Exhibit R-2, RDT&E Budget Item Justification: PB 2022 Office of the Secretary Of Defense	Date: May 2021
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide* / BA 6: *RDT&E Management Support*	**R-1 Program Element (Number/Name)** PE 0606771D8Z / *Cyber Resiliency & Cybersecurity Policy*

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	0.000	31.638	-	31.638	-	-	-	-	-	-
145: *Cyber Resiliency & Cybersecurity Policy*	-	0.000	0.000	31.638	-	31.638	-	-	-	-	-	-

Note

Cyber Resiliency & Cybersecurity Policy is not a new start. It is a continuation of efforts previously contained in PE 0604771D8Z, Joint Tactical Information Distribution System.

A. Mission Description and Budget Item Justification

Cyber Resiliency & Cybersecurity Policy program supports the efforts of OUSD A&S Chief Information Security Office, focusing on the defense of the Department's critical mission weapon systems and Defense Critical Infrastructure from cyber attack, protecting the Department's sensitive unclassified information residing within the Defense Industrial Base(DIB) sector and supply chain, and capability portfolio management for Joint Cyber Capabilities used by the Cyber Mission Force. This program funds the following critical efforts:

1) Cybersecurity for Weapon Systems and Critical Infrastructure: Lead the Department's Strategic Cybersecurity Program (SCP) to continue critical weapon systems and defense infrastructure cybersecurity assessments and mitigations. CISO(A&S) Cyber Resiliency efforts are aligned with the following initiatives:

Assess:
- Conduct of mission focused cyber risk assessments for priority Defense Missions in support of CCMDs.
- Conduct Deep Cyber Resiliency Assessments (DCRA) in support of CCMDs and asset owners.

Inventory:
- Develop, sustain, and employ Cyber Risk Mitigation Tool (CRMT), an Enterprise-wide decision support tool for tracking cyber vulnerability assessments and mitigations.

Prioritize:
- Prioritize Cyber Risk Mitigations based upon mission analysis conducted by Mission Focused Cyber Hardening Teams.

2) DIB Cybersecurity
- Determine the resilience and cybersecurity of DIB contractors and their suppliers which support the associated research, design, development, production, sustainment, and operations of DoD weapon systems.
- Enhance the cybersecurity of the DIB, and improve Supply Chain Risk Management (SCRM) to secure the Department's critical classified and unclassified information.

Exhibit R-2, RDT&E Budget Item Justification: PB 2022 Office of the Secretary Of Defense	Date: May 2021
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide I* BA 6: *RDT&E Management Support*	**R-1 Program Element (Number/Name)** PE 0606771D8Z *I Cyber Resiliency & Cybersecurity Policy*

- Implement and update the Cybersecurity Maturity Model Certification (CMMC) risk based framework to enhance the cybersecurity posture of the DIB sector and protect Controlled Unclassified Information (CUI) and Federal Contract Information (FCI).
- Conduct CMMC pilots and risk reduction pathfinders with Services, Agencies, and/or international partners to support the phased rollout.
- Test and demonstrate full operational capability of the CMMC Enterprise Mission Assurance Support Service (eMASS) database and infrastructure.
- Maintain secure data transfers from third party commercial assessment organizations and CMMC eMASS, and between CMMC eMASS and other DoD databases.

B. Program Change Summary ($ in Millions)	FY 2020	FY 2021	FY 2022 Base	FY 2022 OCO	FY 2022 Total
Previous President's Budget	0.000	0.000	31.638	-	31.638
Current President's Budget	0.000	0.000	31.638	-	31.638
Total Adjustments	0.000	0.000	0.000	-	0.000
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Office of the Secretary Of Defense			Date: May 2021
Appropriation/Budget Activity 0400 / 6	R-1 Program Element (Number/Name) PE 0606771D8Z / *Cyber Resiliency & Cyber security Policy*	Project (Number/Name) 145 / *Cyber Resiliency & Cybersecurity Policy*	

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
145: *Cyber Resiliency & Cybersecurity Policy*	-	0.000	0.000	31.638	-	31.638	-	-	-	-	-	-
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

Note

Cyber Resiliency & Cybersecurity Policy is not a new start. It is a continuation of efforts previously contained in PE 0604771D8Z, Joint Tactical Information Distribution System.

A. Mission Description and Budget Item Justification

Cyber Resiliency & Cybersecurity Policy program supports the efforts of OUSD A&S Chief Information Security Office focusing on the defense of the Department's critical mission weapon systems and Defense Critical Infrastructure from cyber attack, protecting the Department's sensitive unclassified information residing within the defense industrial base(DIB) sector and supply chain, and capability portfolio management for Joint Cyber Capabilities used by the Cyber Mission Force.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2020	FY 2021	FY 2022
Title: Cyber Resiliency & Cybersecurity Policy	-	-	31.638
FY 2022 Plans: Cybersecurity for Weapon Systems and DCI: - Lead the Department's Strategic Cybersecurity Program (SCP) to continue critical weapon systems and defense infrastructure cybersecurity assessments and mitigations. Conduct SCP Pilots to inform cybersecurity best practices for weapon systems in development using multiple acquisition pathways. - Perform Mission Level Cyber Risk Assessments: 1) Plan and Execute Mission Resiliency (MR) II in coordination with the USTRANSCOM and USECUOM. 2) Plan and Execute MR III in collaboration with USSPACECOM. 3) Perform Deep Cyber Resiliency Assessments (DCRAS) in support of CCMD priorities. - Prioritize Mitigations based upon mission analysis conducted by Mission Focused Cyber Hardening Teams. Develop and deploy the CRMT to maintain a Master Cyber Risk Inventory for the Department of Defense for Weapon Systems and DCI based upon CRAs/DCRAs, and other assessments DIB Cybersecurity: - Update and refine CMMC framework based on emerging cyber threats, adjudication of public comments to the interim rule, and outputs from the initial phased rollout			

Exhibit R-2A, RDT&E Project Justification: PB 2022 Office of the Secretary Of Defense		Date: May 2021
Appropriation/Budget Activity 0400 / 6	**R-1 Program Element (Number/Name)** PE 0606771D8Z / *Cyber Resiliency & Cyber security Policy*	**Project (Number/Name)** 145 / *Cyber Resiliency & Cybersecurity Policy*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2020	FY 2021	FY 2022
- Conduct CMMC pilots and risk reduction pathfinders with Services, Agencies, and/or international partners to support the phased rollout - Plan for the phased rollout of acquisitions that implement enhanced cybersecurity requirements (i.e. CMMC Level 4 or 5 requirement) and acquisitions with international contractors/subcontractors within the multi-tier supply chain - Test and demonstrate full operational capability of the CMMC Enterprise Mission Assurance Support Service (eMASS) database and infrastructure - Partner with the DIB sector to analyze and demonstrate promising and cost-effective capabilities and candidate solutions related to supply chain risk management and DIB cybersecurity - Work with DoD stakeholders and appropriate organizations dedicated to enhancing the training and education of cybersecurity best practices to the DIB sector with an emphasis on small businesses and manufacturers Capability Portfolio Management for Cyber Capabilities: - Advance and mature capabilities for conducting mission engineering for cyberspace operations. - Manage the portfolio of Joint Cyber Warfighting Architecture (JCWA) components to enable the cyber mission force to efficiently and effectively conduct offensive and defensive cyber missions. Support offensive and defensive architecture development and portfolio management in collaboration with USCYBERCOM. - As PSA OPR for the UP, oversee the Air Force's, as DoD EA, capability development via portfolio management and governance. Assess UP's interfaces, dependencies, and linkages with other components of the JCWA to integrate and analyze data from offensive and defensive operations and enable effective and efficient offensive and defensive effects. - Manage the portfolio of DoD cyber training systems; including the DoDs PCTE and govern the PCTE as a member of the PCTE governance boards. - Conduct Cybersecurity Review of Joint Cyber Capabilities in development. ***FY 2021 to FY 2022 Increase/Decrease Statement:*** This is not an increase. It is a continuation of efforts previously contained in PE 0604771D8Z, Joint Tactical Information Distribution System.			
Accomplishments/Planned Programs Subtotals	-	-	31.638

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A