Exhibit R-2, RDT&E Budget Item Justification: PB 2023 Office of the Secretary Of Defense	Date: April 2022
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 2021	FY 2022	FY 2023 Base	FY 2023 OCO	FY 2023 Total	FY 2024	FY 2025	FY 2026	FY 2027	Cost To Complete	Total Cost
Total Program Element	0.000	0.000	31.460	32.306	-	32.306	31.813	30.476	30.198	30.153	Continuing	Continuing
145: *Cyber Resiliency & Cybersecurity Policy*	0.000	0.000	31.460	32.306	-	32.306	31.813	30.476	30.198	30.153	Continuing	Continuing

Note

New Start (Y/N): No

A. Mission Description and Budget Item Justification

This program supports the Department's initiatives to Defend the Homeland, and Build Sustainable and Long-Term Advantage.

The Cyber Resiliency & Cybersecurity Policy program supports the efforts of OUSD A&S, 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:

Exhibit R-2, RDT&E Budget Item Justification: PB 2023 Office of the Secretary Of Defense	Date: April 2022
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*

Development, implementation and sustainment of the Cybersecurity Maturity Model Certification (CMMC) framework that incorporates NIST SP 800-171 standards and references into a unified standard that encompasses the progression of cybersecurity practices to secure Controlled Unclassified Information (CUI) within the Defense Industrial Base (DIB) sector.

Conduct pathfinders to assess the feasibility and efficacy of employing emerging commercial services/tools/platforms that provide insights into cybersecurity threats and vulnerabilities that are relevant to the DIB sector and the DoD supply chain.

Partner with the DIB sector to demonstrate cost-effective and scalable cybersecurity services that augment and/or enhance existing commercial capabilities and services. Focus on cybersecurity services for small-to-medium sized DIB companies that are critical to the DoD supply chain but lack sufficient cybersecurity capabilities to protect CUI.

B. Program Change Summary ($ in Millions)	FY 2021	FY 2022	FY 2023 Base	FY 2023 OCO	FY 2023 Total
Previous President's Budget	0.000	31.638	0.000	-	0.000
Current President's Budget	0.000	31.460	32.306	-	32.306
Total Adjustments	0.000	-0.178	32.306	-	32.306
• Congressional General Reductions	-	-0.178			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Adjustments to Budget Year	-	-	32.306	-	32.306

Change Summary Explanation

FY 2023 funding increase reflects the fact that the FY 2022 President’s Budget request did not include out-year funding.

Exhibit R-2A, RDT&E Project Justification: PB 2023 Office of the Secretary Of Defense			Date: April 2022
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 2021	FY 2022	FY 2023 Base	FY 2023 OCO	FY 2023 Total	FY 2024	FY 2025	FY 2026	FY 2027	Cost To Complete	Total Cost
145: *Cyber Resiliency & Cybersecurity Policy*	0.000	0.000	31.460	32.306	-	32.306	31.813	30.476	30.198	30.153	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

Cyber Resiliency & Cybersecurity Policy program supports the efforts of OUSD A&S, 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:
Development, implementation and sustainment of the Cybersecurity Maturity Model Certification (CMMC) framework that incorporates NIST SP 800-171 standards and references into a unified standard that encompasses the progression of cybersecurity practices to secure Controlled Unclassified Information (CUI) within the Defense Industrial Base (DIB) sector.

Conduct pathfinders to assess the feasibility and efficacy of employing emerging commercial services/tools/platforms that provide insights into cybersecurity threats and vulnerabilities that are relevant to the DIB sector and the DoD supply chain.

Exhibit R-2A, RDT&E Project Justification: PB 2023 Office of the Secretary Of Defense		Date: April 2022
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*

Partner with the DIB sector to demonstrate cost-effective and scalable cybersecurity services that augment and/or enhance existing commercial capabilities and services. Focus on cybersecurity services for small-to-medium sized DIB companies that are critical to the DoD supply chain but lack sufficient cybersecurity capabilities to protect CUI.

.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2021	FY 2022	FY 2023
Title: Cyber Resiliency & Cybersecurity Policy	-	31.460	32.306
Description: FY 2021 Accomplishments for this program are reported under PE 0604771D8Z, Joint Tactical Information Distribution System. ***FY 2022 Plans:*** Cybersecurity for Weapon Systems and Defense Critical Infrastructure (DCI): - Lead the Department's Strategic Cybersecurity Program (SCP) to continue critical weapon systems and defense infrastructure cybersecurity assessments and mitigations. - Develop, update, and refine cybersecurity Policy. - Support cybersecurity reviews of MDAPs where USD(A&S) is the MDA. -Conduct SCP Pilots to inform cybersecurity best practices for weapon systems in development using multiple acquisition pathways. Perform Mission Level Cyber Risk Assessments (CRAs): 1) Plan and Execute Mission Resiliency (MR) I in coordination with the USTRANSCOM and USECUOM. 2) Plan and Execute MR II 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. 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.			

Exhibit R-2A, RDT&E Project Justification: PB 2023 Office of the Secretary Of Defense		Date: April 2022
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 2021	FY 2022	FY 2023
- Manage the portfolio of DoD cyber training systems; including the DoDs PCTE and govern the PCTE as a member of the PCTE governance boards. Defense Industrial Base (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. - 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 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.			
FY 2023 Plans: Cybersecurity for Weapon Systems and Defense Critical Infrastructure (DCI): - Lead the Department's Strategic Cybersecurity Program (SCP) to continue critical weapon systems and defense critical infrastructure cybersecurity assessments and mitigations. - Develop, update, and refine cybersecurity Policy. - Support cybersecurity reviews of MDAPs where USD(A&S) is the MDA. Develop enduring solutions for the Department on future 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 (CRAs): 1) Plan and Execute Mission Resiliency (MR) II in coordination with the USTRANSCOM and USEUCOM. 2) Plan and Execute MR III in collaboration with USNORTHCOM 3) Perform Deep Cyber Resiliency Assessments (DCRAs) in support of CCMD priorities. - Prioritize Mitigations and vulnerabilities based upon mission analyses conducted by Mission Focused Cyber Hardening Teams, DCRAs, wargaming, and program management office assessments. - Oversee and track Service/Agency execution of system-level cyber vulnerability assessments for additional priority weapons systems added in JROCM 039-26.			

Exhibit R-2A, RDT&E Project Justification: PB 2023 Office of the Secretary Of Defense		Date: April 2022
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 2021	FY 2022	FY 2023
- Lead Weapons Systems Cybersecurity Council of Colonels, with representation from US Air Force, US Army, US Navy, US Marine Corps, PCA, DoD CIO, Joint Staff J6. - Lead Cybersecurity Community of Practice (CCOP) with OUSD(R&E) to foster sharing of vital cybersecurity information and best practices across the DoD Community. - Participate in PCA-led DoD Cyber Strategy Line of Effort 9, focused on Mission Assurance for weapons systems and critical infrastructure. 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 United Platform (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. - As PSA OPR for the UP component of JCWA, assess the effectiveness of USCYBERCOM requirements generation, mission engineering, and capability prioritization for UP acquisition. Assess the timeliness and effectiveness of UP acquisition in response to USCYBERCOM requirements and involvement in and impact on the mission engineering process. Assess the maturity of UP's Software Acquisition Pathway (SWaP) implementation and coordinate any necessary modifications to DoD SWaP policy. - 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 to enhance the Cybersecurity of Weapon Systems in development and sustainment. Defense Industrial Base (DIB) Cybersecurity: - Implement the revised Cybersecurity Maturity Model Certification (CMMC) framework based on the outcome of rulemaking, emerging cyber threats, and DoD leadership decisions. - Execute CMMC Pilots in concert with Military Services, DoD agencies, and international partners in support of the CMMC roll-out. - Conduct risk reduction pathfinders on the implementation of CMMC Level 3 enhanced security requirements. - Develop and test full operational capability of the CMMC Enterprise Mission Assurance Support Service (Emass) database execute periodic releases.			

Exhibit R-2A, RDT&E Project Justification: PB 2023 Office of the Secretary Of Defense		Date: April 2022
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 2021	FY 2022	FY 2023
- 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 ***FY 2022 to FY 2023 Increase/Decrease Statement:*** There is no significant change between FY 2022 and FY 2023			
Accomplishments/Planned Programs Subtotals	-	31.460	32.306

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A