments	0.000	0.000	-0.035	-	-0.035
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Rate/Misc Adjustments	0.000	0.000	-0.035	-	-0.035

Change Summary Explanation

Funding: The increase in funding from FY2019 to FY2020 will develop and integrate the new capability to identify a specific type of person, as defined above, as required by the Counter Insider Threat Capability (CITC) Mission.

Exhibit R-2A, RDT&E Project Justification: PB 2020 Navy			Date: March 2019
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 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
3442: *Insider Threat*	0.000	0.000	1.682	2.645	-	2.645	2.500	2.532	2.465	2.515	Continuing	Continuing
Quantity of RDT&E Articles		-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

The Navy Counter Insider Threat Capability (CITC) meets National, Department of Defense (DoD) and Department of the Navy (DoN) direction to deter, detect, and mitigate the threat from witting and unwitting insiders. Counter Insider Threat program accomplishes these objectives by monitoring users' computers and network activities, fusing that information with security risk data from multiple other sources, and providing the fused information to analysts for threat identification and initial response action. All agencies that manage classified networks are required to establish an Insider Threat program consisting of User Activity Monitoring (UAM) and an Analytical Hub.

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total
Title: Insider Threat	0.000	1.682	2.645	0.000	2.645
Articles:	-	-	-	-	-
FY 2019 Plans: 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; participate in Trident Warrior 19 to determine effectiveness and impact of the UAM tool (test & evaluate).					
FY 2020 Base Plans: Develop and integrate the new capability to identify a specific type of person, as required by the CITC Mission. Continue to research and design a Hub to receive, analyze and appropriately report data from UAM, Random Polygraph program, Law Enforcement, Counter Intelligence, Travel/Border data, Hotline tips, IMESA, IG and others; participate in Trident Warrior 20 to determine effectiveness and impact of the UAM tool (test & evaluate).					
FY 2020 OCO Plans: N/A					
FY 2019 to FY 2020 Increase/Decrease Statement: The increase in funding from FY2019 to FY2020 will develop and integrate the new capability to identify a specific type of person, as required by the CITC Mission.					
Accomplishments/Planned Programs Subtotals	0.000	1.682	2.645	0.000	2.645

Exhibit R-2A, RDT&E Project Justification: PB 2020 Navy		Date: March 2019
Appropriation/Budget Activity 1319 / 6	**R-1 Program Element (Number/Name)** PE 0305327N / *Insider Threat*	**Project (Number/Name)** 3442 / *Insider Threat*

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
• OPN/8106/0305327N: *Command Support Equipment/Insider Threat*	1.000	1.707	0.000	-	0.000	0.000	0.000	0.000	0.000	0.000	2.707
• OPN/3415/0305327N: *Info Systems Security Program*	0.000	0.000	2.619	-	2.619	6.459	6.756	6.756	6.891	Continuing	Continuing

Remarks

OPN/8106 - FY19 will be the last year Insider Threat is in LI 8106. In FY20 Insider Threat will be part of LI 3415.

D. Acquisition Strategy

N/A

E. Performance Metrics

Test Cases, risk case measure one thing in R&D, but measure other things in operations.

In the R&D phase, performance will be measured by bandwidth utilization and identification of software configuration setting.

Operational performance measurements will include enumeration of false positives, and the successful collection, identification and reporting of insider threat indicators.