Exhibit R-2, RDT&E Budget Item Justification: FY 2018 Office of the Secretary Of Defense											Date: May 2017	

| Appropriation/Budget Activity
0400: *Research, Development, Test & Evaluation, Defense-Wide I* BA 5:
System Development & Demonstration (SDD) | | | | | R-1 Program Element (Number/Name)
PE 0605140D8Z I *Trusted Foundry* | | | | | | | |

COST ($ in Millions)	Prior Years	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
Total Program Element	0.000	7.000	69.000	0.000	-	0.000	0.000	0.000	0.000	0.000	Continuing	Continuing
P837: *Trusted Mask Trust Approach*	0.000	0.000	2.000	0.000	-	0.000	0.000	0.000	0.000	0.000	Continuing	Continuing
P838: *V&V Capabilities and Standards for Trust*	0.000	3.000	19.200	0.000	-	0.000	0.000	0.000	0.000	0.000	Continuing	Continuing
P839: *New Trust Approach*	0.000	4.000	47.800	0.000	-	0.000	0.000	0.000	0.000	0.000	Continuing	Continuing

Note

Beginning in FY 2018, funds from this Program Element (PE) will be transferred to a new Budget Activity (BA) 5 PE 0605294D8Z and BA 4 0604294D8Z to allow more efficient execution of the development and prototyping activities within the body of work.

A. Mission Description and Budget Item Justification

This PE supports activities to ensure critical and sensitive integrated circuits are available to meet the DoD's needs. It refines strategies and management planning activities that will (1) provide support to acquisition programs to address trusted microelectronics supply needs; (2) improve capability to evaluate and validate trust of microelectronic parts and advance standards to incentivize the commercial marketplace to recognize trust as a competitive design standard; and (3) develop and demonstrate alternative approaches to assuring the trust of the microelectronics supply chain in order to enable broader DoD access to commercial state-of-the-art (SOTA) microelectronics technology.

This activity will be coordinated by the Office of the Assistant Secretary of Defense for Research and Engineering, and will include performers from the DoD Components, the Defense Microelectronics Activity (DMEA), the Joint Federated Assurance Center (JFAC), the Defense Advanced Research Programs Agency (DARPA), other DoD and Intelligence Community science and technology (S&T) organizations and laboratories, defense industry, and the broader commercial industrial base. It will integrate the functions of the DoD Trusted Foundry Program, the Trusted Supplier accreditation program, JFAC, and related S&T activities.

This activity implements, maintains and updates the DoD's long-term microelectronics strategy. Recognizing that trusted and assured supply of microelectronics is a Government-wide concern, this activity will interface with interagency partners to take into account interagency requirements, opportunities for collaboration, and strategic decisions that can be made to limit the overall cost of these requirements to the government.

Exhibit R-2, RDT&E Budget Item Justification: FY 2018 Office of the Secretary Of Defense				Date: May 2017	
Appropriation/Budget Activity 0400: *Research, Development, Test & Evaluation, Defense-Wide I* BA 5: *System Development & Demonstration (SDD)*			**R-1 Program Element (Number/Name)** PE 0605140D8Z *I Trusted Foundry*		
B. Program Change Summary ($ in Millions)	**FY 2016**	**FY 2017**	**FY 2018 Base**	**FY 2018 OCO**	**FY 2018 Total**
Previous President's Budget	0.000	69.000	91.300	-	91.300
Current President's Budget	7.000	69.000	0.000	-	0.000
Total Adjustments	7.000	0.000	-91.300	-	-91.300
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	7.000	-			
• SBIR/STTR Transfer	-	-			
• Funds transfer to BA4 PE 0604294D8Z	-	-	-84.200	-	-84.200
• Funds transfer to BA5 PE 0605294D8Z	-	-	-5.251	-	-5.251
• Other	-	-	-1.235	-	-1.235
• DTIC Offset	-	-	-0.614	-	-0.614

Change Summary Explanation

FY 16 add is to support the initiation of Trusted Foundry activities. FY 2018 funds transferred to PE 0604294D8Z in BA 4 for development and prototyping activities and PE 0605294D8Z in BA 5 for demonstration activities.

Exhibit R-2A, RDT&E Project Justification: FY 2018 Office of the Secretary Of Defense										Date: May 2017	

Appropriation/Budget Activity 0400 *I* 5				R-1 Program Element (Number/Name) PE 0605140D8Z *I Trusted Foundry*						Project (Number/Name) P837 *I Trusted Mask Trust Approach*	

COST ($ in Millions)	Prior Years	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
P837: *Trusted Mask Trust Approach*	0.000	0.000	2.000	0.000	-	0.000	0.000	0.000	0.000	0.000	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

This project staffs and supports operation of a new secure (SECRET-level) photomask manufacturing capability down to 14 nanometers (nm) at an existing SOTA commercial photomask manufacturing supplier to secure the masks and design intellectual property (IP) of acquisition programs when using commercial microelectronic fabrication facilities other than the Trusted Foundry. This capability can be used in conjunction with one or more leading-edge commercial foundries. This capability will address trusted masks at technology node sizes < 130nm.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2016	FY 2017	FY 2018
Title: Trusted Mask Trust Approach	-	2.000	-
FY 2017 Plans: Starting in FY 2017, DMEA will conduct management and technical support, as required, to procure secure mask data parsing services for the Department, as well as other Federal entities, by upgrading an existing SOTA commercial photomask manufacturing supplier with a Trusted photomask capability to ensure the integrity of the tape-in/mask release, mask manufacturing, and authentication process for photomasks. Over the FYDP, a SOTA commercial photomask manufacturing supplier will be equipped with a new secure (SECRET-level) photomask manufacturing capability ($7.2M is planned as a FY 2017 Defense Production Act (DPA) Title III project) and staffed to provide the required critical Trusted photomask capabilities.			
Accomplishments/Planned Programs Subtotals	-	2.000	-

C. Other Program Funding Summary ($ in Millions)
N/A
Remarks

D. Acquisition Strategy
N/A

E. Performance Metrics
Performance for this project is monitored in the following ways:

 - Number of photomasks created using the secure photomask manufacturing capability.
 - Number of acquisition programs using the secure photomask manufacturing capability.

Exhibit R-2A, **RDT&E Project Justification:** FY 2018 Office of the Secretary Of Defense		**Date:** May 2017
Appropriation/Budget Activity 0400 *I* 5	**R-1 Program Element (Number/Name)** PE 0605140D8Z *I Trusted Foundry*	**Project (Number/Name)** P837 *I Trusted Mask Trust Approach*
- Number of technology node sizes supported by the secure photomask manufacturing capability. - Number of foundries supported by the secure photomask manufacturing capability.		

Exhibit R-2A, RDT&E Project Justification: FY 2018 Office of the Secretary Of Defense											Date: May 2017	
Appropriation/Budget Activity 0400 I 5				**R-1 Program Element (Number/Name)** PE 0605140D8Z I *Trusted Foundry*					**Project (Number/Name)** P838 I *V&V Capabilities and Standards for Trust*			

COST ($ in Millions)	Prior Years	FY 2016	FY 2017	FY 2018 Base	FY 2018 OCO	FY 2018 Total	FY 2019	FY 2020	FY 2021	FY 2022	Cost To Complete	Total Cost
P838: *V&V Capabilities and Standards for Trust*	0.000	3.000	19.200	0.000	-	0.000	0.000	0.000	0.000	0.000	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

This project improves microelectronics test and verification methodologies in support of assuring commercial parts and develops standards/practices to foster commercial development of secure, trusted, and assured parts. Verification and test technologies are required to provide direct program support for microelectronics assurance verification when DoD Trusted Foundry Program options are not available. Core technical laboratories have recently been chartered as a Joint Federated Assurance Center (JFAC) to provide this support. Out-year demands will require an increase in capacity, which will take the form of additional personnel and/or equipment to permit scaling of microelectronics assessment capabilities. Challenges have been identified, to include the ability to analyze leading-edge technologies, throughput/time required for analysis, ability to analyze third-party IP contained in microelectronic components, and analysis of non-application-specific integrated circuit (ASIC) components that are increasingly being used for agility, e.g., Field-Programmable Gate Arrays (FPGAs). This project addresses these gaps in current technical capabilities in a collaborative nature amongst the core technical laboratories, driven by projected and realized out-year demand. Three capability areas core to microelectronics analysis and verification will be improved:

• Physical verification, i.e., destructive analysis of integrated circuits and printed circuit boards
• Functional analysis, i.e., non-destructive screening/verification of select, critical parts
• Design verification, i.e., verification/assurance of designs, IP, netlists, bitstreams, firmware, etc.

These improvements will address two primary attributes: (1) technical capability including laboratory equipment, analysis tools, such as imaging software, and highly skilled tradecraft, and (2) the capacity to perform microelectronics assessments.

This project also develops standards and practices in support of trustworthy designs and supply chains and formal relationships with industry to foster commercial development of secure, trusted, and assured parts and for acquisition of government access to proprietary designs, software, development, and quality assurance processes and test procedures to develop practices that minimize security flaws in designs and facilitate verification. Two capability areas that are core to improved commercial designs will be improved, i.e., trustworthy designs and supply chains.

Beginning in FY 2018, funding for this project has been transferred to BA 4 PE 0604294D8Z to accurately reflect execution of funds in support of the mission.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2016	FY 2017	FY 2018
Title: Verification and Validation (V&V) Capabilities and Standards for Trust	3.000	19.200	-
FY 2016 Accomplishments:			

Exhibit R-2A, **RDT&E Project Justification:** FY 2018 Office of the Secretary Of Defense		**Date:** May 2017
Appropriation/Budget Activity 0400 *I* 5	**R-1 Program Element (Number/Name)** PE 0605140D8Z *I Trusted Foundry*	**Project (Number/Name)** P838 *I V&V Capabilities and Standards for Trust*

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2016**	**FY 2017**	**FY 2018**
Planned for funding of a dedicated technical government subject matter experts (SME) at JFAC laboratories within the Air Force, Army, Navy, and National Security Agency, starting in FY 2017 and provided support for identified JFAC acquisition program pilots and non-program-related assessments, e.g., suspicious parts acquired by law enforcement or that failed in the field. In addition, utilizing the 2015 JFAC hardware assurance capability survey, developed a plan of action based on incremental technical improvement and capacity across participating JFAC laboratories in the following areas: • Equipment re-capitalization and new equipment • Data and imaging processing • Enhanced automation • Technology and IP licensing • Training and SME development • Maintenance support • Feasibility studies • Reimbursable (test fixtures, boards, parts, and supplies) • Direct program support in related areas beyond the acquisition programs' technical capability or capacity to address ***FY 2017 Plans:*** The JFAC is: (1) improving its microelectronics test and verification methodologies in support of verifying trust and assurance of parts and (2) developing standards/practices to foster commercial development of secure, trusted and assured parts. Verification and test technologies. Initiating: • Improvements to the core JFAC's (1) technical capability, i.e., laboratory equipment, IP, analysis tools, such as imaging software, and highly skilled tradecraft, and (2) the capacity to perform microelectronics assessments. Out-year demands will continue to require an increase in capacity, which will take the form of additional personnel and/or equipment to permit scaling of assessment capabilities. • Enhancement of automation needed to increase the throughput of information produced by individual JFAC laboratory tools as well as to facilitate information sharing across the families of tools used for analysis and testing. • Development of common SME training and protocols based on the existing tool base, to include both commercial and government-developed tools. • Funding for additional SMEs per core JFAC laboratory in support of the microelectronics trust verification and other JFAC-related work. • Cost sharing of direct program support prioritized for FY 2017 focused on addressing technical gaps and trust-related findings. • Investment in the above technical areas based on priority and monitor and report increased technical capability from the baseline 2016 level.			

Exhibit R-2A, **RDT&E Project Justification:** FY 2018 Office of the Secretary Of Defense		**Date:** May 2017
Appropriation/Budget Activity 0400 *I* 5	**R-1 Program Element (Number/Name)** PE 0605140D8Z *I Trusted Foundry*	**Project (Number/Name)** P838 *I V&V Capabilities and Standards for Trust*

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2016**	**FY 2017**	**FY 2018**
Standards and Practices. Initiating the: • Development of standards and best practices, and relationships with industry, to foster commercial development of secure and trusted parts. • Establishment of formal relationships with FPGA vendors and other key commercial suppliers to improve device and IP security. • Acquisition of government access to proprietary designs, software, development, and quality assurance processes and test procedures to develop design practices that minimize security flaws and facilitate verification. • Establishment of government and industry working groups to develop test procedures to validate the trust of designs. • Documentation and promulgation of security-enhancing design practices across government, industry, and academia. • Development of industry-wide standards and practices to establish a common understanding of what constitutes verified and trusted hardware/software/firmware at both the component and systems level. • Development of a common lexicon for secure hardware/software/firmware in collaboration with the Committee for National Security Systems, National Institute of Standards and Technology, and the broader United States Government, industry, and academia. • Definition of supply chain controls for assured chain of custody for critical and other microelectronics devices and IP. • Development of security training and educate government and industry system security engineers and material managers on supply chain and life-cycle management best practices using agreed-upon language, standards, and practices. • Alignment of DoD Instruction 5200.44 (Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)), related policies, and NIST 800-161 (Supply Chain Risk Management Practices for Federal Information Systems and Organizations) with industry standards identifying and addressing gaps in definition and criteria and establishing accepted levels of supplier and part trustworthiness.			
Accomplishments/Planned Programs Subtotals	3.000	19.200	-

C. Other Program Funding Summary ($ in Millions)
 N/A
Remarks

D. Acquisition Strategy
 N/A

E. Performance Metrics
 Performance for this project is monitored in the following ways:

Exhibit R-2A, **RDT&E Project Justification:** FY 2018 Office of the Secretary Of Defense		**Date:** May 2017
Appropriation/Budget Activity 0400 *I* 5	**R-1 Program Element (Number/Name)** PE 0605140D8Z *I Trusted Foundry*	**Project (Number/Name)** P838 *I V&V Capabilities and Standards for Trust*

- Increases in throughput in current JFAC laboratories, and stands-up of additional capability/capacity as required, so that at least two laboratories will have capability in physical verification, functional analysis, and design verification to increase the DoD's overall microelectronics trust verification and test capacity for analysis of state-of-the practice parts.
- Increased Probability of Detection of malicious insertion and/or counterfeit parts.
- Cost to evaluate components.
- Time to evaluate components.

Exhibit R-2A, **RDT&E Project Justification:** FY 2018 Office of the Secretary Of Defense										**Date:** May 2017	
Appropriation/Budget Activity 0400 *I* 5				**R-1 Program Element (Number/Name)** PE 0605140D8Z *I Trusted Foundry*						**Project (Number/Name)** P839 *I New Trust Approach*	
COST ($ in Millions)	**Prior Years**	**FY 2016**	**FY 2017**	**FY 2018 Base**	**FY 2018 OCO**	**FY 2018 Total**	**FY 2019**	**FY 2020**	**FY 2021**	**FY 2022**	**Cost To Complete**	**Total Cost**
P839: *New Trust Approach*	0.000	4.000	47.800	0.000	-	0.000	0.000	0.000	0.000	0.000	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

A. Mission Description and Budget Item Justification

This project funds a program of research to develop, and demonstrate the next generation, technology-driven approach to microelectronics trust and assurance, to include SOTA microelectronics, to ensure continued access to leading-edge microelectronic technologies while maintaining the required level of trust in all environments. DoD's ability to access commercial technology for its custom trusted and assured needs is diminishing as leading-edge suppliers become fewer and more focused on serving the global commercial market. DoD's technology needs are broad, and relying on a single source supplier is not feasible. Alternative, advanced manufacturing methods, technologies, and design tools are needed to produce trusted and assured SOTA parts from untrusted sources and to preserve access to these advanced nodes while protecting DoD and Defense Industrial Base IP from exploitation. It also is intended to dramatically improve the capabilities of the JFAC with regard to verification and validation of microelectronics trust and assurance.

This program of research will demonstrate innovative design, manufacturing, imaging, tagging, and control and assessment approaches for protecting DoD's microelectronics supply chain and intellectual property (IP), including alternatives for trusted, strategic radiation-hardened electronics in advanced technology nodes for next-generation strategic systems, obfuscation and disaggregation technology development, and other assurance mitigations. It develops advanced imaging technologies and forensics, Design for Trust techniques, active hardware trust control, electronic component markers, and a data and analysis capability to enable auditing and independent verification and validation of commercial designs. It also demonstrates, and implements concepts for the cost-effective production of custom microelectronics in low volumes and protection of sensitive IP from exploitation.

Technologies that provide trust and assurance in a broad range of trusted and un-trusted environments can mitigate the risks associated with sole-source suppliers, and increase the Government's ability to leverage commercial capabilities. The suite of demonstrated technologies, e.g., alternative manufacturing methods and design tools, would enable DoD to obfuscate the purpose of sensitive devices, verify their origin and function, and protect sensitive IP from exploitation even while using the global supply chain for most hardware. In cases where the risk involved precludes that level of commercial collaboration, low-volume manufacturing technologies demonstrated under this project would permit DoD to more cheaply produce low volumes of sensitive microelectronics in trusted environments. The project would also support using a repository of third-party IP to expedite circuit design and transition promising technologies to use.

Beginning in FY 2018, funding for this project has been transferred to BA 4 PE 0604294D8Z and BA 5 PE 0605294D8Z.

B. Accomplishments/Planned Programs ($ in Millions)

	FY 2016	**FY 2017**	**FY 2018**
Title: New Trust Approach	4.000	47.800	-
FY 2016 Accomplishments: Conducted a study and coordinated with DARPA for a Broad Agency Announcement (BAA) to fully develop and initiate the program of research. IDA was contracted and coordinated NDIA and industry engagement around new trust approaches and			

Exhibit R-2A, **RDT&E Project Justification:** FY 2018 Office of the Secretary Of Defense		**Date:** May 2017
Appropriation/Budget Activity 0400 **/** 5	**R-1 Program Element (Number/Name)** PE 0605140D8Z **/** *Trusted Foundry*	**Project (Number/Name)** P839 **/** *New Trust Approach*

B. Accomplishments/Planned Programs ($ in Millions)	**FY 2016**	**FY 2017**	**FY 2018**
FPGA Assurance resulting in two workshops and summary reports. In addition, FY 2017 acquisition program pilots and/or technology demonstrations of mature trust technologies and techniques were identified and planned for with DARPA and other programs. ***FY 2017 Plans:*** Initiate the conduct of identified acquisition program pilots and technology demonstrations in accordance with the FY 2016 and FY2017 plans and coordinate research programs across sponsored BAAs, government R&D organizations, academia and industry. FY17 and FY18 primary activities include demonstration of these technologies being developed in PE 0604294D8Z, followed by transition of these capabilities to new programs in the following fiscal years. Assess and report technical progress against the FY 2016 and FY 2017 plan. Engage early on with potential stakeholders to identify potential transition issues and aid in transition through joint collaboration between research teams and stakeholders with a focus on evaluations of prototypes, test articles and beta versions of tools, IP, techniques, methods, etc. and their use in operationally-realistic scenarios.			
Accomplishments/Planned Programs Subtotals	4.000	47.800	-

C. Other Program Funding Summary ($ in Millions)
 N/A
Remarks

D. Acquisition Strategy
 N/A

E. Performance Metrics
 Performance for this project is monitored in the following ways:
 - Effectiveness of developed technologies, as measured by:
 o The speed and reliability of new validation and verification techniques in identifying known microelectronics issues (e.g. tampering) in laboratory and non-laboratory situations;
 o Successful testing of advanced, alternative manufacturing techniques such as disaggregated manufacturing; and
 o Resilience of microelectronics protected by new trust approach technologies in red teaming exercises.
 - Adoption of next-generation trust technologies, as measured by:
 o The number of DoD and other Government programs employing these trust technologies, design approaches, or best practices, possibly as facilitated by the provision of use models;

Exhibit R-2A, **RDT&E Project Justification:** FY 2018 Office of the Secretary Of Defense		**Date:** May 2017
Appropriation/Budget Activity 0400 *I* 5	**R-1 Program Element (Number/Name)** PE 0605140D8Z *I Trusted Foundry*	**Project (Number/Name)** P839 *I New Trust Approach*

o The volume and criticality of components employing these technologies, design approaches, or best practices; and
o Promulgation in DoD guidance and program protection plans.