

[H.A.S.C. No. 114-63]

**ASSESSING DOD'S ASSURED ACCESS
TO MICROELECTRONICS IN SUPPORT OF
U.S. NATIONAL SECURITY REQUIREMENTS**

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT
AND INVESTIGATIONS

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

HEARING HELD
OCTOBER 28, 2015



U.S. GOVERNMENT PUBLISHING OFFICE

97-497

WASHINGTON : 2016

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

VICKY HARTZLER, Missouri, *Chairwoman*

JEFF MILLER, Florida
K. MICHAEL CONAWAY, Texas
JOSEPH J. HECK, Nevada
AUSTIN SCOTT, Georgia
MARTHA McSALLY, Arizona

JACKIE SPEIER, California
JIM COOPER, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
GWEN GRAHAM, Florida

HEATH BOPE, *Professional Staff Member*
MIKE AMATO, *Professional Staff Member*
MIKE CASEY, *Professional Staff Member*
SPENCER JOHNSON, *Counsel*
LINDSAY KAVANAUGH, *Professional Staff Member*
ABIGAIL GAGE, *Clerk*

CONTENTS

	Page
STATEMENTS PRESENTED BY MEMBERS OF CONGRESS	
Hartzler, Hon. Vicky, a Representative from Missouri, Chairwoman, Subcommittee on Oversight and Investigations	1
Speier, Hon. Jackie, a Representative from California, Ranking Member, Subcommittee on Oversight and Investigations	2
WITNESSES	
Baldwin, Kristen, Principal Deputy Assistant Secretary of Defense for Systems Engineering	7
Gudger, André, Acting Deputy Assistant Secretary of Defense for Manufacturing and Industrial Base Policy	6
Hamilton, Brett, Chief Engineer for Trusted Microelectronics, Naval Surface Warfare Center Crane Division	9
Mak, Marie, Director, Acquisition and Sourcing Management Team, Government Accountability Office	4
APPENDIX	
PREPARED STATEMENTS:	
Gudger, André, joint with Kristen Baldwin and Brett Hamilton	39
Hartzler, Hon. Vicky	27
Mak, Marie	29
DOCUMENTS SUBMITTED FOR THE RECORD:	
[There were no Documents submitted.]	
WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING:	
[There were no Questions submitted during the hearing.]	
QUESTIONS SUBMITTED BY MEMBERS POST HEARING:	
Mrs. Hartzler	57
Mr. Hunter	62
Mr. Wilson	60

ASSESSING DOD'S ASSURED ACCESS TO MICROELECTRONICS IN SUPPORT OF U.S. NATIONAL SECURITY REQUIREMENTS

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
Washington, DC, Wednesday, October 28, 2015.

The subcommittee met, pursuant to call, at 3:46 p.m., in room 2118, Rayburn House Office Building, Hon. Vicky Hartzler (chairwoman of the subcommittee) presiding.

OPENING STATEMENT OF HON. VICKY HARTZLER, A REPRESENTATIVE FROM MISSOURI, CHAIRWOMAN, SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

Mrs. HARTZLER. Welcome, everyone. Thank you so much for your patience and for coming today and for being here.

The Department of Defense is highly reliant on acquiring customized and commercial off-the-shelf computers, communications equipment, integrated circuits, application software, and other information communications technology to maintain its crucial advantage over our adversaries, and in support of partner nations and allies around the world.

The Department strives to develop cutting-edge technology that provides superior capabilities to the warfighter to fulfill critical mission operations. In order to achieve that goal, the Department is dependent in part on its ability to incorporate rapidly evolving leading-edge microelectronic devices into its defense systems, including technologies for which there is little or no commercial demand.

More concerning, and with increasing frequency, commercial business trends are forcing the Department and its commercial supplier base to rely on foreign-owned companies to produce some of the most advanced technology solutions.

Although the globalization of the semiconductor industry has increased the pace of technological innovation, it also raises national security concerns for the United States. The functionality of the Department's mission-critical systems and networks extensively leverages commercial, globally sourced microelectronics. However, this consequently provides state and non-state adversaries an opportunity to corrupt our supply chain.

At one end are counterfeit microelectronics, which can have detrimental performance impacts on our systems, all the way to systems specifically designed to introduce malicious code into the supply chain and otherwise gain illicit access to the Department's military systems and networks.

In 2003, the Defense Science Board Task Force on High Performance Microchip Supply concluded that the Department had, and I quote, “no overall vision of its future microelectronics components needs and how to deal with them. Technology and supply problems are addressed as they arise. An overall vision would enable the Department to develop approaches to meeting its needs before each individual supply source becomes an emergency,” unquote.

Not until 6 years later, in 2009, and in response to legislation contained in the fiscal year 2009 National Defense Authorization Act, did the Department develop a strategy to address the issue of assured access to secure and reliable microelectronics. But even today the implementation and successful execution of that strategy is questionable, and the uncertainty of the Department’s ability to maintain military superiority in critical leading-edge microelectronics technology is in doubt by many on this committee.

Recently, the Committee on Foreign Investment in the United States approved the acquisition of IBM’s [International Business Machines] microelectronics foundry, the Department’s sole source U.S.-based supplier for leading-edge microelectronics, by a foreign-owned company. Now that the IBM is no longer available as a guaranteed source for the Department’s needs for trusted microelectronics, the Department is facing potentially alarming vulnerabilities as a consequence of relying on a sole source supplier for leading-edge microelectronics for the past 10 years.

The risk to the Department increases dramatically with the loss of IBM’s Trusted Foundry and will be further exacerbated as long as no clear solution exists for how the Department plans to mitigate this challenge. Together, we must solve the challenges confronting the Department’s assured access to trusted microelectronics in a long-term, sustainable, efficient, and most important, affordable fashion.

Today at this hearing we hope to learn more about the risks and issues confronting the Department in acquiring secure, trusted leading-edge microelectronics. And we hope to understand more about the Department’s strategy and any course corrections needed to address these issues.

But before I introduce the witnesses, I turn to the Oversight Investigation Subcommittee ranking member for her opening remarks, anything she would like to make.

[The prepared statement of Mrs. Hartzler can be found in the Appendix on page 27.]

STATEMENT OF HON. JACKIE SPEIER, A REPRESENTATIVE FROM CALIFORNIA, RANKING MEMBER, SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

Ms. SPEIER. Thank you, Madam Chair.

I would like all of us to imagine the following frightening scenario: Hostilities in the South China Sea are at their peak, the U.S. Navy has formed a blockade around disputed islands, and alarms sound on the bridge of one of our ships. There are aircraft approaching our blockade when suddenly all the monitors on the bridge go dark.

Why is this happening? Well, in our hypothetical story, because the semiconductor manufacturers who created parts for the ship’s

radar system was based in China, and 5 years earlier the Chinese Army had placed a kill switch in our radar. We have just lost the war without ever firing a shot.

This is a stark example, but it is entirely possible. As our reliance on microelectronics grows and the world's production of these components continues its overwhelming shift to Asia, the risk grows right alongside it.

We must be acutely aware that production of these components overseas is a critical vulnerability for the United States. It allows our adversaries an opportunity to corrupt critical infrastructure and introduce malicious code, greatly increases the loss of intellectual property, and it could cut off our access to critical technologies or disrupt supply.

We know that our adversaries are committed in their effort to counter, copy, or kill our weapons and target our technological edge. We should not make it easy for them. We should also be doing everything we can to harness the innovative power of technology companies right here in the United States so that we can pull ourselves back ahead of the curve on this issue.

As the microelectronics production migrates to Asia, we should be investing in the work of capable entrepreneurs and researchers, like those in Silicon Valley, to ensure they develop future technologies that will give us assured access to alternative trusted sources of leading-edge components.

Hardware is an especially critical part of this puzzle. Compared with software, hardware vulnerabilities are harder to detect, more destructive, and harder to repair.

Integrated circuits in microelectronics are used in everything from cruise missiles to drones and classified computer systems. Building a kill switch into a computer chip could mean embedding as few as 1,000 transistors hidden throughout the hundreds of millions that are already in the original design. It could shut down a radar system, steer a missile off course, or cause an airplane engine to fail catastrophically.

The steps we have already taken, such as establishing the Trusted Defense System Strategy, the Trusted Access Program, and the Trusted Foundry Program, are critical. But we must do more. We have to figure out a way to stay ahead of this threat and provide the Department of Defense and the intelligence community with a stable domestic supply chain while maintaining a leading edge on microelectronic devices that have no commercial demand.

We must also do more to collaborate with the private sector and develop innovative ways around this problem. Technology innovators throughout my district push the envelope of what is possible every day. But as we all know too well, pushing the envelope inside the halls of the Pentagon often takes time, too much time.

I look forward to hearing from our witnesses and their analyses of future technological developments and the current progress towards ensuring access to trusted mission-critical microelectronics.

And I would like to thank Mrs. Hartzler for holding this hearing today, and I yield back.

Mrs. HARTZLER. Thank you, Ranking Member Speier.

Our witnesses with us today are Ms. Marie Mak from the Government Accountability Office [GAO]. And she is the Director of the

Acquisition and Sourcing Management Team for GAO. Mr. André Gudger from the Office of the Secretary of Defense. He is the Acting Deputy Assistant Secretary of Defense for Manufacturing and Industrial Based Policy. Ms. Kristen Baldwin, also from the Office of the Secretary of Defense. And she is the Principal Deputy Assistant Secretary of Defense for Systems Engineering. And Mr. Brett Hamilton, a government representative of the United States Navy. He is the Chief Engineer for Trusted Microelectronics in the Flight Systems Division of the Global Deterrence and Defense Department at the Crane Division of the Naval Surface Warfare Center located in Crane, Indiana.

So thank you all for being with us today. And we will now begin with our opening statements.

So, Ms. Mak, we will begin with you as soon as you are ready to proceed. Thank you.

STATEMENT OF MARIE MAK, DIRECTOR, ACQUISITION AND SOURCING MANAGEMENT TEAM, GOVERNMENT ACCOUNTABILITY OFFICE

Ms. MAK. Thank you. Good afternoon, Chairwoman Hartzler, Ranking Member Speier, and members of the subcommittee. Thank you for inviting me here today to discuss GAO's work on DOD's [Department of Defense's] effort to provide access to trusted leading-edge microelectronics.

DOD's ability to provide superior capabilities to the warfighter is dependent in part on its ability to incorporate rapidly evolving leading-edge microelectronic devices into its defense systems while balancing national security concerns. However, market trends have created challenges for DOD. Increasing capital costs to make and produce these devices can be several billion dollars annually. This has resulted in increased specialization and consolidation by industry.

Once dominated by domestic sources, microelectronics manufacturing is now largely conducted outside the U.S., primarily in Asia, and largely focused on high-volume production and short life cycles driven by demand for customer electronics. In contrast, DOD requirements for microelectronics tend to be low volume, with unique requirements, that generally are needed for very long periods because weapon systems are often sustained over decades.

My statement today largely leverages off of our April 2015 sensitive but unclassified report on this topic. The two areas that I would like to highlight today are, first, the implementation of the Trusted Supplier Program, and, second, the extent the Trusted Supplier Program provides for DOD's current and future access to leading-edge trusted microelectronics.

DOD developed the Trusted Supplier Program as part of its overall Trusted Defense System Strategy. This strategy focuses on assessing DOD programs for their vulnerabilities and developing policies for requiring trust, meaning all the people and processes used to design, manufacture, and distribute national security critical components must be assessed for integrity. In 2006, DOD began expanding the number of trusted suppliers through an accreditation process, but only one had the capabilities to provide leading-edge technologies that meet their needs.

Despite DOD's efforts to expand the number of trusted suppliers, it did not address alternative sources for leading-edge microelectronics. It largely focused on two elements of risk: integrity, keeping malicious content out, and confidentiality, keeping critical information from getting out. However, the strategy did not address the risk of relying on a single supplier, leading to DOD's dependence on it for over a decade. As a result, DOD is currently in a situation where, potentially, there are no good answers to address the "what now?" question.

And that brings me to my second point: DOD's current and future access to leading-edge trusted microelectronics. Over 10 years ago, a Defense Science Board Task Force stated that the pace of these technologies being manufactured offshore was alarming due to its strategic significance to the U.S. economy and DOD's ability to maintain a technological advantage, and concluded at that point that urgent action was needed.

DOD sought to mitigate this risk by awarding a contract to the only U.S.-owned corporation that could meet DOD's needs for trusted leading-edge microelectronics. Yet relying on this single supplier all this time created uncertainty regarding current and future access and its capabilities. In July 2015, the single provider transferred its microelectronics fabrication business to a U.S.-based foreign-owned entity, resulting in increased uncertainties about DOD's access.

Our work this past year found that in the short term, DOD has no alternatives to the leading-edge microelectronics. As a result, there are risks for the DOD programs that use these technologies.

For the longer term, we reviewed various options, including ongoing research and the possibility of a government-owned fabrication facility, the details of which are sensitive and therefore cannot be discussed in this forum. However, I would be happy to discuss them at a later time at your convenience.

But the bottom line is that not only is the U.S. reliant on a single provider, it now faces the unknown risk of relying on one that is foreign owned. DOD is in a position where it faces some very difficult and complex decisions with potentially significant costs and national security implications.

Microelectronics is just the latest of several defense industrial base issues. Other examples include rare earth materials, specialty metals, and counterfeit parts. We need an industrial base strategy that is much more proactive and less reactive.

Chairwoman Hartzler, Ranking Member Speier, members of the subcommittee, this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

[The prepared statement of Ms. Mak can be found in the Appendix on page 29.]

Mrs. HARTZLER. Thank you, Ms. Mak. That was very informative. So, Mr. Gudger, you are now recognized for your opening statement.

STATEMENT OF ANDRÉ GUDGER, ACTING DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR MANUFACTURING AND INDUSTRIAL BASE POLICY

Mr. GUDGER. Thank you. Madam Chairwoman Hartzler, Ranking Member Speier, and distinguished members of the subcommittee, my name is André Gudger. I am the Acting Deputy Assistant Secretary for Defense for Manufacturing and Industrial Base Policy, and I appreciate the opportunity to testify today. I am joined here to my left with Ms. Kristen Baldwin, Principal Deputy Assistant Secretary of Defense for Systems Engineering, and to her left, Mr. Brett Hamilton, Naval Surface Warfare Center Crane.

The role of the Office of Manufacturing and Industrial Base Policy is to advise the Secretary of Defense on all matters related to the defense industrial base. My office assesses proposed mergers, acquisitions, and foreign investment involving defense-related companies. Additionally, we assess the entire defense industrial base, make recommendations to the Secretary about its health, and then, when necessary, utilize DOD authorities to advance, sustain, shape, and support the industrial base.

In particular, the global semiconductor industry is a key growth sector in the global economy. The U.S. semiconductor industry dominates 50 percent of the global market share. However, as technology and demand have advanced, it has driven the dynamics of this industry in a way that presents distinct challenges for DOD.

The Department relies on innovation and commercialization of the U.S. semiconductor industry to maintain a healthy industrial supply for its systems. The escalating costs of investment for innovation in this industry is the single biggest factor facing U.S. suppliers wrestling with the decision to either join forces with other cash-rich entities making the necessary billion-dollar investment or simply quit the costly manufacturing business altogether.

The DOD is less than 1 percent market share and has minimal influence over the semiconductor industry. The Department considers the dwindling number of domestic microelectronics manufacturers as a significant risk and may affect the most advanced microelectronics for the defense systems and platforms that must remain technology superior to our adversaries who are gaining traction through global industry players.

In July of 2015, GlobalFoundries purchased IBM's U.S.-based Trusted Foundry, creating concerns associated with the Department's reliance on a sole source and single-qualified IBM-based technology component. These components are designed specifically for and used in many of DOD's major defense acquisition programs.

DOD, the intelligence community, and the Department of Energy assessed how the loss of access to IBM's Trusted Foundry would disrupt their current and future national security programs. For the DOD, the total cost of loss assessed would be greater than a billion dollars. And given the research, redesign, prototyping, requalification tests, reproduction costs required to replace the required Trusted Foundry components, it is unknown. Operationally, the consequences of interrupting the national security programs that use these components are incalculable.

Based on this assessment, the Department determined that the top priority is continuity of supply for these unique trusted prod-

ucts over the short- and mid-term. Concurrently, my office coordinated with other DOD elements, including the Defense Microelectronic Activity and the Defense Security Service, to ensure GlobalFoundries could obtain the appropriate accreditations to be a DOD trusted supplier post this transaction. The Department continues to work closely with GlobalFoundries as a source for the U.S.-based defense microelectronics.

The Department continually conducts vigorous analysis of global markets to ensure the U.S. industrial base remains vibrant, competitive, and supporting all of DOD's needs. The Department's conducting a microelectronics industrial base study. The study goal is to lay a foundation for a dynamic partnership with key microelectronic industry players. A team of government experts interviewed, conducted site visits at several selected microelectronic companies, exchanging views with the Department on how we could pursue business models that would be consistent with industry.

The study both made assessments of industry current capabilities, it summarized the voice of industry, and it is making recommendations on how the Department can engage the microelectronics marketplace not just today, but beyond. At the study's conclusion, the team will recommend strategies to the Department's requirements while addressing sustainable commercial strategy for the future.

Additionally, the Department is taking steps to proactively identify our current and future critical suppliers in fragile sectors, like that of the microelectronics industry. The Department is deploying business intelligence tools utilizing big data principles to leverage the latest technologies and analysis techniques. This will allow DOD to engage proactively in the future to ensure that we have access to commercially driven technologies that maintain the military advantage on the battlefield.

I would like to thank the committee for allowing me to speak today. As you can see, the Department is focused on addressing the challenges that are stemming from domestic and global microelectronics industry trends as DOD expands its Trusted Defense System Strategy. I look forward to answering any questions that you may have. Thank you.

[The joint prepared statement of Mr. Gudger, Ms. Baldwin, and Mr. Hamilton can be found in the Appendix on page 39.]

Mrs. HARTZLER. Thank you.

Ms. Baldwin, you are now recognized for your opening statement.

STATEMENT OF KRISTEN BALDWIN, PRINCIPAL DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR SYSTEMS ENGINEERING

Ms. BALDWIN. Madam Chairwoman Hartzler, Ranking Member Speier, members of the committee, I am pleased to come before you today to testify about the Department of Defense's assured access to microelectronics.

For a number of years the Department has been on a path to implement a Trusted Defense System Strategy. Codified in policy in 2012, this strategy manages risks to our systems from foreign intelligence collection, supply chain exploitation, and battlefield loss.

DOD acquisition programs conduct program protection planning activities throughout the life cycle to mitigate opportunities for adversaries to sabotage or subvert mission-critical system functions, system designs, and critical components of our systems.

Critical components may be comprised of software, firmware, or hardware, whether specifically designed for DOD or commercially sourced. The protection of critical components is addressed through secure engineering designs and architectures, supply chain risk management practices, software and hardware assurance activities, and antitamper techniques.

Program protection planning gives special attention to application specific integrated circuits, or ASICs. For ASICs that are custom designed, custom manufactured, or tailored for specific DOD military use, DOD requires they be procured from a trusted supplier accredited by the Defense Microelectronics Activity, or DMEA. DMEA manages the Trusted Supplier Program.

DMEA accredits suppliers as trusted in the areas of integrated circuit design, aggregation, brokerage, mask manufacturing, foundry, post-processing, packaging and 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 these full-service trusted foundries is the GlobalFoundries trusted foundry.

In addition to trust, this trusted foundry provides the U.S. government guaranteed access to leading-edge trusted microelectronic services. For these leading-edge, state-of-the-art microelectronics technology needs, the Department is concerned not only with trust and protection of our designs, but also the ability to compete for access to these technologies with commercial customers who command high-volume production requirements in comparison with typical low-volume needs of the Department. The trusted foundry has served DOD and interagency needs since 2003.

Another important aspect of program protection is hardware and software assurance or the evaluation of our microelectronics components and our software to ensure they function as intended and have not been altered. Last year the Department established a Joint Federated Assurance Center, federating expertise, tools, and methods to support acquisition program hardware and software assurance needs. The Naval Surface Warfare Center at Crane serves as the chair of this federation, the Hardware Assurance Technical Working Group. In this role, Crane leads coordination of the core hardware assurance laboratories across the Army, Navy, Air Force, and NSA [National Security Agency].

Looking ahead, the Department must seek options that enable both trust and access to needed microelectronics capability from the commercial marketplace. Research is ongoing at the Defense Advanced Research Projects Agency, the Intelligence Advanced Research Project Agency, and also in our military departments, to advance technologies such as improved hardware and software assurance tools for analyzing provenance and functionality; embedded sensors that can uniquely identify and track a device and whether

any tampering has occurred; new microelectronics design techniques to enable transfer of production from one foundry to another, mitigating risk from losing access to a particular supplier; and the ability to disaggregate chip designs and manufacture sub-components in different locations.

Demonstration and transition of technologies such as these will augment the enduring foundations of program protection planning, supply chain risk management, systems security engineering, our DMEA, and the network of certified trusted microelectronics suppliers, and the federation of tools and expertise to evaluate hardware and software that are central to the Department's Trusted Systems Strategy.

Thank you very much.

[The joint prepared statement of Ms. Baldwin, Mr. Gudger, and Mr. Hamilton can be found in the Appendix on page 39.]

Mrs. HARTZLER. Thank you, Ms. Baldwin.

And now last but certainly not least, Mr. Hamilton, very excited to see your show-and-tell that you brought as well.

STATEMENT OF BRETT HAMILTON, CHIEF ENGINEER FOR TRUSTED MICROELECTRONICS, NAVAL SURFACE WARFARE CENTER CRANE DIVISION

Mr. HAMILTON. Thank you, Madam Chairwoman Hartzler, Ranking Member Speier, members of the committee. I appreciate the opportunity to come before you today to testify about our efforts related to microelectronics assurance.

So microelectronics hardware provides the root of trust for many DOD [and] intelligence community 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 prevalent in many vital areas of the global economy, such as energy, transportation, banking, and commerce industries.

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

In order to better quantify the system risk, continued technical reconnaissance is needed to enable a more proactive stance in identifying potential vulnerabilities. Threats assessments can be greatly assisted by taking advantage of the capabilities of other government agencies, such as law enforcement and the intelligence community. The JFAC is exploring information-sharing opportunities with the intelligence, counterintelligence, and law enforcement communities to provide additional insight into the amount of risk associated with particular microelectronics components.

For example, the Air Force Office of Special Investigation has made available select microelectronic components obtained through investigative liaison efforts for forensic analysis. The counterintel-

ligence perspective enables a more thorough assessment of the threat.

Microelectronics technology driven by the commercial sector is advancing at a very rapid pace. It is therefore critical that our JFAC labs establish technical capability in the area of emerging technology. For example, Naval Surface Warfare Center Crane has utilized Naval Innovative Science and Engineering R&D [research and development] opportunities and Naval Sea Systems Command capital improvement program to greatly enhance its microelectronics trust verification capabilities over the past few years.

These capability enhancements also support the Navy's traditional failure analysis and high reliability microelectronics missions which require similar expertise and equipment. The capability is currently supporting the Navy's JFAC hardware assurance pilot program and several other programs of record in the area of trusted assurance, including extensive work with the 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 and other design information 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 current and recent design efforts 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 microelectronic 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.

Not only is the semiconductor manufacturing environment evolving, but so is the threat. There is a growing concern pertaining to unauthorized remanufactured parts, often referred to as clones, which not only pose a potential malicious threat, but also reliability concerns, as very poor quality has been observed in these parts.

Finally, there has been an alarming increase in the number of academic publications discussing the implementation of hardware Trojans. Therefore, we must stay vigilant and evolve our approach to ensure trust in such a dynamic environment.

Thank you. And I welcome your questions.

[The joint prepared statement of Mr. Hamilton, Mr. Gudger, and Ms. Baldwin can be found in the Appendix on page 39.]

Mrs. HARTZLER. Thank you, Mr. Hamilton.

I would just start with you. You brought some examples there. Do you want to share a little bit about those, why you brought them, and what the implications to our hearing today?

Mr. HAMILTON. Okay. The first example that I will pass up for you to examine is a traditional microcircuit, where we actually opened up the lid so you can see what is inside. So that particular part was from an actual counterfeit investigation that we did.

So that particular part is about a 15-year-old design. It was designed in 250 nanometers. So that is the actual size of the transistors in there. State of the art now is 10 nanometer. So that particular part there has probably around a million transistors in it. The current record for the most transistors in a commercial part is a Xilinx FPGA [field programmable gate array], which has 20 billion transistors.

So Ranking Member Speier mentioned 1,000 transistors in a device. So think about trying to find 1,000 transistors out of 20 billion if someone wanted to do something bad to a part like that. So it is a technical challenge, but there is work going on to try to address this through technical means.

The second board is just a representation of a circuit board. And there was some mention of interest in 3D ICs [three-dimensional integrated circuits] and die stacking. So in this particular case, these are the individual integrated circuits on the board.

In die stacking, those individual dies are stacked on each other into one package, and it greatly enhances the density. We have been seeing these in our laboratory, especially in flash memory and devices like that for the commercial sector where they want to pack as much memory as they can into your digital camera and things like that. But this technology is starting to show up in a much broader spectrum to increase performance and help scale the technology.

Mrs. HARTZLER. What can you do maliciously with one transistor?

Mr. HAMILTON. With one transistor, you could make something fail possibly, and denial of service. That is the simplest kind of tack. So the hidden kill switch gets a lot of attention. To do something to that level, you would have to have a lot of information about the design. If you don't know much about the design and you just wanted to do something to cause random problems, intermittent failures, then a single transistor failing could potentially take that integrated circuit down.

Mrs. HARTZLER. Wow. Okay. What is next?

Mr. HAMILTON. So here is another integrated circuit. And this is an example of one without the lid opened up, and it is what is called a ball grid array. So you see the back, those little bitty solder balls?

Mrs. HARTZLER. Yes.

Mr. HAMILTON. That is placed onto the printed circuit board, and then the whole thing is heated up, and they all just make contact at one time.

That particular part, I don't remember exactly how many solder balls that has. I would say probably around 80 or 90. But there are parts now that have 1,000 of those solder balls on there. The complexity of these microelectronics is amazing.

Mrs. HARTZLER. Really is. Next?

Mr. HAMILTON. So the last example is just another circuit board, a little bit newer version. Some of the parts there have the different kinds of bonding package. That particular part also has a fan on it. A lot of our focus has traditionally been on the very critical parts. One thing important is that we have to look at this as

a system approach, and every part in the system is critical to a certain degree. Otherwise it wouldn't be in the system.

Mrs. HARTZLER. So we only have one foundry in our country that puts this together, right, the foundry that IBM had—that is now sold?

Mr. HAMILTON. So the foundry makes the integrated circuits. They make the chips.

Mrs. HARTZLER. Okay. Gotcha. Actually puts it together.

So as co-chairman of the Joint Federated Assurance Center, what challenges and risks do you assess may affect DOD's access to assured and secure microelectronics in the future?

Mr. HAMILTON. Well, that is a tough question. I think to a certain degree the purpose of JFAC is going to be to perform an independent verification of the microelectronics no matter what the source. So a lot of the parts that enter the DOD today aren't from the IBM Trusted Foundry. They are COTS [commercial off-the-shelf] parts. If you look in the Navy systems, we buy racks and racks of circuit boards that are used in the systems.

So the challenge is to come up with tools and techniques that can be used broadly across this. And that is where the working with the other communities of interest is important to help us better focus where we need to apply our limited resources to do these deep technical assessments.

Mrs. HARTZLER. Do you feel confident now that there are systems in place to be able to do an in-depth analysis of that?

Mr. HAMILTON. There are systems in place to do it on a limited basis. We actually, for some of our customers and sponsors, we have been doing this work for years. To try to spread it to the bigger DOD is a challenge because we just use so many microelectronics.

And I like to say we can't really test our way out of this problem. We can't test and screen the hundreds of thousands of microelectronics that we use in DOD. So we have to be very smart and selective where we look and understand the threat and realize that really what we are doing is a threat assessment.

We are always going to have a threat, no matter what the source. So the question is, how do we rank the threat and where do we put our resources where we think the threats are the highest or do things in the supply chain, other activities, to help reduce that threat.

Mrs. HARTZLER. Great. I have more questions, but I will come back to that and turn to Ranking Member Speier for her questions.

Ms. SPEIER. Thank you, Madam Chair.

What is driving the decline in the United States of the microelectronics industry and its migration to Asia?

Mr. GUDGER. Well, there are several factors. One is the cost. As the commercial markets are driving to newer, more state-of-the-art needs, particularly in the consumer electronics and the mobile markets, it is a costly thing to update a fab [fabrication facility]. It is north of a billion dollars. Most fabs cost somewhere between \$5 to \$10 billion to update to a state-of-the-art space that they need to be competitive globally.

So there are very few companies across the globe that can make that kind of investment and get the kind of yields they need in

order to maintain a profitable business. And so you see a decline in new entrants because the barrier is so high and you see an exit of current entrants because it is better to partner with sources globally to compete, not just domestically.

Ms. SPEIER. Any other comments?

Ms. BALDWIN. The United States is overall a net exporter of semiconductors. And so we need to understand that there are leading-edge capabilities and those foundries can take great investment to maintain and to operate. But largely, and with many of the capabilities that the Department of Defense systems, the U.S. Government systems use, as Brett mentioned, multiple types of microelectronics technologies are used in our systems. And so there is a spectrum of capabilities and production capabilities still in the United States.

And so you need to distinguish the cost of the major fabs that have gone from—over the past 10 years the number of leading-edge foundries has drawn down from then about 10 major foundries to now we have about 4. And in comparison, we have got multiple capabilities of domestic manufacturing at other state-of-the-practice nodes and other technology types.

Ms. SPEIER. Well, if we believe that this is a national security risk, which I think we could certainly make the argument that it could be, isn't it in our best interest to maintain a foundry or supplier here and do whatever is necessary to make sure that their bottom line is reasonably successful so that the manufacturing continues to be done locally?

Ms. BALDWIN. We do agree that there is a long-term need for a trusted supplier, a network of trusted suppliers, just like we have established. And we are taking action to make sure that we maintain that access.

Ms. SPEIER. So what are the actions you are taking? We have one foundry that has now been sold to a non-U.S. company and it is unclear whether or not they are going to keep manufacturing here. What are you doing to make sure that that does not get exported?

Mr. GUDGER. Well, just a couple points of clarity. There are more than one foundry in the United States, and there are more than one trusted supplier in the United States. There are over a dozen trusted suppliers in the DOD network.

Yes, it is in the U.S. interest to maintain as much of the current and legacy capability in the United States as possible. But we are also looking to make investments in the future where technology is driving which gives us a different view. And so trust network as we know it today may look much different as we design for security throughout all of our major weapon systems and how we bring a consistent way of approaching microelectronics and future technologies and innovation into those major weapon systems.

So there is a lot of programs that I use out of my office, particularly the Defense Production Act, Title III, that we have used, and we have funded many chip technology programs and made the investment, along with industry, to develop and maintain the capacity. We have used our Industrial Base Sustainment Fund to fund companies to keep design skills and engineering tradecraft moving forward. And so we will continue to look at those both as a part

of the short-term, mid-term, and long-term strategy for the United States.

Ms. SPEIER. You know there is a lot of companies that have offshored a lot of money that they would like to repatriate. And I would think this would be a great opportunity to allow companies who are so inclined to repatriate their money if it were to go to manufacturing of microelectronics, because we could make the case that it is a national security issue.

Ms. MAK, do you have any thoughts on that or any other incentives we can create for companies?

Ms. MAK. I think, like you said earlier, why it was going offshore, there are so many other countries that have industrial base strategies that include more strategic investments, that encourage critical industries and innovation, where here in the defense industrial base it is much more reactive instead of proactive. So if there is more thought in terms of why do we wait until it is a potential crisis before we actually start coming up with alternatives, then that applied in this particular case with microelectronics.

As to what DOD could do in this particular case, we tend to rely on the market to be able to figure out the best strategy. DOD has so little influence on the market when it comes to microelectronics, so this may not have been their best strategy.

I think part of the issue was when we talked about leading-edge microelectronics, there wasn't a sense of urgency when Defense Science Board first brought it up. IBM has been renewing the contract. It has been always there. DOD was addressing the risk because IBM was there. And if earlier steps had been taken to address some of the alternatives that they are considering now, we may not be in the same situation, especially when it comes to cost, because now you have all the cost that has to be addressed as soon as possible versus spread out over time.

Ms. SPEIER. All right. Madam Chair, I yield back.

Mrs. HARTZLER. Thank you.

Mr. Scott from Georgia.

Mr. SCOTT. Thank you, Madam Chair.

And you will have to forgive me. This is certainly an area that is outside of my area of expertise by a long shot.

But GlobalFoundries was owned by IBM and they sold them. Do I understand that correctly?

Mr. GUDGER. No. IBM sold part of its microelectronics business to GlobalFoundries.

Mr. SCOTT. To GlobalFoundries. Okay. All right. And GlobalFoundries has factories in many countries, Singapore and—

Mr. GUDGER. And Germany and in the State of New York.

Mr. SCOTT. And then the U.S. companies that we have left I would assume would be Intel. Who would the others be that are—

Mr. GUDGER. Yeah. There is other very good U.S.—

Mr. SCOTT. Micron.

Mr. GUDGER. Micron. We have had Freescale, Photronix. Cypress is here in the room. And there is others. I don't want to single out any one because there is so many suppliers in this area.

Mr. SCOTT. Okay. But you do have a tremendous number of suppliers, it is just that we don't have that many who are trusted suppliers. Is that where the problem is coming in?

Ms. BALDWIN. So right. If I can just categorize. The leading-edge suppliers, that was the role that the IBM and now GlobalFoundries foundry was fulfilling. Our trusted supplier network, if I can just refer to my opening statement, we have 72 that are accredited trusted now suppliers. Twenty-two of those can provide full-service foundry operations similar to what the IBM Trusted Foundry was able to provide.

Mr. SCOTT. Okay. And so in many instances when we contract with a private vendor to build a weapons system, for example, we have DOD employees that are on-site at that manufacturer to double-check and to look at quality control and make sure that there are no problems there. Are we doing that with the foundries as well, are we checking the chips once they come to us? How do we do that with regard to—are we on-site, in other words, at the foundries?

Ms. BALDWIN. No. Great question. Part of this accreditation that the Defense Microelectronics Activity does is works with these companies that are interested in becoming trusted suppliers and certifies that those companies are able to process classified information as well as unclassified information and that they possess the right checks and balances, that they can provide an assured chain of custody, that they have processes in place to ensure that there would be no threats related to disruption of the supply, that they have processes in place to prevent intentional or unintentional modification of the designs during the manufacture or the services that that supplier is providing, and that they protect the design information from any reverse engineering or other exploitation to prevent the loss of that U.S. technology.

And that is the process by which these suppliers that wish to become accredited must go through, and the DMEA inspects that capability.

Mr. SCOTT. And so for the suppliers who want to become accredited, one of the challenges with doing business with the government is that if you are a small business, it becomes such a large percentage of your volume that if you ever lose the contract it would effectively bankrupt you.

And so what is the average volume that we spend with one of these suppliers? And do we do multiyear buys or is it something where we just every 12 months we do a new contract?

Ms. BALDWIN. Right. So when we accredit one of these suppliers, these are suppliers that provide services on a regular basis to broader than just the DOD. So we basically give them sort of a seal of approval, if you will. And then many of the suppliers actually see it as a competitive advantage, you know, because they have been through this rigor, and it actually can have the effect of potentially increasing their future business space.

Mr. SCOTT. But it would take a billion dollars to build a small foundry?

Ms. BALDWIN. Correct. As you go down into the technology, as you increase the technology, as you move down the Moore's Law of these sizes of these microelectronics components that Mr. Hamilton

was describing, the cost to maintain those foundries increases exponentially. So that leading-edge foundry is the one where we were talking about, that is in the billions of dollars to maintain and operate, because in order to be able to produce the yield of microelectronics that are useable, you have to have a certain amount of production that is running through that foundry.

Mr. SCOTT. Sure.

Ms. BALDWIN. It operates 24/7. And I would just say again that the DOD and the U.S. Government orders for that don't rise to that level. We have typically low-volume orders. Which is why looking forward we need to find ways that we can—technologies, new approaches to be able to make use of more commercial sources, because that would allow us to protect our designs and our IP [intellectual property] and ensure that the microelectronics would perform as intended, but also enable us a much broader set of options so we are not narrowly focused on a sole source supplier, because we recognize that that is not a good risk posture.

Mr. HAMILTON. If I could just add one thing to that. So in this recent Chip Scale magazine, there is a chart that plotted the escalating design costs for custom ASICs manufactured at state-of-the-art technology node, which is estimated to be over \$300 million for a 10-nanometer design. This makes COTS a very appealing approach to program managers where performance is a driver, especially given the performance exhibited in commercial FPGAs, an industry that is pushing state of the art.

Basically the FPGA manufacturers are pushing state of the art, and they are using these twenty-eight 14-nanometer nodes, because they have enough volume that they can take the \$300 million design cost. The problem is there aren't that many DOD programs that can afford to put \$300 million into a single design. There are cases potentially where a common part could be used across multiple programs and then you might be able to do something like that more cost-effectively.

Mr. SCOTT. Thank you for being here. I have an appointment in my office, so I will be missing the rest of the meeting. But thank you for what you have done.

Mrs. HARTZLER. Thank you, Mr. Scott.

Ms. Graham from Florida.

Ms. GRAHAM. Thank you, Ms. Chairman. I appreciate it very much.

And thank you for you all being here today. I really appreciate it.

This is kind of scary. So I have a question. Really what I would like to know, I mean, how reliant are we on these microelectronics? What is our level of risk? It seems like there aren't many systems that aren't exposed. And I have a follow-up question after that one.

Ms. BALDWIN. So we are very reliant on microelectronics, and it is not only these ASIC chips that we have been talking about, but multiple types of microelectronics components. Mr. Hamilton just mentioned FPGAs as an example.

I think a point that I would like to make is that it takes a spectrum of risk-reduction measures. In some cases we would want to restrict where we procure that item, from only a trusted supplier. In some cases another option is to be able to evaluate the compo-

ment or the software that is contained in that component, because in an FPGA [field programmable gate array]—there are no FPGAs that are made onshore. The two major FPGA companies are U.S. companies, but they fab offshore.

But when you take a look at what the risk is of an FPGA device, that is largely in the software, because that is a reprogrammable device, which means that regardless of where I might manufacture that device, I can change the software. And so if an adversary wanted to have an effect and could get access to that software, which is all very difficult to do, but it is a real opportunity, then the threat comes in making sure that the software that is programmed on that device is assured. And so then we want to bring to bear additional software evaluation tools, and we are doing that as well.

We may also want to design our systems. I mentioned the approach of system security engineering, because we realize many of our systems do need to use commercial devices, and we absolutely do, for reasons of cost and functionality. But we are able to design our systems with architectures in a way that we don't use those commercial components necessarily in sort of the core or heartbeat of the system, that critical portion of the system.

So the way that we approached, the way that we built this trusted system design strategy, the methodology that our programs go through and our engineers go through is to sort of decompose the system and understand the functions of that system, and then allow us to focus on what are the critical components. And then for those critical components, select from a menu of opportunities, risk-reduction opportunities, which could be procure from a certain supplier, test it through laboratories, and equipment and tools like we have assembled, or architect the system in such a way that if that component is a bad component, it will not have the overall effect to degrade the operation of the performance of the system. So we could have sensors on the system that would just shut that part of the system down. So there is a menu of options that we have.

Ms. GRAHAM. Thank you very much. That was a very thorough answer, and I really appreciate it.

Ms. MAK, you mentioned the potential of possibly bringing this within DOD. I don't want to violate any security, clearly, in an unclassified hearing. But is that, based on what Ms. Baldwin just said, is that something considering the private sector's innovation or would we be able to compete, or is this something that we are sort of tied to because of the need to have that innovation that is available in the private sector?

Ms. MAK. I think the opportunities to compete are definitely there, but let me make it clear, for the FPGAs that have been discussed, those are offshore, those are commercial uses, it is not in a trusted environment. When we are talking about leading-edge technologies that are in mission-critical defense systems, it has to be in a trusted environment, so that means the offshore companies, it doesn't even qualify. So it is going to take a lot of time and it is going to take a lot of cost.

I mean, we have talked to several major defense contractors, and their concerns were that even if there was a supplier that could meet leading edge at this point, which is not, except for IBM and

now GlobalFoundries, if it could, it would take them significant time, talking about years, and significant cost, talking at least millions, to do redesign work to be able to work with those suppliers, assuming that they exist.

Ms. GRAHAM. Okay. I am about out of time, so thank you very much. I would just say that I think the conclusion is that we just need to make sure that our public-private partnerships, that the threat level is, whether it is in the supply chain or just in general, keeping track of the threat assessment, and we are focused on that on a regular basis.

I am sorry, Ms. Chairman, I will conclude with this. My son is a computer engineer, so I understand the importance of the microelectronics. And if we are not certain that our microelectronics are secure, our system is not going to be secure.

So thank you very much. I yield back what time I don't have, Ms. Chairman.

Mrs. HARTZLER. All right. That is okay. Well said. Maybe your son can help solve this problem. So that is very good.

I wanted to go back to you, Ms. Baldwin, though. You mentioned there were 72 trusted suppliers, and that may be true, but not leading-edge suppliers. There was one, IBM, which has been sold. And so how are you going to make up for that shortfall?

Ms. BALDWIN. So we have been work looking into this situation obviously for some time now. And when you look at the types of leading-edge technologies that the IBM foundry was providing, it was over a series of technology nodes. They had a series of products that we could acquire through that one foundry. And there was no single provider that was available domestically that could replace, no one single source that could replace all of those product lines.

So finding number one is we knew we had to develop, we knew we had to take a look at a menu of options. So we are in the process of doing that right now. And we are in the process of, as has been mentioned, reaching out to the industrial base and really getting a sense of where they are going and taking all that into account.

We also want to look at the future of the economics of the situation, and we do not want—the last thing we want to do is find ourselves in a similar situation of a sole source supplier. I think long term, the types of solutions that we see as being needed in this menu are we do need to have alternative sources for critical components. We do need to have a capability to evaluate microelectronics, because of this threat, so the types of labs that we federated are a continuing need. And we do think that there are technology opportunities to maybe allow us to take a look at this problem from a different standpoint.

Some of the technologies that are being invested in right now by some of the performers that I mentioned before could potentially allow us to utilize different manufacturing sources, but still be able to protect our critical IP and our critical intellectual property and the functionality of the chip and provide that level of assurance just by the way—by these manufacturing processes and design techniques.

Or these embedded sensors that we might be able to, if the technology is demonstrated and can transition, can really provide a chain of custody, so that we could potentially use a commercial source but then have an ability to control the critical design intellectual property domestically.

And so it is these types of technologies. And so I think in summary, we see going forward that we must get out of this sole source problem that we are in right now and we must create a menu of options for the Department and its agency partners, and that is exactly what we are studying and seeking to do.

Mrs. HARTZLER. So this is happening right now, you are doing this study. You say over time—I know Mr. Gudger, you talked about doing a study that you are doing—but at this point in time our only foundry has been purchased, correct, by another—a leading-edge supplier. So we have all kinds of defense assets and platforms that are being built today.

So how vulnerable and how big a problem is this right now, because we don't have a solution today, even though we have all kinds of platforms being manufactured?

Mr. GUDGER. Today, on the short term, we are getting essentially what we were getting prior to the acquisition. Part of what we worked through the interagency process when we evaluated this very complex transaction was its national security implication and could the Federal agencies and major weapon systems still have access to the critical technologies that we needed. And on the short term, the answer was we were able to come up with an agreement, a way to work through getting the Department and getting its brother and sister agencies the current access that they had by way of trust or something very close to trust.

And that was part of the process in evaluating the acquirer's ability to become a trusted partner and, quite frankly, as Kristen said earlier, gain the halo effect to allow them to do business with the Federal Government.

So we believe in the short term that we have addressed the short-term need and issue and we can continue to get what we need today and for the foreseeable next few years, but we are working in real time on what the future will look like. And the study is to address things beyond fiscal year 2017 and what the menu of options will be.

Mrs. HARTZLER. So your study looks for beyond 2017? But until then, you feel comfortable at this point—

Mr. GUDGER. Yes.

Mrs. HARTZLER [continuing]. That we will be able to access what we need.

You mentioned, Ms. Baldwin, an accreditation process, that you are reaching out. So are you reaching out to these other suppliers and talking to them about how they can become accredited in defense-related work to become more trusted?

Ms. BALDWIN. Yes. Actually we work pretty regularly with industry associations, and several working groups have stood up. And that allows us a vehicle to communicate. So the existing trusted supplier network, we engage with regularly. And there has grown an industry consortium or working group through our National Defense Industrial Association, as an example, which is an oppor-

tunity for the Department and our agency partners and the services to meet with these industries. Yes. Thank you.

Mrs. HARTZLER. Ms. Mak, what are your thoughts on this strategy that DOD has presented for moving forward to maintain longer-term access to leading-edge microelectronics?

Ms. MAK. I agree with what Ms. Baldwin talked about in terms of a menu of options. It is pretty much like a patchwork-type approach, because what IBM offered was that wide spectrum of options to meet their needs. There are definitely trusted suppliers in the U.S., but they don't provide the leading edge. Could they get there? Potentially. It is going to cost and it is going to take time.

I would like to go back to the one question that you mentioned earlier to clarify. With respect to the short term, from our work we found that the agreements that they went through, we are not convinced that they are going to be able to provide continued access even for the next year unless there are still discussions ongoing for that. So short term, it may be a bigger issue than we are acknowledging here, I think.

Mrs. HARTZLER. Okay. Thank you.

Ms. Speier.

Ms. SPEIER. Thank you, Madam Chair.

I would like to go back in time. IBM had a 10-year contract, it had a sole source contract in a very rarefied position. Are we basically saying we didn't have a contract with them that was so ironclad that they would be required to maintain that operation in terms of providing leading-edge microelectronics as a component of that sole source contract? And why wasn't it for 30 years or 40 years? Was this a contract that was only for 10 years or was this a contract that was renewed every year so they were in a position to sell it? And they do business with us in lots of other areas, so why are we tiptoeing around this?

Mr. GUDGER. Well, I agree with you. I am in violent agreement with you. Back up. So IBM's contract was a competitive bid. What happened as a successful offerer, they became the sole supplier because they were the successful offerer on the competitive bid. It was for 10 years with 1-year options. And IBM found themselves in a very difficult place with this business, where they were losing a lot of money. I think in the last balance sheet they stated they were going to lose \$750 million a year by maintaining the capability.

And so having a contract with the U.S. Government and then forcing them to stay in business in something that they are losing money in, it is a very difficult balance. We don't have the tools and the authorities through the regulatory process, whether it is anti-trust or foreign investment, to make anyone stay in business when they are losing money.

And so they searched aggressively and they worked with GlobalFoundries to find a partner that they thought that they would still continue to need to get access from that they could have as a trusted supplier to them, not just to the Federal Government. And so I think those things went into the reason why IBM decided to exit the business and turn it over to GlobalFoundries, because they maintain a state-of-the-art facility not far from the ones that

they—GlobalFoundries, that is—not far from the ones that they acquired.

Ms. SPEIER. So when did they notify you that they were going to sell off the business?

Mr. GUDGER. I think the official notification happened in the second quarter of the calendar year of this year, that the official notification—

Ms. SPEIER. So when were you first aware? When did they first tell you they were having trouble and that they needed some work-out?

Mr. GUDGER. I am not sure on that answer. But the first that I heard about it was when they made the official announcement and filed with the interagency committee, is when it became real.

Ms. SPEIER. Well, at some point, if it was a 10-year contract, you would start negotiating a new contract in year 8, right?

Mr. GUDGER. They still had multiyears left on the contract that they were maintaining. So it wasn't a year 8—

Ms. SPEIER. I am not following you. I thought you said that it was a 10-year contract and at the end of the 10 years, they chose not—

Mr. GUDGER. No. We had just awarded the contract.

Ms. SPEIER. What?

Mr. GUDGER. Yeah. We were about 2 years into it. And I will let Kristen pick up on—

Ms. SPEIER. Wait a second. You are saying it was a 10-year contract and they were 2 years into it, and now they are not going to comply with the contract?

Ms. BALDWIN. It was a 10-year multi—it was an option year—it was a 10-year contract that was awarded with 10 option—it was a 1-year contract with 10 option years.

Ms. SPEIER. Oh, that is really smart, isn't it?

Ms. BALDWIN. There was—right.

Ms. SPEIER. So you are saying that for something as important for our national security as leading-edge microelectronics, we were awarding a 1-year contract with options to renegotiate? So we were setting ourselves up—

Ms. BALDWIN. Right.

Ms. SPEIER [continuing]. In a very bad negotiating position.

Ms. BALDWIN. That was what the offerer was willing to negotiate with the Department of Defense and that they were the—we did run a full and open competition, and they were the sole offerer.

Ms. SPEIER. I thought you said there were two.

Mr. GUDGER. No.

Ms. SPEIER. And that one went out of business or one—

Mr. GUDGER. I didn't say that.

Ms. BALDWIN. No.

Ms. SPEIER. All right. So this foundry, this building still exists, right?

Mr. GUDGER. Yes.

Ms. SPEIER. Because it cost so much money to create. This billion dollar facility exists?

Mr. GUDGER. Yes. Essentially, though, the two facilities that GlobalFoundries had acquired through this process still exist today and they still produce the products that the U.S. Government

needs. It is just owned by a different company, GlobalFoundries. Many of the same processes, the same people are there. They acquired the assets from IBM.

Ms. SPEIER. All right. I yield back.

Mrs. HARTZLER. Thank you.

And we are taking votes, so you have the last question.

Ms. GRAHAM. No. Thank you. I have no questions.

Mrs. HARTZLER. So we very much appreciate you being here. This has been very enlightening, very concerning at the same time, but certainly raises the issue of how we need to address this for our national security. And I appreciate your efforts, all of you, to help in this endeavor as we move forward. So thank you so much for being here.

And this will conclude our hearing.

[Whereupon, at 4:56 p.m., the subcommittee was adjourned.]

A P P E N D I X

OCTOBER 28, 2015

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

OCTOBER 28, 2015

**Opening Remarks of Chairwoman Vicky Hartzler
Subcommittee on Oversight & Investigation Hearing
“Assessing DOD’s Assured Access to Micro-Electronics in Support of U.S.
National Security Requirements”
October 28, 2015**

Welcome.

I am delighted to convene this hearing.

The Department of Defense is highly reliant on acquiring customized and commercial off-the-shelf computers, communications equipment, integrated circuits, application software, and other information communications technology to maintain its crucial advantage over our adversaries, and in support of partner nations and allies around the world. The Department strives to develop cutting edge technology that provides superior capabilities to the warfighter to fulfill critical mission operations. In order to achieve that goal, the Department is dependent, in part, on its ability to incorporate rapidly evolving, leading-edge microelectronic devices into its defense systems, including technologies for which there is little or no commercial demand. More concerning, and with increasing frequency, commercial business trends are forcing the Department and its commercial supplier base to rely on foreign owned companies to produce some of the most advanced technology solutions.

Although the globalization of the semi-conductor industry has increased the pace of technological innovation, it also raises national security concerns for the United States. The functionality of the Department’s mission-critical systems and networks extensively leverages commercial, globally sourced microelectronics. However, this consequently provides state and non-state adversaries an opportunity to corrupt our supply chain. At one end are counterfeit microelectronics, which can have detrimental performance impacts on our systems, all the way to systems specifically designed to introduce malicious code into the supply chain, and otherwise gain illicit access to the Department’s military systems and networks.

In 2003, the Defense Science Board Task Force on High Performance Microchip Supply concluded that the Department had, and I quote, “no overall vision of its future microelectronics components needs and how to deal with them. Technology and supply problems are addressed as they arise. An overall vision would enable the Department to develop approaches to meeting its needs before each individual supply source becomes an emergency”, un-quote. Not until six years later, in 2009 and in response to legislation contained in the fiscal year 2009 National Defense Authorization Act, did the Department develop a strategy to address the issue of assured access to secure and reliable microelectronics. But

even today, the implementation and successful execution of that strategy is questionable, and the uncertainty of the Department's ability to maintain military superiority in critical leading-edge microelectronics technologies is in doubt by many on this committee.

Recently, the Committee on Foreign Investment in the United States, approved the acquisition of IBM's microelectronics foundry, the Department's sole-source, U.S.-based supplier for leading-edge microelectronics, by a foreign-owned company. Now that the IBM is no longer available as a guaranteed source for the Department's needs for trusted microelectronics, the Department is facing potentially alarming vulnerabilities as a consequence of relying on a sole-source supplier for leading-edge microelectronics for the past 10 years.

The risks to the Department's increases dramatically with the loss of IBM's Trusted Foundry, and will be further exacerbated as long as no clear solution exists for how the Department plans to mitigate this challenge. Together, we must solve the challenges confronting the Department's assured access to trusted microelectronics in a long-term, sustainable, efficient, and most important, affordable fashion.

Today at this hearing we hope to learn more about the risks and issues confronting the Department in acquiring secure, trusted leading-edge microelectronics, and we hope to understand more about the Department's strategy, and any course corrections needed, to address these issues.

But before I introduce the witnesses, I turn to the Oversight and Investigations Subcommittee Ranking Member for any opening remarks she'd wish to make.

United States Government Accountability Office



Testimony
Before the Subcommittee on Oversight
and Investigations, Committee on Armed
Services, House of Representatives

For Release on Delivery
Expected at 3:30 p.m., EDT
Wednesday, October 28,
2015

TRUSTED DEFENSE MICROELECTRONICS

Future Access and Capabilities Are Uncertain

Statement of Marie A. Mak, Director
Acquisition and Sourcing Management

GAO Highlights

Highlights of GAO-16-185T, a testimony before the Subcommittee on Oversight and Investigations, Committee on Armed Services, House of Representatives

Why GAO Did This Study

DOD's ability to provide superior capabilities to the warfighter is dependent, in part, on its ability to incorporate rapidly evolving, leading-edge microelectronic devices into its defense systems, while also balancing national security concerns. In April 2015, GAO issued a report based on a House Armed Services Committee provision in a bill for the Howard P. "Buck" McKeon National Defense Authorization Act (NDAA) for Fiscal Year 2015, for GAO to review the trusted supplier program. The NDAA for Fiscal Year 2009 required DOD to develop a strategy to ensure access to trusted sources of microelectronics. In response, DOD developed its Trusted Defense Systems Strategy, which included its trusted supplier program.

GAO's testimony addresses DOD's efforts to provide access to trusted leading-edge microelectronics. This testimony is based on GAO's April 2015 report on this topic and also draws on conclusions from past work on the defense supplier base issued in October 2008, as well as the February 2005 Defense Science Board Task Force on High Performance Microchip Supply and documentation and discussions with industry and DOD officials in September and October 2015. For its April 2015 report, GAO reviewed DOD's trusted supplier program and policy guidance, interviewed DOD officials, and officials from the defense and microelectronics industry. DOD's review of this report deemed some of this information as sensitive but unclassified.

View GAO-16-185T. For more information, contact Marie A. Mak, 202-512-4841, MakM@gao.gov

October 2015

TRUSTED DEFENSE MICROELECTRONICS

Future Access and Capabilities Are Uncertain

What GAO Found

In April 2015, GAO found that the Department of Defense's (DOD) 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.

- Capital costs associated with producing leading edge microelectronics increase with each new generation of technology. Leading-edge microelectronics fabrication facilities can cost several billion dollars annually and rising capital costs of manufacturing have led to increased specialization and industry consolidation.
- Once dominated by domestic sources, the supply chain for microelectronics manufacturing is a global one—primarily in Asia.
- Industry is largely focused on high-volume production driven by demand for consumer electronics. The rapidly evolving commercial microelectronics market has short life cycles, with little need to support older technologies. Conversely, DOD's needs for microelectronics are low-volume, unique, and, in some cases, for technologies for which there is no commercial demand. As a result, DOD's requirements have very little influence on the commercial market.

A decade ago, the Defense Science Board concluded that DOD had "no overall vision of its future microelectronics components needs and how to deal with them. Technology and supply problems are addressed as they arise." GAO found, in April 2015, that DOD took some efforts to address access to trusted microelectronics. For example, to address risk related to foreign sources, DOD initiated its Trusted Foundry Program (later renamed "trusted supplier program") in 2004 through an annual contract with the IBM Corporation to provide government-wide access to leading-edge microelectronics in a trusted environment. Trust is established by assessing the integrity of the people and processes used to design, generate, manufacture, and distribute national security critical microelectronics. As part of its Trusted Defense Systems Strategy, DOD expanded, through an accreditation process which includes obtaining facility and personnel security clearances, the number of trusted suppliers—which totaled 64 as of August 2014. However, none, other than IBM, offered leading-edge technologies that met DOD's needs.

In October 2014, IBM, which had been DOD's sole-source supplier for leading-edge technologies for over a decade, announced the planned transfer of its microelectronics fabrication business to GlobalFoundries—a U.S.-based, foreign-owned entity; and in July 2015, the transfer was completed. As a result, continued access by DOD to the leading-edge technologies formerly provided by IBM is uncertain. By not addressing alternative options when the Defense Science Board first raised them as urgent issues and by relying on a sole source supplier for leading-edge microelectronics, DOD now faces some difficult decisions with potentially significant cost and schedule impacts to programs that rely on these technologies, as well as national security implications.

United States Government Accountability Office

Chairwoman Hartzler, Ranking Member Speier, and Members of the Subcommittee:

I am pleased to be here today to discuss the Department of Defense's (DOD) efforts to provide access to trusted leading-edge microelectronics.¹ As we reported in April 2015, DOD's ability to provide superior capabilities to the warfighter is dependent, in part, on its ability to incorporate rapidly evolving, leading-edge microelectronic devices into its defense systems, while also balancing national security concerns.² However, market trends and globalization of the supply chain have created challenging consequences for DOD. The capital costs associated with production are increasing with each new generation of technology. Leading-edge microelectronics fabrication facilities now require initial capital costs of several billion dollars, in addition to facility operating costs, which can be another several billion dollars annually. Increasing capital costs of manufacturing have led to increased specialization and industry consolidation. Once dominated by domestic sources, microelectronics manufacturing is now largely conducted outside the United States—primarily in Asia—and largely focused on high-volume production driven by demand for consumer electronics. Further, the commercial microelectronics market has short life cycles—commercial firms move on to the latest technology rapidly and have no need to support older technologies. In contrast, DOD requirements for microelectronics are generally low-volume with unique requirements that cover a wide range of technologies, including, in some cases, technologies for which there is no commercial demand. In addition, these requirements are generally needed for long periods because weapon systems are often sustained over decades. As a result, DOD's low-volume requirements have little influence on the commercial market. According to the Defense Science Board and DOD officials, the use of foreign suppliers increases

¹Microelectronics includes various micro devices, commonly referred to as "integrated circuits," that form the basis of all electronic products. A trusted environment is required 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, and include fabrication of classified designs. Smaller feature sizes generally represent more advanced technologies and higher performance, with feature sizes of 90 nanometers or smaller generally considered leading-edge.

²GAO, *Defense Technologies: Future Access to Leading-Edge Microelectronics is Uncertain*, GAO-15-422RSU (Washington, D.C., April 15, 2015). This report was issued as "For Official Use Only" given the sensitive and proprietary information involved. Details DOD deemed sensitive and proprietary must be protected from disclosure and are not disclosed in this statement.

opportunities for adversaries to corrupt technologies and introduce malicious code, and for potential loss of national security-related intellectual property.

To mitigate vulnerabilities associated with the increasing reliance on foreign manufacturers for microelectronics and to meet low-volume government needs, DOD and the National Security Agency (NSA) initiated the Trusted Foundry Program for microelectronics in 2004. Implementation of the program included the formation of the NSA's Trusted Access Program Office, which managed a sole-source contract with the IBM Corporation—the only U.S.-based company able to meet DOD and intelligence community needs for trusted leading-edge microelectronics—to provide government-wide access to these types of microelectronics. In 2006, the Trusted Foundry Program was expanded to include firms offering mature technologies and became the “trusted supplier program.” Further, the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009 required DOD to develop a strategy to ensure access to trusted sources of microelectronics.³ In response, DOD developed its Trusted Defense Systems Strategy, which includes its trusted supplier program for providing access to critical microelectronics.

I am here today to discuss the extent that the trusted supplier program provides for DOD's current and future access to trusted microelectronics. This testimony largely leverages our April 2015 sensitive but unclassified report on DOD access to leading-edge trusted microelectronics. This statement also includes updates to information on the transfer of IBM's microelectronics business based on program documentation and discussions with industry and DOD officials that we conducted in September and October 2015. In addition, the statement draws on some conclusions from our October 2008 work on the defense supplier base, confirmed by DOD officials in 2015, and the Defense Science Board Task Force on High Performance Microchip Supply.⁴

³Pub. L. No. 110-417, § 254 (2008).

⁴GAO, *Department of Defense: A Departmentwide Framework to Identify and Report Gaps in the Defense Supplier Base Is Needed*, GAO-09-5 (Washington, D.C.: October 7, 2008). The Defense Science Board, established in accordance with the provisions of the Federal Advisory Committee Act (FACA) of 1972 (5 U.S.C., Appendix, as amended) and 41 C.F.R. 102-3.50(d), provides independent advice and recommendations on matters relating to the DOD scientific and technical enterprise.

For our April 2015 report, we reviewed DOD's trusted supplier program and policy guidance documents.⁵ We also analyzed utilization data for trusted suppliers and interviewed three of the top defense contractors based on trusted supplier utilization data. In addition, we interviewed officials in the offices of the Secretary of Defense, Defense Microelectronics Activity, NSA, Defense Advanced Research Projects Agency, Intelligence Advanced Research Projects Activity, and Institute for Defense Analysis. For further details on the scope and methodology, see our April 2015 report. We conducted the work on which this statement is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

DOD's Future Access to and Capabilities from Trusted Leading-edge Microelectronics is Uncertain

A decade ago, the Defense Science Board Task Force on High Performance Microchip Supply concluded that DOD had "no overall vision of its future microelectronics components needs and how to deal with them. Technology and supply problems are addressed as they arise. An overall vision would enable the Department to develop approaches to meeting its needs before each individual supply source becomes an emergency."⁶ In addition, the report called for the U.S. government, DOD, and its suppliers to establish a series of activities to ensure that the United States maintains reliable access to the full spectrum of microelectronics components. Moreover, it acknowledged that the pace of technology development shifting to offshore locations was alarming because of the strategic significance this technology has on the U.S. economy and the ability of the U.S. to maintain a technological advantage in DOD, government, commercial, and industrial sectors. At that time of its review, the Defense Science Board strongly recommended urgent action to be taken.

⁵GAO issued this report based on a House Armed Services Committee provision in a bill for the Howard P. "Buck" McKeon National Defense Authorization Act (NDAA) for Fiscal Year 2015. H.R. Rep. No. 113-446, at 179 (2014).

⁶Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, *Report of the Defense Science Board Task Force on High Performance Microchip Supply* (February 2005).

In April 2015, we found, as part of DOD's Trusted Defense Systems Strategy, the trusted supplier program was, and still is, a primary risk reduction technique for acquiring certain microelectronics for use in mission-critical components in DOD systems. In 2006, DOD began expanding the number of trusted suppliers to establish a trusted supply chain for mature "non-leading-edge" technologies. At that time, the Defense Microelectronics Activity, under the Office of the Secretary of Defense and in conjunction with other organizations, finalized criteria for trusted microelectronics suppliers deemed as "trusted" through an accreditation process, which included obtaining facility and personnel security clearances. As of August 2014, there were 63 other trusted suppliers in addition to IBM, including 15 with fabrication capabilities. Although these other suppliers do not have the leading-edge capabilities of IBM, they do provide access to a range of mature technologies. However, industry officials stated that use of accredited suppliers other than IBM has been minimal primarily because they do not have the same technologies available, especially at the leading edge. Despite DOD's efforts to expand the number of trusted suppliers, the Department's strategy did not address alternatives for leading-edge microelectronics. DOD's strategy focused on two critical elements of risk: integrity—keeping malicious content out, and confidentiality—keeping critical information from getting out. However, it did not address the risk of relying on a single source. For access to leading-edge trusted microelectronics, DOD's strategy since 2004 has been to rely on IBM as their sole-source provider of leading-edge trusted microelectronics.

In October 2014, IBM announced that its microelectronics fabrication business may be acquired by GlobalFoundries—a U.S.-based foreign-owned entity, subject to completion of applicable regulatory reviews. After this announcement, DOD initiated several actions to identify the risk of potential loss of access to leading-edge microelectronics and to identify and assess alternatives. By July 2015, GlobalFoundries announced that it cleared U.S. regulatory review and it completed the acquisition of IBM's microelectronics business. As a result, continued future access to the technologies formerly provided by IBM is uncertain. Our work in April 2015 reviewed potential near-term options for access to IBM foundry services, including accredited trusted suppliers other than IBM, other U.S.-owned leading-edge on-shore foundries, and offshore foundries. Although the details of this work are sensitive, based on limitations DOD and defense industry officials described to us, there are no near-term alternatives to the foundry services formerly provided by IBM. We also reviewed potential longer-term options for access, including ongoing research into verification techniques and alternative manufacturing approaches, and a possible government-owned fabrication facility, the

details of which are sensitive. However, we did note that these longer-term options all have associated risks and limitations.

As far back as our October 2008 report, and confirmed by DOD officials in 2015, we found that increasing globalization in the defense industry has intensified debate over the use of foreign versus domestic suppliers and presents uncertainty over the ability of the United States to maintain military superiority in critical technology areas. Moreover, as the defense supplier base has consolidated into a few prime contractors, competition has been reduced and single source suppliers have become more common for components and subsystems. This is definitely the case for defense microelectronics. By not addressing alternative options when the Defense Science Board first raised them as urgent issues and by relying on a sole source supplier for leading-edge microelectronics, DOD now faces some difficult decisions with potentially significant cost and schedule impacts to programs that rely on these technologies, as well as national security implications.

Chairwoman Hartzler, Ranking Member Speier, and Members of the Subcommittee, this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

**GAO Contact and
Staff
Acknowledgments**

If you or your staff has any questions about this statement, please contact Marie A. Mak at (202) 512-4841 or MakM@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Lisa Gardner, Assistant Director; Bradley Terry; Mary C. Diop; Stephanie Gustafson; Andrew Redd; Penney Harwell Caramia; Joseph Kirschbaum; Timothy Persons; and Sylvia Schatz.

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (<http://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <http://www.gao.gov> and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts and read The Watchblog. Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548



Please Print on Recycled Paper.

Marie A. Mak

Marie Mak is a Director in the Acquisition and Sourcing Management team with the Government Accountability Office (GAO). Ms. Mak leads work on a wide range of defense contract management issues and acquisitions, as well as the defense industrial base and critical technologies, designated as one of GAO's High Risk areas. Ms. Mak joined GAO in 2002 in the Defense Capabilities and Management team, conducting reviews focused largely on logistics issues and eventually managing a portfolio on national security interagency collaboration and partner capacity building, ballistic missile, and defense management issues. She serves in various stewardship activities, including GAO's recruitment and hiring efforts and leading a Continuous Process Improvement project to assist mission teams in establishing outreach priorities for Congressional clients.

Prior to GAO, Ms. Mak worked at the Naval Air Systems Command and the U.S. Coast Guard Headquarters. In the Coast Guard, she was primarily responsible for engineering oversight and coordinating resources and priorities with program managers for Coast Guard command and control systems for afloat and ashore units. She later moved into strategic planning, developing strategic plans and a performance measurements framework for the engineering logistics directorate.

Ms. Mak has received numerous GAO awards, including a Customer Service Award, Meritorious Service Award, and the John Henry Luke Mentoring Award. Ms. Mak graduated with a Bachelor of Science in Electrical Engineering with a Cooperative Education Program with the National Security Agency, from the University of Maryland, College Park in 1989. In 2001, she received a Master of Science degree in National Resource Strategy from the Industrial College of the Armed Forces, National Defense University.

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 uninterrupted 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 reliability¹ or security² 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 trojans³ 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 trojans⁴.

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 program⁶ 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.

MICROELECTRONICS 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 analysis⁷ 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.

Mr. André Gudger
Department of Defense
Deputy Assistant Secretary of Defense, Manufacturing and
Industrial Base Policy (acting)

André J. Gudger currently serves as the Deputy Assistant Secretary of Defense for Manufacturing and Industrial Base Policy (MIBP). In this role Mr. Gudger is responsible for ensuring a robust, secure, resilient, and innovative industrial base to meet the needs of the Department of Defense. Mr. Gudger supports the Office of the Secretary of Defense by providing detailed analyses and in-depth understanding of the increasingly global, commercial, and financially complex industrial supply chain essential to our national defense, and recommending or taking appropriate actions to maintain the health, integrity and technical superiority of that supply chain.

Prior to this role, Mr. Gudger served as the Director of the Office of Small Business Programs. In this role, Mr. Gudger served as the principle advisor to the Secretary of Defense on all small business matters, overseeing more than \$120 billion of annual awards to small business. During Mr. Gudger's tenure the Department of Defense met its small business prime contracting goal and its Service Disabled Veteran Owned Small Business goal for the first time in history.

Previously, Mr. Gudger worked on key technical and financial initiatives with the Federal Deposit Insurance Corporation, Union Bank of Switzerland, and AT&T. From 2003-2009, Mr. Gudger served as Chairman and Chief Executive Officer of Solvern Innovations, a corporate entity which provided acquisition support and cyber solutions through training, research, and innovation. Mr. Gudger currently serves on several boards throughout the region, including the University of Maryland Baltimore County, the Maryland BRAC Small & Minority Business Advisory Board, and the Cyber Advisory Council.

Mr. Gudger received his Bachelor of Science degree from the University of Maryland at Baltimore County and his Master in Business Administration from the University of North Carolina at Chapel Hill.

Ms. Kristen J. Baldwin
Principal Deputy
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

Kristen Baldwin is the Principal Deputy in the Office of the Deputy Assistant Secretary of Defense for Systems Engineering (ODASD(SE)). Ms. Baldwin acts on behalf of the DASD and is responsible for engineering and technical workforce, policy, and acquisition program implementation across the Department of Defense (DoD). This includes concept engineering and analysis, design, development and manufacturing, and independent program review and assessment for all DoD major weapon system acquisition programs. She supports ODASD(SE) in its role as the systems engineering workforce leader with responsibility for more than 40,000 DoD acquisition professionals. She is also overseeing the DoD's strategy for Trusted Systems Design.

A member of the Senior Executive Service, Ms. Baldwin is also the acting Director for Systems Analysis. She leads modeling and simulation activities across DoD, system assurance, program protection, systems engineering for systems of systems, and SE research and development initiatives. She oversees the DoD Systems Engineering Research Center, a University Affiliated Research Center dedicated to advancing systems engineering methods, processes, and tools, and the MITRE National Security Engineering Center, a DoD Federally Funded Research and Development Center.

Ms. Baldwin has been with OSD since 1998, where she has led the application of capabilities-based planning in the acquisition process, with a focus on the integration of requirements, acquisition, and programming processes; served as Deputy Director, Software Intensive Systems; and managed the Tri-Service Assessment Initiative. Before working with OSD, Ms. Baldwin served as a Science and Technology Advisor in the Army's Office of the Deputy Chief of Staff for Operations and Plans, and at the Dismounted Battlespace Battle Lab, Fort Benning, GA. Ms. Baldwin began her career at the U.S. Army's Armament Research, Development, and Engineering Center, Picatinny Arsenal, where she was responsible for infantry weapons and ammunition design and production.

Ms. Baldwin received a bachelor's degree in mechanical engineering from the Virginia Polytechnic Institute and a master's degree in systems management from the Florida Institute of Technology.

Mr. Brett Hamilton

Mr. Brett Hamilton is the Chief Engineer for Trusted Microelectronics in the Flight Systems Division of the Global Deterrence and Defense Department at Crane Division, Naval Surface Warfare Center, Crane, Indiana. Mr. Hamilton serves as the technical lead and subject matter expert on issues pertaining to microelectronics integrity of electronic components used in Department of Defense Weapon and Cyber Systems. His experience includes the development of advanced techniques for malicious and counterfeit circuit detection and security feature robustness evaluations. Brett holds multiple patents, and his expertise is nationally-recognized as he is routinely called upon to advise senior leadership regarding issues involving microelectronics trust and integrity issues. Brett currently serves as the Navy's technical representative supporting DASN (RDT&E) on developing a long-term mitigation strategy for insuring microelectronics integrity in the aftermath of the IBM foundry sale and as the DoD lead for the recently chartered Joint Federation Assurance Center (JFAC) for Hardware Assurance (HwA). Mr. Hamilton is also a key government team member on ONR, DARPA and IARPA programs involved in microelectronic integrity and trust.

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

OCTOBER 28, 2015

QUESTIONS SUBMITTED BY MRS. HARTZLER

Mrs. HARTZLER. You mentioned in your oral statement that DOD's Trusted Defense Systems Strategy did not address the risk of relying on a sole source provider. What more could DOD have done to prevent this situation?

Ms. MAK. DOD has been aware of the risk of using a sole source supplier for about a decade, but did not begin to take actions to assess and address this risk until late last year when IBM announced the proposed transfer of its microelectronics fabrication facilities to GlobalFoundries. Had DOD taken actions earlier, investments in alternative suppliers may have reduced the risk programs now face due to potential gaps in availability for specific technologies.

Mrs. HARTZLER. What are your thoughts on the strategy DOD has presented for moving forward to maintain longer-term access to leading-edge microelectronics?

Ms. MAK. GAO is in the process of reviewing DOD's strategy as part of our ongoing work and will report our findings in mid-2016.

Mrs. HARTZLER. For DOD programs, is the purchase of all of the integrated circuits needed for a given technology, otherwise known as making lifetime buys, a possible alternative if access to former IBM leading-edge technologies is no longer available?

Ms. MAK. Because the response involves sensitive or proprietary information, it is provided in a separate document marked "For Official Use Only//Proprietary Information Involved" and must be protected from disclosure. (Document in Committee Possession.)

Mrs. HARTZLER. What commitments has GlobalFoundries provided to the U.S. Government regarding access to the trusted leading-edge microelectronics formerly provided by IBM, including the status of the contract between the U.S. Government and GlobalFoundries?

Ms. MAK. Because the response involves sensitive or proprietary information, it is provided in a separate document marked "For Official Use Only//Proprietary Information Involved" and must be protected from disclosure. (Document in Committee Possession.)

Mrs. HARTZLER. Are other trusted suppliers able to provide technologies similar to the IBM technologies now provided through GlobalFoundries?

Ms. MAK. As GAO noted in its report GAO-15-422RSU, as of August 2014, in addition to IBM, there were 63 other trusted suppliers, including 15 with fabrication capabilities. These other suppliers do not have the leading-edge capabilities of IBM/GlobalFoundries (below 90 nanometers), but provide access to a range of mature technologies.

Mrs. HARTZLER. What will it take for other trusted suppliers to be able to provide leading-edge microelectronics needed by DOD?

Ms. MAK. Because the response involves sensitive or proprietary information, it is provided in a separate document marked "For Official Use Only//Proprietary Information Involved" and must be protected from disclosure. (Document in Committee Possession.)

Mrs. HARTZLER. For DOD programs, are there any near-term (within 3 years) alternatives for the former IBM technologies?

Ms. MAK. Because the response involves sensitive or proprietary information, it is provided in a separate document marked "For Official Use Only//Proprietary Information Involved" and must be protected from disclosure. (Document in Committee Possession.)

Mrs. HARTZLER. Are Field Programmable Gate Arrays (FPGAs) a possible alternative to the trusted microelectronics formerly provided by IBM?

Ms. MAK. Because the response involves sensitive or proprietary information, it is provided in a separate document marked "For Official Use Only//Proprietary Information Involved" and must be protected from disclosure. (Document in Committee Possession.)

Mrs. HARTZLER. Is there anything DOD or the U.S. Government can do to incentivize the microelectronics industry to locate or maintain manufacturing on-shore in the U.S.?

Mr. GUDGER and Ms. BALDWIN. The microelectronics industry is very capital intensive. DOD endorses public-private manufacturing partnerships that produce new and advanced manufacturing techniques and ecosystems on-shore in the U.S. DOD supports initiatives like the President's manufacturing institutes where DOD is investing hundreds of millions of dollars to incentivize and grow on-shore microelectronics manufacturing.

DOD is concurrently working to remove barriers to commercial technology utilization in areas such as the microelectronics industry by seeking out novel and flexible acquisition authorities and practices that will allow microelectronics manufacturers to have speedier, less encumbered contracting with the Department.

Mrs. HARTZLER. Given GAO's assessment that access to leading-edge technology for DOD is uncertain, are there any actions that DOD is undertaking to communicate to DOD components, programs, and contractors regarding actions they should be taking to mitigate any potential risk?

Mr. GUDGER and Ms. BALDWIN. The DOD meets regularly with industry associations and companies to promote the integrity of microelectronics and the supply chain that provides them. For example, the DOD participates in the National Defense Industrial Association (NDIA) Trusted Systems Steering Group, which represents the Defense Microelectronics Activity (DMEA)-accredited Trusted Suppliers, NDIA Systems Engineering Division, and the space community's Mission Assurance Improvement Working Group.

Mrs. HARTZLER. Is the Department considering lifetime buys or other near-term mitigation strategies, given the uncertainty of access? Is there an indication of the cost of these possible actions?

Mr. GUDGER and Ms. BALDWIN. In a memorandum dated November 13, 2015, the Assistant Secretary of Defense for Acquisition asked the DOD Component Acquisition Executives, National Reconnaissance Office, and National Security Agency to adjust Fiscal Year (FY) 2018 through FY 2020 budgets to accommodate Life Time Buys (LTBs) of at-risk Trusted microelectronic products and avoid costly program disruptions. DOD acquisition programs are considering the use of LTBs of at-risk Trusted microelectronic products, as well as other options, to address the risk of loss of access to Trusted microelectronic technologies. This analysis is done on a case-by-case basis, and includes the cost-benefit of LTBs of production-ready application-specific integrated circuit (ASIC) designs versus the redevelopment of ASICs using alternate design and foundry technologies and any components using those ASICs. In many cases, dollars are programmed in future years for these ASICs.

In addition, the DOD is in the process of expanding DMEA's capabilities to fabricate ASICs.

Mrs. HARTZLER. What is the status of DOD access to former IBM technologies, and how long is that access expected?

Mr. GUDGER and Ms. BALDWIN. DOD has uninterrupted access to all pertinent IBM technologies that were commercially available prior to the transaction. The contract with IBM was novated to GlobalFoundries U.S. 2, LLC (GF2) to prevent any interruption in access. According to the existing contract and other methods, the access to former IBM technologies is assured through June 2017 with an option to extend. DOD is currently negotiating a new multi-year manufacturing contract which will assure longer-term supply of former IBM technologies.

Mrs. HARTZLER. Will DOD maintain any government purpose rights to IBM leading-edge technology semiconductors after the year 2017? If possible, how could that arrangement be implemented?

Mr. GUDGER and Ms. BALDWIN. DOD's access to IBM leading-edge technology will continue beyond 2017, provided a new manufacturing contract is executed with GlobalFoundries U.S. 2, LLC (GF2). To assure long-term supply, DOD is working with GF2 to transfer the intellectual property for certain technologies to DMEA and/or to alternate foundries.

Mrs. HARTZLER. What is the potential effect to DOD programs in terms of cost, schedule or performance if current access to trusted leading-edge technologies is lost?

Mr. GUDGER and Ms. BALDWIN. A recent survey of USG customers using the National Security Agency Trusted Access Program Office contract revealed that 139 programs were using the GlobalFoundries U.S. 2, LLC (GF2) Trusted Foundry, and 120 (86%) of them required Trusted services. Therefore, the total cost and schedule effect from losing access to Trusted microelectronics would be significant; roughly estimated in \$100s of millions.

Mrs. HARTZLER. What actions has DOD taken or is planning to take to mitigate the near-term risk of loss of access to former IBM technologies?

Mr. GUDGER and Ms. BALDWIN. DOD has taken prudent steps to assure access to all pertinent IBM technologies that were commercially available prior to the

transaction. The contract with IBM was novated to GlobalFoundries U.S. 2, LLC (GF2) to prevent any interruption in access. According to the existing contract, the access to former IBM technologies is assured through June 2017 with an option to extend. DOD is currently negotiating a new multi-year manufacturing contract which will assure longer term of supply of former IBM technologies.

The Department is considering its near- and long-term Trusted Foundry options and alternatives to address supply chain risks and preserve state-of-the-art microelectronics access and trust. Recent and ongoing studies are providing the basis for budget proposals and future investments, which are currently being evaluated by Department leadership.

In addition, the Department has formed a federation of technical experts and laboratory capabilities. The Joint Federated Assurance Center (JFAC) supports programs throughout their life cycle by providing microelectronics expertise, capabilities, guidance and best practices for mitigating risks associated with preserving access and trust.

Mrs. HARTZLER. What assurances, if any, does the Department have from GlobalFoundries that they will remain a Trusted Supplier?

Mr. GUDGER and Ms. BALDWIN. DMEA has granted an interim Trusted Supplier accreditation for facilities acquired from IBM. According to the existing contract, the former IBM foundries are required to remain a Trusted Supplier until March 31, 2016. DOD is currently negotiating a new multi-year manufacturing contract with GlobalFoundries U.S. 2, LLC (GF2) to remain a Trusted Supplier.

Mrs. HARTZLER. Were DOD's national security concerns adequately addressed in the CFIUS process?

Mr. GUDGER and Ms. BALDWIN. DOD is a member of an interagency process and can present any national security concerns it deems important regarding a transaction to the Committee that may cause concern.

Mrs. HARTZLER. Is DOD monitoring China's efforts to acquire U.S. semiconductor companies (including GlobalFoundries), and what steps is DOD taking to ensure the security of the U.S. semiconductor industrial base?

Mr. GUDGER and Ms. BALDWIN. DOD actively identifies and tracks foreign acquisitions of U.S. companies. This includes tracking the Chinese government's public initiatives to develop a self-sufficient domestic semiconductor industry and its plan to encourage foreign acquisitions as part of its strategy. If needed, DOD could utilize its membership on CFIUS to evaluate a Chinese acquisition of a U.S. semiconductor company for national security concerns. DOD has seen and is monitoring public reports regarding China's interest in GlobalFoundries. Furthermore, DOD has regular engagements with GlobalFoundries U.S. 2, LLC (GF2), as a Trusted Supplier, and has discussed these public reports. As a cleared defense contractor, GF2 is required to report to DOD any potential foreign acquisition of its cleared facilities.

Mrs. HARTZLER. Are there industrial base options for unique technologies that IBM supplied as a sole-source?

Mr. GUDGER and Ms. BALDWIN. The microelectronics industrial base, while undergoing rapid consolidation, continues to maintain capabilities across the spectrum of DOD requirements. In specific instances where IBM supplied unique, sole-sourced technologies, the industrial base possesses capabilities that can be cultivated to fill technology gaps or develop different solutions to address the need.

Mrs. HARTZLER. Is there anything DOD or the U.S. Government can do to incentivize the microelectronics industry to locate or maintain manufacturing on-shore in the U.S.?

Ms. BALDWIN. The microelectronics industry is very capital intensive. DOD endorses public-private manufacturing partnerships that produce new and advanced manufacturing techniques and ecosystems on-shore in the U.S. DOD supports initiatives like the President's manufacturing institutes where DOD is investing hundreds of millions of dollars to incentivize and grow on-shore microelectronics manufacturing.

DOD is concurrently working to remove barriers to commercial technology utilization in areas such as the microelectronics industry by seeking out novel and flexible acquisition authorities and practices that will allow microelectronics manufacturers to have speedier, less encumbered contracting with the Department.

Mrs. HARTZLER. Is there anything DOD or the U.S. Government can do to incentivize the microelectronics industry to locate or maintain manufacturing on-shore in the U.S.?

Mr. HAMILTON. I defer this answer to the Office of the Undersecretary of Defense for Acquisition, Technology and Logistics.

Mrs. HARTZLER. Is the Joint Federated Assurance Center sufficiently resourced to handle current and the predicted future workloads, with sufficient and timely

throughput, in assessing the security and authenticity of various microelectronics that will be used for DOD applications?

Mr. HAMILTON. Respectfully defer to DOD for official department response.

Mrs. HARTZLER. Given GAO's assessment that access to leading-edge technology for DOD is uncertain, are there any actions that DOD is undertaking to communicate to DOD components, programs, and contractors regarding actions they should be taking to mitigate any potential risk?

Mr. HAMILTON. I defer this answer to the Office of the Undersecretary of Defense for Acquisition, Technology and Logistics.

Mrs. HARTZLER. Is the Department considering lifetime buys or other near-term mitigation strategies, given the uncertainty of access? Is there an indication of the cost of these possible actions?

Mr. HAMILTON. Respectfully defer to DOD for official department response.

Mrs. HARTZLER. What is the status of DOD access to former IBM technologies, and how long is that access expected?

Mr. HAMILTON. Respectfully defer to DOD for official department response.

Mrs. HARTZLER. Will DOD maintain any government purpose rights to IBM leading-edge technology semiconductors after the year 2017? If possible, how could that arrangement be implemented?

Mr. HAMILTON. Respectfully defer to DOD for official department response.

Mrs. HARTZLER. What is the potential effect to DOD programs in terms of cost, schedule or performance if current access to trusted leading-edge technologies is lost?

Mr. HAMILTON. Respectfully defer to DOD for official department response.

Mrs. HARTZLER. What actions has DOD taken or is planning to take to mitigate the near-term risk of loss of access to former IBM technologies?

Mr. HAMILTON. Respectfully defer to DOD for official department response.

Mrs. HARTZLER. What assurances, if any, does the Department have from GlobalFoundries that they will remain a Trusted Supplier?

Mr. HAMILTON. Respectfully defer to DOD for official department response.

Mrs. HARTZLER. Were DOD's national security concerns adequately addressed in the CFIUS process?

Mr. HAMILTON. Respectfully defer to DOD for official department response.

Mrs. HARTZLER. Is DOD monitoring China's efforts to acquire U.S. semiconductor companies (including GlobalFoundries), and what steps is DOD taking to ensure the security of the U.S. semiconductor industrial base?

Mr. HAMILTON. Respectfully defer to DOD for official department response.

Mrs. HARTZLER. Are there industrial base options for unique technologies that IBM supplied as a sole-source?

Mr. HAMILTON. Respectfully defer to DOD for official department response.

QUESTIONS SUBMITTED BY MR. WILSON

Mr. WILSON. Please tell me what your office is planning to do in the immediate term to harden the defense industrial base as it relates to the USG's need for microelectronics and semiconductors. Are there targeted investments that are being considered for FY16, or as part of the upcoming budget request?

Mr. GUDGER. DOD has a growing concern that the United States' technological superiority over potential adversaries is being threatened today in a way that we have not seen for decades. DOD recognizes that microelectronics and semiconductors are at the center of the threat with the remarkable leveling of the state of technology in the world, where commercial technologies with military applications such as advanced computing technologies, microelectronics, sophisticated sensors, and many advanced materials, are now widely available. The Deputy Assistant Secretary of Defense (DASD) for Manufacturing and Industrial Base Policy (MIBP), in conjunction with high priority Department initiatives, is working toward achieving dominant capabilities through innovation and technical excellence within the Department and specifically in the industrial base.

For the integrated circuit, the fundamental building block of microelectronics, DOD is furthering its strength derived from the long-standing link between the high-tech community and the United States Government (USG) using Manufacturing Innovation Institutes in areas like flexible hybrid electronics and integrated photonics.

DOD is partnering with a consortium of 96 companies, 41 universities, 14 state and local government organizations, and 11 laboratories and non-profits—to establish a new Manufacturing Innovation Institute focused on flexible hybrid electronics. This is an emerging technology that takes advanced flexible materials for circuits

with thinned silicon chips to ultimately produce the next generation of electronic products. DOD's \$75 Million investment over five years in "Flexible Hybrid Electronics" will be matched by \$96 Million private "FlexTech Alliance" funding. Partner organizations include industrial base players across the technology spectrum that differentiate using the world's most sophisticated technology, not the least of which is microelectronics capabilities.

The Department stood up and is growing its Defense Innovation Unit Experimental (DIUx) specifically to scout for new technology and build a bridge to Silicon Valley. DIUx brings together the cutting-edge represented by the Silicon Valley tech industry and helps to foster the necessary open avenue between DOD and Silicon Valley.

Mr. WILSON. The DOD seems to have been caught somewhat off guard by the IBM divestiture and Global Foundries purchase, despite the fact that it had been rumored in the trade press for upwards of three years. Current industry trade press suggests that Chinese controlled entities may now be looking at purchasing a controlling share of Global Foundries. Are you aware of these industry reports? How are you planning for the impacts that this will cause? If a Chinese controlled entity were to purchase some or all of Global Foundries, what affect would that have on DOD plans for acquiring trusted microelectronics?

Mr. GUDGER and Ms. BALDWIN. DOD has seen and is monitoring public reports regarding China's interest in GlobalFoundries. Furthermore, DOD has regular engagements with GlobalFoundries U.S. 2, LLC (GF2), as a Trusted Supplier, and has discussed these public reports. As a cleared defense contractor, GF2 is required to report to DOD any potential foreign acquisition of its cleared facilities.

Commercial sources of Trusted microelectronics remain in inherently unpredictable and constitute a continued supply chain risk despite USG investments. The Department is considering long-term Trusted Foundry options and alternatives to address its supply chain risk and preserve leading-edge microelectronics access and trust. Experts from across the community contributed to the recommendations to ensure continued access to advanced microelectronics while retaining the ability to employ them in a trusted manner. A portfolio of innovative technology solutions and business models is under review.

Mr. WILSON. What functionality might be lost by prematurely moving to smaller design nodes and how does this impact the health of the industrial base given the reality that large geometries exist domestically and small geometries exist mostly overseas?

Mr. GUDGER and Ms. BALDWIN. Although there are significant upsides to designing and manufacturing at smaller node sizes, the impact of shifting between nodes varies by system. Smaller node sizes would particularly benefit those systems that require high processing efficiencies. Many consumer electronics are therefore aggressively pushing towards more advanced nodes. Military systems that analyze large data sets in real-time, such as radar and electronic warfare systems, also depend on advances in technology node. More advanced nodes also benefit systems requiring difficult computational tasks with reduced size, weight, and power requirements, a critical metric for tactical systems including unmanned aerial vehicles and soldier-borne equipment.

The transition between nodes, however, could require that DOD replicate or port functionalities designed for less advanced nodes in order to apply them at more advanced nodes. In addition, jumping to advanced nodes can potentially sacrifice analog performance in certain systems. DOD will therefore need a suite of options, from smaller high-performance nodes to less advanced nodes, to meet the needs of its various systems.

DOD is investing in concepts that utilize existing onshore fabrication facilities at less advanced nodes while providing advanced capabilities. However, the volume of electronic components purchased by DOD is very small. As a result, healthy foundries increasingly depend less on DOD as a primary revenue source and more on global commercial demand.

Mr. WILSON. What would the approximate cost (rough order of magnitude) be of trying to establish domestic foundry capabilities for integrated circuits in the 65 nm to 45 nm node size range, or to up gun the capabilities for one of the other existing domestic foundries for capacity in that range?

Mr. GUDGER and Ms. BALDWIN. The cost to establish such a facility would be roughly \$500 Million to \$2 Billion, depending upon the existing infrastructure.

Mr. WILSON. With respect to the program itself, it was indicated that there are 72 partner companies within the trusted supplier program. However, it is my understanding that there are only four foundry companies in the program with others addressing other aspects such as design and packaging. What are the impacts of the

limited number of foundry companies? Given the limited number, how might we use these companies to mitigate the risk of further capability loss?

Ms. BALDWIN. There are 72 Trusted Suppliers within the DOD Trusted Supplier program that provide trusted services across the application-specific integrated circuit (ASIC) supply chain. Fifty of those Trusted Suppliers provide trusted design, aggregation, mask manufacturing, post-processing, packaging/assembly and/or test services. Twenty two of those Trusted Suppliers are Trusted Foundries, i.e., semiconductor manufacturers. There are three domestic foundries, i.e., GlobalFoundries U.S. 2, LLC (GF2), Intel Corporation, and Samsung, that produce state-of-the-art microelectronics, one of which is part of the Trusted Supplier program, i.e., GF2. The DOD will continue to rely upon the Trusted Supplier network, but is also considering additional solutions and business models to mitigate the risk of sole sources of supply, and further capability loss.

Mr. WILSON. How would you characterize the effectiveness of DODI#5200.44 and the enforcement of Program Protection Plans for most suppliers?

Ms. BALDWIN. Since the publication of DOD Instruction (DODI) 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems Networks (TSN), November 5, 2012, the Department has mandated that program protection plans address the use of trusted microelectronics design and manufacturing suppliers and practices for ASICs that are DOD-unique. Risk to system trust is now managed throughout the entire system life cycle beginning with design and before the acquisition or integration of critical components into covered systems. Programs are integrating robust systems engineering, supply chain risk management, security, counter intelligence, intelligence, cybersecurity, and software and hardware assurance. DMEA-accredited Trusted Suppliers report seeing an increase in interest in Trusted services from their customers since the implementation of DODI 5200.44.

Mr. WILSON. What is the approximate total annual Federal expenditure on Trusted Supplier contracts (including the take-or-pay contract)? What is the average cost of an integrated circuit within the program and how does this compare to other integrated circuits bought outside of the program?

Ms. BALDWIN. The recent total annual outlays to contractors for Trusted services is approximately \$65 Million per year. The average cost per integrated circuit has a very large standard deviation due to the wide range of design sizes, manufacturing processes, and quantities of parts being ordered. For example, a 3mm x 4mm chip could cost less than \$290 per good die in a dedicated prototype run using one process to over \$3300 per device in a multi-project wafer run using an advanced process node.

Products obtained through these contracts are comparable in price to what a similar volume commercial customer would pay if it contracted directly with the same foundry for similar services.

Mr. WILSON. With respect to the program itself, it was indicated that there are 72 partner companies within the trusted supplier program. However, it is my understanding that there are only four foundry companies in the program with others addressing other aspects such as design and packaging. What are the impacts of the limited number of foundry companies? Given the limited number, how might we use these companies to mitigate the risk of further capability loss?

Mr. HAMILTON. Respectfully defer to DOD for official department response.

QUESTIONS SUBMITTED BY MR. HUNTER

Mr. HUNTER. Recently, Under Secretary Frank Kendall and you attended an event sponsored by Defense One, and during that event, he highlighted how integrated micro-electronics were an area of particular concern for the Department of Defense and how the Department was using a number of tools to ensure a reliable supply of these components to the Military Services and the Intelligence Community.

a. What industrial base tools—such as Committee on Foreign Investment in the United States (CFIUS) reviews and the Defense Production Act (title I and title III)—has your office deployed with respect to micro-electronics, and what is the comparative effectiveness of these tools to achieving the objective of a reliable supply of micro-electronics?

Mr. GUDGER. The Department maintains awareness and conducts detailed analyses of domestic and global industry trends affecting its available capabilities. As part of its mission to ensure the maintenance of a healthy defense industrial base, including in microelectronics, the Deputy Assistant Secretary of Defense (DASD) for Manufacturing and Industrial Base Policy (MIBP) has a number of tools and authorities at its disposal to support the advancement of new enabling capabilities

that aid in achieving a reliable microelectronics supply. The 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 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 Department of Treasury-chaired CFIUS.
- 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 which advances the development and application of advanced manufacturing technologies and processes DOD-wide. MIBP, 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.
- Defense Production Act (DPA) Title III, 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's 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 of companies 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 research and development and qualification testing to develop Trusted 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.

Mr. HUNTER. During the course of the hearing before the Subcommittee on Oversight and Investigation, multiple witnesses discussed the relatively recent sale of IBM's micro-electronics business to GlobalFoundries Inc. The owner of GlobalFoundries Inc. is the Mubadala Development Company PJSC, a sovereign wealth fund of the Government of Abu Dhabi.

a. Since this transaction must have undergone a CFIUS review, what national defense risks to the Department of Defense and the Intelligence Community were evaluated during this process?

b. What additional safeguards, if any, has the Department put in place at these former IBM facilities to ensure that export-controlled items, or the technology and manufacturing techniques that enables their production, are handled in an appropriate and lawful manner?

Mr. GUDGER. DOD is a member of CFIUS and can present any national security concerns it deems important regarding a covered transaction to the Committee. Due to the confidentiality requirements of CFIUS, the Department cannot confirm whether the IBM sale to GlobalFoundries U.S. 2, LLC (GF2) was a covered transaction by CFIUS. Please contact Treasury as the Chair for CFIUS regarding any questions regarding CFIUS' reviews or decisions.

All the stringent security measures in place prior to the transaction are still largely present, including Global Business Solutions (GBS), a business unit of IBM, continuing to provide security oversight. GBS was not part of the IBM sale to GF2

and remains under the control of IBM. In addition, the facilities under control of GF2 currently have an interim facility clearance from the Defense Security Service (DSS) and an interim Trusted Supplier accreditation from the Defense Microelectronics Activity (DMEA), and are subject to all associated security requirements. Due to the foreign ownership of GlobalFoundries, DSS required additional security requirements to address visitation, export controls, collaborative business endeavors, etc. where there were any concerns.

Mr. HUNTER. If I understand the testimony before the subcommittee correctly, one compound risks confronting the Department of Defense in the micro-electronics space is that (1) micro-electronics are part of thousands of items that the Department of Defense buys, including many commercial items, but (2) the volume of micro-electronics that the Department of Defense buys is so small, relative to the commercial market, that it has little influence on market dynamics. Said another way, the ability of the Department to protect national security equities for micro-electronics through normal procurement practices is limited by the Department's market share.

a. Has your office identified this trend—(1) many important defense uses for a particular material or component but (2) small defense demand relative to commercial markets—occurring in other industrial base sectors?

b. How does your office address this trend differently from those industrial base sectors, such as binders and propellants for solid rocket motors, where the Department of Defense is the primary driver of demand and private investment?

Mr. GUDGER. Yes. The Department identified several sectors where defense-related demand is small compared to commercial demand, such as ground supply and transportation subsystems (transmissions, diesel engines, brakes, etc.); service sectors, such as medical, transportation, and construction; and solid rocket motor propellant components. However, the Department's purchase of these items does not approach the scale that we see with microelectronics since microelectronics are prevalent in almost all of the systems we buy. Unlike the examples cited above, the microelectronics industry is continuously evolving its technology, roughly every two years, thus requiring billion dollar investments in research and development and in new production facilities every couple of years. The rate of commercial technology advancement and the significant investment necessary to establish microelectronic production facilities creates barriers for new firms to enter the market. Accordingly, it is the combination of the Department's small market share, the rate of technology advancement, and the significant investment necessary to establish microelectronics production facilities that limit the Department's ability to impact market dynamics for microelectronics.

There is no one right answer for addressing low market share trends or DOD dominant market share trends. We address industrial base issues associated with each industrial sector on a case-by-case basis depending on many variables, to include market share, competitive forces (numbers of domestic sources or foreign suppliers), mature or emerging technology, and barriers to entering the market. The Department has several options available for mitigating supply base risks, including propellants or propellant ingredients, such as using a reliable foreign source, establishing a domestic source, or investing in research and development to develop a second source. The Department used IBAS funding to help establish a domestic source for this material. A current high-priority item for a low DOD market share issue is hydroxyl-terminated polybutadiene (HTPB), where variability in the product from the sole-source domestic supplier has caused issues for many DOD missile systems. Various mitigation activities, including research and development funding from the Defense Logistics Agency and IBAS are helping to characterize the material more thoroughly, and also to establish a reliable second source. An example of a material that scores very high in terms of risk, but has been determined that no action is required at this time is nitrocellulose (NC)—a material that is in all DOD ammunition systems and for which there is a sole domestic source. However, that source is a Government-Owned, Contractor-Operated (GOCO) facility, and is therefore stable; no mitigation is necessary at this time. A final example of a dominant DOD demand issue was the solid rocket motor for the Advanced Medium Range Air-to-Air Missile where the program office used a foreign source to mitigate the supply issue.

Mr. HUNTER. During her opening statement, Ms. Marie Mak (Director, Acquisition & Sourcing Management Team, U.S. Government Accountability Office) made the following remarks with respect to micro-electronics and industrial base policy more broadly:

“But the bottom line is that, not only is the U.S. reliant on a single provider, it now faces the unknown risk of relying on one that is foreign-owned. DOD is in a

position where it faces some very difficult and complex decisions with potentially significant costs and national security implications.

“Microelectronics is just the latest of several defense industrial base issues. Other examples include rare earth materials, specialty metals, and counterfeit parts. We need an industrial base strategy that is much more proactive and less reactive.”

a. Since the duties of the DASD-Manufacturing and Industrial Base Policy include being the principal advisor to Under Secretary Kendall on ensuring a reliable supply of critical materials like rare earths and specialty metals (10 U.S.C. 139c(b)(16)), would you characterize the national security drivers associated with rare earths as similar to that of micro-electronics (small defense demand, minimal Department of Defense market influence, outsized presence of foreign and Chinese manufacturers, etc.)? If not, why not?

b. What steps is the Department of Defense taking to promote domestic and/or allied nation production—not low technology readiness level research projects and surveys—of rare earth materials to meet defense requirements?

Mr. GUDGER. There are similarities between microelectronics and rare earth supply chains (small defense demand, minimal DOD market influence, outsized presence of foreign and Chinese manufacturers, etc.). There are also key differences. Microelectronics are manufactured components which can be sabotaged or counterfeited resulting in significant national security risks. Rare earths are raw, semi-finished, or alloy products which go into manufactured items, which substantially limits the ability to tamper or sabotage the materials. DOD is reliant on thousands of different microelectronic components, while rare earths consist of just 17 elements. DOD can stockpile a handful of different forms of these rare earth elements to mitigate the majority of its risk. Therefore, DOD’s primary risk mitigation for rare earths is stockpiling. Stockpiling is generally ineffective for addressing microelectronic components because the technology advances so rapidly, and stockpiled components become obsolete before being used. Additionally, the cost of the multitude of components required to be stockpiled would be too high. Consequently, stockpiling of select critical microelectronics is considered by DOD acquisition programs on a case-by-case basis, when necessary, carefully considering its cost/benefit.

There is not a sustainable business case for developing rare earth mining and production capabilities in the United States at this time due to the current overcapacity in the market. Compared to domestic commercial demand for rare earth materials, the Department’s industrial base requirements are very small. Accordingly, the current risk mitigation effort being pursued by the Department is stockpiling. The ongoing establishment of rare earth inventories will mitigate much of the Department’s risk for a relatively small investment.

