HOLD UNTIL RELEASED BY THE COMMITTEE

Testimony

Before the United States House of Representatives

Committee on Armed Services

Subcommittee on Oversight and Investigations

Witness Statement of

Mr. André Gudger, Acting Deputy Assistant Secretary of Defense for Manufacturing and Industrial Base Policy

Mrs. Kristen Baldwin, Principal Deputy Assistant Secretary of Defense for Systems Engineering

Mr. Brett Hamilton, Naval Surface Warfare Center Crane Division Chief Engineer for Trusted Microelectronics

October 28, 2015

INTRODUCTION

Chairwoman Hartzler, Ranking Member Speier and distinguished members of the subcommittee, I am André Gudger, Acting Deputy Secretary of Defense for Manufacturing and Industrial Base Policy (MIBP), and I appreciate the opportunity to testify today. I am joined here by Ms. Kristen Baldwin, Principal Deputy Assistant Secretary of Defense for Systems Engineering, and Mr. Brett Hamilton, Naval Surface Warfare Center Crane.

The Department of Defense (DoD) and the Intelligence Community (IC) require uninterruptible access to state-of-the-art design and manufacturing processes to produce custom integrated circuits designed specifically for military and IC purposes. Secure communications, electronic warfare, and cryptographic applications, among other defense and IC applications, depend heavily upon high-performance semiconductors where a generation of improvement can translate into a significant force multiplier and capability advantage. Important defense technology investments and demonstrations carry size, weight, power, and performance goals that can only be met through the use of the most sophisticated semiconductor devices.

Historically, microelectronics integrity was only of concern to programs with the most stringent reliability[1] or security[2] needs. The microelectronics ecosystem was also considerably different. For example, (1) most foundries supplying parts were U.S.-owned and located in the U.S.; (2) the U.S. military was a major consumer, and thus had significant influence on the industry; 3) Military Specification parts were readily available, providing extra reliability margin; (4) microelectronic designs were fairly simple and could be extensively tested; and (5) hardware trojans[3] were not yet part of the lexicon.

In the past few decades, the situation has changed drastically. Today, the microelectronics foundry industry operates using a global supply chain that supports continuous foundry operations. Advanced factories rely on the extremely large volumes of product required by the fast paced commercial mobile communications and consumer electronics sectors. These commercial technologies have a technology refresh cycle that is a small fraction of a major weapon system's development or recapitalization cycles. For example, by the time a major DoD system is typically fielded, the semiconductor technology embedded in the system is often several generations behind the products being produced by the manufacturer. DoD/IC program volumes are also typically in hundreds to thousands of parts versus the sometimes millions to hundreds of millions of parts that are demanded by commercial industries. Advanced microelectronics are extremely complex with extensive use of third-party intellectual property (IP). Often, the designer has little knowledge about the IP's pedigree. Finally, there has been an alarming increase in the number of academic publications discussing the implementation of hardware trojans[4].

Microelectronics hardware provides the "root-of-trust" for many DoD and IC systems. It is absolutely critical that this hardware be both trustworthy and reliable to perform, as designed, when needed. This is a critical national issue as trustworthy microelectronics hardware is also

[1] Space-based applications and strategic weapons are two example applications

[2] Secure communications, particularly involving cryptography

[3] A hardware Trojan is a malicious modification to an integrated circuit.

[4] Whitepaper "Open Source Hardware Trojan Research", Brett Hamilton et al. (classified)

prevalent in many vital areas of the global economy, such as the energy, transportation, banking, and commerce industries.

All of these factors are major contributors to the need to address microelectronics integrity and define the nature of the hardware assurance and software assurance capabilities needed to assure DoD and IC system components. For the past several years, the Department has implemented immediate and enduring actions to address this need as part of the DoD Trusted Defense Systems Strategy. Recently, the Department established a Joint Federated Assurance Center (JFAC) to coordinate hardware assurance and software assurance capabilities and support to programs. In light of the recent sale of the IBM Trusted Foundry to GlobalFoundries (GF), the Department is working to set a long-term strategy in place to ensure access to trusted state-of-the-art microelectronics.

THE MICROELECTRONICS INDUSTRY

The global semiconductor industry is a key growth sector in the global economy with more than $330B in sales in 2014. The U.S. semiconductor industry dominates 50 percent of the global market share. However, the commercial mobile communications and consumer devices markets drive the dynamics of this multi-billion dollar industry in a way that presents distinct challenges to the DoD and U.S. commercial industry.

DoD relies upon the innovation and commercialization of U.S. semiconductor manufacturers' technologies to maintain a healthy industrial base supply for its systems. The escalating cost of investment for innovation in this industry is the single biggest factor facing U.S. commercial suppliers wrestling with the decision to either join forces with other cash-rich entities to afford the necessary billion-dollar, state-of-the-art fabrication facilities, or simply quit the costly manufacturing business altogether. Today, there are a dwindling number of domestic microelectronics manufacturers that the Department can rely on for assured access to support U.S. national security requirements.

At the very leading edge of technology, only four companies in the world provide products to the global market: Taiwan Semiconductor Manufacturing Company in Taiwan, United Arab Emirates owned Global Foundries in New York, Samsung Semiconductor in Texas, which is wholly owned and closely managed by Korea, and Intel Corporation in Oregon, Arizona, and Ireland. The Department sees this as a significant risk to assured supply of the most advanced microelectronics for defense systems and platforms that must remain technologically superior to our adversaries. The Department is engaging companies across the technology spectrum to get an understanding of potential recommendations that would bolster the U.S. microelectronics industrial base, and in turn, offer DoD more options to secure microelectronics that are imperative to U.S. technological dominance for years to come.

The DoD, with its less than 1% market share, has minimal influence over the semiconductor industry. The semiconductor industry is a very capital- and Research and Development (R&D)-intensive industry, with suppliers often producing new manufacturing facilities housing next generation technology roughly every two years. Each new reduction in the size of chips requires a new, more expensive foundry, which drives the need for large volumes to take advantage of economies of scale and realize the required chip yields.

In order for the DoD's military capabilities to remain state-of-the-art, the Department is working new approaches to microelectronics trust that will allow more flexibility in the incorporation of advanced technologies. In addition, the Department is using industrial base analysis to identify key industry players with whom to partner.

MICROELECTRONICS TRENDS

The DoD is tracking trends that contribute to the ability of the Department to access needed microelectronics technologies. Some key trends include the remaining technology advancement down the path of Moore's law, the reliance upon Field-Programmable Gate Arrays (FPGA) and other types of programmable devices, as well as innovations in microelectronics integration technologies and advanced packaging.

Global competitive pressures continue to drive the pursuit of transistor scaling, i.e., advancement of Moore's law. The current, most advanced microcircuit production technology is the 14nm generation. GF, Intel, and Samsung each have commercial 14nm foundries in the U.S. The next technology generation (10nm) is expected to be in volume production in 2017 and scaling is predicted to continue for another generation or two. Scaling of transistors generally leads to increased functionality and performance of microelectronics subsystems so there will likely always be some defense interest in leading-edge semiconductor technology, e.g., System-On-Chip capabilities. For example, several organizations have already initiated programs to investigate both the radiation and reliability performance of 14nm technology for critical DoD/IC space and missile system applications.

As semiconductor technology has scaled, FPGAs have correspondingly increased in complexity and functionality. FPGAs are very flexible components that can be re-programmed by downloading new circuit configurations under software control. However, custom, end-use Application-Specific Integrated Circuits, which are the focus of the DoD Trusted Foundry Program, often have significant advantages over FPGAs with regard to power dissipation and speed. The DoD has been a relatively large consumer of FPGAs. The major FPGA vendors have supported the special needs of the DoD for extended temperature and reliability characterization and radiation tolerance. The FPGA market is dominated by 2 main companies, Xilinx and Altera, who account for about 90% of the total market share. Both companies have headquarters in the U.S., but are fabless, choosing to partner with external foundries for the production of their components.

Advanced packaging refers to a variety of technologies and approaches for protecting microelectronics components and for connecting them to the rest of the system. The mainstream commercial packaging industry is mainly off-shore in Asia. There are still some advanced packaging capabilities in the U.S., including some captive facilities at aerospace and defense firms. The U.S. electronics research community has been looking at ways to leverage advances in packaging and related chip integration technologies to provide greater system-level performance and security.

3D integrated circuit technologies are an emerging form of advanced packaging and are poised to enable higher performance electronics with lower power dissipation. DoD has been involved in the creation of viable 3D integration technologies and stands to benefit as these technologies are proven out and gain acceptance in non-defense applications. The field is still in flux, but the near-term 3D integrated circuit technologies are a hybrid of semiconductor processing and conventional packaging. The main DoD/IC need for now is to actively engage with the 3D integrated circuit R&D community to ensure these industrial capabilities continue to mature and remain accessible.

DoD TRUSTED DEFENSE SYSTEMS STRATEGY

The DoD Trusted Defense Systems Strategy is codified in DoD Instruction 5200.44, "Protection of Mission-Critical Functions to Achieve Trusted Systems and Networks (TSN)," November 5, 2012. It provides a strategy for acquisition programs to integrate robust systems engineering, supply chain risk management, security, counter-intelligence, intelligence, cybersecurity, software assurance, and hardware assurance (with an emphasis on microelectronics) to manage risks to system integrity and trust. In particular, DoD Instruction 5200.44 provides guidance for managing the risk that foreign intelligence or other hostile elements could exploit supply chain vulnerabilities to sabotage or subvert mission-critical functions, system designs, or critical functions and critical components.

The policy requires that these programs perform a criticality analysis to identify mission-critical functions and the supporting critical components to determine the information and communications technology that must be assessed for security risks and be protected. Critical components can be software, firmware, or hardware. DoD systems are typically comprised of numerous microelectronics components, many of which are commercial off-the-shelf products. The protection of critical components can be addressed by supply chain risk management, secure engineering designs and architectures, and other security-related countermeasures. Special attention is given to the subset of microelectronics that is custom-designed for DoD use. For these specific components, the policy requires that "In applicable systems, integrated circuit-related products and services shall be procured from a trusted supplier accredited by the Defense Microelectronics Activity (DMEA) when they are custom-designed, custom-manufactured, or tailored for a specific DoD military end use (generally referred to as application-specific integrated circuits (ASICs)."

In this context, "trusted" is the confidence in one's ability to secure national security systems by assessing the integrity of the people and processes used to design, generate, manufacture and distribute national security critical components, i.e., microelectronics. Trusted sources:

- Provide an assured "chain of custody" for both classified and unclassified integrated circuits;
- Ensure that there will not be any reasonable threats related to disruption in the supply chain;
- Prevent intentional or unintentional modification or tampering of the integrated circuits; and
- Protect the integrated circuits from unauthorized attempts at reverse engineering, exposure of functionality or evaluation of their possible vulnerabilities.

As codified in DoD Instruction 5000.02, "Operation of the Defense Acquisition System," January 7, 2015, the Department requires its acquisition programs to produce and maintain robust program protection planning throughout the acquisition life cycle. Program Protection Plans are used by programs to manage risks to warfighting capability from foreign intelligence collection; from hardware, software, and cyber vulnerability or supply chain exploitation; and from battlefield loss throughout the system life cycle. The Program Protection Plan is the primary means by which DoD is integrating assured microelectronics policy into program management, engineering, and the configuration, parts, and contract management disciplines.

DoD has made considerable progress in implementing its Trusted Defense System Strategy, to include its assured microelectronics strategy.

DOD TRUSTED FOUNDRY PROGRAM

The DMEA manages the DoD Trusted Foundry Program. This program provides the Department, as well as the National Security Agency (NSA) and other agencies, with access to the trusted state-of-the-art microelectronics design and manufacturing capabilities necessary to meet the confidentiality, integrity, availability, performance and delivery needs of U.S. Government customers. DMEA accredits suppliers as “trusted” in the areas of integrated circuit design, aggregation, brokerage, mask manufacturing, foundry, post processing, packaging/assembly, and test services. These services cover a broad range of technologies and are intended to support both new and legacy applications; both classified and unclassified. There are currently 72 DMEA-accredited suppliers covering 153 services, including 22 suppliers that can provide full-service trusted foundry capabilities.

One of the full-service trusted foundries is the GF Trusted Foundry. In addition to trust, the GF Trusted Foundry provides guaranteed access to leading-edge trusted microelectronics services for the typically low-volume needs of the government. The NSA Trusted Access Program Office (TAPO) provides oversight of the GF Trusted Foundry contracts to facilitate access to trusted services at the GF facilities in East Fishkill, NY and Burlington, VT. These contracts provide a variety of benefits, including:

- Access to leading-edge manufacturing, IP, and expertise for R&D as well as production
- Multi-project wafer runs to facilitate R&D and prototype development without a production commitment
- Access fees paid once for all U.S. Government end-users
- Enterprise design IP licenses that facilitate the reuse of commercial design IP previously licensed for use under the contract.

MANUFACTURING AND INDUSTRIAL BASE TOOLS AND ASSESSMENTS

The Department maintains awareness and conducts detailed analyses of domestic and global industry trends affecting its available capabilities. Where issues are identified, the Department leverages multiple tools and authorities to potentially help sustain or shape the microelectronics industrial base and support the advancement of new enabling capabilities that aid the Department’s Trusted Defense Systems Strategy.

TRANSACTION REVIEWS

The Department assesses proposed mergers, acquisitions, and foreign investments involving defense-related companies and acts to mitigate identified issues. DoD’s participation in the interagency merger and acquisition review processes is a tool that enables the protection of

DoD’s interests when required. The Department works cooperatively with the Department of Justice and the Federal Trade Commission on antitrust reviews of mergers and acquisitions (Hart-Scott-Rodino) and serves as a voting member on the Treasury-chaired Committee on Foreign Investment in the United States (CFIUS).

Through the CFIUS process, DoD conducts in-depth and comprehensive reviews of proposed foreign acquisitions of U.S. companies. DoD reviews several aspects of each transaction, including the importance of the firm to the U.S. defense industrial base; that is, whether it is a sole source supplier and, if so, what security and financial costs would be incurred in finding and/or qualifying a new supplier. Is the company involved in the proliferation of sensitive technology? Is the company to be acquired part of the critical infrastructure that DoD depends on to accomplish its mission? And can any potential national security concerns that are posed by the transaction be eliminated by the application of risk mitigation measures either under the Department’s own regulations, alternate existing statutory authority, or through negotiations with the companies?

China’s recent significant investment in the microelectronics industry is an example of foreign transactions that DoD is actively monitoring from a technology and market share perspective. When appropriate, DoD works with CFIUS to mitigate any concerns regarding individual transactions and their aggregate effect on the defense industrial base. The DoD defers discussion of any CFIUS consideration of specific cases to the Department of Treasury as the Chair of the CFIUS.

INDUSTRY CONSOLIDATION

Consolidation in the microelectronics industry has raised DoD concerns for assured supply for national security missions. In the past fifteen months alone, twenty-one mergers and acquisitions worth over $51 billion are pending or have been completed, including two of the top-ten largest U.S. semiconductor firms.[5]

GLOBAL FOUNDRIES ACQUISITION

In July 2015, Global Foundries purchased IBM’s U.S.-based Trusted Foundry creating concerns associated with DoD's reliance on sole-source and single-qualified IBM technology-based components, which are designed specifically for and used in many of the DoD’s Major Defense Acquisition Programs. DoD, the IC, and the Department of Energy assessed how the loss of access to the Trusted Foundry’s specialized IBM technology, IP, and R&D knowledge would disrupt their current and future national security programs. For DoD, the total cost of such loss of access would total billions to tens of billions of dollars given the research, redesign, prototyping, requalification, test and reproduction costs required to replace the required Trusted Foundry components. Operationally, the consequences of interrupting the national security programs that use these components are incalculable. Based on this assessment, the DoD determined that the top priority is continuity of supply of unique trusted products over the short- and mid-term.

Concurrently, MIBP coordinated with other elements of DoD, including the DMEA and Defense Security Service, to ensure GF could obtain the appropriate accreditations to be a DoD Trusted

[5] Bloomberg Professional Data, exported September 3, 2015.

Supplier following the transaction. DoD continues to work directly with GF as a potential key U.S.-based microelectronics supplier to the Department.

MANUFACTURING AND INDUSTRIAL BASE POLICY AUTHORITIES

As part of its mission to ensure the maintenance of a healthy defense industrial base, including in microelectronics, the Deputy Assistant Secretary for Manufacturing and Industrial Base Policy (DASD, MIBP) has a number of authorities at its disposal. These authorities support the health of the defense industrial base across the entire life cycle of DoD systems and consist of support for the development of emerging technologies, maturation of those technologies, manufacturing refinement, and effective sustainment:

- The Department is supporting the development of new areas of the industrial base and cutting-edge manufacturing technologies through initiatives such as the National Network for Manufacturing Innovation. This emerging network of manufacturing institutes leverages public-private partnerships to reduce barriers to rapid and efficient development and commercialization of new manufacturing technologies. This innovative approach can enable the DoD Trusted Defense Systems Strategy by supporting flexible hybrid electronics and integrated photonics manufacturing institutes, which deliver new manufacturing capabilities in electronics.

- MIBP oversees the DoD Manufacturing Technology program[6] which advances the development and application of advanced manufacturing technologies and processes DoD-wide. MIBP's role, through its Defense-wide Manufacturing Science and Technology program, helps to coordinate the manufacturing technology efforts of the DoD Components, which advances the DoD mission by reducing acquisition and support costs as well as manufacturing and repair cycle times across the life of DoD systems in a cost-constrained budget environment.

- Title III of the Defense Production Act, which Congress reauthorized last year, gives MIBP the ability to use special economic incentives to develop, maintain, modernize, and expand the productive capacities of domestic sources for critical components, technologies, and industrial resources essential for the execution of the national security strategy of the U.S. In the field of microelectronics, Congress has provided funds that have allowed the Department to improve industry's ability to support the DoD efforts to preserve and expand supplies of defense critical microelectronics.

- The Industrial Base Analysis and Sustainment (IBAS) fund provides the means to support critical, unique capabilities in the defense industrial base with fragile business cases, preserve critical skills for technological superiority, and maintain reliable sources of strategic materials. In the microelectronics sector, IBAS has provided critical investments in R&D and qualification testing to develop trusted foundry technologies. These technologies include focal plane arrays to meet advanced imaging requirements for the space, ground and aviation sectors, as well as radiation-hardened microelectronics, and a specialized integrated circuit approach to ensure the preservation of strategic national security systems, such as the Trident missile in high-threat environments.

[6] 10 U.S.C. § 2521.

MICROELECRONICS INDUSTRIAL BASE NEAR-TERM ASSESSMENT

The Department continually conducts rigorous analysis of global markets to ensure the U.S. industrial base remains vibrant and competitive in supporting DoD's needs. The Department is conducting a Microelectronics Industrial Base Study to develop and offer industry-derived recommendations to the Secretary on strategies to increase DoD's access to the microelectronics industrial base. The study's goal is to lay the foundation for ongoing and dynamic partnerships with key microelectronics industry players. A team of DoD subject matters experts interviewed and conducted site visits at several select microelectronics companies exchanging ideas on how the Department could pursue effective business models in the industry. The study team inventoried current capabilities, summarized the voice of industry, and is developing concrete recommendations about how the Department can engage the very expensive and commercially-driven high-tech microelectronics market place of today and beyond. At the conclusion of the study, using the amassed input from the microelectronics companies, the team will recommend sustainable commercial strategies that address the Department's various specific needs.

In addition to the Department's response to the current microelectronics industry conditions, the Department understands the need to proactively identify current and future suppliers in key markets to sustain and support the health of the industrial base. To enable effective market research and identification of our most critical suppliers and fragile sectors like that of the microelectronics industry, the DoD is deploying business intelligence tools utilizing big data principles to allow the Department to leverage the latest technologies and analysis techniques. This will allow DoD to engage proactively in the future to ensure the Department has access to commercially-driven technologies and maintains the warfighter's military advantage on the battlefield.

JOINT FEDERATED ASSURANCE CENTER

On February 9, 2015, Deputy Secretary of Defense Robert O. Work signed the charter for a new organization, the JFAC, to establish it as a joint federation of capabilities to support trusted defense system needs and the security of the Department's software and hardware. The JFAC will support program offices throughout the life cycle with software assurance and hardware assurance expertise, capabilities, policies, guidance, and best practices. The JFAC is also given responsibility for coordinating with DoD organizations and laboratories that are developing, maintaining, and offering software and hardware vulnerability detection, analysis, and remediation support. The Naval Surface Warfare Center Crane serves as the chair of the JFAC hardware assurance technical working group, and in this role, leads the coordination of the core technical laboratories across the Army, Navy, Air Force, NSA. The JFAC is also engaging with partners in our DoE national laboratories.

The Department's counterfeit detection and screening laboratories are also engaged in parts evaluation. Technical evaluations of the data from these parts are being archived in a data repository at Naval Surface Warfare Center Crane with ongoing work to apply big data analysis and search techniques. When these laboratories identify unusual or suspected maliciously modified parts, the JFAC can be utilized for a more in-depth technical analysis. The JFAC is also exploring information sharing opportunities with the IC, counter-intelligence, and law enforcement communities to provide additional insight into the amount of risk associated with particular microelectronic components. For example, the Air Force Office of Special

Investigations has made available select counterfeit microelectronics obtained through investigative liaison efforts. This counterintelligence perspective enables a more thorough assessment of the threat.

The JFAC laboratories have a long history of ensuring microelectronics integrity, including support for the Navy's Strategic Systems Program and NSA's cryptographic systems. These laboratories are unique in expertise and capabilities that address the malicious threat. These government laboratories have experience in safeguarding sensitive information relating to uncovered threats and vulnerabilities, specialized analysis techniques, and details of system use.

For example, Naval Surface Warfare Center Crane has leveraged several million dollars of Naval Innovative Science and Engineering 219 R&D funds and the Naval Sea Systems Command Capital Improvement Program funds to greatly enhance its microelectronics trust verification capabilities over the past few years. These investments also support the Navy's traditional failure analysis and high reliability microelectronics missions, which requires similar expertise and equipment. The work also supports the Navy's JFAC hardware assurance pilot program and several other programs of record in the area of trust assurance, including extensive work with Strategic Systems Program and Integrated Warfare Systems.

Access to design information is very important to the ability to cost-effectively perform independent verification of microelectronic components. If these files are delivered to the government as one of the deliverables in a contract, the time and cost to verify these components can be minimized. The term "Acquire to Verify" has been coined to promote this idea. JFAC members are compiling lessons learned from to generate a general design guide that will include best practices to support independent verification for trust assurance.

It is also critical to establish and maintain relationships with microelectronics manufacturers. This is particularly important in the case of commercial parts where the design information is held by these manufacturers. A few such relationships have been fostered by DoD organizations, and they have proven to be very beneficial to trust verification efforts.

TECHNOLOGICAL DEVELOPMENTS ON THE HORIZON

As Secretary Carter emphasized in an April 2015 lecture on DoD innovation, "The potential in leveraging commercially-driven technology is so huge, that we have to embrace it going forward." This vision requires shifting the burden of hardware assurance from policies that restrict access to the commercial sector, to technologies that enable cooperation. Technological solutions under development will reduce the need for restrictive DoD hardware assurance policies and maximize secure access to the latest commercial fabrication facilities, IP, and designs.

Ongoing research at the Defense Advanced Research Projects Agency (DARPA), Intelligence Advanced Research Projects Agency (IARPA), and other agencies focuses on long-term solutions for protecting the supply chain and for leveraging commercial capabilities. In the future, the national security customer will be able to:

- Determine the origin of an integrated circuit by analyzing unique chip features. DARPA produced a font recognition and analysis[7] tool capable of identifying chip provenance based on the characters printed on the chip and its packaging material.

- Determine the operational functionality of a section of an integrated circuit, ensuring that it performs exactly and only as specified. DARPA's Integrity and Reliability of Integrated Circuits produced an advanced scanning optical microscope (ASOM)[8] that for the first time gives information about chip construction and function by monitoring charge flow through a circuit. ASOM was successfully transitioned to Naval Surface Warfare Center Crane use.

- Authenticate a device's origin and monitor its supply chain using microscopic embedded sensors. DARPA's Supply Chain Hardware Integrity for Electronics Defense will incorporate into integrated circuit packages an inexpensive silicon chip that both detects tampering and provides for unique and encrypted identification of authentic parts.

- Rapidly design and develop new systems and switch between technology nodes and foundries. DARPA's Circuit Realization At Faster Timescales develops an object-oriented-design language to make hardware design as simple as software development. This capability will help mitigate the risks associated with loss of access to a given trusted foundry by porting to the next suitable location and maximizing the reuse of IP.

- Manufacture a device across multiple commercial locations while concealing its functionality. DARPA's Diverse and Accessible Heterogeneous Integration and IARPA's Trusted Integrated Circuit programs will disaggregate chip designs. DoD can potentially then select manufacturers for each disaggregated component without revealing the function of the completed circuit. These programs are part of a broader effort to obtain trusted devices from an untrusted facility while protecting and controlling government IP.

These and similar programs have already substantially improved tools for acquiring, analyzing, and validating the security and provenance of microelectronic components. Even as the dangers posed by counterfeiting and tampering vary, these technologies will enable more tailored risk-management approaches, enhance security, allow for broad commercial engagement, and improve access to the advanced electronics required by the DoD/IC community. Building trust through technology as opposed to solely on policy allows solutions to be dynamically tailored to the risk assessed for a given program and a given component.

CONCLUSIONS

DoD has a history of using advances in microelectronics for tactical and strategic advantage. Maximizing secure access to the latest commercial fabrication facilities, IP, and design practices is critical to further leverage new technologies. Acquiring military equipment from commercial sources in a global supply chain carries some level of risk. However, DoD is taking the steps required to ensure the reliability and integrity of our commercially-acquired microelectronics. Whereas policies that isolate the Department from commercial practices increases the risk of

[7] DARPA Foundry of Origin Program

[8] DARPA IRIS Program, http://www.darpa.mil/news-events/2014-09-30

foregoing new capabilities, providing integrity through technology will open the doors for leading-edge electronics and for new military advantages.