

**UNCLASSIFIED**

**Exhibit R-2, RDT&E Budget Item Justification:** PB 2022 Navy **Date:** May 2021

<b>Appropriation/Budget Activity</b> 1319: <i>Research, Development, Test &amp; Evaluation, Navy / BA 6: RDT&amp;E Management Support</i>	<b>R-1 Program Element (Number/Name)</b> PE 0305327N / <i>Insider Threat</i>
--	---

COST (\$ in Millions)	Prior Years	FY 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total	FY 2023	FY 2024	FY 2025	FY 2026	Cost To Complete	Total Cost
Total Program Element	0.000	2.592	2.293	2.581	-	2.581	-	-	-	-	-	-
3442: <i>Insider Threat</i>	0.000	2.592	2.293	2.581	-	2.581	-	-	-	-	-	-

**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 Platform for Risk Evaluation and Engagement to Neutralize Threat (PREVENT) 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 PREVENT system will provide the technology required by the Department of 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, integrate, and perform testing and evaluation of this capability.

<b>B. Program Change Summary (\$ in Millions)</b>	<b>FY 2020</b>	<b>FY 2021</b>	<b>FY 2022 Base</b>	<b>FY 2022 OCO</b>	<b>FY 2022 Total</b>
Previous President's Budget	2.645	2.310	2.676	-	2.676
Current President's Budget	2.592	2.293	2.581	-	2.581
Total Adjustments	-0.053	-0.017	-0.095	-	-0.095
• Congressional General Reductions	-	-0.017			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-0.053	0.000			
• Program Adjustments	0.000	0.000	-0.087	-	-0.087
• Rate/Misc Adjustments	0.000	0.000	-0.008	-	-0.008

**Change Summary Explanation**

The FY 2022 funding request was reduced by \$0.087 million to account for the availability of prior year execution balances.

The FY21 to FY22 increase of \$0.288M is due to the testing and evaluation of Integrated Tool Suite (ITS) on JWICS, continued expansion of UAM capability to SIPRNet excepted networks, initiation of testing of long-term UAM capability, and research and development of UAM capability on NIPRNet.

**UNCLASSIFIED**

<b>Exhibit R-2A, RDT&amp;E Project Justification:</b> PB 2022 Navy										<b>Date:</b> May 2021		
<b>Appropriation/Budget Activity</b> 1319 / 6					<b>R-1 Program Element (Number/Name)</b> PE 0305327N / <i>Insider Threat</i>				<b>Project (Number/Name)</b> 3442 / <i>Insider Threat</i>			
<b>COST (\$ in Millions)</b>	<b>Prior Years</b>	<b>FY 2020</b>	<b>FY 2021</b>	<b>FY 2022 Base</b>	<b>FY 2022 OCO</b>	<b>FY 2022 Total</b>	<b>FY 2023</b>	<b>FY 2024</b>	<b>FY 2025</b>	<b>FY 2026</b>	<b>Cost To Complete</b>	<b>Total Cost</b>
3442: <i>Insider Threat</i>	0.000	2.592	2.293	2.581	-	2.581	-	-	-	-	-	-
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 Platform for Risk Evaluation and Engagement to Neutralize Threat (PREVENT) 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 PREVENT system will provide the technology required by the Department of 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, integrate, and perform testing and evaluation of this capability.

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

	<b>FY 2020</b>	<b>FY 2021</b>	<b>FY 2022 Base</b>	<b>FY 2022 OCO</b>	<b>FY 2022 Total</b>
<b>Title:</b> Counter Insider Threat Capability (CITC)	2.592	2.293	2.581	0.000	2.581
<b>Articles:</b>	-	-	-	-	-
<b>FY 2021 Plans:</b>					
<ul style="list-style-type: none"> <li>- Initiate development and integration of interim solution for ITS.</li> <li>- Complete UAM tool integration into the software baselines of SIPRNet including NMCI and ONE-Net.</li> <li>- Initiate testing and evaluation of UAM on SIPRNet excepted networks and continue integration efforts on to SIPRNet afloat networks (CANES).</li> <li>- Continue evaluation of alternate technologies for future increments of UAM and ITS capability including proof of concept for Defense Information Systems Agency (DISA) Big Data Platform (BDP).</li> <li>- Perform integration of additional data feeds to the ITS.</li> <li>- Complete assessment and authorization of JWICS and SIPRNet cloud infrastructure for UAM capability.</li> </ul>					
<b>FY 2022 Base Plans:</b>					
<ul style="list-style-type: none"> <li>- Perform testing and evaluation of ITS long-term solution on to JWICS including integration of at least 4 data sources and integration of complex analytics to identify insider threat risk indicators.</li> <li>- Research and development of centralized repository of ITS ingested data that will store structured and unstructured data for the long-term materiel solution.</li> <li>- Perform research and development of cross domain solution for ITS data ingestion between SIPRNet, JWICS, and NIPRNet for future expansion to NIPRNet.</li> </ul>					

**UNCLASSIFIED**

<b>Exhibit R-2A, RDT&amp;E Project Justification:</b> PB 2022 Navy		<b>Date:</b> May 2021
<b>Appropriation/Budget Activity</b> 1319 / 6	<b>R-1 Program Element (Number/Name)</b> PE 0305327N / <i>Insider Threat</i>	<b>Project (Number/Name)</b> 3442 / <i>Insider Threat</i>

<b>B. Accomplishments/Planned Programs (\$ in Millions, Article Quantities in Each)</b>	<b>FY 2020</b>	<b>FY 2021</b>	<b>FY 2022 Base</b>	<b>FY 2022 OCO</b>	<b>FY 2022 Total</b>
- Continue development efforts to expand the UAM SIPRNet excepted networks across multiple networks. - Initiate testing and development of long-term UAM capability on JWICS and SIPRNet. - Investigate commercial cloud environments and UAM capabilities for future increments of PREVENT capability on Non-classified Internet Protocol Router System (NIPRNet) including alternative technologies and existing solutions.  <b>FY 2022 OCO Plans:</b> N/A  <b>FY 2021 to FY 2022 Increase/Decrease Statement:</b> FY22 increase is due to testing and evaluation of Integrated Tool Suite (ITS) on JWICS, continued expansion of UAM capability to SIPRNet excepted networks, initiation of testing of long-term UAM capability, and research and development of UAM capability on NIPRNet.					
<b>Accomplishments/Planned Programs Subtotals</b>	2.592	2.293	2.581	0.000	2.581

<b>C. Other Program Funding Summary (\$ in Millions)</b>											
<u>Line Item</u>	<u>FY 2020</u>	<u>FY 2021</u>	<u>FY 2022 Base</u>	<u>FY 2022 OCO</u>	<u>FY 2022 Total</u>	<u>FY 2023</u>	<u>FY 2024</u>	<u>FY 2025</u>	<u>FY 2026</u>	<u>Cost To Complete</u>	<u>Total Cost</u>
• OPN/3415: <i>Info Systems Security Program (ISSP)</i>	166.540	157.551	146.879	-	146.879	-	-	-	-	-	-

**Remarks**

**D. Acquisition Strategy**  
 CITC is employing 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 increment of capability are scoped by validated Capability Drop requirements documents. The initial increment of capability, defined by Capability Drop 1 (CD-1), is designed to achieve Initial Operational Capability (IOC) in FY21 by rapidly fielding existing Commercial Off the Shelf (COTS) tools using Section 804 Middle Tier Acquisition (MTA) authority. The future Program of Record (POR) will build toward Full Operational Capability (FOC) requirements by incrementally expanding UAM coverage and integrating additional data feeds and analytic capabilities in the ITS, as specified in future Capability Drops.