

CUI

INSPECTOR GENERAL

U.S. Department of Defense

MAY 2, 2022



(U) Evaluation of the Department of Defense's Transition From a Trusted Foundry Model to a Quantifiable Assurance Method for Procuring Custom Microelectronics

Controlled by: DoD OIG
Controlled by: Evaluations Component
CUI Category: OPSEC
Distribution/Dissemination Control: FEDCON
POC: [REDACTED]

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE

CUI





CUI

(U) Results in Brief

(U) Evaluation of the Department of Defense's Transition From a Trusted Foundry Model to a Quantifiable Assurance Method for Procuring Custom Microelectronics

May 2, 2022

(U) Objective

(U) We determined the extent to which the DoD has made the preparations necessary to transition from a trusted foundry model for procuring custom microelectronics to a quantifiable assurance method for procuring custom microelectronics from the commercial market.

(U) Background

(U) Microelectronics refers to the design and manufacturing of extremely small electronic components, often in the form of microchips and microcircuits. A foundry is a microchip fabrication facility. Microelectronics are one of the DoD's top technology modernization priorities.

(U) Section 224 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2020 requires the DoD to establish trusted supply chain and operational security standards for the purchase of microelectronics products by January 1, 2021. Section 224 also requires microelectronics products or services that the DoD purchases on or after January 1, 2023, to meet those standards. Quantifiable assurance is the DoD's method to achieve these requirements for custom, state-of-the-art microelectronics.

(U) In May 2020, the Director of Defense Research and Engineering for Modernization within the Office of the Under Secretary of Defense for Research and Engineering (OUSD[R&E]) stated that the current method for acquiring custom microelectronics

(U) Background (cont'd)

(U) from a trusted supplier (trusted foundry) had failed. The Director further stated that to access state-of-the-art microelectronics, the DoD decided to move to a quantifiable assurance method that can leverage commercial industry while maintaining hardware security.

(U) Quantifiable assurance is a method being developed to measurably protect the integrity and confidentiality of custom state-of-the-art microelectronic components. The quantifiable assurance method consists of:

- (U) a quantitative risk analysis of potential threats;
- (U) a quantitative risk plan to implement mitigations, and a program justification for residual risks; and
- (U) an evaluation of the quantitative risk analysis and the quantitative risk plan for completeness and correctness.

(U) Finding

(U) The OUSD(R&E) developed plans to transition from a trusted foundry model to a quantifiable assurance method for procuring custom state-of-the-art microelectronics from the commercial market. However, the OUSD(R&E) is behind schedule for establishing trusted supply chain and operational security standards by the January 1, 2021, deadline, as required by the NDAA for FY 2020.

(U) Specifically, programs and policies already established included:

- (U) a Joint Federated Assurance Center (JFAC) Charter and Concept of Operations (CONOPS),
- (U) a JFAC Coordination Center and ticketing portal to route requests for assistance from the program offices,
- (U) a program to fund the JFAC's work, and
- (U) JFAC laboratories designated to support implementation of the quantifiable assurance method.

CUI



CUI

(U) Results in Brief

(U) Evaluation of the Department of Defense's Transition From a Trusted Foundry Model to a Quantifiable Assurance Method for Procuring Custom Microelectronics

(U) Finding (cont'd)

(U) However, the JFAC Charter and CONOPS predate the creation of the OUSD(R&E) and the OUSD(R&E)'s Principal Director for Microelectronics. The JFAC CONOPS does not provide the Principal Director for Microelectronics with authorities to resolve competing priorities between the program offices requesting JFAC support and insufficient capacity among the JFAC service providers.

(U) In addition, the OUSD(R&E) intended to designate the Naval Surface Warfare Center-Crane Division and the National Security Agency (NSA) as the two co-leads for establishing the quantifiable assurance method. The Naval Surface Warfare Center-Crane Division is managing several prototype projects that test quantifiable assurance procedures. The NSA would provide an analysis of potential threats. However, in April 2021, the Director of the NSA's Cyber Security Directorate declined the designation of the NSA as a co-lead for the quantifiable assurance method because the NSA could not increase its mission capability in the timeframes required by the OUSD(R&E). NSA personnel acknowledged the need for coordination between the OUSD(R&E) and the Office of the Under Secretary of Defense for Intelligence and Security (OUSD[I&S]) to determine the NSA's role in the quantifiable assurance method.

(U) In addition, the OUSD(R&E) did not meet the January 2021 deadline established in the FY 2020 NDAA and is still developing the standards and instructions necessary to implement a quantifiable assurance method to procure custom microelectronics. Specifically, the OUSD(R&E) was still establishing:

- (U) new standards for DoD Custom Integrated Circuits,
- (U) updates to DoD Instruction 5200.44, and

- (U) a new DoD policy to implement the quantifiable assurance method.¹

(U) OUSD(R&E) officials told us that these delays occurred because:

- (U) the transition to the quantifiable assurance method started in July 2020 and the OUSD(R&E) encountered difficulties in developing and staffing new processes and procedures by the January 1, 2021 deadline established in the FY 2020 NDAA;
- (U) the coronavirus disease-2019 (COVID-19) pandemic created challenges; and
- (U) there was turnover of key personnel at the OUSD(R&E) and the NSA.

(U) As a result, the OUSD(R&E) did not establish trusted supply chain and operational security standards for procuring custom microelectronics by January 1, 2021, as required by the NDAA for FY 2020.

(U) Recommendations

(U) We recommend that the OUSD(R&E) update the JFAC Charter and the JFAC Concept of Operations and develop a process to prioritize the quantifiable assurance method efforts of the supporting DoD laboratories.

(U) We also recommend that the OUSD(R&E), in coordination with the Under Secretary of Defense for Intelligence and Security (USD[I&S]), identify the resources required to support the NSA's role in the threat analysis for quantifiable assurance or identify another DoD organization capable of performing the role currently assigned to the NSA.

¹ (U) DoD Instruction 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," November 5, 2012 (Incorporating Change 3, October 15, 2018).

CUI



CUI

(U) Results in Brief

(U) Evaluation of the Department of Defense's Transition From a Trusted Foundry Model to a Quantifiable Assurance Method for Procuring Custom Microelectronics

(U) Management Comments and Our Response

(U) On February 18, 2022, the OUSD(R&E) Director of Defense Research and Engineering for Modernization, responding on behalf of the USD(R&E), agreed with both recommendations. The Director of Defense Research and Engineering for Modernization stated that to support these recommendations, in October 2021, the Principal Director for Microelectronics added the position of Assistant Deputy Director for Microelectronics for Assurance Standards. Additionally, the Principal Director for Microelectronics updated the strategy for quantifiable assurance policy, guidance, and standards that included feedback from the National Defense Industry Association and the DoD.

(U) On April 21, 2022, the Deputy Under Secretary of Defense for Research and Engineering provided us with a memorandum with additional management comments that he stated are necessary to understand the potential of the quantifiable assurance method. The Deputy Under Secretary stated that it is not possible to create a plan for a transition to a quantifiable assurance methodology until such time as the methodology has been proven to effectively provide required levels of protection. According to the Deputy Under Secretary, the impacts on cost, schedule, and performance for programs of record remain to be evaluated. For the complete comments, see the Management Comments appendix at the end of this report.

(U) Additionally, the Deputy Under Secretary stated that we mischaracterized the effectiveness of the trusted foundry model. However, in our report we do not discuss the effectiveness of either the trusted foundry or quantifiable assurance models. Our report focused on the DoD's transition from the trusted foundry model to the quantifiable assurance method.

(U) Furthermore, documents that OUSD(R&E) officials provided to us at the outset of this evaluation stated that they would "replace outdated security protocols based on 'Trusted Foundry' with Quantitative Assurance and Microelectronics Security Standards," and that the Defense Microelectronics Activity created a team of engineers to help transition the organization to quantifiable assurance and that the trusted certification approach was being phased out. The Deputy Under Secretary did not provide us with any documentary evidence to the contrary.

(U) Lastly, in this report we make no determination on what the DoD's microelectronics procurement policies should be. We evaluated the status of the OUSD(R&E)'s quantifiable assurance efforts. The conclusions set forth in this report are based on the evidence provided by officials from the OUSD(R&E), the NSA, and the Naval Surface Warfare Center-Crane Division.

(U) The OUSD(I&S) Director for Defense Intelligence, Counterintelligence, Law Enforcement, and Security, responding on behalf of the USD(I&S), agreed to collaborate with the OUSD(R&E) to identify either the resources required to support the NSA's role, or identify another agency capable of performing that role.

(U) Therefore, both recommendations are resolved, but will remain open. We will close the recommendations when we verify that the actions to implement the recommendations are completed. Please see the Recommendations Table on the next page for the status of recommendations.

CUI

(U) Recommendations Table

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
(U) Under Secretary of Defense for Research and Engineering	(U) None	(U) 1, 2	(U) None
(U) Under Secretary of Defense for Intelligence and Security	(U) None	(U) 2	(U) None

Please provide Management Comments by June 6, 2022.

Note: The following categories are used to describe agency management's comments to individual recommendations.

- **Unresolved** – Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- **Resolved** – Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- **Closed** – OIG verified that the agreed upon corrective actions were implemented.



**INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500**

May 2, 2022

(U) MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING
UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY
DIRECTOR, NATIONAL SECURITY AGENCY
COMMANDING OFFICER, NAVAL SURFACE WARFARE
CENTER CRANE DIVISION

(U) SUBJECT: (U) Evaluation of the Department of Defense's Transition From a Trusted Foundry Model to a Quantifiable Assurance Method for Procuring Custom Microelectronics (Report No. DODIG-2022-084)

(U) This final report provides the results of the DoD Office of Inspector General's evaluation. We previously provided copies of the draft report and requested written comments on the recommendations. We considered management's comments on the draft report when preparing the final report. These comments are included in the report.

(U) OUSD(R&E) and OUSD(I&S) officials agreed to address all the recommendations presented in the report; therefore, we consider the recommendations resolved and open. As described in the Recommendations, Management Comments, and Our Response section of this report, we will close the recommendations when you provide us documentation showing that all agreed-upon actions to implement the recommendations are completed. Therefore, please provide us within 90 days your response concerning specific actions in process or completed on the recommendations. Send your response to [REDACTED]
[REDACTED]

(U) We appreciate the cooperation and assistance received during the evaluation. If you have any questions, please contact [REDACTED]
[REDACTED]

A handwritten signature in black ink, appearing to read "Randolph R. Stone", is located above the name and title of the signatory.

Randolph R. Stone
Assistant Inspector General for Evaluations
Space, Intelligence, Engineering, and Oversight

(U) Contents

(U) Introduction

(U) Objective	1
(U) Background	1

(U) Finding. The OUSD(R&E) Has Plans and Milestones to Transition From a Trusted Foundry Model to a Quantifiable Assurance Method for Procuring Custom State-of-the-Art Microelectronics; However, Standards and Instructions to Implement the Quantifiable Assurance Method Are Still in Development	13
--	----

(U) The OUSD(R&E) Has Developed Plans and Milestones to Transition from a Trusted Foundry Model to a Quantifiable Assurance Method for Procuring Custom State-of-the-Art Microelectronics	15
(U) The Impact of Quantifiable Assurance Implementation Delays	22
(U) Recommendations, Management Comments, and Our Response	23

(U) Appendix

(U) Scope and Methodology	27
(U) Use of Computer-Processed Data	29
(U) Use of Technical Assistance	29
(U) Prior Coverage	29

(U) Management Comments

(U) Under Secretary of Defense for Research and Engineering	31
(U) Under Secretary of Defense for Intelligence and Security	38
(U) Naval Sea Systems Command	39

(U) Acronyms and Abbreviations	40
---	----

(U) Glossary	41
---------------------------	----

(U) Introduction

(U) Objective

(U) We determined the extent to which the DoD has made the preparations necessary to transition from a trusted foundry model for procuring custom microelectronics to a quantifiable assurance method for procuring custom microelectronics from the commercial market.²

(U) Background

(U) Microelectronics refers to the design and manufacturing of extremely small electronic components, often in the form of microchips and microcircuits. A foundry is a microchip fabrication facility.³ Section 224 of the National Defense Authorization Act (NDAA) for FY 2020 requires the DoD to establish trusted supply chain and operational security standards for the purchase of microelectronics products by January 1, 2021.⁴ The Secretary of Defense is responsible for ensuring microelectronics products or services that the DoD purchases on or after January 1, 2023, meet those standards. Quantifiable assurance is the DoD's method to achieve these requirements for custom state-of-the-art microelectronics.

(U) In May 2020, the Director of Defense Research and Engineering for Modernization, within the Office of the Under Secretary of Defense for Research and Engineering (OUSD[R&E]), identified microelectronics as the DoD's number one technology modernization priority. According to the Director, microelectronics are crucial for ensuring that the warfighter has access to state-of-the-art warfighting capabilities. Additionally, in May 2020, the Director told an industry forum that the trusted foundry model has failed and that the DoD was adopting a "zero trust" approach to buying microelectronics.⁵ More specifically, the DoD was seeking to adapt a quantifiable assurance method, using zero trust principles, to procure custom microelectronics.

² (U) According to a draft DoD Manual, subsequent to our fieldwork, the term "quantifiable assurance" changed to "microelectronics quantifiable assurance (MQA)." We use the term "quantifiable assurance method" throughout this report.

³ (U) A trusted foundry, or trusted supplier, is a Defense Microelectronics Activity-accredited supplier of integrated circuit-related products and services.

⁴ (U) Public Law 116-92, "National Defense Authorization Act for Fiscal Year 2020," Section 224, "Requiring Defense Microelectronics Products and Services Meet Trusted Supply Chain and Operational Security Standards," December 20, 2019. The NDAA covers all microelectronics and services to include commercial off-the-shelf components; however, the scope of this evaluation focuses only on custom state-of-the-art microelectronics.

⁵ (U) Zero trust principles assume "that nothing the DoD buys is safe, and that everything must be validated before it can be used." (DoD Press Release, "DOD Adopts 'Zero Trust' Approach to Buying Microelectronics," May 19, 2020).

(U) Quantifiable assurance is a method being developed to measurably protect the integrity and confidentiality of custom microelectronic components based on zero trust principles and attack-countermeasure analysis (ACMA).⁶

The method consists of:

- (U) a quantitative analysis of potential threats, mitigations and an ACMA;
- (U) a quantitative risk plan to implement mitigations and a program justification for residual risks; and
- (U) an evaluation of the quantitative risk analysis and the quantitative risk plan for completeness and correctness.

(U) DoD Organizations and Their Roles in the Quantifiable Assurance Method

(U) Establishing the quantifiable assurance method for microelectronics involves multiple DoD organizations. Some of the key organizations involved are the OUSD(R&E), the Joint Federated Assurance Center (JFAC), and supporting Service and DoD component laboratories.

(U) The Office of the Under Secretary of Defense for Research and Engineering

(U) The USD(R&E) is the DoD's chief technology officer and has the mission of advancing technology and innovation for the Military Services and the DoD. The USD(R&E) advises the Secretary of Defense on all matters related to research; engineering; manufacturing; developmental test and evaluation; and technology development, innovation, and protection activities and programs. Microelectronics are one of the USD(R&E)'s 10 designated modernization priorities.

(U) The OUSD(R&E) has a Principal Director for each of its technology modernization priorities, including microelectronics. According to Section 217 of the FY 2021 NDAA, responsibilities of the Principal Directors include:

- (U) developing and continuously updating research and technology development roadmaps, funding strategies, and technology transition strategies;
- (U) reviewing the relevant research and engineering budgets of appropriate organizations;
- (U) coordinating research and engineering activities; and

⁶ (U) ACMA helps assess risks, define mitigation approaches, and assess risks remaining after mitigation plans are implemented. Inputs to the ACMA includes the microelectronics component risk profile, expected threats, threat criticality, and mitigation methods.

- (U) tasking appropriate DoD intelligence agencies to develop a direct comparison between the capabilities of the United States in the technology area concerned and the capabilities of U.S. adversaries in that area.⁷

(U) The Joint Federated Assurance Center

(U) The JFAC is a federation of DoD organizations that promotes and enables software and hardware assurance by providing expertise and support to defense acquisition programs.⁸ Section 937 of the FY 2014 NDAA required the DoD to establish a joint federation of capabilities to support trusted defense system needs to ensure the security of software and hardware developed, acquired, maintained, and used by the DoD.⁹ DoD Instruction (DoDI) 5000.83, “Technology and Program Protection to Maintain Technological Advantage,” July 20, 2020, as amended, states that the USD(R&E) establishes and maintains the JFAC and that lead systems engineers will, when appropriate, request assistance from the JFAC to support software and hardware assurance requirements.

(U) The JFAC is governed by a Charter and Concept of Operations (CONOPS); however, these documents predate the creation of the OUSD(R&E) and the OUSD(R&E)’s Principal Director for Microelectronics. The JFAC is managed by a steering committee that includes senior representatives from the OUSD(R&E), the DoD Chief Information Officer, the Military Departments, the National Security Agency (NSA), the Defense Microelectronics Activity (DMEA), and other Defense Agencies. The USD(R&E) presides over meetings of the JFAC steering committee and associated working groups.

(U) The federation is composed of a JFAC Coordination Center that coordinates requests for support activities among the JFAC members and DoD and Service laboratories and organizations with hardware and software assurance capabilities that provide services to the federation. The JFAC coordination center receives requests for assistance from program offices and coordinates with and identifies DoD and Service laboratories to respond to the program office request. Each of these laboratories has their own chain-of-command and processes to receive funding from program offices that are requesting support.

⁷ (U) Public Law 116-283, “William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021,” Section 217, “Designation of Senior Officials for Critical Technology Areas Supportive of the National Defense Strategy,” January 1, 2021.

⁸ (U) Software assurance is the level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the lifecycle. (DoDI 5200.44)

(U) Hardware assurance is the level of confidence that microelectronics function as intended and are free of known vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system’s hardware and its embedded software and intellectual property, throughout the life cycle. (Defense Acquisition University, “Glossary of Defense Acquisition Acronyms and Terms,” July 21, 2020.)

⁹ (U) Public Law 113-66, “National Defense Authorization Act for Fiscal Year 2014,” Section 937, “Joint Federated Centers for Trusted Defense Systems for the Department of Defense,” December 26, 2013.

(U) The OUSD(R&E) intended to designate the Naval Surface Warfare Center (NSWC)-Crane Division and the NSA as the two co-leads for the quantifiable assurance method. However, in April 2021, the Director of the NSA's Cyber Security Directorate notified the OUSD(R&E) via a memorandum that the NSA declined the NSA's role as a co-lead for the quantifiable assurance method.

(U) [REDACTED]

(U) The Trusted and Assured Microelectronics Program

(U) The OUSD(R&E) manages the Trusted and Assured Microelectronics Program line of funding to develop the quantifiable assurance method. The OUSD(R&E)'s Trusted and Assured Microelectronics Program provides funding for the JFAC's partnerships to develop a data-driven, risk-based approach to supply chain protection and develop the assured access, secure design, and manufacturing capability for advanced microelectronics technology and electronic components. The Trusted and Assured Microelectronics Program provides support to organizations involved in the JFAC and the implementation of the quantifiable assurance method.¹⁰

(U) The Naval Surface Warfare Center-Crane Division

(U) The NSWC-Crane Division, located in Crane, Indiana, is a major component and field activity within Navy Sea Systems Command. The NSWC-Crane Division supports the JFAC with training subject matter experts to assist the DoD and the defense industrial base to implement the quantifiable assurance method for state-of-the-art microelectronics. The NSWC-Crane Division supervises several

¹⁰ (U) The President's FY 2022 budget requested \$509.2 million for the Trusted and Assured Microelectronics Program for microelectronics modernization activities, including \$243.2 million for secure design and quantifiable assurance method development.

(U) prototype programs that the OUSD(R&E)'s Trusted and Assured Microelectronics Program is using to improve access to state-of-the-art microelectronics. Two of these programs are the Rapid Assured Microelectronics Prototypes Using Advanced Commercial Capabilities (RAMP), and State-of-the-Art Heterogeneous Integrated Packaging (SHIP) prototype projects.

(U) The NSWC-Crane Division's RAMP program seeks to facilitate rapid development of assured microelectronics hardware for further evaluation and to generate workflow prototypes using commercial best practices to enable the defense industrial base to access state-of-the-art technologies that are unavailable in the trusted foundry model. The DoD awarded a \$24.5 million other transaction agreement to Microsoft and IBM for Phase 1 of the RAMP project, which is tasked with:

- (U) establishing a secure design capability that supports an enhanced physical design by the defense industrial base in state-of-the-art technology nodes;
- (U) applying methods to ensure confidentiality and integrity of circuits during the manufacturing flow; and
- (U) creating a DoD supply chain standard that leverages commercial microelectronics supply chain security methods to meet DoD needs.¹¹

(U) The NSWC-Crane Division's SHIP program seeks to leverage commercially available heterogeneous integration technology. This allows the DoD to separate different microchip functions and technologies into separate manufacturing lines that use different hardware standards that are then combined in a final product.¹² By allowing components to be manufactured separately, in a secure setting, the security of the larger function of combined components can be maintained. According to a DoD press release on October 15, 2020, the DoD awarded a \$172.7 million other transaction agreement for SHIP Phase 2 to Intel Federal and Qorvo to develop and demonstrate a novel approach towards secure, heterogeneous integration and testing of advanced packaging solutions.

¹¹ (U) Other transactions are contractual instruments other than standard procurement contracts, grants, or cooperative agreements. Other transaction agreements can include flexible business arrangements to acquire research and development activities to advance new technologies and prototypes or models to evaluate technical or manufacturing feasibility or military utility of new or existing technology.

¹² (U) Heterogeneous (diverse in content) integration is integration of separately manufactured components into a higher level assembly that, in the aggregate, provides enhanced functionality and improved operating characteristics.

(U) The National Security Agency

(U) The NSA, located in Fort Meade, Maryland, is a DoD intelligence agency and combat support agency. The NSA supports the JFAC with hardware and software assurance subject matter expertise and the development of threat assessments.¹³ According to OUSD(R&E) and NSA officials, the OUSD(R&E) and the NSA were still determining the extent of the NSA's role as a JFAC laboratory in support of the quantifiable assurance method after the NSA declined the designation as co-lead. According to OUSD(R&E) and NSA officials, on August 9, 2021, the NSA sent the OUSD(R&E) a resource estimate with the scope and cost required for the NSA to support hardware analysis and assurance activities for the quantifiable assurance method in a supporting role.¹⁴

(U) The Defense Microelectronics Activity

(U) The DMEA, located in McClellan, California, performs accreditations of trusted suppliers, reviews those accreditations on an annual basis, issues followup guidance for the use of trusted suppliers, and establishes criteria for accrediting trusted suppliers of integrated circuit-related products and services. The DMEA was part of the OUSD(R&E) until January 2021, when DMEA was transferred and placed under the authority, direction, and control of the Under Secretary of Defense for Acquisition and Sustainment. Under the current DoDI 5200.44, integrated circuit-related products and services that are custom-designed, custom-manufactured, or tailored for a specific end-use, referred to as an Application Specific Integrated Circuit (ASIC), must be procured from a trusted supplier using DMEA-accredited trusted processes.¹⁵

¹³ (U) According to the current versions of DoDI 5200.44 and DoDI O-5240.24, "Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)," June 8, 2011, as amended, the Director of the Defense Intelligence Agency has the threat analysis responsibility for the DoD. See DoD OIG Report No. DODIG-2020-106, "Evaluation of Security Controls for Intelligence, Surveillance, and Reconnaissance Supply Chains," July 22, 2020, for additional information on the DIA's threat analysis responsibilities. This report is classified.

¹⁴ (U) According to an NSA official, the cost estimate included only resources for hardware analysis and assurance activities and not for full NSA leadership and support of quantifiable assurance.

¹⁵ (CUI) In DODIG-2020-072, "Audit of DoD Hotline Allegations Concerning the Defense Microelectronics Activity," March 24, 2020, we provide background on the DMEA and recommended an assessment of the use of DMEA's own foundry and whether it is still needed. [REDACTED]

(U) Current DoD Policy and Access to State-of-the-Art Custom Microelectronics

(U) As discussed above, the Director of Defense Research and Engineering for Modernization told an industry forum that the trusted foundry model has failed. Specifically, current DoD policy requires the use of a DMEA-accredited trusted supplier for procuring custom microelectronics; however, this approach is no longer viable for the acquisition of state-of-the-art custom microelectronics.

(U) Federal Regulations and DoD Policy

(U) Title 22 Code of Federal Regulations, sections 120 through 130, also known as the International Traffic in Arms Regulations (ITAR), controls items on the U.S. Munitions List, including custom microelectronics specifically designed for defense articles, such as ASICs and Programmable Logic Devices programmed for defense articles.¹⁶ The ITAR is a Federal regulation that requires companies to place restrictions on foreign nationals' access to data and information.

(U) DoDI 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," is a DoD policy that requires the use of DMEA-accredited suppliers for the procurement of custom designed microelectronics.

(U) The Trusted Foundry Is No Longer Viable for Custom State-of-the-Art Microelectronics Procurement

(U) The current DoDI 5200.44 relies on domestic and accredited facilities to protect custom microelectronic components with specific military end-use by manufacturing microelectronics in a trusted foundry. However, OUSD(R&E) personnel told us and provided documentation and background briefings that identified that this policy is no longer viable for adoption by microelectronics foundries for two reasons.

1. (U) Modern state-of-the-art fabrication facilities cannot succeed in the commercial marketplace if they meet DoDI 5200.44 trusted foundry requirements for the following reasons.
 - a. (U) Engineering skillsets required for a successful fabrication facility are so specialized that they can only be obtained through a global workforce. As a result, there are no state-of-the-art facilities that are DMEA-accredited trusted foundries.

¹⁶ (U) International Traffic in Arms Regulations, 22 CFR 120-130, Section 121.1, "The United States Munitions List," Category XI, "Military Electronics," paragraph (c) lists custom electronics, including ASICs and Programmable Logic Devices programmed for defense articles. Defense articles include technical data recorded or stored in any physical form, models, mockups, or other items that reveal technical data directly relating to items on the U.S. Munitions List.

- b. (U) Commercial pressures restrict the available trusted foundries to increasingly obsolete technology.
2. (U) Current DoD trusted foundry policy does not account for the programmability in state-of-the-art System-on-a-Chip designs.¹⁷ Technology advances have increased the amount of programmability available to designers of state-of-the-art integrated circuits. This additional programmability enables a custom integrated circuit design in which critical information is programmed into the System-on-a-Chip after fabrication is complete.

~~(CUI)~~ OUSD(R&E) officials told us that the DoD currently does not have access to U.S.-based foundry technology capable of meeting the long-term leading edge microelectronics fabrication needs for DoD-specific designs or commercial off-the-shelf or available components. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED].¹⁸

(U) Quantifiable Assurance Method Initiatives and Milestones

(U) The NDAA for FY 2020 required the Secretary of Defense to establish trusted supply chain and operational security standards for the purchase of microelectronics products and services by January 1, 2021. To meet the NDAA requirement, the OUSD(R&E) was developing Standards for DoD Custom Integrated Circuits, updating current DoD policies including DoDI 5200.44, and creating new policy and guidance to facilitate DoD access to assured state-of-the-art microelectronics.

(U) Standards for DoD Custom Integrated Circuits

(U) The OUSD(R&E) is developing new standards for both custom integrated circuits and field programmable gate arrays.¹⁹ According to an OUSD(R&E) official, as of January 15, 2021, the first draft of the standards for DoD Custom Integrated Circuits, which includes ASICs, and the standards for Field Programmable Gate Arrays (the Standards) were in internal review within the OUSD(R&E).

¹⁷ (U) A System-on-a-Chip is an integrated circuit that integrates all or most components of a computer or other electronic system on a single microchip.

¹⁸ (U) Government Accountability Office Report No. GAO-16-185T, "Trusted Defense Microelectronics - Future Access and Capabilities Are Uncertain," October 28, 2015, also identified the challenges to the DoD's access to trusted leading-edge microelectronics stemming from manufacturing costs, supply chain globalization, and market trends, creating uncertainty regarding future access about U.S.-based microelectronics sources.

¹⁹ (U) A field programmable gate array is an integrated circuit designed to be configured by a customer or designer after manufacturing.

(U) The internal review includes solicitation of feedback from within the DoD as well as from the defense and commercial organizations participating in the trusted and assured microelectronics programs.

(U) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

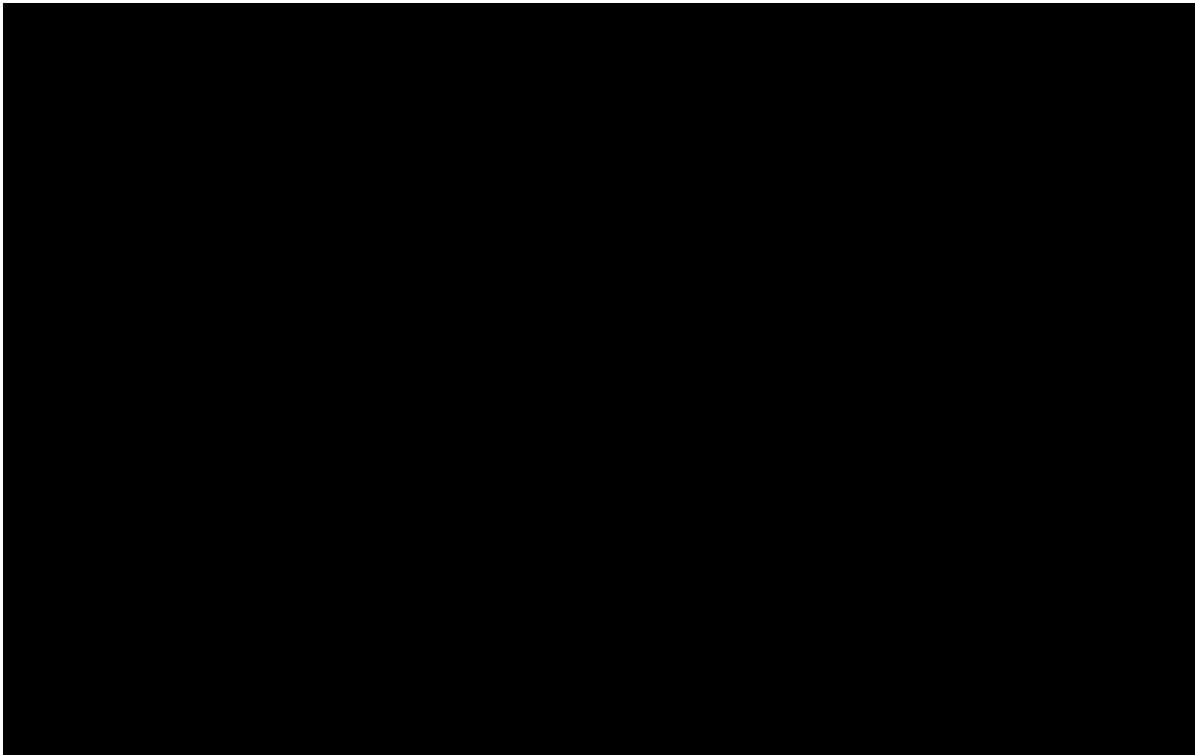
(U) The OUSD(R&E), in support of the quantifiable assurance method for procuring microelectronics, also developed a microelectronics roadmap that includes clarifications to export control policy, updates to DoD instructions that govern microelectronics procurement, and prototype programs to test potential acquisition strategies.

(U) U.S. Government Export Controls Regulations

(U) U.S. Government export controls place limits on the export of custom microelectronics designs for manufacture overseas. The ITAR specifically controls items on the U.S. Munitions List, including ASICs and programmable logic devices programmed for defense articles. The ITAR limits the export of custom microelectronics designs for manufacture overseas and prohibits release of technical data associated with these devices to non-U.S. persons. Export of this technical data requires a licensing process for each non-U.S. person. One technique used in the quantifiable assurance method is to design microelectronic components so that U.S. Munitions List controlled functions and data are programmed into the component after the component manufacturing is complete. In August 2019, the U.S. State Department issued a document to clarify that if all of the defense-specific programmable elements in an integrated circuit are not yet programmed, then the integrated circuit is not subject to the U.S. Munitions List restrictions. This allowed for greater flexibility in state-of-the-art microelectronics

²⁰ (U) The FY 2020 NDAA requires that the standards are developed in consultation with the Secretary of Homeland Security, the Secretary of State, the Secretary of Commerce, and the Director of the National Institute of Standards and Technology; suppliers of microelectronics products and services from the United States, and allies and partners of the United States; representatives of major U.S. industry sectors that rely on a trusted supply chain and the operational security of microelectronics products and services; and representatives of the U.S. insurance industry.

(U) acquisition. The OUSD(R&E) used the Military Global Positioning System (GPS) User Equipment (MGUE) Increment 2 program to test the use of this policy.²¹ Table 1 provides additional details on how the OUSD(R&E) used the MGUE Increment 2 program to test new ways to acquire state-of-the-art microelectronics.



(U) DoD Policy for Trusted and Secure Networks and Assured Microelectronics

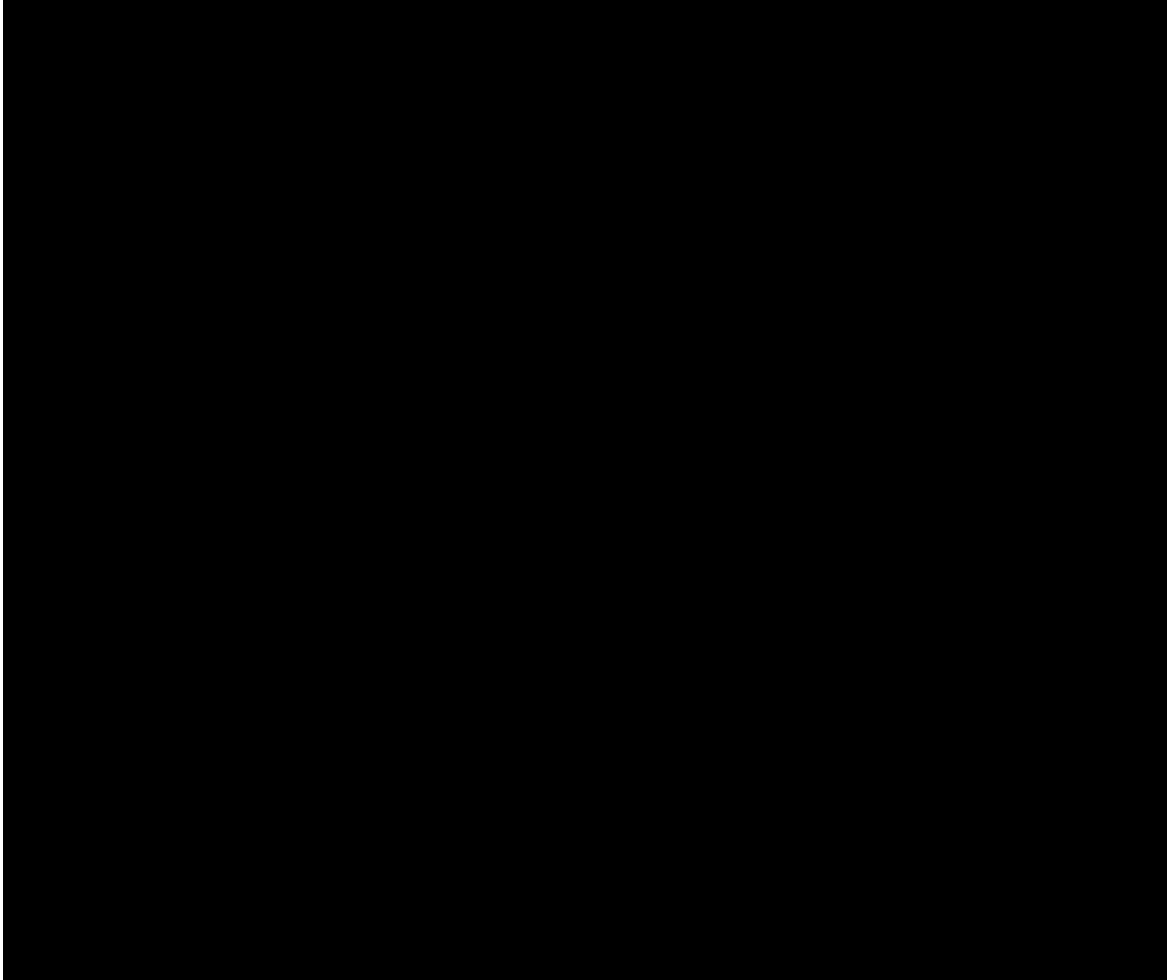
(U) The OUSD(R&E) is updating DoDI 5200.44 to incorporate the quantifiable assurance method. The instruction currently requires the use of DMEA-accredited suppliers for the procurement of custom designed microelectronics for applicable systems.²² Furthermore, the OUSD(R&E) is drafting a new DoD Instruction, “Access and Assurance for Microelectronics,” that would establish policy and assign

²¹ (U) Government Accountability Office Report No. GAO-21-145, “GPS Modernization-DoD Continuing to Develop New Jam-Resistant Capability, But Widespread Use Remains Years Away,” January 19, 2021, discusses the U.S. Air Force’s MGUE programs, including access to trusted and export compliant microelectronics.

(CUI) [REDACTED]

²² (U) The current version of DoDI 5200.44 defines applicable systems as: national security systems as defined by section 3552, Title 44, United States Code, with the exception of the DoD’s Non-classified Internet Protocol Router Network (NIPRNet) and its enclaves; any DoD system with a high impact level for any of the three security objectives (confidentiality, integrity, and availability) in accordance with the system categorization procedures in DoDI 8510.01, “Risk Management Framework (RMF) for DoD Information Technology (IT),” March 12, 2014, as amended; or other DoD information systems that the DoD Component’s acquisition executive or chief information officer, or designee, determines are critical to the direct fulfillment of military or intelligence missions, which may include some connections to or enclaves of NIPRNet and some industrial control systems.

(U) responsibilities for the quantifiable assurance method, including a requirement for individual programs to develop a quantitative risk analysis and quantitative risk plan for each custom microelectronic component. The instruction would require the JFAC to evaluate these plans for completeness and correctness. The program office would include the analysis, plan, and results of the evaluation in the Program Protection Plan associated with the custom microelectronic component.²³ Table 2 summarizes the proposed policy in the new Access and Assurance for Microelectronics Instruction.



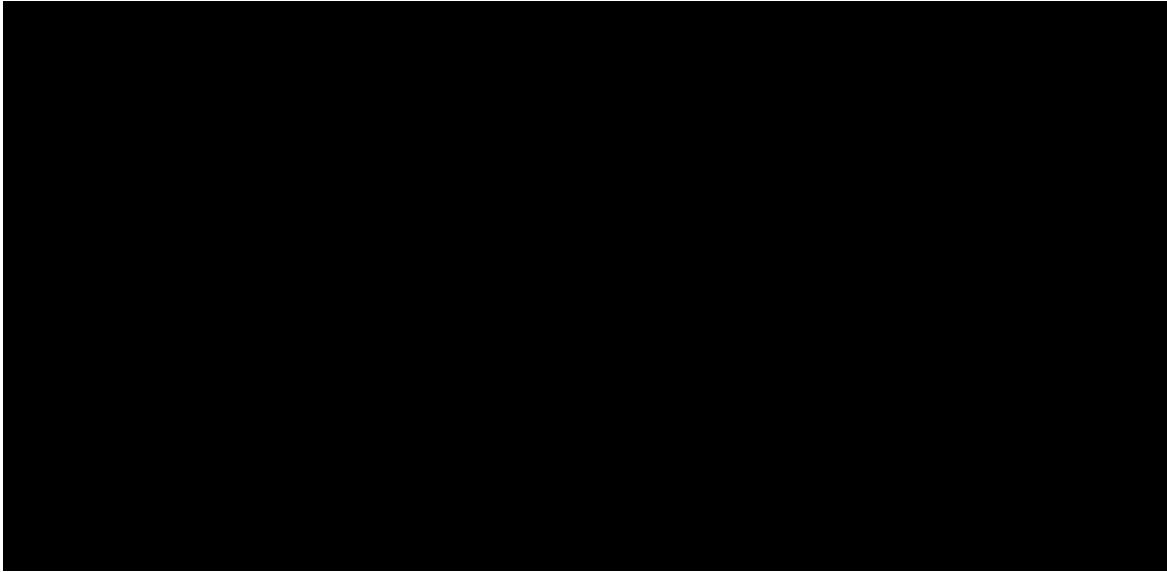
(U) [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]²⁴

²³ (U) The new policy is tentatively titled DoDI.XX, "Access and Assurance for Microelectronics."

²⁴ (U) For an updated status of the DoD draft issuances, please see Management Comments following the Appendix.

(U) Figure 1 shows the status of the update to DoDI 5200.44 and the release process of the “Access and Assurance for Microelectronics Instruction,” as of June 2021.



(U) Finding

(U) The OUSD(R&E) Has Plans and Milestones to Transition From a Trusted Foundry Model to a Quantifiable Assurance Method for Procuring Custom State-of-the-Art Microelectronics; However, Standards and Instructions to Implement the Quantifiable Assurance Method Are Still in Development

(U) The OUSD(R&E) developed plans to transition from a trusted foundry model to a quantifiable assurance method for procuring custom state-of-the-art microelectronics from the commercial market.²⁵ However, the OUSD(R&E) is behind schedule for establishing trusted supply chain and operational security standards by the January 1, 2021, deadline, as required by the NDAA for FY 2020.

(U) Specifically, programs and policies already established included:

- (U) a JFAC Charter and CONOPS,
- (U) a JFAC Coordination Center and ticketing portal to route requests for assistance from the program offices,
- (U) a program to fund the JFAC's work, and
- (U) JFAC laboratories designated to support implementation of the quantifiable assurance method.²⁶

(U) However, the JFAC Charter and CONOPS predate the creation of the OUSD(R&E) and the OUSD(R&E)'s Principal Director for Microelectronics. The JFAC CONOPS does not provide the Principal Director for Microelectronics with authorities to resolve competing priorities between the program offices requesting JFAC support and insufficient capacity among the JFAC service providers.

(U) In addition, the OUSD(R&E) designated the NSWC-Crane Division and the NSA as the two co-leads for the quantifiable assurance method. The NSWC-Crane Division manages several contracts that test quantifiable assurance procedures. However, in April 2021 the Director of the NSA's Cyber Security Directorate notified the OUSD(R&E) that the NSA declined the designation as a co-lead for

²⁵ (U) Plan refers to a collection of internal OUSD(R&E) milestones, roadmaps, and strategies to develop policies, standards, and guidance for quantifiable assurance.

²⁶ (U) Quantifiable assurance is a method used to measurably protect the integrity and confidentiality of custom microelectronic components based on Zero Trust concepts and Attack-Countermeasure Analysis (ACMA). The method consists of: 1) a quantitative risk analysis, 2) a quantitative risk plan, and 3) an evaluation by the JFAC of the quantitative risk analysis and the quantitative risk plan for completeness and correctness.

(U) implementing the quantifiable assurance method because the NSA could not increase its mission capability in the timeframes required by the OUSD(R&E). According to OUSD(R&E) and NSA officials, on August 9, 2021, the NSA sent the OUSD(R&E) a resource estimate with the scope and cost required for the NSA to support hardware analysis and assurance activities for the quantifiable assurance method for procuring custom microelectronics in a supporting role.

(U) Despite the January 1, 2021 deadline in the FY 2020 NDAA for establishing draft security standards, the OUSD(R&E) Principal Director for Microelectronics is still developing the standards and instructions necessary to implement a quantifiable assurance method for procuring custom microelectronics. Specifically, the OUSD(R&E) is still establishing:

- (U) new security standards for DoD Custom Integrated Circuits,
- (U) updates to DoDI 5200.44 to enable use of the quantifiable assurance method for access to assured microelectronics, and
- (U) a new DoD policy to implement the quantifiable assurance method.

(U) OUSD(R&E) officials told us that these delays occurred because:

- (U) the transition to the quantifiable assurance method started in July 2020 and OUSD(R&E) encountered difficulties in developing and staffing new processes and procedures by the FY 2020 NDAA deadline of January 1, 2021;
- (U) the coronavirus disease–2019 (COVID-19) pandemic created challenges; and
- (U) there was turnover of key personnel at the OUSD(R&E) and the NSA.

(U) As a result of delays, the OUSD(R&E) did not establish trusted supply chain and operational security standards for procuring custom state-of-the-art microelectronics by January 1, 2021, as required by the NDAA for FY 2020. Delays in releasing the draft Standard for DoD Custom Integrated Circuits reduced the time available for industry and interagency review and adoption. If milestones for the release of the draft Standards for DoD Custom Integrated Circuits continue to experience delays, it could negatively affect the DoD's ability to procure state-of-the-art custom microelectronics.

(U) The OUSD(R&E) Has Developed Plans and Milestones to Transition from a Trusted Foundry Model to a Quantifiable Assurance Method for Procuring Custom State-of-the-Art Microelectronics

(U) The OUSD(R&E) developed plans to transition from a trusted foundry model to a quantifiable assurance method for procuring custom state-of-the-art microelectronics from the commercial market. However, the OUSD(R&E) is behind schedule for having trusted supply chain and operational security standards by the January 1, 2021 deadline.

(U) The OUSD(R&E) Has Some Processes to Support Quantifiable Assurance Method

(U) The OUSD(R&E) has some current processes to support the quantifiable assurance method. Specific elements of the transition plan already in place are a JFAC Charter and CONOPS, a JFAC Coordination Center and ticketing portal to route requests for assistance from the program offices, a program to fund the JFAC's work, and JFAC laboratories designated to support the quantifiable assurance method. As discussed earlier in the report, the current procedures and documentation include the following.

(U) The JFAC Charter Needs to Be Updated

(U) The JFAC Charter, dated February 9, 2015, establishes a JFAC steering committee; directs the creation of the JFAC Working Group and a JFAC CONOPS; and describes the mission, functions, construct, and responsibilities of the JFAC.²⁷ The charter states that the JFAC Working Group will resolve conflicting policies, schedules, and priorities.

(U) However, the JFAC Charter predates the establishment of the OUSD(R&E) in 2018 and the enactment of section 217 of the NDAA for FY 2021, which designated duties for the OUSD(R&E)'s Principal Director for Microelectronics, as discussed in the background. Details on the responsibilities and operations of the JFAC resides in other documents, including the JFAC CONOPS.

(U) The JFAC Concept of Operations Needs to Be Updated

(CUI) The JFAC CONOPS, dated October 9, 2015, expands on the JFAC Charter to outline plans for establishing the various elements and working relationships of the JFAC organizational structure. The JFAC CONOPS also predates the establishment

²⁷ (U) Deputy Secretary of Defense Policy Memorandum 15-001, "Joint Federated Assurance Center (JFAC) Charter," February 9, 2015.

(~~CUI~~) of the OUSD(R&E) in 2018 and the enactment of section 217 of the NDAA for FY 2021, which designated duties for the OUSD(R&E)'s Principal Director for Microelectronics, as discussed in the background. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(U) The JFAC CONOPS outlines how the JFAC supports hardware and software assurance efforts for defense systems, of which microelectronics is a subset. The JFAC CONOPS provides case scenarios such as the above instances in which the JFAC does not have the capacity to meet requirements. However, like the JFAC Charter, the JFAC CONOPS also predates the creation of the OUSD(R&E) and the OUSD(R&E)'s Principal Director for Microelectronics. The JFAC CONOPS does not provide the Principal Director for Microelectronics with authorities to resolve competing priorities between the program offices requesting JFAC assistance and insufficient support capacity among the JFAC service providers. The potential increase in requests for JFAC support under the quantifiable assurance method requires the JFAC CONOPS to be updated to incorporate the new roles and responsibilities.

(U) According to an OUSD(R&E) official, OUSD(R&E) personnel are having internal discussions to examine the structure of the JFAC Steering Committee and the JFAC Action Officer Working Group.

(U) The Trusted and Assured Microelectronics Program Supports the JFAC's Quantifiable Assurance Method Efforts

(U) As stated in the background, the OUSD(R&E) has a Trusted and Assured Microelectronics Program to provide support to organizations involved in the JFAC and the quantifiable assurance method. According to an OUSD(R&E) official, the trusted and assured microelectronics program is a way the OUSD(R&E) supports the JFAC's laboratories and the implementation of the quantifiable assurance method. According to the DoD's FY 2021 Budget Estimates, four project codes under the Trusted and Assured Microelectronics Program Element were realigned so that funding would support the quantifiable assurance method and reflect

(U) current priorities.²⁸ In sum, the OUSD(R&E) established four replacement project codes to provide funding traceability to the DoD's microelectronics programs for state-of-the-art access, heterogeneous packaging, quantifiable assurance, DoD unique microelectronic needs, and enhanced microelectronics dominance.

(U) The NSWC-Crane Division and the NSA Laboratories Will Support Much of the Effort for Quantifiable Assurance

~~(U)~~ The OUSD(R&E) designated the NSWC-Crane Division and the NSA as the two co-leads for the quantifiable assurance method. The NSWC-Crane Division manages several other transaction agreements to develop and demonstrate quantifiable assurance method procedures. The NSA would provide an analysis of potential threats. However, in an April 2021 memorandum from the Director of the NSA's Cyber Security Directorate to the OUSD(R&E), the Director of the NSA's Cyber Security Directorate declined the designation of the NSA as a co-lead for the quantifiable assurance method. The Director of the NSA's Cyber Security Directorate further stated that the decision to decline was because [REDACTED]

According to OUSD(R&E) and NSA officials, on August 9, 2021, the NSA sent the OUSD(R&E) a resource estimate with the scope and cost required for the NSA to support hardware analysis and assurance guidance activities for the quantifiable assurance method in a supporting role.

(U) Naval Surface Warfare Center-Crane Division Support to Quantifiable Assurance Method Efforts

~~(U)~~ The NSWC-Crane Division has a standard operating procedure that defines the requirements for receiving and fulfilling hardware assurance support requests (tickets from the ticketing portal) in support of the quantifiable assurance method. Additionally, as discussed earlier in the report, the NSWC-Crane Division is using the RAMP and SHIP prototype test procedures for the quantifiable assurance method. The RAMP and SHIP prototype projects facilitate the rapid development of integrated circuit hardware and the development of heterogeneous integration technology. We reviewed contract status updates for the NSWC-Crane Division's RAMP and SHIP prototype projects that were awarded in late 2020 and 2019 respectively and determined they were meeting their scheduled milestones. According to a presentation provided to us by the former OUSD(R&E) Principal Director of Microelectronics in January 2021, the OUSD(R&E) expects that [REDACTED]

²⁸ (U) The DoD FY 2021 Budget Estimates, "Office of the Secretary of Defense Defense-Wide Justification Book Volume 3 of 5, Research, Development, Test & Evaluation, Defense-Wide," February 2020; Program Element 0604294D8Z / Trusted and Assured Microelectronics.

(CUI) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

- (CUI) [REDACTED]
[REDACTED]
- (CUI) [REDACTED]
[REDACTED]
[REDACTED]
- (CUI) [REDACTED]
[REDACTED]

(CUI) [REDACTED]
[REDACTED]
[REDACTED]

(U) National Security Agency Declines Designation of Co-Lead for the Quantifiable Assurance Method, but Will Continue to Support Quantifiable Assurance Efforts

(CUI) The OUSD(R&E) designated the NSWC-Crane Division and the NSA as the two co-leads for the quantifiable assurance method; however, the Director of the NSA's Cyber Security Directorate declined the designation of the NSA as a co-lead for quantifiable assurance. The NSA's decision to decline the co-lead for implementation of the quantifiable assurance method was because [REDACTED]
[REDACTED]

(CUI) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

- (CUI) [REDACTED]
- (CUI) [REDACTED]
- (CUI) [REDACTED]
- (CUI) [REDACTED]

(CUI) Furthermore, an NSA official in the Cyber Security Directorate told us that to support all four areas for the quantifiable assurance method, [REDACTED]
[REDACTED]
[REDACTED]

[REDACTED] According to OUSD(R&E) and NSA officials, the NSA provided a resource

(~~CUI~~) estimate to the OUSD(R&E) leadership on August 9, 2021, detailing the scope and cost for the NSA to support hardware analysis and assurance guidance activities for the quantifiable assurance method in a supporting role. The cost estimate only included resources for hardware analysis and assurance activities. The cost estimate did not provide for full NSA leadership and support of quantifiable assurance. [REDACTED]

(U) The OUSD(R&E) Is Developing Standards and Instructions to Implement the Quantifiable Assurance Method for Custom Microelectronics; Milestones Have Been Adjusted, but the OUSD(R&E) Continues to Make Progress

(U) As discussed earlier in this report, the NDAA for FY 2020 required the DoD to establish “trusted supply chain and operational security standards” for the purchase of microelectronics products by January 1, 2021. The OUSD(R&E) missed the January 1, 2021 deadline to establish trusted supply chain and operational security standards for the purchase of microelectronics products. However, the OUSD(R&E) is developing the standards and instructions necessary to implement a quantifiable assurance method to procure custom microelectronics. These include development and coordination of a new set of standards for DoD Custom Integrated Circuits, updates to DoDI 5200.44, and development of a new Access and Assurance for Microelectronics instruction to implement the quantifiable assurance method. However, delays in release of the draft Standard for DoD Custom Integrated Circuits reduce the time available for industry and interagency review, the development of any necessary contract clauses to collect information for attack-countermeasure analysis, and the amount of time for the program offices to adjust to the new standard prior to the January 1, 2023 implementation date for new microelectronics products and services specified in the NDAA for FY 2020.

(U) Continued Development of the OUSD(R&E) Standards for DoD Custom Integrated Circuits

(U) The OUSD(R&E) is developing standards for Custom Integrated Circuits and Field Programmable Gate Arrays to meet part of the NDAA for FY 2020 requirement.²⁹ However, as of October 2021, the coordination with other agencies

²⁹ (U) The FY 2020 NDAA requirement covers all microelectronics and services to include commercial off-the-shelf components; however, the scope of this evaluation focuses only on custom state-of-the-art microelectronics.

(U) and organizations is only partially complete and still in progress. The NDAA for FY 2020 requires that the standards are developed in consultation and coordination with the following agencies and organizations:

- (U) the Secretary of Homeland Security, the Secretary of State, the Secretary of Commerce, and the Director of the National Institute of Standards and Technology;
- (U) suppliers of microelectronics products and services from the United States, and allies and partners of the United States;
- (U) representatives of major U.S. industry sectors that rely on a trusted supply chain and the operational security of microelectronics products and services; and
- (U) representatives of the U.S. insurance industry.

(U) In order to meet the NDAA for FY 2020 requirement to develop the standards in consultation with other agencies and organizations, a senior OUSD(R&E) official for Microelectronics told us that:

- (U) industry partner feedback from the first draft Standard for DoD Custom Integrated Circuits was incorporated and completed in July 2021;
- (U) a second draft of the standards was issued to a wider DoD and industry stakeholder community in July 2021;
- (U) feedback from the second draft will be incorporated by December 31, 2021 (one year after the January 1, 2021, date required in Section 224 of the NDAA for FY 2020); and that
- (U) a third draft of the standards will be formally coordinated within the DoD and with other U.S. agencies and industry, as mandated by Congress.³⁰

(U) Continued Work on Updates to DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks

~~(CUI)~~ The OUSD(R&E) is updating DoDI 5200.44. The current version of DoDI 5200.44 requires the use of suppliers who have DMEA trusted foundry accreditation for the procurement of custom designed microelectronics. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

³⁰ (U) The OUSD(R&E) plans to develop separate standards for COTS microelectronics.

(U) Continued Work on a New DoD Instruction to Implement the Quantifiable Assurance Method: Access and Assurance for Microelectronics

~~(CUI)~~ OUSD(R&E) personnel are also drafting a new instruction, tentatively titled DoDI 5200.XX, “Access and Assurance for Microelectronics,” to ensure access to assured microelectronics, including use of the quantifiable assurance method.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

31

(U) Factors Delaying the DoD Standards for Custom Microelectronics and Other Quantifiable Assurance Policies

(U) The OUSD(R&E) Principal Director for Microelectronics is still developing the standards and instructions necessary to implement a quantifiable assurance method to procure custom microelectronics. A senior OUSD(R&E) official told us that the delays in the creation and release of the standards and instructions necessary to implement a quantifiable assurance method to procure custom microelectronics were due to the following:

- (U) the transition to the quantifiable assurance method started in earnest in July 2020 and encountered difficulties in the development and staffing of new policies by the January 1, 2021 deadline established in the FY 2020 NDAA;
- (U) the COVID-19 pandemic; and
- (U) turnover of key personnel at the OUSD(R&E) and the NSA.

(U) However, the OUSD(R&E) continues to make progress implementing a quantifiable assurance method for procuring custom microelectronics.³²

(U) Specifically, a senior OUSD(R&E) official told us that COVID-19 was one of the factors that prolonged the development of the draft Standard for DoD Custom Integrated Circuits. Furthermore, in a separate e-mail, he stated that there had been some uncertainty regarding the processes for coordinating the draft to the broader industry, which required OUSD(R&E) legal counsel to review. We interviewed a DoD Office of the General Counsel representative and confirmed that this legal concern has been resolved. A former senior OUSD(R&E) official told

³¹ (U) See Table 2 in the background section of this report for additional information on the draft “Access and Assurance for Microelectronics” instruction.

³² (U) The FY 2020 NDAA became law on December 20, 2019, and required actions across a diverse group of DoD and Federal agencies by January 1, 2021. The scope of this evaluation did not include determining whether the COVID-19 pandemic affected Congress’s timeline for implementation of actions required by the FY 2020 NDAA.

(U) us about similar process difficulties. She told us that the DoD process to issue policy is a lengthy process to coordinate and review documents, especially for the updated DoDI 5200.44, which has been in coordination and review for over a year.

(U) The Impact of Quantifiable Assurance Implementation Delays

(U) DoD and Government Accountability Office (GAO) reports and studies have stated that as a result of commercial pressures and increasing globalization, the DoD faces increased risk of not having access to U.S.-based state-of-the-art custom microelectronics sources.³³ To increase the DoD's access to state-of-the-art microelectronics, the OUSD(R&E) is developing standards and instructions to implement the quantifiable assurance method. Continued delays in the release of the draft Standard for DoD Custom Integrated Circuits and Field Programmable Gate Arrays may reduce time for industry review and the amount of time for the program offices to adjust to the new standard prior to the January 1, 2023, implementation date for new microelectronics products and services specified in the FY 2020 NDAA.

(U) As discussed earlier in the report, the JFAC Charter and the JFAC CONOPS do not account for the creation of the OUSD(R&E) Director for Microelectronics or the quantifiable assurance method. The JFAC's process for prioritizing competing demands on DoD laboratories to support both their parent agencies and the JFAC creates potential challenges for the program offices when requesting JFAC support. Additionally, the NSA leadership declined the OUSD(R&E)'s designation of the NSA as a co-lead for the quantifiable assurance method for the DoD. Therefore, the NSA's role in the quantifiable assurance method is still being determined.

³³ (U) For example, see Office of the Director for Defense Microelectronics, "Initial Report on the Independent Technical Review of the Defense Microelectronics Activity Foundry," September 28, 2020, which included an independent technical review of the DMEA in response to the findings of DoD OIG Report No. DODIG-2020-072, "Audit of DoD Hotline Allegations Concerning the Defense Microelectronics Activity," March 24, 2020 (this report is not publicly releasable). See also the prior coverage listed in Appendix A of this report.

(U) Recommendations, Management Comments, and Our Response

(U) Under Secretary of Defense for Research and Engineering Comments on the Quantifiable Assurance Method

(U) On February 18, 2022, The OUSD(R&E) Director of Defense Research and Engineering for Modernization, responding on behalf of the USD(R&E), agreed with the recommendation. The Director of Defense Research and Engineering for Modernization stated that to support the recommendation, in October 2021, the Principal Director for Microelectronics added the position of Assistant Deputy Director for Microelectronics for Assurance Standards. Additionally, the Principal Director for Microelectronics updated the strategy for quantifiable assurance policy, guidance, and standards that included feedback from the National Defense Industry Association and the DoD. The Director of Defense Research and Engineering for Modernization also provided updates in the comments on the status of the draft policies and guidance under development, as well as an updated definition for microelectronics quantifiable assurance that removed references to the ITAR.

(U) On April 21, 2022, the Deputy Under Secretary of Defense for Research and Engineering provided us with a memorandum with additional management comments that he stated are necessary to understand the potential of the quantifiable assurance method. The Deputy Under Secretary stated that it is not possible to create a plan for a transition to a quantifiable assurance methodology until such time as the methodology has been proven to effectively provide required levels of protection. According to the Deputy Under Secretary, the impacts on cost, schedule, and performance for programs of record remain to be evaluated. For the complete comments, see the Management Comments appendix at the end of this report.

(U) Our Response

(U) Regarding the Deputy Under Secretary's statement that we mischaracterized the trusted foundry model, in our report we do not discuss the effectiveness of either the trusted foundry or quantifiable assurance models. Our report focused on the DoD's transition from the trusted foundry model to the quantifiable assurance method. Furthermore, documents that OUSD(R&E) officials gave us at the outset of this evaluation stated that they would "replace outdated security protocols based on 'Trusted Foundry' with Quantitative Assurance and Microelectronics Security Standards," and that the DMEA was "managing and operating the Trusted Supplier activity which has provided a framework for evaluating trust

(U) of vendors throughout the microelectronics supply chain, but is based heavily on facility-centric evaluation criteria, rather than the current shift towards an assurance approach which seeks more of a holistic, technical methodology. DMEA created a team of engineers to help transition the organization to Quantifiable Assurance, but much of DMEA still seems focused on the older Trusted Foundry and trusted certification approach which is being phased out.”³⁴ The Deputy Under Secretary did not provide us with any documentary evidence to the contrary.

(U) Lastly, in this report we make no determination on what the DoD’s microelectronics procurement policies should be. We evaluated the status of the OUSD(R&E)’s quantifiable assurance efforts. The conclusions set forth in this report are based on the evidence provided by officials from the OUSD(R&E), the NSA, and the NSWC-Crane Division.

(U) Recommendation 1

(U) We recommend that the Under Secretary of Defense for Research and Engineering update the Joint Federated Assurance Center Charter and the Joint Federated Assurance Center Concept of Operations and develop a process to prioritize the quantifiable assurance method efforts of the supporting DoD laboratories.

(U) Under Secretary of Defense for Research and Engineering Comments

(U) The Deputy Under Secretary of Defense for Research and Engineering and the Director of Defense Research and Engineering for Modernization both agreed with the recommendation in their responses.

(U) Our Response

(U) The comments from the Deputy Under Secretary of Defense for Research and Engineering and the Director of Defense Research and Engineering for Modernization addressed the specifics of the recommendation.

(U) Therefore, the recommendation is resolved, but will remain open. We will close the recommendation once we verify that the USD(R&E) updated the JFAC Charter and JFAC Concept of Operations, or upon release of the quantifiable assurance policy, guidance, and standards.

³⁴ (U) “Joint DOD & ODNI Microelectronics Strategy Status & DOD OMB Passback Briefing,” August 27, 2020 and Office of the Director for Defense Microelectronics, “Initial Report on the Independent Technical Review of the Defense Microelectronics Activity Foundry,” September 29, 2020.

(U) Additionally, we updated the definition of quantifiable assurance used in this report to remove references to the ITAR.

(U) Recommendation 2

(U) We recommend that the Under Secretary of Defense for Research and Engineering, in coordination with the Under Secretary of Defense for Intelligence and Security, identify the resources required to support the National Security Agency's role in the threat analysis for quantifiable assurance or identify another DoD organization capable of providing the same expertise.

(U) Under Secretary of Defense for Research and Engineering Comments

(U) The OUSD(R&E) Director of Defense Research and Engineering for Modernization, on behalf of the USD(R&E), agreed with the recommendation. The Director of Defense Research and Engineering for Modernization stated that the microelectronics quantifiable assurance strategy makes assumptions that the Office of the Secretary of Defense and JFAC principals have defined JFAC roles and responsibilities and a funding strategy by June 2022. The Director further stated that the quantifiable assurance strategy is being adjusted to state that the independent assessment of risk analysis and plan may be performed by the JFAC or a Service-identified alternative.

(U) Under Secretary of Defense for Intelligence and Security Comments

(U) The OUSD(I&S) Director for Defense Intelligence, Counterintelligence, Law Enforcement, and Security, responding on behalf of the USD(I&S), agreed to collaborate with the OUSD(R&E) to ensure that Recommendation 2 is implemented. The Deputy Under Secretary of Defense for Research and Engineering also stated that he fully supported this recommendation.

(U) National Security Agency Comments

~~(CUI)~~ The NSA Cyber Security Directorate Technical Director provided informal comments to a discussion draft of this report, which stated [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(CUI) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(U) Our Response

(CUI) The comments from the Director of Defense Research and Engineering for Modernization; the Director for Defense Intelligence, Counterintelligence, Law Enforcement, and Security; and the National Security Agency addressed the specifics of the recommendation. [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED] Therefore, the recommendation is resolved, but will remain open. We will close the recommendation when we obtain and analyze the completed quantifiable assurance policy, guidance, and standards.

(U) Appendix

(U) Scope and Methodology

(U) We conducted this evaluation from October 2020 through October 2021 in accordance with the “Quality Standards for Inspection and Evaluation,” published in January 2012 by the Council of Inspectors General on Integrity and Efficiency. Those standards require that we adequately plan the evaluation to ensure that objectives are met and that we perform the evaluation to obtain sufficient, competent, and relevant evidence to support the findings, conclusions, and recommendations. We believe that the evidence obtained was sufficient, competent, and relevant to lead a reasonable person to sustain the findings, conclusions, and recommendations.

(U) This report was reviewed by the DoD Components associated with this oversight project to identify whether any of their reported information, including legacy FOUO information, should be safeguarded and marked in accordance with the DoD CUI Program. In preparing and marking this report, we considered any comments submitted by the DoD Components about the CUI treatment of their information. If the DoD Components failed to provide any or sufficient comments about the CUI treatment of their information, we marked the report based on our assessment of the available information.

(U) The scope of this evaluation focused on the DoD’s efforts to transition from a trusted assurance model to a quantifiable assurance method for acquiring custom microelectronics and included the OUSD(R&E), the NSWC-Crane Division, and the NSA. We did not evaluate the development of draft standards for non-custom or COTS microelectronics.

(U) To determine how the DoD will manage and mitigate risk in its transition from a trusted foundry model for procuring custom microelectronics to a quantifiable assurance method for procuring custom microelectronics, we used requests for information, data calls, and interviews. We obtained and reviewed laws, plans, policies, procedures, directives, and guidance on how the DoD will validate and verify microelectronics. We reviewed program performance against internal milestones. We interviewed key stakeholders on the development of quantifiable assurance policy, programs, and support.

(U) Laws and Regulations

(U) Public Law 113-66, “National Defense Authorization Act for Fiscal Year 2014,” Section 937, “Joint Federated Centers for Trusted Defense Systems for the Department of Defense,” December 26, 2013

(U) Public Law 116-92, “National Defense Authorization Act for Fiscal Year 2020,” Section 224, “Requiring Defense Microelectronics Products and Services Meet Trusted Supply Chain and Operational Security Standards,” December 20, 2019

(U) Public Law 116-283, “William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021,” Section 217, “Designation of Senior Officials for Critical Technology Areas Supportive of the National Defense Strategy,” January 1, 2021

(U) ITAR, 22 CFR 120-130, Section 121.1, “The United States Munitions List,” Category XI, “Military Electronics”

(U) Several national level microelectronics initiatives were developed during the course of this evaluation but were outside the scope of this evaluation. The following are two of these initiatives.

- (U) Potential impacts from Executive Order 14017, “America’s Supply Chains,” February 24, 2021, which directed the Secretary of Commerce to submit a report identifying risks in the semiconductor manufacturing and advanced packaging supply chains and making policy recommendations to address these risks.
- (U) Potential impacts from Section 9902 of the FY 2021 NDAA, which states that the Secretary of Commerce will establish a program to provide Federal financial assistance to private entities, a consortium of private entities, or a consortium of public and private entities to incentivize investment in facilities and equipment in the United States for semiconductor fabrication, assembly, testing, advanced packaging, or research and development.³⁵

(U) DoD Directives and Instructions

(U) DoD Directive 5137.02, “Under Secretary of Defense for Research and Engineering (USD(R&E)),” July 15, 2020

(U) DoD Instruction 5200.44, “Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN),” November 5, 2012 (Incorporating Change 3, October 15, 2018)

(U) Evidence and Documentation Reviewed

(U) To determine the extent to which the DoD has made the preparations necessary to transition from a trusted foundry model for procuring microelectronics to a quantifiable assurance method for procuring microelectronics from the commercial

³⁵ (U) Public Law 116-283.

(U) market, we reviewed current and draft policies establishing the roles of the OUSD(R&E) and other DoD Components in quantifiable assurance, such as the OUSD(R&E)'s draft standards for custom microelectronics, the current and draft DoDI 5200.44, and a new draft instruction to implement the quantifiable assurance method, as well as microelectronics roadmaps and contract status updates.

(U) Interviews Conducted

(U) We interviewed key stakeholders at the OUSD(R&E) who worked with the Trusted and Assured Microelectronics Program and the JFAC; the NSWC-Crane Division's Trusted and Assured Microelectronics Office; the NSA's Embedded Devices Solutions Office and Cyber Security Directorate; a Defense Science Board member; and the Director of the Defense Advanced Research Projects Agency to determine internal DoD Component policies, procedures, guidance, standards, technologies, risk management, and mitigation measures and to address any gaps identified during data calls.

(U) Use of Computer-Processed Data

(U) We did not use computer-processed data to perform this evaluation.

(U) Use of Technical Assistance

(U) A member of the DoD OIG Research & Engineering Division provided technical assistance to this evaluation. Specifically, the engineer reviewed the report to ensure technical accuracy and interpreted technical documents to ensure the team had an understanding of technical source documents.

(U) Prior Coverage

(U) During the last 5 years, the GAO and the DoD OIG issued five reports discussing microelectronics acquisition.

(U) Unrestricted GAO reports can be accessed at <http://www.gao.gov>. Unrestricted DoD OIG reports can be accessed at <http://www.dodig.mil/reports.html/>.

(U) GAO

(U) Report No. GAO-16-185T, "Trusted Defense Microelectronics - Future Access and Capabilities Are Uncertain," October 28, 2015

(U) The GAO determined that the DoD's access to trusted leading-edge microelectronics faced challenging consequences stemming from manufacturing costs, supply chain globalization, and market trends, creating uncertainty regarding future access about U.S.-based microelectronics sources.

(U) Report No. GAO-21-145, “GPS Modernization - DoD Continuing to Develop New Jam-Resistant Capability, But Widespread Use Remains Years Away,” January 19, 2021

(U) The GAO reviewed the U.S. Air Force’s two MGUE programs, including access to trusted and export compliant microelectronics.

(U) DoD OIG

(U) Report No. DODIG-2020-072, “Audit of DoD Hotline Allegations Concerning the Defense Microelectronics Activity,” March 24, 2020

(U) The DoD OIG determined that the DMEA generally resolved customer requests for microelectronics using the Advanced Reconfigurable Manufacturing for Semiconductors (ARMS) facilities. The DoD OIG recommended that the Director of Defense Research and Engineering for Research and Technology and OUSD(R&E) complete an assessment of the use of the existing foundry and determine whether the existing foundry is still needed.

(U) Report No. DODIG-2020-106, “Evaluation of Security Controls for Intelligence, Surveillance, and Reconnaissance Supply Chains,” July 22, 2020

(U) This report provided recommendations regarding the DoD’s Supply Chain Resource Management Threat Analysis Center and the Defense Counterintelligence and Security Agency. This report is classified.

(U) Management Comments

(U) Under Secretary of Defense for Research and Engineering



DEPUTY UNDER SECRETARY OF DEFENSE
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

21 APR 2020

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: OIG Report Project No. D2021-DEVOSI-00300.000 "Evaluation of the Department of Defense's Transition from a Trusted Foundry Model to a Quantifiable Assurance Method for Procuring Custom Microelectronics"

The Department of Defense's (DoD) Office of the Inspector General (OIG) is issuing its report entitled "Evaluation of DoD's Transition from a Trusted Foundry Model to a Quantifiable Assurance Method for Procuring Custom Microelectronics." While the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) and the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) fully support the report's two recommendations to:

- Update the Joint Federated Assurance Center's charter and concept of operations; and
- Include coordination with the Under Secretary of Defense for Intelligence and Security;

we would like to submit a letter of concern that this report is missing important details that are critical for an accurate understanding of both the potential of the Microelectronics Quantifiable Assurance (MQA) methodology and of the DoD Trusted Foundry (TF) model.

To begin, MQA is a proposed methodology that has not been verified or validated through the design, fabrication, packaging, assembly, and testing phases of a microelectronic chip. In order to assess its potential, the OUSD(R&E)'s Trusted and Assured Microelectronics program is evaluating the MQA methodology through multiple pilot projects supported through the Rapid Assured Microelectronics Prototype (RAMP), RAMP-Commercial (RAMP-C), and State-of-the-Art (SOTA) Heterogeneous Integrated Packaging (SHIP) efforts. The data and analysis for an independent assessment of the MQA methodology is expected in the March-April 2023 timeframe. It is not possible to create a plan for a transition to the MQA methodology until such time as the methodology has been proven to effectively provide required levels of protection equal to or greater than what is currently provided by the TF model. A number of questions related to the MQA methodology, such as the impacts on cost, schedule and performance for programs of record (PORs), remain to be evaluated. The OUSD(R&E) MQA team has developed a fourth version of draft standards (or best practices) for custom integrated circuits (CICs) and field programmable gate arrays (FPGAs) and has initiated engagement with standards development organizations for draft standards related to commercial-off-the-shelf (COTS) products. These draft standards are being developed in response to section 224 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2020, *Requiring defense microelectronics products and services meet trusted supply chain and operational security*

(U) Under Secretary of Defense for Research and Engineering (cont'd)

standards, which directs the Secretary of Defense to ensure that microelectronics purchased by the Department meet applicable trusted supply chain and operational security standards by January 1, 2023.

Additionally, the OUSD(R&E) MQA team, together with the OUSD(A&S) Defense Microelectronics Activity (DMEA) team, have determined that the DoD will need secure facilities in the United States (U.S.) microelectronics ecosystem. This includes a secure layer in the foundry and pre- and post-foundry processing for International Traffic in Arms Regulations (ITAR) reasons, as well as to manufacture classified microelectronics components and systems.

The DoD OIG report also mischaracterizes the TF model. The National Security Agency (NSA) established the TF model and the associated Trusted Access Program Office (TAPO) in 2004 to provide trusted access to components used in their systems rather than recapitalize their captive integrated circuit facility. From 2005-2012, the TF provided access to State-of-the-Art (SOTA) technology nodes for NSA, the DoD, and other government agencies, keeping pace with commercial firms; however, this access temporarily stopped at the 32 nanometer (nm) technology node due to rising operating costs. Through recent arrangements, DoD's national security needs for microelectronics are being addressed through the TF model for technology nodes from 250nm down to 12nm and, to date, there is no known substitute for this capability. In summary, the TF model has proven effective over many years at supplying secure access to microelectronics for certain classes of DoD and national security systems and currently supports many of the Department's PORs. Most DoD weapons systems and platforms are heavily reliant on these technology nodes. Additionally, the TF model provides for low volume access that is critical for many programs to affordably conduct low volume prototyping and production of custom microelectronics that are subject to ITAR and other restrictive Export Administration Regulations export controls.

It is clear that even if the MQA methodology is proven successful and provides a means other than the TF model for the DoD to procure secure SOTA microelectronics, the DoD will still have a need to continue to use TFs for certain applications. The DoD will require multiple tools in its toolbox to ensure that the DoD and the United States Government writ large have access to secure sources of the microelectronics needed for critical national security systems.

Additionally, although outside the scope of the DoD OIG report, there is strong support throughout the U.S. Government for SOTA secure microelectronics manufacturing, including from the Office of Management and Budget (OMB), the National Security Council (NSC), the Office of Science and Technology Policy (OSTP), the National Economic Council (NEC), the Office of the Director for National Intelligence (ODNI), and the Department of Commerce (DOC). The DoD and the IC have led multiple discussions in the past few months to elucidate the need for secure facilities to address the joint DoD-IC national security needs. This whole of government coordination and cooperation has helped develop a strategy to address the nation's critical national security microelectronics needs for access to assured leading-edge, state-of-the-practice, and legacy microelectronics technologies.

As the DoD OIG publishes this report, we want to submit for the record that all of these stakeholders have been engaged in discussions and have reiterated the need to plan for a security

(U) Under Secretary of Defense for Research and Engineering (cont'd)

model that integrates the TF model with secure manufacturing of SOTA microelectronics. It is simply not possible to fully transition away from the TF model to an MQA methodology that itself requires at least a year more of scientific review in current and ongoing research and development programs.

OUSDR(R&E) leadership has recently formed a Red Team consisting of subject matter experts spanning reputable organizations from industry, academia, and Federally Funded Research and Development Corporations (FFRDCs) to evaluate the MQA methodology, the draft standards, the MQA pilots, reports and presentations on MQA, and feedback received from the National Defense Industry Association (NDIA) on the MQA methodology for its potential to assure microelectronics hardware for the DOD and the IC.

We appreciate the work and effort the DoD OIG has put into this evaluation and thank you for the opportunity to provide this information.

We look forward to working with Congress and the Interagency in supporting the vision, intent, and implementation of section 224 of the NDAA for FY 2020 (on which a briefing was provided to science and technology Professional Staff Members on March 16, 2022); Title XCIX of the NDAA for FY 2021—*Creating Helpful Incentives to Produce Semiconductors (CHIPS) for America Act*; and the current United States Innovation and Competition Act (USICA) of 2021 and America COMPETES Act bills' semiconductor funding provisions.



David A. Honey, PhD

Cc: Under Secretary of Defense for Acquisition and Sustainment

(U) Under Secretary of Defense for Research and Engineering (cont'd)



RESEARCH
AND ENGINEERING

OFFICE OF THE UNDER SECRETARY OF DEFENSE

3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

MEMORANDUM FOR: ASSISTANT INSPECTOR GENERAL FOR EVALUATIONS
SPACE, INTELLIGENCE, ENGINEERING, AND
OVERSIGHT

FROM: Mr. Maynard A. Holliday, Director of Defense Research and Engineering for Modernization

SUBJECT: OIG Report Project No. D2021-DEVOSI-00300.000 "Evaluation of the Department of Defense's Transition From a Trusted Foundry Model to a Quantifiable Assurance Method for Procuring Custom Microelectronics"

In response to the subject report, OUSD (R&E) Director of Defense Research and Engineering for Modernization concurs with OIG recommendations pending resolution of the comment below. OUSD (R&E) Microelectronics Modernization Office identifies that some report content does not accurately represent the current state of Quantifiable Assurance (now Microelectronics Quantifiable Assurance (MQA)).

Recommendation 1: We recommend that the Under Secretary of Defense for Research and Engineering update the Joint Federated Assurance Center Charter and the Joint Federated Assurance Center Concept of Operations and develop a process to prioritize the quantifiable assurance method efforts of the supporting DoD laboratories.

Response: OUSD (R&E) Director of Defense Research and Engineering for Modernization concurs with Recommendations 1.

Recommendation 2: We recommend that the Under Secretary of Defense for Research and Engineering, in coordination with the Under Secretary of Defense for Intelligence and Security, identify the resources required to support the National Security Agency's role in the threat analysis for quantifiable assurance or identify another DoD organization capable of providing the same expertise.

Response: OUSD (R&E) Director of Defense Research and Engineering for Modernization concurs with Recommendations 2.

Comment: International Traffic in Arms Regulations (ITAR) and ITAR-related topics are no longer a principle of MQA. We have coordinated with the DoD OIG evaluators to redact ITAR as a part of MQA. It is critical that MQA framework principles do not conflict with ITAR or other export control regulations.

Additional non-critical comments and concerns that OUSD (R&E) would like to add to the record, regarding report content in the attached OIG Response Comments document. (TAB A).

(U) Under Secretary of Defense for Research and Engineering (cont'd)

Please contact [REDACTED] if additional information is required.



Maynard A. Holliday
Director, Defense Research and Engineering for
Modernization

Attachment(s):
As stated

(U) Under Secretary of Defense for Research and Engineering (cont'd)

**DEPARTMENT OF DEFENSE INSPECTOR GENERAL DISCUSSION DRAFT
REPORT NUMBER: OIG D2021-DEV0SI-0003.000, "Evaluation of the Department of
Defense's Transition Foundry Model to a Quantifiable Assurance Method for Procuring
Custom Microelectronics"**

**Office of the Under Secretary of Defense for Research and Engineering Comments
To the Inspector General Recommendations**

DoD OIG RECOMMENDATION 1: We recommend that the Under Secretary of Defense for Research and Engineering update the Joint Federated Assurance Center Charter and the Joint Federated Assurance Center Concept of Operations and develop a process to prioritize the quantifiable assurance method efforts of the supporting DoD laboratories.

DoD OIG RECOMMENDATION 2: We recommend that the Under Secretary of Defense for Research and Engineering, in coordination with the Under Secretary of Defense for Intelligence and Security, identify the resources required to support the National Security Agency's role in the threat analysis for quantifiable assurance or identify another DoD organization capable of providing the same expertise.

RESPONSE: Office of the Director for Defense Research and Engineering for Modernization (ODDRE(M)) accepts the DoD OIG report recommendations as written, but notes that actions taken throughout the evaluation and reporting period have made substantive progress in addressing both recommendations. Specifically:

- ODDRE(M) provided draft Microelectronics Quantifiable Assurance (MQA) guidance to National Defense Industry Association (NDIA) Electronics Division members in July 2021 to support an MQA workshop held September 2021. The Principal Director (PD) for Microelectronics within ODDRE(M) requested feedback from NDIA and DoD reviewers by 1 Oct 2021. In feedback relevant to this report, reviewers expressed concerns focused on the ability of Joint Federated Assurance Center (JFAC) to handle the volume of all DoD custom microelectronics developments, MQA alignment to the JFAC charter, and a hesitation to rely on JFAC vs. service or program identified alternative expertise.
- The PD for Microelectronics added the position of Assistant Deputy Director for Microelectronics Assurance Standards on 1 October 2021. The PD for Microelectronics updated the strategy for MQA policy, guidance, and standards in November 2021 to include DoD and industry feedback. OUSD briefed the updated strategy to the NDIA Electronics Division Trust and Assurance Subcommittee on 16 Dec 2021.
- The updated strategy for MQA makes the following assumptions associated with JFAC:
 - Office of the Secretary of Defense leadership / JFAC principals have defined JFAC roles and responsibilities and funding strategy for MQA by June 2022.
 - In parallel to Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) / JFAC decision making activities, MQA is being adjusted to be executable and technically sound, independent of the specific decisions made by the leadership team, by including the following:

(U) Under Secretary of Defense for Research and Engineering (cont'd)

- Independent assessment of risk analysis and plan by may be performed by JFAC *or service identified alternative*.
 - While independent assessments are utilized as mitigation activities, there is no requirement in current draft guidance for JFAC to perform these technical assessments.
- PD for Microelectronics development of work instructions to be used to assess completeness and correctness of risk analysis and plan and perform independent assessment of design and/or mitigation efficacy at pre- and post-silicon milestones.
- JFAC recommendations for resource requirements to perform MQA related tasks commensurate to the level of component risk.

Additional ODDRE(M) comments to the report content that do not impact the recommendations are as follows:

- MQA is not intended to *replace the* Defense Microelectronics Activity (DMEA) trust accreditation as indicated in the OIG Draft Report. DMEA accredited supplier usage is credited as mitigation in MQA. MQA requires mitigations of threats in excess of those addressed by DMEA accreditation of trusted suppliers. The MQA framework enables access to microelectronics technology beyond what is currently available in the Trusted Supplier Network.
- DoDI 5200.44 re-entered formal coordination for the Washington Headquarter Service (WHS) issuance process on 21 January 2021. The current draft Instruction in coordination does not require use of the “quantifiable assurance method” but does require that programs “Use risk-based quantifiable assurance methods, processes, and procedures to ensure the integrity and confidentiality of critical custom microelectronic components designed or manufactured for the DoD, independent of the use of microelectronics-related trusted suppliers or services, consulting with the [JFAC], as appropriate.”
- ODDRE(M) updated the issuance strategy for policy and guidance for MQA.
 - A planned DoD Instruction focusing on access and assurance to microelectronics – drafted as DoDI 5200.xx – is projected to enter the WHS issuance process February 2022.
 - MQA requirements will be issued in OUSD (R&E) guidance instead of a WHS issued DoD Manual.
- The timeline for RAMP-C production has been delayed by four months due to COVID-19 impacts.
- OUSD (R&E) custom microelectronics policy and guidance is applicable to both custom integrated circuits and DoD applications for field programmable gate arrays.

(U) Under Secretary of Defense for Intelligence and Security



INTELLIGENCE
AND SECURITY

OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

March 1, 2022

MEMORANDUM FOR OFFICE OF THE DOD DEPUTY INSPECTOR GENERAL FOR
EVALUATIONS (ATTN: MR. RANDOLPH STONE)

SUBJECT: DRAFT DoD OIG REPORT-Evaluation of the DoD's Transition from a Trusted
Foundry Model D2021-DEV0SI-003.00

Thank you for the opportunity to review the Department of Defense Inspector General's (DoD IG) Draft Report No. D2021-DEV0SI-003.00, "Evaluation of the Department of Defense's Transition Foundry Model to a Quantifiable Assurance Method for Procuring Custom Microelectronics." The Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)) concurs with the report and findings as written. I&S will collaborate with the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) to ensure Recommendation #2 is implemented. My point of contract for this report is [REDACTED]

REID.GARRY [REDACTED]

Garry P. Reid
Director for Defense Intelligence
Counterintelligence, Law Enforcement,
& Security

(U) Naval Sea Systems Command



INTELLIGENCE
AND SECURITY

OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

March 1, 2022

MEMORANDUM FOR OFFICE OF THE DOD DEPUTY INSPECTOR GENERAL FOR
EVALUATIONS (ATTN: MR. RANDOLPH STONE)

SUBJECT: DRAFT DoD OIG REPORT-Evaluation of the DoD's Transition from a Trusted
Foundry Model D2021-DEV0SI-003.00

Thank you for the opportunity to review the Department of Defense Inspector General's (DoD IG) Draft Report No. D2021-DEV0SI-003.00, "Evaluation of the Department of Defense's Transition Foundry Model to a Quantifiable Assurance Method for Procuring Custom Microelectronics." The Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)) concurs with the report and findings as written. I&S will collaborate with the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) to ensure Recommendation #2 is implemented. My point of contract for this report is [REDACTED]

REID.GARRY [REDACTED]

Garry P. Reid
Director for Defense Intelligence
Counterintelligence, Law Enforcement,
& Security

(U) Acronyms and Abbreviations

ACMA	Attack-Countermeasure Analysis
AMARO	Automated Microelectronics Analysis and Reporting Optimization
ASIC	Application-Specific Integrated Circuits
CONOPS	Concept of Operations
COTS	Commercial Off-the-Shelf
DMEA	Defense Microelectronics Activity
GPS	Global Positioning System
ITAR	International Traffic-in-Arms Regulations
JFAC	Joint Federated Assurance Center
MGUE	Military Global Positioning System (GPS) User Equipment
NDAA	National Defense Authorization Act
NIPRNet	Non-classified Internet Protocol Router Network
NSA	National Security Agency
NSWC	Naval Surface Warfare Center
OUSD(R&E)	Office of the Under Secretary of Defense for Research and Engineering
RAMP	Rapid Assured Microelectronics Prototypes
SHIP	State-of-the-Art Heterogeneous Integrated Packaging
USD(R&E)	Under Secretary of Defense for Research and Engineering

(U) Glossary

(U) Attack-Countermeasure Analysis. A method to help assess risks, define mitigation approaches, and assess risks remaining after mitigation plans are implemented. Inputs to the attack-countermeasure analysis will include the program risk profile, expected threats, threat criticality, and mitigation methods.

(U) Hardware assurance. The level of confidence that microelectronics function as intended and are free of known vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system's hardware, its embedded software, or intellectual property throughout the life cycle.

(U) Microelectronics Quantifiable Assurance. The method used to quantitatively assure custom microelectronic components based on Zero Trust concepts and Attack-Countermeasure Analysis. The method consists of: 1) a quantitative risk analysis; 2) a quantitative risk plan; and 3) an evaluation by the JFAC of the quantitative risk analysis and the quantitative risk plan for completeness and correctness.

(U) Software assurance. The level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the life cycle.

CUI



CUI

Whistleblower Protection

U.S. DEPARTMENT OF DEFENSE

Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible fraud, waste, and abuse in Government programs. For more information, please visit the Whistleblower webpage at <http://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whistleblower-Reprisal/> or contact the Whistleblower Protection Coordinator at Whistleblowerprotectioncoordinator@dodig.mil

For more information about DoD OIG reports or activities, please contact us:

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

DoD OIG Mailing Lists
www.dodig.mil/Mailing-Lists/

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

CUI



DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, Virginia 22350-1500
www.dodig.mil
DoD Hotline 1.800.424.9098

CUI