Exhibit R-2, RDT&E Budget Item Justification: PB 2025 Office of the Secretary Of Defense	Date: March 2024
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 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total	FY 2026	FY 2027	FY 2028	FY 2029	Cost To Complete	Total Cost
Total Program Element	34.450	50.077	45.194	40.401	-	40.401	16.863	16.713	16.981	17.300	Continuing	Continuing
145: *Cyber Resiliency & Cybersecurity Policy*	26.699	38.524	45.194	40.401	-	40.401	16.863	16.713	16.981	17.300	Continuing	Continuing
147: *Securing the Defense Industrial Base (DIB): Cybersecurity Maturity Model Certification (CMMC)*	7.751	11.553	0.000	0.000	-	0.000	0.000	0.000	0.000	0.000	Continuing	Continuing

Note

New Start (Y/N): No

A. Mission Description and Budget Item Justification

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 and cyber harden priority DoD missions.

OASD(A)/Cyber Warfare Directorate Cyber Resiliency efforts are aligned with the following initiatives:
Assess:
- Conduct mission based cyber risk assessments for priority Defense Missions in support of CCMDs.
- Conduct Deep Cyber Resiliency Assessments (DCRA) in support of CCMDs and asset owners.
- Conduct CCMD Mission Analytics in support of the Joint Staff and CCMDs.

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

Prioritize:
- Prioritize and advocate for Cyber Risk Mitigations based upon mission analysis conducted by program offices, the National Security Agency (NSA), Deep Cyber Resiliency Assessment teams, USCYBERCOM (USCC), and other cybersecurity professionals.

Exhibit R-2, RDT&E Budget Item Justification: PB 2025 Office of the Secretary Of Defense	Date: March 2024
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*

2) Weapon System Cyber Security - Cybersecurity Supply Chain Risk Management Pilots (C-SCRM)
In collaboration with DoD CIO, partner with other DoD organizations and the DIB sector to demonstrate cost-effective and scalable cybersecurity services that augment and/or enhance existing commercial capabilities and services. Focus on identifying options and assessing the efficacy of 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.

3) Capability Portfolio Management for Cyberspace Operations

Conduct Capability Portfolio Management of the Joint Cyber Capabilities employed by Cyber Mission Force in collaboration with USCYBERCOM. Assess the capabilities of JWCA for supporting the conduct of offensive and defensive cyberspace operations.

B. Program Change Summary ($ in Millions)	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total
Previous President's Budget	51.901	45.194	43.160	-	43.160
Current President's Budget	50.077	45.194	40.401	-	40.401
Total Adjustments	-1.824	0.000	-2.759	-	-2.759
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-1.824	-			
• Defense-Wide Topline Adjustment	-	-	-2.759	-	-2.759

Congressional Add Details ($ in Millions, and Includes General Reductions)	FY 2023	FY 2024
Project: 145: *Cyber Resiliency & Cybersecurity Policy*		
Congressional Add: *Deep Cyber Resiliency Assessments*	20.000	-
Congressional Add Subtotals for Project: 145	20.000	-
Congressional Add Totals for all Projects	20.000	-

Change Summary Explanation
FY 2025 decrease to fund higher departmental priorities.

Exhibit R-2A, RDT&E Project Justification: PB 2025 Office of the Secretary Of Defense											Date: March 2024	
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 2023**	**FY 2024**	**FY 2025 Base**	**FY 2025 OCO**	**FY 2025 Total**	**FY 2026**	**FY 2027**	**FY 2028**	**FY 2029**	**Cost To Complete**	**Total Cost**
145: *Cyber Resiliency & Cybersecurity Policy*	26.699	38.524	45.194	40.401	-	40.401	16.863	16.713	16.981	17.300	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

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 in support of the NDS and the DoD Cyber Strategy.

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 and cyber harden priority DoD missions.

OASD(A)/Cyber Warfare Directorate Cyber Resiliency efforts are aligned with the following initiatives:
Assess:
- Conduct mission based cyber risk assessments for priority Defense Missions in support of CCMDs.
- Conduct Deep Cyber Resiliency Assessments (DCRA) in support of CCMDs and asset owners.
- Conduct CCMD Mission Analytics in support of the Joint Staff and CCMDs.

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

Prioritize:
- Prioritize and advocate for Cyber Risk Mitigations based upon mission analysis conducted by program offices, the National Security Agency (NSA), Deep Cyber Resiliency Assessment teams, USCYBERCOM (USCC), and other cybersecurity professionals.

2) Weapon System Cyber Security - Cybersecurity Supply Chain Risk Management Pilots (C-SCRM)

Exhibit R-2A, RDT&E Project Justification: PB 2025 Office of the Secretary Of Defense		Date: March 2024
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*

In collaboration with DoD CIO, partner with other DoD organizations and the DIB sector to demonstrate cost-effective and scalable cybersecurity services that augment and/or enhance existing commercial capabilities and services. Focus on identifying options and assessing the efficacy of 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.

3) Capability Portfolio Management for Cyberspace Operations

Conduct Capability Portfolio Management of the Joint Cyber Capabilities employed by Cyber Mission Force in collaboration with USCYBERCOM. Assess the capabilities of JWCA for supporting the conduct of offensive and defensive cyberspace operations.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2023	FY 2024	FY 2025
Title: Cyber Resiliency & Cybersecurity Policy	18.524	45.194	40.401
Description: FY 2023 Accomplishments: Assessments: Conduct Cyber Risk Assessments in support of CCMDs: Combatant Commands Mission Level Cyber Risk Assessments (MLCRA): - Completed a year-long campaign of learning with the capstone being Mission Resilience II in support of USSPACECOM. Emphasis and focus were placed on the Command-and-Control capabilities and the cyber risk to the mission sets served by the system. The process identified several cyber risks to mission operations of the system. Results informed the 2023 Weapon System and DCI Cyber Hardening IAPR, USSPACECOM Integrated Priorities, and Strategic Cybersecurity Program 4-Star Level Briefings. Deep Cyber Resiliency Assessments (DCRAs): - Completed six DCRAs for Mission Partners across the DoD including a high priority special request from a Combatant Command (CCMD). Mission partners include Army Materiel Command, NASA, USTRANSCOM, USSTRATCOM, and USINDOPACOM. - DCRA continues to provide mitigation strategies based on mission analytics for DoD and OGA partners to prioritize critical cyber risk to mission elements in policy and priority risks. - DCRA efforts continue to develop tools and assessment capabilities to map and quantify non-kinetic effects to weapon platforms, weapon systems, and critical infrastructure (CCMD) Mission Analytics (CCMA): - Developed a methodology to measure and weigh combatant commands mission interdependencies and how to define risk to mission from kinetic and non-kinetic fires.			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Office of the Secretary Of Defense		Date: March 2024
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 2023	FY 2024	FY 2025
- Defined the scope of the risk to mission effort to steady state and combat operations dependencies and how these dependencies change when moving between these postures. - Established working relationships with nine of 11 Combatant Commands (CCMD) and developed initial risk to mission dependency weightings for 14 of 55 relationship threats with a plan to be at 30 by the end of calendar year 2023. Prioritized this effort by functional to geographic command relationships first and functional to functional command relationships second. - Integrated and tested provisional results into Mission Level Cyber Risk Assessment (MR-II) with complete concurrence with results as valid and relevant. - Provided risk to mission insight to Deep Cyber Resilience Assessments to elevate developed tactical level cyber result to their relevant operational level mission impacts. Cyber Risk Mitigation: - In coordination with the Services, National Security Agency, DoD CIO, Joint Staff, USTRANSCOM, USEUCOM, USINDOPACOM, USCYBERCOM, Air Force Cyber Resiliency Office for Weapons Systems (CROWS), OUSD(I&S), and USSTRATCOM, refined the requirements and desired functionality for the Cyber Risk Mitigation Tool (CRMT). - Based on these requirements, the CRMT team refined visualizations to include dynamic scorecards, tree charts based on National Institute of Standards and Technology (NIST) vulnerability family, visualization of risk against operational and contingency planning (OPLAN/CONPLAN), mission and system decomposition, the interrelationship of systems/vulnerabilities via link diagram, potential mitigations based on available budget, and dynamic Sankey charts showing the relationship of missions, systems, planning, and organizations. - Updated SIPRnet-based version of the CRMT, which focuses on the status of Service Cybersecurity assessments covering priority weapon systems and critical infrastructure, to automatically import data from systems of record. - Successfully advocated to place additional ADVANA dashboards in the JWICs tool to show depth analytics on cyber vulnerabilities and mitigations. - Advocated and provided initial funding to put ADVANA on JWICS to enable the CRMT to provide in depth analytics on cyber vulnerabilities and mitigations while ensuring data security. - SIPRnet version of the tool is projected to be at full operational capability in September 2023 and the JWICS version is projected to be at initial operational capability in December 2023. - CRMT Data Analysis Team developed high impact Cybersecurity Scorecards in support of the Weapon System and Defense Critical Infrastructure (DCI) IAPR. Cybersecurity for Weapon Systems and Defense Critical Infrastructure (DCI): - Developed and coordinated the Strategic Cybersecurity Program Directive Type Memorandum for issuance.			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Office of the Secretary Of Defense		Date: March 2024
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 2023	FY 2024	FY 2025
- Supported multiple OUSD(A&S) Integrated Acquisition Portfolio Reviews with cybersecurity contributions as a factor in determining overall acquisition risk – to include the conduct of an IAPR focused solely on cyber hardening of weapon systems and defense critical infrastructure which was conducted in collaboration with multiple Combatant Commands. - Established Competitive Acquisition Pathfinder aligned with Cybersecurity for a priority DoD mission area. - Developed a Cyber Risk Mitigation Plan (CRMP) in support of identified installation cyber risks. - Supported Cyber Supply Chain Risk Management initiatives across the Department including support to implementation of Section 889/1656 Prohibitions on covered information and communication technologies for programs in acquisition and sustainment. - Began development and establishment of a standardized risk calculus for reporting control systems in relation to critical infrastructure, a control systems and critical infrastructure common lexicon, taxonomy, and ontology and an assessment reporting template of minimum required data for control systems and critical infrastructure. Initiated Planning for Installation Critical Infrastructure (ICI) Cybersecurity Engagement with NATO and supported ICI cybersecurity engagement with Poland. Weapon System Cyber Security - Cybersecurity Supply Chain Risk Management(C-SCRM): -Initiated conduct study of DIB Cybersecurity in Collaboration with DoD CIO. Collaborated with DoD CIO and other DoD Stakeholders in the Development of the initial DoD DIB Cybersecurity Strategy. Initiated planning for Weapon System C-SCRM Pilots. Capability Portfolio Management for Cyber Capabilities: - Conducted follow-on mission analysis to the USD(A&S)-chaired Cyberspace Operations Enterprise Integrated Acquisition Portfolio review (IAPR) meeting on June 28, 2022, which highlighted the need for a dedicated and enduring joint cyberspace operations capabilities System of Systems (SoS) Systems Engineering & Integration (SE&I) lead organization. Developed an Acquisition Decision Memorandum which formalized USSCYBEROMs authorities and responsibilities in this area. - In coordination with USCYBERCOM, developed options for PEO JWCA organization at USCYBERCOM. Cybersecurity Maturity Model Certification (CMMC): - Completed formal review and coordination of the 32 Code of Federal Regulations (CFR) proposed rule text on the Cybersecurity Maturity Model Certification (CMMC) 2.0 program with the DoD Office of General Counsel (OGC) and the Small Business Administration. Submitted the proposed rule to the Office of Information and Regulatory Affairs (OIRA) in the Office of Management and Budget (OMB) in July 2023 to support their mandatory review requirement.			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Office of the Secretary Of Defense		Date: March 2024
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 2023	FY 2024	FY 2025
- Completed and submitted the Initial Regulatory Flexibility Analysis (IRFA), the Regulatory Impact Analysis (RIA) and the Paperwork Reduction Act (PRA) documentation to OMB/OIRA in July 2023 - Developed updates to CMMC Enterprise Mission Assurance Support Service (eMASS) to support the DCMA-developed NIST SP 800-171 scoring algorithm and POA&Ms for CMMC Level 2. Updated the data standard to reflect changes in CMMC 2.0, including change from 5 levels to 3; changes in assessor types; assessment scoring for security requirement objectives; conditional and final assessment certificates; and assessing against the NIST standard instead of the CMMC 1.0 model. Developed CMMC program adoption and effective-ness metrics. Developed a tool to map attack TTPS to CMMC security requirements. - Partnered with OUSD(A&S) to conduct a study related to securing the DIB and provided resources to support a pilot for DIB Cybersecurity Services to support small businesses that is being led by OUSD(A&S) Office of Small Business Programs. Supported a supply chain illumination associated with a supply chain for a key weapons system. The effort focused on identifying manufacturers, direct suppliers, and indirect suppliers to the program. The illumination identified potential fragile nodes within the supply chain that could hamper or halt production of the weapon, including but not limited to foreign exposer, financial and operational health, and raw or refined materials bottlenecks. ***FY 2024 Plans:*** Conduct Cyber Risk Assessments in support of CCMDs: - Combatant Command (CCMD) Mission Analysis: Complete second CCMD assist with analytic approach. - Mission Resilience (MR) Games: Prepare for MR IV with CCMD and complete MR III. - Deep Cyber Resiliency Assessments: Perform multiple DCRAs for Mission Partners across the DoD. 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 Milestone Decision Authority (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. - Codify USD(A&S) cybersecurity reviews across programs to inform milestone decision authority determinations - Codify USD(A&S) cybersecurity policy and implementation guides for DoD installations, facilities, and DoD-owned critical infrastructure.			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Office of the Secretary Of Defense		Date: March 2024
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 2023	FY 2024	FY 2025
- Codify USD(A&S) cyber Supply Chain Risk Management policy and implementation guides in coordination with DoD CIO and USD(I&S) for programs and procurement. - Support identification of knowledge, skills, and abilities required of personnel to implement cybersecurity policy, plans, and initiatives to defend DoD's critical infrastructure, installations, and facilities. Cyber Risk Information Management: - Continue refine CRMT Functionality in response to user feedback. Address updating of data not available by automated means, and build out connection to additional APIs as appropriate. - Aggressively engage CRMT user community and drive user employment of the CRMT in support of multiple cyber risk management forums. 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 the OUSD(A&S) Cyberspace Operations Enterprise portfolio manager OPR, assess the effectiveness of USCYBERCOM requirements generation, mission engineering, and capability prioritization for cyberspace operations capabilities acquisition. In support of the calendar year 2024 USD(A&S)-chaired Cyberspace Operations Enterprise Integrated Acquisition Portfolio review (IAPR) meeting, conduct mission engineering analysis to identify capability gaps across the priority cyberspace operations mission thread. The results will inform OSD fiscal year 2026 program budget review. Defense Industrial Base (DIB) Cybersecurity: - Partner with the DoD CIO and 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 2025 Plans: Conduct Cyber Risk Assessments in support of CCMDs: - Mission Resilience (MR) Games: Prepare for MR IV with CCMD and complete MR III.			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Office of the Secretary Of Defense		Date: March 2024
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 2023	FY 2024	FY 2025
- Deep Cyber Resiliency Assessments: Perform multiple DCRAs for Mission Partners across the DoD in support Department priorities. Conduct Cyber Risk Assessments of priority DoD Assets (+$10 million in FY 2025). - Combatant Command (CCMD) Mission Analysis: Complete third CCMD assist with analytic approach. 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. - Enable USD(A&S) cybersecurity reviews across programs to inform milestone decision authority determinations. - Codify USD(A&S) cybersecurity policy and implementation guides for DoD installations, facilities, and DoD-owned critical infrastructure. - Codify USD(A&S) cyber Supply Chain Risk Management policy and implementation guides in coordination with DoD CIO and USD(I&S) for programs and procurement. - Support identification of knowledge, skills, and abilities required of personnel to implement cybersecurity policy, plans, and initiatives to defend DoD's critical infrastructure, installations, and facilities. Cyber Risk Information Management: - With both classified versions of the CRMT at full operational capability and datasets being loaded automatically via machine-to-machine interface, focus will be placed on adding Service datasets, threat reporting, and other datasets to meet stakeholder needs, as appropriate. - CRMT use will further expand within the Cyber Warfare Directorate to incorporate all section information and expand tool use in wargames and at CCMDs. Develop Cybersecurity Scorecards for Priority DoD Missions Weapon System Cyber Security - Cybersecurity Supply Chain Risk Management(C-SCRM): -Conduct Phase II of Weapon System C-SCRM Pilots (+$15 million in FY 2025). Demonstrate the efficacy of C-SCRM capabilities and continue to develop and refine C-SCRM best practices. Capability Portfolio Management for Cyber Capabilities: - Continue to 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.			

Exhibit R-2A, RDT&E Project Justification: PB 2025 Office of the Secretary Of Defense		Date: March 2024
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 2023	FY 2024	FY 2025
- As the OUSD(A&S) Cyberspace Operations Enterprise portfolio manager OPR, assess the effectiveness of USCYBERCOM requirements generation, mission engineering, and capability prioritization for cyberspace operations capabilities acquisition. In support of the calendar year 2025 USD(A&S)-chaired Cyberspace Operations Enterprise Integrated Acquisition Portfolio review (IAPR) meeting, conduct mission engineering analysis to identify capability gaps across the priority cyberspace operations mission thread. The results will inform OSD fiscal year 2026 Program Budget Review. ***FY 2024 to FY 2025 Increase/Decrease Statement:*** FY 2025 decrease supports higher departmental priorities.			
Accomplishments/Planned Programs Subtotals	18.524	45.194	40.401

	FY 2023	FY 2024
Congressional Add: Deep Cyber Resiliency Assessments	20.000	-
FY 2023 Accomplishments: - Deep Cyber Resiliency Assessments (DCRAs): Completed four DCRAs for Mission Partners across the DoD including a high priority special request from USINDOPACOM. Matured DCRA methodology and demonstrated the exceptional proficiency of DCRA team. Demonstrated the performance of DCRA Teams Advanced Data Collection Capabilities in a stressing operational environment. - Provided Combatant Command Mission Analytics support to USSPACECOM and USINDOPACOM and demonstrated CCMD proof of concept. - Procured equipment for a new facility in Huntsville, AL and Crystal City, VA to enable the teams to conduct Cyber Risk Assessments in a Top Secret environment. - Established Mission Level Cyber Risk Assessment capability in Crystal City, VA.		
Congressional Adds Subtotals	20.000	-

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2025 Office of the Secretary Of Defense			Date: March 2024
Appropriation/Budget Activity 0400 / 6	R-1 Program Element (Number/Name) PE 0606771D8Z / *Cyber Resiliency & Cyber security Policy*	Project (Number/Name) 147 / *Securing the Defense Industrial Base (DIB): Cybersecurity Maturity Model Certification (CMMC)*	

COST ($ in Millions)	Prior Years	FY 2023	FY 2024	FY 2025 Base	FY 2025 OCO	FY 2025 Total	FY 2026	FY 2027	FY 2028	FY 2029	Cost To Complete	Total Cost
147: *Securing the Defense Industrial Base (DIB): Cybersecurity Maturity Model Certification (CMMC)*	7.751	11.553	0.000	0.000	-	0.000	0.000	0.000	0.000	0.000	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

Note

This program has been moved to PE 0305104D8Z / Securing the Defense Industrial Base (DIB): Cybersecurity Maturity Model Certification (CMMC)

A. Mission Description and Budget Item Justification

This program supports the Department's initiatives to Deter Aggression and Prevail in Conflict, Defend the Homeland, and Build Enduring Advantage

Development, implementation and sustainment of the Cybersecurity Maturity Model Certification (CMMC) framework that incorporates multiple cybersecurity standards and references into a unified standard that encompasses both the progression of cybersecurity practices as well as the maturity of processes 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. Accomplishments/Planned Programs ($ in Millions)	FY 2023	FY 2024	FY 2025
Title: Securing the Defense Industrial Base (DIB): Cybersecurity Maturity Model Certification (CMMC)	11.553	-	-
Accomplishments/Planned Programs Subtotals	11.553	-	-

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

Exhibit R-2A, RDT&E Project Justification: PB 2025 Office of the Secretary Of Defense		Date: March 2024
Appropriation/Budget Activity 0400 / 6	**R-1 Program Element (Number/Name)** PE 0606771D8Z / *Cyber Resiliency & Cyber security Policy*	**Project (Number/Name)** 147 / *Securing the Defense Industrial Base (DIB): Cybersecurity Maturity Model Certification (CMMC)*

D. Acquisition Strategy

N/A