Exhibit R-2, RDT&E Budget Item Justification: PB 2021 Office of the Secretary Of Defense	Date: February 2020
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide* / BA 2: *Applied Research*	**R-1 Program Element (Number/Name)** PE 0602751D8Z / *Software Engineering Institute (SEI) Applied Research*

COST ($ in Millions)	Prior Years	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
Total Program Element	8.614	8.942	9.580	9.573	-	9.573	9.712	9.749	10.001	10.204	Continuing	Continuing
278: *Software Engineering Institute (SEI) Applied Research*	8.614	7.942	8.580	8.573	-	8.573	8.712	8.749	9.001	9.204	Continuing	Continuing
817: *Cyber Security, Applied Research*	0.000	1.000	1.000	1.000	-	1.000	1.000	1.000	1.000	1.000	Continuing	Continuing

Note

The Software Engineering Institute (SEI) Applied Research Program Element (PE) develops and evaluates the feasibility and practicality of software and computer science concepts at the applied research level, with the potential to improve future DoD systems through research, development, and application in the SEI Advanced Technology Development Program Element (PE) 0603781D8Z. Promising projects proceed into advanced technology development through this PE.

A. Mission Description and Budget Item Justification

The Software Engineering Institute (SEI) Federally Funded Research and Development Center (FFRDC) was established in 1984 as an integral part of the DoD's initiative to identify, evaluate, and transition software engineering technologies and practices. The mission of the SEI is to provide the DoD with technical leadership and innovation through research and development to advance the practice of software engineering and technology. The SEI works across government, industry, and academia to improve the state of software engineering from the technical, acquisition, and management perspectives. The SEI engages in research and development of critical software technologies and tools and collaborates with the larger software engineering research community. It facilitates rapid transition of software engineering technologies into practice and evaluates emerging software engineering technologies to determine their potential for improving software-intensive DoD systems. Since its inception, the SEI has helped to transform the fields of software engineering and acquisition, network security, real-time systems, software architectures, and software-engineering process management.

Software is critical to meeting the Department of Defense's (DoD) increasing demand for national defense systems that are high-quality, affordable, and deployed in a timely way. With growing global parity in software engineering, the DoD must maintain leadership in all aspects of software-based system development, operation, defense, and evolution to avoid strategic surprise. To assist the DoD in retaining a long-term differential advantage over potential adversaries, the Software Engineering Institute (SEI) Applied Research program element (PE) develops and evaluates the feasibility and practicality of software and computer science concepts, with the potential to improve future DoD systems. The research conducted by this PE directly benefits the technical domains Autonomous Systems and Artificial Intelligence (AI), Cyber, and Engineered Resilient Systems.

Exhibit R-2, RDT&E Budget Item Justification: PB 2021 Office of the Secretary Of Defense	Date: February 2020
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide I* BA 2: *Applied Research*	**R-1 Program Element (Number/Name)** PE 0602751D8Z *I Software Engineering Institute (SEI) Applied Research*

B. Program Change Summary ($ in Millions)	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total
Previous President's Budget	9.279	9.580	9.662	-	9.662
Current President's Budget	8.942	9.580	9.573	-	9.573
Total Adjustments	-0.337	0.000	-0.089	-	-0.089
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-0.335	-			
• Other Adjustments	-0.002	-	-0.080	-	-0.080
• Economic Assumption	-	-	-0.009	-	-0.009

Exhibit R-2A, RDT&E Project Justification: PB 2021 Office of the Secretary Of Defense			Date: February 2020
Appropriation/Budget Activity 0400 / 2	R-1 Program Element (Number/Name) PE 0602751D8Z / *Software Engineering Institute (SEI) Applied Research*	Project (Number/Name) 278 / *Software Engineering Institute (SEI) Applied Research*	

COST ($ in Millions)	Prior Years	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
278: *Software Engineering Institute (SEI) Applied Research*	8.614	7.942	8.580	8.573	-	8.573	8.712	8.749	9.001	9.204	Continuing	Continuing

A. Mission Description and Budget Item Justification

Work conducted under this PE will enable resilient mission assurance in heterogeneous and contested environments through the verification and validation of system performance and architecture. The program will also assist the DoD in retaining a long-term advantage in the areas of software-intensive systems and cyber security by enhancing assurance, exploiting automation and AI, and understanding human-computer interaction.

The SEI Applied Research PE has two main research thrusts with known military applications: (1) Software Engineering, Systems Verification and Validation, and Mission Assurance (formerly Mission Assurance); and (2) Information Assurance. This area is increasingly being applied to AI and autonomous systems.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2019	FY 2020	FY 2021
Title: SEI Applied Research in the Area of Software Engineering, Systems Verification and Validation, and Mission Assurance (formerly Mission Assurance)	5.765	6.006	6.023
Description: Increasingly complex and AI-enabled systems will require a commensurate increase in sophistication of verification and validation mechanisms. This thrust seeks to develop verification techniques for requirements identification, systems of systems architectures, and virtual integration of components. Additionally, research in this area will enable requirements verification for software assurance, analysis and control of unverified code, and automated repair of damaged code. Software production and code analysis methods developed through this program will also improve the accuracy of behavior prediction of complex software, including AI-enabled systems, in untested environments.			
FY 2020 Plans: • Create tools to automatically assure untrusted external software components to enable rapid software composition for DoD systems. • Develop AI engineering techniques to train AI systems with expected security properties requiring two to three orders of magnitude less computation and verified security properties under known attacks. • Develop algorithms and approaches to automate code changes that enable developers to quickly and confidently restructure software, including harvesting code for reuse and the ability to replace large-scale software components.			
FY 2021 Plans:			

Exhibit R-2A, RDT&E Project Justification: PB 2021 Office of the Secretary Of Defense		Date: February 2020
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602751D8Z / *Software Engineering Institute (SEI) Applied Research*	**Project (Number/Name)** 278 / *Software Engineering Institute (SEI) Applied Research*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2019	FY 2020	FY 2021
• Develop automated design conformance checkers, as part of a continuous integration toolchain, to correctly identify significant design non-conformance in order to advance DoD capabilities to rapidly compose software systems, including secure AI/ML systems. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** Level of effort is consistent from FY 2020 to FY 2021. Small changes reflect minor budget fluctuations.			
Title: SEI Applied Research in the areas of Information Assurance (IA) ***Description:*** To gain full advantage from data and information generated by software for use in missions, DoD needs to assure its software is free of vulnerabilities. In its complex systems, DoD may use software developed from an unknown supply chain that may include intentionally or unintentionally introduced vulnerabilities. This thrust seeks to develop scalable automated methods to locate, understand, and mitigate the effects of these vulnerabilities. Automated solutions developed through this thrust will be used to discover vulnerabilities in system software source code and to generate proofs of correctness or fault. Additionally, they will be used to model and simulate operational environments to support software and cyber tactics, techniques, and procedures testing. ***FY 2020 Plans:*** • Devise practical formal methods which can be utilized to produce trustworthy and assured software on more complex systems and the emerging technologies of interest to the DoD. • Develop compositional verification techniques to allow the use of multiple enforced components. This enables the use of unverified commodity software components containing non-secure behavior with verified enforcers. ***FY 2021 Plans:*** • Advance compositional verification techniques to allow the use of unverified commodity software components in DoD systems, including secure and robust AI/ML systems. • Use machine learning and semantic analysis of data generated during Continuous Integration/Continuous Delivery to reduce the number of alerts requiring human adjudication during the deployment of multiple situational awareness tools and increase the security of software without slowing the development process. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** Level of effort is consistent from FY 2020 to FY 2021. Small changes reflect minor budget fluctuations.	2.177	2.574	2.550
Accomplishments/Planned Programs Subtotals	7.942	8.580	8.573

Exhibit R-2A, RDT&E Project Justification: PB 2021 Office of the Secretary Of Defense		Date: February 2020
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602751D8Z / *Software Engineering Institute (SEI) Applied Research*	**Project (Number/Name)** 278 / *Software Engineering Institute (SEI) Applied Research*

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
• BA 3, PE# 0603781D8Z: *Software Engineering Institute (SEI)*	15.016	15.111	12.598	-	12.598	12.825	13.090	13.491	13.816	Continuing	Continuing

Remarks

The SEI Applied Research PE represents a pivot toward more fundamental research that enables the DoD to address longer-term challenges in software technology and engineering. The SEI Applied Research PE bolsters the organic research at the SEI Federally Funded Research and Development Center (FFRDC), enables stronger collaborations between the SEI FFRDC and academia, attracts top researchers to the SEI, and gives the DoD access to top experts in information science, which generally enhances the DoD's ability to benefit from the military applications of research in software and computer science.

D. Acquisition Strategy

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2021 Office of the Secretary Of Defense			Date: February 2020
Appropriation/Budget Activity 0400 / 2	R-1 Program Element (Number/Name) PE 0602751D8Z / *Software Engineering Institute (SEI) Applied Research*	Project (Number/Name) 817 / *Cyber Security, Applied Research*	

COST ($ in Millions)	Prior Years	FY 2019	FY 2020	FY 2021 Base	FY 2021 OCO	FY 2021 Total	FY 2022	FY 2023	FY 2024	FY 2025	Cost To Complete	Total Cost
817: *Cyber Security, Applied Research*	0.000	1.000	1.000	1.000	-	1.000	1.000	1.000	1.000	1.000	Continuing	Continuing

A. Mission Description and Budget Item Justification

Work conducted under this project will enable resilient mission assurance in heterogeneous and contested environments through the verification and validation of system performance and architecture. The program will also assist the DoD in retaining a long-term advantage in the area of cybersecurity by enhancing assurance, exploiting automation, and understanding human-computer interaction.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2019	FY 2020	FY 2021
Title: Cyber Security	1.000	1.000	1.000
Description: Warfighting in the cyber domain often operates at sub-second timescales and across multiple domains of authority. Methods used to accomplish many tasks (e.g., malware analysis, coordinating multiple agents) demand large amounts of time, attention, and special skills and are not scalable. This thrust seeks to develop and increase the use of automation to simplify the completion of these tasks. Example activities include automation of moving target defenses, code artifact reverse engineering, analysis of network flows at enterprise scale, assessing the operating boundaries for Artificial Intelligence (AI) and Machine Learning (ML) algorithms, and development and assessment of workforce skills. ***FY 2020 Plans:*** • Develop means to assure and verify trustworthiness of AI/ML systems via new techniques to continuously assess the operating boundaries for AI/ML algorithms. ***FY 2021 Plans:*** • Develop techniques to evaluate the effectiveness of proposed system defenses against code reuse attacks on multiple architectures and platforms of interest to the DoD including AI/ML systems. • Apply and advance new techniques to continuously assess the operating boundaries for AI/ML algorithms to assure and verify trustworthiness. ***FY 2020 to FY 2021 Increase/Decrease Statement:*** There is no change in the Cyber investment between FY 2020 and FY 2021.			
Accomplishments/Planned Programs Subtotals	1.000	1.000	1.000

C. Other Program Funding Summary ($ in Millions)

N/A

Exhibit R-2A, RDT&E Project Justification: PB 2021 Office of the Secretary Of Defense		Date: February 2020
Appropriation/Budget Activity 0400 / 2	**R-1 Program Element (Number/Name)** PE 0602751D8Z / *Software Engineering Institute (SEI) Applied Research*	**Project (Number/Name)** 817 / *Cyber Security, Applied Research*

C. Other Program Funding Summary ($ in Millions)

Remarks

D. Acquisition Strategy

N/A