Exhibit R-2, **RDT&E Budget Item Justification:** PB 2020 Office of the Secretary Of Defense	**Date:** February 2019
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide* / BA 6: *RDT&E Management Support*	**R-1 Program Element (Number/Name)** PE 0605797D8Z / *Maintaining Technology Advantage*

COST ($ in Millions)	Prior Years	FY 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
Total Program Element	-	0.000	0.000	19.936	-	19.936	19.748	19.244	19.500	19.808	Continuing	Continuing
138: *Data Vulnerability Assessment and Analysis*	-	0.000	0.000	9.344	-	9.344	9.044	8.426	8.569	8.755	Continuing	Continuing
139: *Joint Acquisition Protection Exploitation Cell (JAPEC)*	-	0.000	0.000	5.592	-	5.592	5.704	5.818	5.931	6.053	Continuing	Continuing
158: *Program and Technology Protection*	-	0.000	0.000	5.000	-	5.000	5.000	5.000	5.000	5.000	Continuing	Continuing

Note

This continuity of effort is being transferred from the Defense Technical Analysis PE 0605798D8Z and the Systems Engineering PE 0605142D8Z beginning in FY 2020 to more appropriately align the efforts within the current Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) organization.

A. Mission Description and Budget Item Justification

This Program Element provides funding to support efforts to maintain DoD's technology advantage. The targeting of U.S. capabilities by our strategic competitors create the potential to degrade core U.S. military technological advantages through unwanted technology transfer. The technology transfer, primarily unclassified technology, threatens DoD's ability to maintain the technology advantage required to support the lethality and survivability of the Joint Force. DoD is executing a campaign plan to maintain DoD's technology advantage. First DoD is promoting strategic technology investment to provide DoD access to new and innovative technology. These investments are required to create breakthroughs in key areas of basic research, foster transition and decrease time to market of applied research to economically viable companies, and harvest U.S. innovation or with likeminded allies. Secondly, DoD must ensure its strategic technology investments are protected against unwanted technology transfer by developing and maintaining the tools and techniques that enable the U.S. engage in technology transfer at the time, place, and parties of our choosing. Thirdly, DoD must combat adversaries' attempts to thwart U.S. technology security mechanisms to control technology transfer. The Department will support these three efforts by developing the appropriate suite of analytic tools, a data acquisition strategy, and utilize program protection activities to address the threat over the long term. Program Protection Planning includes protection of critical program information, critical components and mission functions, and integrates high level security policies and practical expertise to specific RDA practices, systems engineering activities, and risk reduction activities. Through this initiative the Department is maturing system security engineering methodologies to protect controlled unclassified information, to include controlled technical information on contractor networks; improve mitigation of supply chain risk management risks, improve integration of cybersecurity into the engineering processes, mature processes to identify Critical Program Information integration of defense exportability features and improve program protection planning.

Exhibit R-2, RDT&E Budget Item Justification: PB 2020 Office of the Secretary Of Defense	**Date:** February 2019
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide* / BA 6: *RDT&E Management Support*	**R-1 Program Element (Number/Name)** PE 0605797D8Z / *Maintaining Technology Advantage*

B. Program Change Summary ($ in Millions)	**FY 2018**	**FY 2019**	**FY 2020 Base**	**FY 2020 OCO**	**FY 2020 Total**
Previous President's Budget	0.000	0.000	0.000	-	0.000
Current President's Budget	0.000	0.000	19.936	-	19.936
Total Adjustments	0.000	0.000	19.936	-	19.936
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• FY 2020 Transfer from Exisiting Program Elements	-	-	19.936	-	19.936

Change Summary Explanation

This continuity of effort is being transferred from the Defense Technical Analysis PE 0605798D8Z and the Systems Engineering PE 0605142D8Z beginning in FY 2020 to more appropriately align the efforts within the current OUSD(R&E) organization.

Exhibit R-2A, RDT&E Project Justification: PB 2020 Office of the Secretary Of Defense			Date: February 2019
Appropriation/Budget Activity 0400 / 6	**R-1 Program Element (Number/Name)** PE 0605797D8Z / *Maintaining Technology Advantage*	**Project (Number/Name)** 138 / *Data Vulnerability Assessment and Analysis*	

COST ($ in Millions)	Prior Years	FY 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
138: *Data Vulnerability Assessment and Analysis*	-	0.000	0.000	9.344	-	9.344	9.044	8.426	8.569	8.755	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

Significant amounts of DoD's technical information resides on unclassified networks where it is at risk of being targeted by adversarial cyber espionage campaigns. In addition, DoD's technical information is subject to other loss mechanisms. Protecting DoD unclassified controlled technical information is a high priority for the Department, and is critical to preserving intellectual property, enhancing the competitive capabilities of our national industrial base, and maintaining DoD's technology advantage. This information, while unclassified, includes data and intellectual property concerning defense systems requirements, concepts of operations, technologies, designs, engineering, systems production, system maintenance /sustainment and component manufacturing. To maintain full confidence in our systems, the Department must also assess the effect the loss of this information has on our warfighting capabilities. DoD contractors who produce or access controlled technical information must incorporate security (e.g., implement cybersecurity standards on contractor information system networks, report cyber-intrusion incidents, manage deemed exports, and other mechanisms that result in the loss of this information) to protect this information from all loss mechanisms. These requirements are important, but insufficient in the face of a determined adversary. The Department must take steps to understand the impacts of losses, rethink how we safeguard our capabilities, and deter our strategic competitors.

This project supports protection of unclassified controlled technical information, and an analysis of losses, to determine consequences and appropriate requirements, acquisition, programmatic, and strategic courses of action to include deterring our strategic competitors and identifying opportunities to promote our innovation base.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
Title: Data Vulnerability Program ***Description:*** The Data Vulnerability Assessment and Analysis project will support efforts to maintain DoD's technology advantage. The data vulnerability program will invest in advancing analytic tool suite capabilities and build common data model for supply chain analytics. The Initial Operating Capability (IOC) of the technical solution should improve the capability to continuously monitor and assess the Defense Industrial Base and the National Security Innovation Base in order to detect and characterize threats and enable partners with relevant authorities to address these threats in a timely manner and collaborate on these efforts. The data vulnerability program will continue to support projects with stakeholders. ***FY 2020 Plans:*** In FY 2020, the program will fully incorporate changes from the FY 2017 NDAA Section 901 reorganization by adjusting to the new organizational structures within both the new USD(R&E) and USD(A&S). The program will continue to collect and integrate proactive protection efforts and conduct trend analysis of protection efforts for the Department's critical acquisition programs and	-	-	9.344

Exhibit R-2A, RDT&E Project Justification: PB 2020 Office of the Secretary Of Defense		Date: February 2019
Appropriation/Budget Activity 0400 / 6	**R-1 Program Element (Number/Name)** PE 0605797D8Z / *Maintaining Technology Advantage*	**Project (Number/Name)** 138 / *Data Vulnerability Assessment and Analysis*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
technologies and incorporate findings into protection processes and activities. The program will continue to advance analytic tool suite capabilities and build common data model. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** Funding was transferred from PE 0605798D8Z in FY 2020.			
Accomplishments/Planned Programs Subtotals	-	-	9.344

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

E. Performance Metrics

The Data Vulnerability Assessment and Analysis metric is the number of completed cases.

Exhibit R-2A, **RDT&E Project Justification:** PB 2020 Office of the Secretary Of Defense			**Date:** February 2019
Appropriation/Budget Activity 0400 / 6	**R-1 Program Element (Number/Name)** PE 0605797D8Z / *Maintaining Technology Advantage*	**Project (Number/Name)** 139 / *Joint Acquisition Protection Exploitation Cell (JAPEC)*	

COST ($ in Millions)	Prior Years	FY 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
139: *Joint Acquisition Protection Exploitation Cell (JAPEC)*	-	0.000	0.000	5.592	-	5.592	5.704	5.818	5.931	6.053	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

DoD established a joint analysis capability (Joint Acquisition Program and Exploitation Cell (JAPEC)) to conduct comprehensive assessments of controlled unclassified technical information losses, and engage acquisition and intelligence sources, to determine consequences and appropriate preventative/mitigation actions. The JAPEC requires the ability to detect and characterize past technology losses, conduct damage assessments of lost information, and provide various insights with predictive value. Together with supporting organizations, the JAPEC enables comprehensive, detailed assessments of U.S. military technological vulnerability, as well as inform the development and application of effective policies, countermeasures, and enforcement actions to preserve U.S. technical superiority in all warfighting domains.

JAPEC, and supporting organizations, require an analytic capability to synchronize, integrate, coordinate and inform DoD efforts in order protect the acquisition and investment in sensitive U.S. technologies from adversaries and better exploit opportunities to deter, deny and disrupt adversary activities.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
Title: Joint Acquisition Protection Exploitation Cell (JAPEC) ***Description:*** Integrate controlled unclassified information, to include Controlled Technical Information (CTI) protection efforts across DoD to proactively mitigate losses and exploit opportunities to deter, deny, and disrupt adversaries that may threaten U.S. military advantage. ***FY 2020 Plans:*** - Identify critical acquisition programs and technologies requiring elevated protection. - Identify threats and recommend advanced protection mechanisms within and across DoD programs/technologies. - Support assessment of vulnerabilities associated with known losses. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** Funding was transferred from PE 0605798D8Z in FY 2020.	-	-	5.592
Accomplishments/Planned Programs Subtotals	-	-	5.592

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

Exhibit R-2A, RDT&E Project Justification: PB 2020 Office of the Secretary Of Defense		**Date:** February 2019
Appropriation/Budget Activity 0400 / 6	**R-1 Program Element (Number/Name)** PE 0605797D8Z / *Maintaining Technology Advantage*	**Project (Number/Name)** 139 / *Joint Acquisition Protection Exploitation Cell (JAPEC)*

D. Acquisition Strategy

N/A

E. Performance Metrics

Programmatic performance will be assessed against the specific items listed in the Planned Program section.

Exhibit R-2A, RDT&E Project Justification: PB 2020 Office of the Secretary Of Defense		Date: February 2019
Appropriation/Budget Activity 0400 / 6	**R-1 Program Element (Number/Name)** PE 0605797D8Z / *Maintaining Technology Advantage*	**Project (Number/Name)** 158 / *Program and Technology Protection*

COST ($ in Millions)	Prior Years	FY 2018	FY 2019	FY 2020 Base	FY 2020 OCO	FY 2020 Total	FY 2021	FY 2022	FY 2023	FY 2024	Cost To Complete	Total Cost
158: *Program and Technology Protection*	-	0.000	0.000	5.000	-	5.000	5.000	5.000	5.000	5.000	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

The Department of Defense (DoD) must address cybersecurity and supply chain risks to DoD networks, weapons systems, and information stored and processed on both DoD and Defense Industrial Base (DIB) unclassified contractor information networks that support DoD programs. Increased reliance on the internet as a vehicle for sharing information, globalization of the supply chain, and advanced persistent threats (APTs) that can evade commercially available security tools and defeat generic security best practices, drives the need for diligent program protection planning and execution. Program Protection Planning includes protection of classified and unclassified controlled technical information, critical program information, critical components and critical mission functions, and integrates high level security policies and practical expertise to specific acquisition and S&T practices, systems engineering activities, and risk reduction activities. Through this initiative the Department is maturing system security engineering methodologies to protect controlled unclassified information, to include controlled technical information on contractor information networks; improve mitigation and management of supply chain risk management risks, improve integration of cybersecurity into the engineering processes, improve software assurance practices, mature processes to identify and protect Critical Program Information and improve program protection planning. Activities carried out, support implementation of DoD Instruction 5200.44 Trusted Systems and Networks with the use of proven mitigation techniques and tools, the ongoing refinement of risk management processes, and creation of needed technology; implementation of DoD Instruction 5200.39 Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E) to identify and protect Critical Program Information; and implementation of DoD Instruction 8582.01 Security of Unclassified DoD Information on Non-DoD Information Systems for Safeguarding Controlled Unclassified Information on contractor owned networks.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
Title: Program and Technology Protection ***Description:*** The project provides system security engineering policy, guidance and objective assessments to reduce risks in sharing and storing Controlled Technical Information, improve mitigation of supply chain risk management risks, improve integration of cybersecurity into the engineering processes, integrate defense exportability and anti-tamper practices, mature processes to identify Critical Program Information and improve program protection planning. Activities carried out support implementation of DoD Instruction 5200.44 Trusted Systems and Networks with the use of proven mitigation techniques and tools, the ongoing refinement of risk management processes; implementation of DoD Instruction 5200.39 Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E) to identify and protect Critical Program Information; and implementation of DoD Instruction 8582.01 Security of Unclassified DoD Information on Non-DoD Information Systems for Safeguarding Controlled Unclassified Information on contractor owned networks. ***FY 2020 Plans:***	-	-	5.000

Exhibit R-2A, RDT&E Project Justification: PB 2020 Office of the Secretary Of Defense		Date: February 2019
Appropriation/Budget Activity 0400 / 6	**R-1 Program Element (Number/Name)** PE 0605797D8Z / *Maintaining Technology Advantage*	**Project (Number/Name)** 158 / *Program and Technology Protection*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2018	FY 2019	FY 2020
Provide support to Independent Technical Review Assessment and Cyber Vulnerability Review Assessment teams in conduct of broad program protection planning activities to assess: - Conduct of criticality analyses to determine capability, systems and technology vulnerabilities. - Conduct of Critical Program Information analysis to determine capability, systems and technology anti-tamper protections. - Conduct Program Protection planning activities, and track progress to verify protection of capability, systems and technologies. • Advance the state of the practice of systems security engineering: - Continue development of methodology to identify and mitigate system security risk, to include cybersecurity and supply chain risk. - Continue to develop courseware, refine guidance, provide training, and outreach with government and industry. - Refine guidance, tools and mitigation approaches to mitigate capability, system and technology risks. • Safeguard Controlled Unclassified Information, including Controlled Technical Information: - Refine implementation and guidance of marking and dissemination of distribution of technical information. - Refine safeguarding information protection methods for contractor unclassified information networks. • Safeguard Critical Program Information: - Refine implementation, guidance and tools to identify Critical Program Information. - Develop and refine Anti-Tamper protections methods to safeguard Critical Program Information. • Defense exportability features integration: - Mature processes, methods and guidance for defense exportability features integration. - Develop and refine defense exportability protection methods to improve planning for the exportability of U.S. Defense systems. ***FY 2019 to FY 2020 Increase/Decrease Statement:*** This effort was transferred from PE 0605142D8Z in FY 2020.			
Accomplishments/Planned Programs Subtotals	-	-	5.000

C. Other Program Funding Summary ($ in Millions)

N/A

Remarks

D. Acquisition Strategy

N/A

E. Performance Metrics

The program protection project supports activities focused on: (1) improve system security engineering to reduce risks in sharing and storing controlled unclassified information, to include controlled technical information, (2) improve mitigation to supply chain risks, (3) support cyber vulnerability review assessments, to include review

Exhibit R-2A, RDT&E Project Justification: PB 2020 Office of the Secretary Of Defense		**Date:** February 2019
Appropriation/Budget Activity 0400 / 6	**R-1 Program Element (Number/Name)** PE 0605797D8Z / *Maintaining Technology Advantage*	**Project (Number/Name)** 158 / *Program and Technology Protection*

of Program Protection Plans and formal independent technical reviews , (4) mature system security engineering policy and guidance, and (5) mature processes to identify and protect critical program information, controlled unclassified information, critical components and mission functions.

Impact of the program protection initiative is assessed based upon number of supported cyber vulnerability assessments, formal independent technical review assessments, critical programs and technology capabilities cyber vulnerability assessments , and through engagement supporting research, development, acquisition, counterintelligence, intelligence and cybersecurity policy initiatives related to program protection.