Exhibit R-2, RDT&E Budget Item Justification: PB 2024 Office of the Secretary Of Defense	Date: March 2023
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 2022	FY 2023	FY 2024 Base	FY 2024 OCO	FY 2024 Total	FY 2025	FY 2026	FY 2027	FY 2028	Cost To Complete	Total Cost
Total Program Element	0.000	34.450	51.901	45.194	-	45.194	43.160	17.929	17.790	18.161	Continuing	Continuing
145: *Cyber Resiliency & Cybersecurity Policy*	0.000	26.699	51.901	45.194	-	45.194	43.160	17.929	17.790	18.161	Continuing	Continuing
147: *Securing the Defense Industrial Base (DIB): Cybersecurity Maturity Model Certification (CMMC)*	-	7.751	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

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.

OASD(A)/Cyber Warfare Directorate Cyber Resiliency efforts are aligned with the following initiatives:

Assess:
- Conduct of 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.

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

Prioritize:

Exhibit R-2, RDT&E Budget Item Justification: PB 2024 Office of the Secretary Of Defense	Date: March 2023
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*

- 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 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 2022	FY 2023	FY 2024 Base	FY 2024 OCO	FY 2024 Total
Previous President's Budget	31.460	32.306	31.813	-	31.813
Current President's Budget	34.450	51.901	45.194	-	45.194
Total Adjustments	2.990	19.595	13.381	-	13.381
• Congressional General Reductions	-	-0.405			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	20.000			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Program Adjustments	2.990	-	13.381	-	13.381

Congressional Add Details ($ in Millions, and Includes General Reductions)	FY 2022	FY 2023
Project: 145: *Cyber Resiliency & Cybersecurity Policy*		
Congressional Add: *Deep Cyber Resiliency Assesments*	-	20.000
Congressional Add Subtotals for Project: 145	-	20.000
Congressional Add Totals for all Projects	-	20.000

Change Summary Explanation
FY 2024 increase to support Deep Cyber Resiliency Assessments.

Exhibit R-2A, RDT&E Project Justification: PB 2024 Office of the Secretary Of Defense											Date: March 2023	
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 2022**	**FY 2023**	**FY 2024 Base**	**FY 2024 OCO**	**FY 2024 Total**	**FY 2025**	**FY 2026**	**FY 2027**	**FY 2028**	**Cost To Complete**	**Total Cost**
145: *Cyber Resiliency & Cybersecurity Policy*	0.000	26.699	51.901	45.194	-	45.194	43.160	17.929	17.790	18.161	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.

OASD(A)/Cyber Warfare Directorate 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 2024 Office of the Secretary Of Defense		Date: March 2023
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 2022	FY 2023	FY 2024
Title: Cyber Resiliency & Cybersecurity Policy	26.699	31.901	45.194

Description: FY 2022 Accomplishments:
Assessments:

Conduct Cyber Risk Assessments in support of CCMDs:
- Combatant Command (CCMD) Mission Analysis: Began pilot of analytic approach with USSPACECOM to define mission essential tasks.
- Mission Resilience (MR) Games: Completed MR I in support of USTRANSCOM and USEUCOM to assess Global Logistics mission in a contested cyberspace environment. Began preparation for MR II in support of USSPACECOM.
- Deep Cyber Resiliency Assessments (DCRAs): Completed multiple DCRAs for Mission Partners across the DoD including a high priority special request from a CCMD.
- In coordination with the Services, National Security Agency, DoD CIO, Joint Staff, USCYBERCOM, and USSTRATCOM, developed the requirements and desired functionality for the Cyber Risk Mitigation Tool (CRMT).
- Based on these requirements, the CRMT team worked with the Defense Threat Reduction Agency, Air Force Research Laboratory, MITRE, Johns Hopkins Applied Physics Laboratory, Air Force Cyber Resiliency Office for Weapons Systems (CROWS), and Advance Analytics (ADVANA) leadership to develop the general implementation and schema of the CRMT.
- Launched a NIPRnet-based version of the CRMT tool during the COVID restrictions to allow for demonstration of potential functions and enable gathering of specific use cases.
- Launched SIPRnet-based version of the CRMT providing analysis and status of Cybersecurity assessments under Section 1647 of the National Defense Authorization (NDAA) Act for FY 2016 and Section 1650 of the NDAA for FY 2017, covering priority weapon systems and critical infrastructure respectively.
- 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.
- Began development of the structure and functions in the JWICS environment to enable Initial Operational Capability (IOC) of the CRMT by the end of FY 2022.
- Collected, compiled, and standardized the data required to meet IOC functionality of the CRMT on JWICS.

Cybersecurity for Weapon Systems and Defense Critical Infrastructure (DCI):
- Developed Strategic Cybersecurity Program Directive Type Memorandum establishing with support from stakeholders for issuance.

Exhibit R-2A, RDT&E Project Justification: PB 2024 Office of the Secretary Of Defense		Date: March 2023
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 2022	FY 2023	FY 2024
- Inaugurated cybersecurity contribution as a factor in determining overall acquisition risk through OUSD(A&S) Integrated Acquisition Portfolio Reviews. - Established working group to address section 1521 of the NDAA for FY 2022 requirement for identification of Executive Agent for procurement of cyber tools, data, and services. - 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. Capability Portfolio Management for Cyber Capabilities: - Conducted mission engineering analysis to support 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. - In coordination with USCYBERCOM, updated the cyber access and tools acquisition, development, and sustainment strategy and conducted an internal DoD directed study on Joint Cyber Warfighting Architecture (JCWA) enhancement. ***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.			

Exhibit R-2A, RDT&E Project Justification: PB 2024 Office of the Secretary Of Defense		Date: March 2023
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 2022	FY 2023	FY 2024
- 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. - 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 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 Unified Platform 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 rollout. - Conduct risk reduction pathfinders on the implementation of CMMC Level 3 enhanced security requirements.			

Exhibit R-2A, RDT&E Project Justification: PB 2024 Office of the Secretary Of Defense		Date: March 2023
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 2022	FY 2023	FY 2024
- Develop and test full operational capability of the CMMC Enterprise Mission Assurance Support Service (Emass) database execute periodic releases. - 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 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 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. - 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:			

Exhibit R-2A, RDT&E Project Justification: PB 2024 Office of the Secretary Of Defense		Date: March 2023
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 2022	FY 2023	FY 2024
- 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 2023 to FY 2024 Increase/Decrease Statement:*** FY 2024 decrease is due to this PE receiving a congressional add in FY 2023 for Deep Cyber Resiliency Assessments. This program received a baseline increase to conduct four Deep Cyber Resiliency Assessments in CONUS on Defense Critical Infrastructure and conduct a pilot to improve cybersecurity and cyber harden a mission critical supply chain in the Defense Industrial Base (DIB). Cybersecurity Maturity Model Certification program moved to Program Element 0305104D8Z starting in FY 2024.			
Accomplishments/Planned Programs Subtotals	26.699	31.901	45.194

	FY 2022	FY 2023
Congressional Add: Deep Cyber Resiliency Assesments	-	20.000
FY 2023 Plans: Congressional add funds were provided to conduct four additional Deep Cyber Resilience Assessments in support of Combatant Commands and asset owners.		

Exhibit R-2A, RDT&E Project Justification: PB 2024 Office of the Secretary Of Defense		Date: March 2023
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*

	FY 2022	FY 2023
Provide support to the Combatant Command Mission Analytics with United States Space Command and United States Indo-Pacific Command. Procure equipment for a new facility in Huntsville, AL and Crystal City, VA to enable the teams to conduct the Assessments in a Top Secret environment. Establish 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 2024 Office of the Secretary Of Defense			Date: March 2023
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 2022	FY 2023	FY 2024 Base	FY 2024 OCO	FY 2024 Total	FY 2025	FY 2026	FY 2027	FY 2028	Cost To Complete	Total Cost
147: *Securing the Defense Industrial Base (DIB): Cybersecurity Maturity Model Certification (CMMC)*	-	7.751	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 2022	FY 2023	FY 2024
Title: Securing the Defense Industrial Base (DIB): Cybersecurity Maturity Model Certification (CMMC)	7.751	-	-
Description: FY 2022 Accomplishments: Completed an eight month programmatic review of Cybersecurity Maturity Model Certification (CMMC) in November of 2021 resulting CMMC 2.0 with a more streamlined and improved program implementation.			

Exhibit R-2A, RDT&E Project Justification: PB 2024 Office of the Secretary Of Defense		Date: March 2023
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)*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2022	FY 2023	FY 2024
Developed Enterprise Mission Assurance Support Service (eMASS) CMMC 2.0 compliant database which required significant changes for artifacts and metrics. Developed a comprehensive 32 Code of Federal Regulations(CFR) Rule for CMMC that went into coordination August of 2022 Completed five congressional on Defense Industrial Base Cybersecurity information requests.			
Accomplishments/Planned Programs Subtotals	7.751	-	-

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A