Department of Defense

(Amended for Open Publication)

Under Secretary of Defense for Research and Engineering

April 2018

The estimated cost of this report or study for the Department of Defense is approximately $467,000 in Fiscal Years 2017 - 2018. This includes $419,000 in expenses and $48,000 in DoD labor.
Generated on 2018Feb26 Ref ID: 7-DEEB88C

DISTRIBUTION STATEMENT A: Approved for public release. Distribution is unlimited.
DOPS Case #18-S-2455
Contents

Executive Summary ........................................................................................................................ 1
1. Microelectronics Needs of the Department of Defense .............................................................. 4
   1.1. Future Needs ...................................................................................................................... 4
   1.2. Present Needs .................................................................................................................. 6
   1.3. Threats to DoD Microelectronics ....................................................................................... 8
      1.3.1. Technical Threats ....................................................................................................... 9
      1.3.2. Foreign Competitors in Manufacturing .................................................................... 9
2. Status of Access, Availability, and Assurance Today .............................................................. 11
   2.1. Trusted Access Program Office ......................................................................................... 11
   2.2. Trusted and Assured Microelectronics Program ............................................................... 12
      2.2.1. V&V: Joint Federated Assurance Center ................................................................ 13
      2.2.2. Advanced R&D for Assurance ............................................................................... 13
   2.3. Access and Availability: DoD Microelectronics Innovation for National Security and Economic Competitiveness ................................................................. 14
   2.4. Research and Development ............................................................................................ 15
3. A Renewed Approach to Access and Assurance: Implementation View ................................. 17
   3.1. The Assurance Process .................................................................................................... 17
      3.1.1. Decision Flow for Assurance ................................................................................. 18
      3.1.2. Example Decision Paths ...................................................................................... 21
   3.2. Mitigations ..................................................................................................................... 23
      3.2.1. Secure Design Ecosystem ....................................................................................... 24
      3.2.2. Supply Chain Awareness ....................................................................................... 25
      3.2.3. Trusted Practices .................................................................................................... 25
      3.2.4. New Technologies for Provenance, Authenticity, and Assurance ......................... 25
      3.2.5. Disaggregation ....................................................................................................... 27
      3.2.6. Obfuscation ............................................................................................................ 28
      3.2.7. Marking for Provenance and Authenticity ............................................................... 28
      3.2.8. Verification and Validation ..................................................................................... 28
      3.2.9. Full Board Replacement for Countering Obsolescence ......................................... 29
4. Availability: Increasing the Supplier Base ............................................................................... 30
   4.1. Government-Owned SOTA Foundries ............................................................................ 30

DISTRIBUTION STATEMENT A: Approved for public release. Distribution is unlimited.
DOPSR Case #18-S-2455
Contents

4.2. DoD-Led Solutions ............................................................................................................ 31
4.3. Upgrading Existing Infrastructure .................................................................................... 31
4.4. New Commercial Partnerships ........................................................................................ 31
   4.4.1. Ecosystem for Innovation ....................................................................................... 32
   4.4.2. Benefits of Public-Private Partnerships ................................................................. 34
5. Changes in Policy .................................................................................................................... 36
   5.1. Acquisition ....................................................................................................................... 36
   5.2. Authority Outside DoD .................................................................................................... 37
   5.3. Program R&D Investment ............................................................................................. 38
6. Results of the Strategy ............................................................................................................ 39
Appendix I – Full Text of NDAA 2017 § 231 ........................................................................ 40
Appendix II – Lexicon .............................................................................................................. 42
Appendix III – Policy Reference Documents ........................................................................ 47
Appendix IV – Traceability Matrix ........................................................................................ 49
Appendix V – MINSEC: DEPSECDEF Priorities and Problem Areas of Focus .................... 50
Appendix VI – DoD MINSEC Initiative Funding Plans ......................................................... 55

Figures

Figure 1 – The Future Battlefield ............................................................................................ 5
Figure 2 – Range of DoD Microelectronics Needs ................................................................ 7
Figure 3 – DoD Microelectronics Segments ......................................................................... 8
Figure 4 – DoD Microelectronics Process Flow .................................................................... 18
Figure 5 – Microelectronics Decision Flow Diagram for Assurance .................................... 19
Figure 6 – Decision Flow Diagram ....................................................................................... 20
Figure 7 – Technology-Enabled Portfolio of Protections ...................................................... 24
Figure 8 – Evolving World Models ....................................................................................... 26
Executive Summary

Section 231 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2017 states “The Secretary of Defense shall develop a strategy to ensure the Department of Defense (DoD) has assured access\textsuperscript{1,2} to trusted\textsuperscript{3} microelectronics” (see Appendix I for the full text of Section 231). This report\textsuperscript{4} describes the strategy (referred to throughout as the strategy) that DoD will implement to ensure continuing access to assured, advanced microelectronics. Microelectronics are at the core of the critical hardware that provides DoD with overmatch capabilities against adversaries and the U.S. with commercial advantage and competitiveness. Economic trends are moving microelectronics manufacturing overseas, mainly to Asia, which introduces vulnerabilities into the supply chain and hinders the ability for the U.S. to manufacture advanced microelectronics and secure research and development (R&D) leadership in a domestic ecosystem. There are gaps in the domestic ecosystem for the military’s assured microelectronics needs, especially for state-of-the-art (SOTA) technology. Investments by other nations to build numerous new foundries threaten to surpass the state of the practice (SOTP) fabrication ecosystem in the U.S. Thus, the U.S. could be at risk both militarily and economically unless it takes decisive and significant action.

DoD’s microelectronics strategy will augment existing policy to promote the availability of and access to the assured microelectronics that are critical for national security systems. The strategy will deliver tools and guidance to protect the intellectual property (IP) confidentiality and integrity for a broad range of systems and missions, and will provide a path for the production of these articles. The strategy has the following components that cover the life cycle of the microelectronics development, production, acquisition, and sustainment:

- **Identification of Needs:** the microelectronics that are required to enable the DoD’s current and future missions;

\textsuperscript{1} In this response, “assurance” refers to the NDAA § 231 Definition of “trust” as the ability of the Department of Defense to have confidence that the microelectronics function as intended and are free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during its life cycle, which aligns with the Department’s definition of software assurance (see Lexicon).

\textsuperscript{2} In this response, “availability and access” terminology are compatible with the NDAA § 231(f)(1) Definition of “assured”; “The term “assured” refers, with respect to microelectronics, to the ability of the Department of Defense to guarantee availability of microelectronics parts at the necessary volumes and with the performance characteristics required to meet the needs of the Department of Defense.”

\textsuperscript{3} In this response, “Trusted Foundry Accreditation” and “Trusted Supplier Accreditation” refer to the accreditations referenced in USD(AT&L) 2004 Deputy Secretary of Defense memos that relate to 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; prevent intentional or unintentional modification or tampering of the integrated circuits (ICs); provide an assured\textsuperscript{1} “chain of custody” for both classified and unclassified ICs; protect the ICs from unauthorized attempts at reverse engineering, exposure of functionality, or evaluation of their possible vulnerabilities; and ensure that there will not be any reasonable threats related to disruption of supply.

\textsuperscript{4} Fulfilling the requirement under NDAA 2017 § 231(c)(1).
Executive Summary

- **R&D Investment to lead development of the next generation microelectronics:** disruptive R&D in partnership with industry, that deliver novel materials, devices, circuits, architectures, and design tools to unlock domestic microelectronics innovation and maintain DoD’s technical superiority in this critical technology area.

- **A modernized strategy to enable use of commercial parts in DoD systems:** demonstration and transition of design and supply chain security tools, standards, and techniques that enable the use of commercial application-specific integrated circuit (ASIC) sources and extend assurance approaches to additional commercial components, such as field programmable gate arrays (FPGAs).

- **Revised assurance policy:** update DoD trusted systems and networks risk-based policy and guidance that enables DoD components to adapt microelectronics assurance practices to SOTA technology applications, and extend life cycle vulnerability protection, beginning with secure design and protection of IP.

- **A healthy microelectronics verification and validation (V&V) capability:** continued enhancement of the Joint Federated Assurance Center (JFAC) capability and capacity to monitor, validate, and protect supply chains in addition to testing, qualifying, and improving assurance and mitigation techniques.

- **Adequate workforce expertise:** leverage public-private partnerships and engagement with academia, defense industrial base (DIB), and DoD user communities in prototyping and development activities to build a domestic knowledge base for future design and manufacturing of advanced microelectronics components that will enable DoD missions and meet capability requirements.

- **Access to DoD unique needs:** enhancements of Government and industry foundry capabilities and technology development to address requirement for which no source is otherwise available, for example, providing access to radiation-hardened by process and radiation-hardened by design technologies in support of space and nuclear modernization.

- **Reduced reliance on legacy parts through modernization:** co-development between the DoD/DIB and industry to deliver assured, modern ASICs and system on chip (SoCs) to replace obsolete systems in concert with the enactment of acquisition policies that promote rapid modernization, standards and best practices to facilitate validation and verification, supply chain tracking and risk assessment, and counterfeit detection.

- **A Diminishing Manufacturing Sources and Material Shortages (DMSMS) foundry of last resort:** continue to upgrade existing DMSMS foundry capabilities through tool enhancements and the acquisition of legacy IP.

A significant, coordinated effort by the nation is necessary to fully address DoD and broader U.S. Government (USG) needs and the threat to the U.S. domestic microelectronics supply base. Since 98 percent of DoD’s parts are purchased from commercial sources, the strategy will seek to develop a set of effective authorities and assurance best practices that, through public-private partnerships, foster a robust domestic and allied ecosystem for the design and manufacture of
Executive Summary

microelectronics components. An important underlying tenet of this strategy is to engage effectively with the domestic supply base to achieve DoD assurance needs, thereby broadening the access to a spectrum of technologies for future systems, and minimizing the cost and risk of captive Government foundry solutions.

These partnerships will connect Warfighter needs with emerging industrial capabilities and academic advancements to develop new capabilities and enable critical modernization. Developing and embedding standards of practice for assured microelectronics will have the added benefit of providing U.S. industry with an important market differentiator that is important for critical commercial sector capabilities—such as autonomous transportation, financial and big data systems, biomedical, and robust communications—that might otherwise be subject to threats from unsecured foreign sources. Combined with investments through the Defense Advanced Research Projects Agency (DARPA) in the R&D of disruptive technologies, DoD and the broader U.S. industrial base can lead the next generation of assured technology and maintain a competitive advantage over foreign actors intent on taking control of the evolving microelectronics market. The proposed microelectronics strategy will allow DoD to:

- maintain technological leadership and a secure domestic microelectronics ecosystem now and into the future;
- promote access to all necessary current and future semiconductor technologies—including design, fabrication, packaging, and testing—from a robust base of suppliers;
- provide DoD programs and the DIB with the guidance, tools, and assured access to deliver microelectronics best suited for critical systems with the confidence that they are free of vulnerabilities and perform as intended over their life cycle;
- provide multiple options for programs and the DIB to quickly upgrade microelectronic components and realize a decreasing cost per function while leveraging industry;
- create a competitive industrial base of microelectronics suppliers that can rapidly adjust to the dynamics of the industry; and
- provide DoD’s captive specialty needs suppliers and dedicated facilities with cost-effective upgrade capabilities and resources so they can deliver advanced technologies.

The sections following this Executive Summary describe the basis for the strategy; the related programs and activities that DoD has initiated and planned; provide details and case examples of how microelectronics assurance will be implemented in policy and program guidance; describe the strategy to ensure continued access to the spectrum of microelectronics needs; and identify considerations for additional policy and authorities needed to achieve a broader, whole-of-Government solution. This report informs DoD Directive required under section 231, which is currently under development for publication by September 30, 2019. The appendices provide the full text of the NDAA section 231, a lexicon including definitions and acronyms, references, and a traceability matrix.
1. Microelectronics Needs of the Department of Defense

Microelectronics represent a critical cross-cutting technology that supports all DoD operations, including: command, control, communications, intelligence, conventional and nuclear weapons, air-land-sea systems, and space. Many DoD systems use legacy microelectronics that are no longer available from non-DoD sources. Significant modernization is necessary to maintain current and deliver future overmatch capabilities of defense systems.

1.1. Future Needs

Maintaining U.S. military systems’ superiority depends on DoD’s ability to acquire assured SOTA microelectronics that deliver overmatch capabilities on numerous challenging battlefields (see Figure 3), including:

- big data and artificial intelligence systems that can deliver computational capabilities and actionable information in real-time;
- open and distributed processing architectures for collaborative, autonomous, miniature, and swarming platforms operating as systems of systems;
- modernization of legacy systems to allow the operation in joint and collaborative environments across DoD;
- sensory, precision navigation, and semantic processing necessary for human and robotic systems to operate as teams in real-time;
- diverse and protected communication technologies with high signal processing throughputs that can sustain awareness and operations in harsh and denied environments; and
- Radiation hardened (RH) and other high-reliability components for harsh environment, space, and strategic systems.
1. Microelectronics Needs of the Department of Defense

Figure 1 – The Future Battlefield
DoD future requirements must deliver overmatch capabilities in harsh and denied environments—both cyber and physical—on the land, underwater, sea, air, and space.

While DoD and USG in general continue to rely on SOTA commercial off-the-shelf (COTS) parts for many applications, DoD will require more highly assured COTS variants in addition to leading-edge ASICs (which encompass about 3 percent of the microelectronics currently used by the Services) that will deliver significant improvement in performance over COTS for its most critical missions. The latter will ensure DoD capabilities overmatch those that adversaries can acquire from commercial sources.

In addition to SOTA components, there will be a continued need for nearly every semiconductor technology from the last 30-40 years as existing platforms age. Many of these are no longer in commercial production and are increasingly difficult to locate in open markets, due to low non-DoD demand or transition to new manufacturing methods. Thus, DoD will need domestic sources for uninterruptible access to custom parts and means to deal with obsolescence replacement and modernization to avoid losing capabilities, especially in times of conflict and global supply disruption.

The strategy will seek ways to engage DoD systems to replace legacy microelectronics components with newer technologies and SoC design architectures to provide a foundation of DoD and DIB expertise and system designs, a means for efficient technology refresh, a reduction in legacy obsolescence costs, and a mechanism to address future requirements through SOTA components. The DoD will pilot an early obsolescence replacement program with a Service program office in FY 2018.
DoD microelectronics are often required to operate in harsh conditions for which commercial parts are not designed. There is a critical need to modernize space platforms and strategic systems designed to be resistant to the effects of ionizing radiation and operate through nuclear events, displacement damage, and other hostile space environments. Obsolescence in RH systems can be addressed both by enhancing radiation hardened by process (RHBP) and by providing access to strategic RH components through radiation hardened by design (RHBD) to avoid supply chain risk. In addition, advanced RH microelectronics and their incumbent abilities will be necessary to support delivery platforms that function through modern countermeasures.

To support these future space and nuclear modernization needs, DoD will also continue to research and qualify higher-performing components that function in high-radiation environments. RH microelectronics can be made by either applying RHBD methods to design circuits that can tolerate and mitigate those environments or applying special RHBP modifications during fabrication. While RHBD microelectronics can be manufactured at both commercial and custom foundries, the RHBP is a specialty service and not easily integrated into commercial offerings. DoD will require access to both to meet its current and future needs. RHBD will require access to critical IP and SOTA foundries, while RHBP will require access to and enhancement of specialty foundries that supply the processes.

1.2. Present Needs

DoD purchases billions of dollars of microelectronics per year, of which most is sourced from the commercial marketplace and the rest from the military specialty marketplace; this has been roughly constant over the past few years. While these outlays represent significant portions of the world’s market for some components (e.g., 10 percent of FPGAs), DoD represents only about 1 percent of the total microelectronics market, which limits its ability to influence the market. DoD also needs a large variety of ASIC and COTS parts to accomplish its missions (see Figure 1), which includes digital, analog, mixed signal, and radio frequency; power electronics; memories; programmable logic devices; optoelectronic devices; and custom high-performance digital devices and systems that span R&D prototypes, legacy and boutique, SOTP, and SOTA technologies. In the near term, DoD systems require access to a wide variety of legacy and SOTP parts, which may have unwieldy supply chains and diminishing numbers of commercial applications and suppliers.
1. Microelectronics Needs of the Department of Defense

Figure 2 – Range of DoD Microelectronics Needs
DoD microelectronics needs are spread across legacy and boutique devices for unique needs, SOTP and SOTA technologies, and the science and technology bridges and ecosystems necessary to deliver new capabilities into the production ecosystem.

To meet these needs, DoD and other USG agencies need to work together for efficient procurement, use, and USG laboratory microelectronics R&D efforts to ensure an assured supply of:

- SOTA (e.g., <32 nm feature size/300 mm wafer size CMOS technology);\(^5\)
- SOTP (e.g., \(\geq 32\) nm feature size/200 and 300 mm wafer size CMOS technology);
- legacy (e.g., >150 nm feature size/150 and 200 mm wafer size CMOS technology);\(^6\)
- and
- specialized (e.g., RH) microelectronics that may include SOTA or SOTP for satellite and missile systems.

The many types of DoD microelectronics are sourced from different market segments (see Figure 2). Commercial merchants (segments 1 and 2) provide the largest share of SOTA and SOTP components used by DoD across all areas. When higher levels of assurance are needed, cooperative commercial opportunities exist in which DoD and commercial vendors can work together to deliver enhanced performance and assurance features in commercial product offerings (segments 3 and 4).

---

\(^5\) Includes technologies other than CMOS, including LDMOS, BiCMOS, CMOS SOI, and III-V semiconductor materials for communications, electronic warfare, and radar.

\(^6\) Some applications like ROICs and power devices rely on >150 nm feature sizes and are not included under the legacy designation.
1. Microelectronics Needs of the Department of Defense

Figure 3 – DoD Microelectronics Segments
DoD microelectronics segments include COTS parts and ASIC parts that are largely commercial in their application and practices (1 and 2), parts that require increased assurance and cooperation from commercial manufacturers (3, which may include Government off the shelf [GOTS], and 4), or captive Government capabilities for DoD unique parts (5).

There is a small segment of specialized DoD microelectronics requirements that is served only by captive suppliers and USG sources (segment 5). These parts account for 2-3 percent of the overall DoD microelectronics needs and serve critical functions for national defense and deterrence. These microelectronic components and their applications vary widely, for example, the National Nuclear Security Administration requires digital, mixed signal, and analog integrated circuits (ICs) that satisfy nuclear weapons strategic RH requirements, but do not require leading-edge technology.

The strategy seeks to expand and develop manufacturing options for DoD systems to promote a healthy domestic industrial base. As SOTA technology advances, there are exponentially higher costs and risks to build, design, and operate commercially viable foundries.

1.3. Threats to DoD Microelectronics

The ability of DoD to meet its microelectronics needs now and in the future is threatened from multiple sources. The capability of components and systems can be degraded or eliminated by technical threats and supply manipulation throughout the supply chain. The ability to source and innovate domestically is threatened by off-shore capital investments, foreign investments in R&D and technological advancements, and the ever-increasing cost and complexity of design and fabrication. Especially concerning are threats posed by nation states who have the capability to manipulate the entire global market. Geographic consolidation of microelectronics manufacturing in small regions put the global supply chain at risk of disruption or destruction by natural disaster or military action.
1.3.1. Technical Threats

The Defense Science Board (DSB) and other Government organizations (e.g., Defense Security Service (DSS), Department of Homeland Security, National Institute of Standards and Technology, and the Government Accountability Office) have enumerated risks from malicious actors surreptitiously exploiting vulnerabilities in the electronics supply chain to gain unauthorized access or even sabotage USG information and communications technology. The DSB has reported threats from both malicious and negligent actors and the vulnerabilities they could exploit; risks to microelectronics fabrication and assembly are a particular concern.

There are several major categories of IP threat. Loss-of-information involves the unauthorized extraction of sensitive information by malicious or negligent agents, including hardware design data theft, IP theft, and reverse engineering (see Appendix II for full definitions). Potential sources of fraudulent microelectronics include counterfeits, clones, unauthorized production, gray market distribution, and rogue agents adulterating legitimate design and manufacturing processes. Threats to control or compromise DoD systems may arise from malicious insertion of tainted microcircuits containing Trojans or other intentional defects anywhere in the supply chain. Loss-of-access threats include a loss of suppliers, supply chain disruptions, and component obsolescence. Nations can manipulate or restrict access to technology produced in their country, which can inhibit DoD’s ability to make improvements to or maintain mission-critical systems due to throttled access.

Product defects, introduced either maliciously or through negligence, can lead to system vulnerabilities or degraded life cycle performance.

1.3.2. Foreign Competitors in Manufacturing

The U.S. is a world leader in microelectronics technology and innovation, but this position is at risk in a globally connected and increasingly consolidated environment. China has publicly stated its goal to achieve world-class capabilities in all areas of microelectronics by 2030. It announced a national investment strategy of at least $150 billion to achieve this goal, which is similar to the all-in investment strategy China has followed to capture other markets such as solar manufacturing, aluminum and steel production, and rare earths mining. For example, in the $70 billion annual memory market, China has announced a $50 billion investment in the fabrication of three new memory foundries and guaranteed that their losses would be covered for

---

5-10 years, which could seriously disrupt our domestic manufactures’ ability to remain competitive. China will also build at least 30 new domestic foundries at SOTP and seven at SOTA (14 nm) in the next decade, which will continue their production trajectory from the last decade and further outpace U.S. output. In addition, China and others lead the world in the number of hardware-focused microelectronics startups (approximately 1,100 in 2017) and offers heavily subsidized access to design tools, IP, and foundry fabrication for these startups, giving them a significant advantage. Saudi Arabia and other oil-producers have announced similar orders of magnitude investments in microelectronics and other advanced technologies.10

The inability or unwillingness of the U.S. to invest in leading-edge manufacturing will pose both a near- and long-term threat to U.S. leadership in microelectronics R&D and innovation. Ignoring the threats to our SOTP and SOTA domestic foundries will create near-term supply risk, loss of the SOTP foundries to capture innovative technologies, and loss of the profits that drive R&D investment. The ecosystem for innovation serves as a key intellectual underpinning for long-term cross-cutting microelectronics and process technologies. Continued leadership in IC ecosystems for innovation is critical to maintaining technological superiority of commercial and, by extension, national security missions. Reducing barriers to innovation in the domestic ecosystem is critical for allowing DoD, DIB, and domestic commercial innovators to deliver modern defense systems and innovative products that can dominate the commercial and military sectors.

Foreign entities can also threaten the U.S. base through mergers, acquisition, or outright IP theft. An increased awareness of the supply chain and market along with policy authority is necessary for the U.S. to identify these actions and take appropriate countermeasures under this strategy.

10 https://www.ft.com/content/e4fe85cc-037e-11e7-ace0-1ce02ef0def9
2. Status of Access, Availability, and Assurance Today

Since 2004,\textsuperscript{11} the National Security Agency (NSA) and, subsequently, the Defense Microelectronics Activity (DMEA) have accredited suppliers for the production of custom ASICs for DoD end-use by programs. The accreditations relate to 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; prevent intentional or unintentional modification or tampering of the ICs; provide an assured “chain of custody” for both classified and unclassified ICs; protect the ICs from unauthorized attempts at reverse engineering, exposure of functionality or evaluation of their possible vulnerabilities; and ensure there will be no reasonable threats related to disruption of supply.\textsuperscript{12} For the vast majority of other microcircuit types, including COTS products, the risk mitigation methods thus far employed have principally relied upon industry supply chain risk management (SCRM) best-practices and DoD manufacturer, distributor, and electronic parts qualification programs.

A number of factors, as described in the previous section, have caused DoD to revisit these needs and approaches to access and assurance. This has resulted in revising existing programs, establishing new programs and implementing investment plans in the future years defense program. The following paragraphs in this section will describe these actions and programs which include the Trusted Access Program Office, Trusted Supplier Network, the Trusted and Assured Microelectronics Program (T&AM), and the DoD Microelectronics Innovation for National Security and Economic Competitiveness program (MINSEC).

2.1. Trusted Access Program Office

The current policy for protecting ASIC design confidentiality and integrity in the supply chain is by use of DoD-accredited Trusted Foundries and other Trusted Suppliers. Assured access to SOTA Trusted foundries is accomplished by aggregating DoD’s relatively low volume requirements (which individually would not be sufficient for affording access) into a large, multi-year contract. The efforts to establish a cadre of entities has been successful for SOTP technology, as evidenced by the accreditation of 76 sources of design and fabrication for DoD’s most critical SOTP microelectronics technologies.\textsuperscript{13} These suppliers compete for work on services related to defense microelectronics components from design to fabrication to packaging.

\textsuperscript{12} DoDI 5200.44
\textsuperscript{13} See current list on DMEA website; http://www.dmea.osd.mil/otherdocs/AccreditedSuppliers.pdf (viewed on Sept 8, 2017)
2. Status of Access, Availability, and Assurance Today

and test. The products and technologies offered by accredited sources are continuously monitored to maximize the offering of SOTP ASIC technologies for DoD program offices.

The scope of DoD’s needs extend beyond what is currently available from accredited Trusted Suppliers. For example, DoD is reliant upon the Defense Logistics Agency Qualified Manufacturers List (QML) of suppliers for many high reliability electronic hardware applications, most of whom are not accredited.\(^\text{14}\) Although DoD has access to a SOTA foundry through the Trusted Foundry program, at present there is not an accredited SOTA foundry. The accreditation process is designed to be adaptable and to ensure mitigations are appropriate and cost-effective for a wide variety of fabrication facilities, including SOTA facilities that are fully automated and do not have the same vulnerabilities or attack surface as SOTP facilities. Notable Government needs that are not currently served by an accredited Trusted Supplier include: SOTA complementary metal-oxide-semiconductor (CMOS), advanced packaging capabilities, some advanced compound semiconductor processes, and COTS parts, such as FPGAs and memory devices. Accredited design and manufacturing flows are being developed for COTS parts, such as FPGAs and standard processor cores, for military specific applications. DoD is working to implement these flows in cooperation with DIB partners.

The most advanced Trusted Foundry accredited node is a 32 nm process. There are currently no Trusted Foundry accredited sources for SOTA technology. The barriers for additional leading-edge foundries to provide assured access to DoD are significant, including low production volume purchases and extended temperature range requirements. Additionally, International Traffic in Arms Regulations (ITAR) and requirements for facility and personnel clearances are disruptive to the internationally sourced workforces in most modern fabrication facilities.

DoD initiated a formal T&AM program to advance assurance practices and expand the supply of assured microelectronics parts available to DoD, with the overall goal of mitigating the risk of a sole-source foundry.

2.2. Trusted and Assured Microelectronics Program

The T&AM program initiated in 2017 is one aspect of the Department’s strategy to address long-term availability, access, and assurance needs. The T&AM program is investing in the demonstration and transition of technology to enable assurance through design features and is establishing enhanced capability to evaluate microelectronics for vulnerabilities. JFAC is instituting this capability in laboratories across the USG. Congress has recognized and endorsed T&AM’s efforts to address microelectronics assurance needs.\(^\text{15}\)


\(^{15}\) From House Report Defense Appropriations, HR 5293 pgs. 263-264.
2. Status of Access, Availability, and Assurance Today

2.2.1. V&V: Joint Federated Assurance Center

Commercial parts form a large segment of DoD’s microelectronics needs, including growing use of FPGAs and other COTS devices. Additional risks arise with use of COTS, including counterfeits and cloned parts. At the SOTA technology nodes, operating and design costs increase and commercial suppliers become the only option for DoD needs. A healthy V&V capability is therefore important to enable evaluation of hardware and software components.

DoD established\textsuperscript{16} the JFAC to coordinate and promote software and hardware assurance capabilities for use by defense programs. Under JFAC, hardware and software vulnerability detection, analysis, and remediation capabilities are being developed by Government laboratories. The JFAC identifies and maintains software and hardware technical expertise and capabilities, policies, guidance, requirements, best practices, contracting language, training, and testing support to program offices and other organizations across the life cycle. Participants are working to develop a set of procedures that provide varying levels of assurance that can be used as part of the risk mitigation process and program protection planning.

2.2.2. Advanced R&D for Assurance

There are multiple agencies and organizations involved in the R&D enterprise for advancing and assuring microelectronics and related technologies, such as DARPA, DIUx, DTRA, NSA, Service labs (including JFAC), and basic research enterprises (e.g., ONR and DTRA). The strategy will seek to coordinate across these R&D investments. The Advanced Electronics Community of Interest is an important enabler for this coordination. The T&AM program broadens this coordination to other USG partners, including the Intelligence Advanced Research Projects Agency (IARPA), and Department of Energy laboratories (e.g., Sandia National Lab).

DoD is making significant enhancements to the V&V capabilities of the JFAC to meet the increasing challenges of validating and assuring advanced node technologies. As a complement to the V&V focus, the T&AM program is executing a focused technology development, demonstration, and transition program to enable a new security approach. Significant advances in secure design and chain-of-custody technologies offer a new approach that is based on a foundation of assurance through technology (vice foundry manufacturing). These efforts aim to enable DoD to employ a variety of mitigations across the conventional supply chain by applying new technologies (detailed in section 3.2.). Successful application and promotion of these techniques through private-public partnerships will enable broader access to the capabilities in the global microelectronics supply base.

\textsuperscript{16} National Defense Authorization Act of 2014 § 937
2. Status of Access, Availability, and Assurance Today

2.3. Access and Availability: DoD Microelectronics Innovation for National Security and Economic Competitiveness

Given the significant efforts by China and others to acquire and build their own microelectronics dominance, significant concerns remain about the availability of and access to technologies and productions in a healthy domestic ecosystem. Realizing the need for an augmented strategy, beyond the T&AM program, to address future microelectronics needs, and the threats to assured access from a robust industrial base discussed in this report, DoD, in coordination with interagency partners, developed the MINSEC strategy. The MINSEC strategy drew from numerous studies and reports by performers including: DSB, PCAST, DIUx, SIA, and NDIA. MINSEC augments and builds upon the existing T&AM program, JFAC, Trusted Access Program Office, and the Trusted Supplier Network investment described in this report. To leverage R&D advances and enable alignment with the domestic ecosystem to deliver new capabilities for the Warfighter, the MINSEC strategy outlines a whole-of-Government solution to align resources, policies, and incentives in—

• proactive awareness and security, including supply chain tracking with proactive authorities, intelligence and counterintelligence, standards, and the implementation of new approaches like block chain;
• disruptive R&D, consisting of specialized circuits for computing and strategic applications, rapid redesign of complex systems, and disruptive materials and electronic architectures to ensure U.S. technological leadership and provide the U.S. with a continuing strategic advantage;
• access and assurance to secure design, IP, electronic design automation (EDA) tools, experts’ developments, foundries and processes, shared fab runs, and prototype demonstrations;
• enhanced manufacturing, including SOTP back-end technologies for assurance, SOTA processing using a low volume manufacturing paradigm, and agile fabrication facilities for high-mix, low-volume, and custom processing;

---

18 Report to the President: Ensuring Long-Term U.S. Leadership in Semiconductors. President’s Council of Advisors on Science and Technology. Executive Office of the President, 2017.
2. Status of Access, Availability, and Assurance Today

- incentives for market growth through novel circuits for defense and dual-use, piloting reforms to contracting and acquisition of advanced microelectronics, and R&D and domestic processing access to fab incentives; and
- strategic alliances for cooperative R&D, trade, and Foreign Military Sales.

The MINSEC objectives align with and support the required strategy described herein. DoD cannot address the entire national strategy, but plans to make a determined focus on the DoD issues of assured access within the defense microelectronics ecosystem. DoD has developed a resourcing strategy to address assured access to microelectronics, which will fund a number of critical elements, including:

- disruptive R&D secured in a domestic ecosystem to lead the next generation microelectronics technology;
- advanced microelectronics designs for modernized DoD systems delivered through secure design environments, with access to IP, experts, foundry and packaging capabilities, and matching funds for prototype development with industry;
- advancement of assurance and V&V capabilities across all microelectronics development activities to deliver overmatch capabilities in the form of microelectronics designs with security and chain of custody features to enable assured DoD use of parts from commercial suppliers and a competitive advantage for those parts in the marketplace;
- enhancement of Government and industry SOTP domestic foundry capabilities and IP to—
  - foster greater capture of R&D by enabling a domestic capability to manufacture innovative design and then transition technologies to high-volume production; and
  - provide obsolescence replacement capabilities;
- delivery of Government unique microelectronics needs such as RH, RF and optical nodes for strategic and space applications; and
- growth of a robust microelectronics workforce and expertise in DoD and DIB through scholarship and fellowship programs, execution of R&D programs, and new capability development by the department.

2.4. Research and Development

A final significant element of the strategy is aggressive, strategic R&D investment to lead the development of the next generation of microelectronics technologies and deliver beyond-Moore’s Law innovations for defense end-use, advancing the U.S. and allied nations’ technical superiority. R&D will focus on novel materials, devices, circuits, architectures, and design tools.
The DARPA Electronics Resurgence Initiative (ERI) is the primary investment for this next generation objective. 22

ERI investments within these “thrust areas” will foster and secure the environment needed for the next wave of U.S. semiconductor advancements. New materials will enhance conventional silicon circuits and continue the progress in performance traditionally associated with scaling. Novel designs will dramatically lower the time and complexity required to design modern SoCs, and unleash a new era of circuit and system specialization. Advanced architectures will provide the benefits of chip specialization while maintaining standard programming.

Improving the efficiency of microelectronics technology development, including qualification and packaging technologies for flight and military systems, is vital to counter the significant and aggressive investments by other nations. The primary barriers to maintaining innovation are the lack of access to design IP, EDA tools, and the production and packaging facilities to build their prototype and test designs. Foreign nations seeking to gain access to leading edge technology will provide start-ups the access to EDA tools, and production runs they need at discounted costs. The U.S. must also address the significant barriers and non-competitive environments around innovation if it is to maintain its leadership in microelectronics technology. To supplement the next generation R&D investments, the strategy seeks to reduce innovation barriers and enhance the capabilities of our captive and semi-captive suppliers in Government and industry to transition R&D into production within a domestic ecosystem to serve critical areas. New models and science and technology can create a new manufacturing paradigm based on proven process tools in agile fabrication facilities. These enhanced manufacturing capabilities could allow cost-effective ways to capture and incentivize domestic R&D and provide a low-volume production environment for a high-mix of technologies as they are incubated and nurtured for DoD and commercial market applications.

To help reduce the barriers for access and innovation, the cost and complexity associated with microelectronics development should also be an R&D focus. These costs are factors that limit the number of custom ICs that can be designed and built for low-volume customers. By increasing design modularity and reuse, DoD could sharply reduce the amount of effort required to design high-performance ASICs. This could also alleviate the challenge resulting from loss of access to a particular foundry by minimizing the effort required to move IC designs across facilities. An additional benefit of modularity is that it can take much of the sensitive IP out of hardware and into software, allowing for greater access without other confidentiality concerns. Modular IP used across the DoD and the DIB can also deliver improved economics of scale and efficiencies in the development and procurement of new overmatch capabilities.

---

3. A Renewed Approach to Access and Assurance: Implementation View

As the need for SOTA ASIC capabilities and the use of COTS programmable devices continues to increase, a new strategy is needed to ensure the availability of, access to, and assurance of these devices from healthy domestic and global sources. DoD’s actions to renew and address these needs were outlined in Section 2 of this report (T&AM, TAPO, MINSEC). This section provides a view of the strategy as it will be implemented by the variety of stakeholders.

In this new strategy, the process for protecting microelectronic components is gated through a systems and networks risk-based decision flow based on the criticality and vulnerability of the component, which informs the mitigations that can be applied to increase assurance.

3.1. The Assurance Process

In 2009, DoD delivered a report to Congress in response to Section 254 of the NDAA for FY 2009,23 outlining the DoD strategy for Trusted Systems and Networks. Following this strategy report, DoD issued policy in 2012, which set the requirement for supply chain risk management.24 Since then, DoD has developed and employed risk-based system security engineering policies, guidance, methodologies, and training, including classifying the mission criticality of logic-bearing software and hardware functions and components in its systems. Microelectronic parts currently in inventory, under development, and planned for procurement in the future are required to comply with these existing policies (see Appendix III for applicable policy documents). To incorporate the microelectronics strategy into existing policy, DoD will:

- align the trusted microelectronics terminology with the existing system security engineering (SSE) terminology to ensure uniformity of application and implementation of microelectronics protection measures;
- update existing policies, methodologies, guidance, and training listed above, as necessary, to ensure sufficient emphasis or reemphasis is being given to microelectronic components; and
- ensure the planned DoD Directive for microelectronics complements the existing system security engineering-related DoD Directives and Instructions.

DoD categorizes systems based on a comprehensive end-to-end analysis of all subsystems, including: hardware, software, operational, and functional elements across the entire subsystems

---

24 DoDI 5200.44
life cycle (defined in the Defense Acquisition Guidebook\textsuperscript{25}). Initially, the identified systems and components are decomposed and sorted by their criticality level (see Appendix II for definitions), threats, weaknesses, vulnerabilities, and residual risk (see Figure 4). The resulting risk assessment informs the programs’ choice of appropriate mitigations that will provide the necessary levels of assurance (see section 3.1.1). The level of assurance required for a specific component is determined relative to its impact on the mission, and the same or similar microelectronic components may require different levels of assurance based on the system into which that component will be integrated. DoD further distinguishes microelectronics parts based on their incorporation of critical program information (CPI, e.g., ASICs) or not (COTS).\textsuperscript{26}

Figure 4 – DoD Microelectronics Process Flow
DoD microelectronics process flow. Risk will be assessed based on threat, vulnerabilities, and consequence to missions (criticality), which will be used assess assurance level down to specific IP. These will drive mitigation selections by the programs. Mitigations and manufacturing will enhance assurance at the component and circuit board levels and provide program protections at the system and systems of systems levels (the mitigation levels on the figure are conceptual). This process flow incorporates existing program protection planning guidance.

3.1.1. Decision Flow for Assurance

A decision flow process, which maps the component criticality level and levels of assurance provided by available protections, guides the assurance process for microelectronics parts (Figure 5). A series of questions based on the criticality of the component’s IP confidentiality and integrity, or critical functionality (CF), the mitigations available to protect the component, and the availability of manufacturing processes are evaluated to determine the resulting manufacturing process. Thresholds for these decisions are set based on the risk analysis of the function delivered by the parts and the required assurance to mitigate risk to an acceptable level. Improved design risk mitigations and industry-adopted protections allow access to more commercial options and reduced dependency onsole-source or captive foundries.

\textsuperscript{25} Defense Acquisition Guidebook, Chapter 9, Program Protection
\textsuperscript{26} DoDI 5200.44
3. A Renewed Approach to Access and Assurance: Implementation View

Figure 5 – Microelectronics Decision Flow Diagram for Assurance

Microelectronics decision flow diagram for assurance. Risk to the parts and levels of assurance provided by available protections guides the assurance process for microelectronics parts (Figure 5). A series of questions based on the criticality of the component’s IP confidentiality (CPI) and integrity or critical functionality (CF), the mitigations available to protect the component, and the availability of manufacturing processes are evaluated to determine the resulting manufacturing process.

Figure 6 highlights the different decision pathways, which map onto the microelectronics segments used by DoD. The process for determining the choice of a microelectronic part for a given application depends initially on the confidentiality of the IP expressed in the part throughout the production life cycle. If the part does not contain CPI, a COTS part can be acquired in its publically-available state (purple path, sector 1) if it does not perform a critical function or if it meets the required assurance level. If a higher level of assurance of the part integrity is required, a COTS or GOTS component part with additional validation or modification via cooperative agreements or co-development can be used (green path, sector 3).

Confidential IP or CPI may be expressed within an ASIC. If the IP can be protected in the design phase, those ASICs can be sourced from purely commercial sources (orange path, sector 2), or augmented for increased assurance through cooperative manufacturing agreements or co-development (blue path, sector 4); for example, new assurance mitigations for integrity and...
confidentiality protection and disaggregation techniques, such as split manufacturing. The final category represents ASICs that cannot be sourced from a commercial source at any level because of their confidentiality, criticality, and lack of mitigations in the design phase for protection before manufacturing; the lack of existing technology to create them, necessitating additional R&D and production capability; or the unwillingness of commercial partners to produce the part with the required manufacturing mitigations, requiring trusted flows (red path, sector 5). IP protection does not preclude the use of a Trusted Foundry or Trusted Supplier if it is more efficient or readily available.

Examples of using this chart for different parts are detailed below. While it enumerates some situations, the figure is not exhaustive with regard to all caveats or situations. The mitigations described in these examples are defined in greater detail in section 3.1.

Figure 6 – Decision Flow Diagram
Pathways through the decision flow diagram for choosing the type of part for a DoD application.
3. A Renewed Approach to Access and Assurance: Implementation View

3.1.2. Example Decision Paths

FPGA COTS

FPGAs are COTS parts that represent an important category of DoD microelectronics that provide SOTA functionality through custom programmability of the configuration data (bit-stream) by the designer to optimize the part for its application. Four elements of the FPGA assurance need to be considered:

1. hardware assurance of COTS parts (that contain no CPI at purchase);
2. assurance and validation of software design tools either provided by FPGA manufacturer or third-party EDA tool vendor, along with associated third-party design IP (e.g., embedded hard IP macros like GPP and HBM) used by the designer to generate the bit-stream that are avenues for threat actors to insert unwanted/malicious functionality;
3. configuration or provisioning and validation of the FPGA bitstream using COTS hardware and design tools, where CPI may be added in a user controlled facility or by a third-party; and
4. addition of security features necessary to field the devices to provide CPI security and integrity through their life cycle.

Generally FPGAs follow the purple path through the decision analysis in Figure 6. The IP confidentiality of the FPGA chip or the SW design tools are not critical because the part itself contains no CPI. Additionally, the IP integrity of the FPGA hardware can be addressed through a combination of assurance approaches. During provisioning of the FPGA, CPI can be added in the form of the bit-stream data file used to configure the FPGA, however, this can be protected in a user controlled facility with the application of software assurance and third-party IP and bitstream validation tools. If the FPGA is determined to have CF, and requires a higher level of integrity assurance, it may be possible for the user to perform additional V&V testing, as represented separately by the green path (section 3). Manufacturers have a significant business interest in providing security features that help protect IP once it is installed. The strategy involves engagement with programmable logic device manufacturers early as they are developing new capabilities to get access to the V&V articles and promote the insertion of security and other features throughout the life cycle that will enable assured DoD end-use.

The JFAC and T&AM program are working on V&V for commonly used hardware, software assurance of third-party IP, independent V&V of the bit-stream, and private-public partnerships for co-development and vendor engagement to encourage the insertion of features that facilitate V&V and provide security features relevant to the DoD. The broader MINSEC initiative can facilitate the adoption of mitigation strategies to expand the base of assured FPGAs and other programmable logic devices for DoD use. The JFAC, T&AM program, and DARPA are currently engaging with FPGA vendors to co-develop commonly used COTS FGPAs with

DISTRIBUTION STATEMENT A: Approved for public release. Distribution is unlimited.
DOPSR Case #18-S-2455
necessary performance, security, and assurance considerations for use in DoD systems. For example, the T&AM program has issued a sources sought effort\textsuperscript{27} through DMEA for FPGA assurance with major FPGA manufacturers.

*Commercial ASICs*

The use of purely commercial flows can extend beyond ubiquitous COTS parts like central processing units (CPUs) and graphic processing units (GPUs) that provide high levels of performance and programmability. Some systems require significantly more (10-100x) performance to execute their functions to fit size weight and performance (SWAP) of the intended mission. For example, the microelectronics used in global positioning systems rely on ASICs that enable functionality for consumer and military use (Figure 6 section 2). For some DoD missions, these ASICs can contain CPI and it is necessary to keep specifics of its functionality confidential to prevent adversaries from being able to interfere with or compromise the operation.

The JFAC, T&AM program, DARPA, DMEA, and industry (in partnership with DSS) have and are developing methods of protecting CPI that is expressed in ASIC designs before they are delivered to a manufacturer or foundry (yellow path). The basic method of CPI protections include using cleared personnel to handle the CPI or disaggregating the IP and combining it later. These disaggregation methods include split fabrication, logic locking, state-space obfuscations, camouflage, and software CPI insertion post-fabrication where different IP components are combined in a second manufacturing stage to reveal the ultimate IP. If portions of the chips’ CPI cannot be protected during the design stage, additional protections through a trusted flow may be necessary.

Depending on the criticality of the mission, it may be necessary to protect the part’s integrity from threats like malicious insertion, alteration, or unauthorized reproduction. The JFAC, T&AM program, DARPA, and industry are developing methods that establish provenance in the design and manufacturing process of the device, including features that prevent, thwart, or reveal malicious insert or alteration and promote the rapid and cost-effective validation and authentication of genuine articles. The development of secure, cloud-based design environments, validation of third-party IP using software assurance tools, and the creation of a repository of assured IP will enable access to parts with high integrity and fewer vulnerabilities to IP theft.

While not all portions of an ASIC perform critical functions, some may require higher levels of assurance (e.g., security hypervisors and encryption modules). This may be accomplished using

\textsuperscript{27}https://www.fbo.gov/spg/ODA/DMEA/DMEA/HQ072717S4201/listing.html, Solicitation #: HQ072717S4201
split-fabrication, obfuscation, state-space locking, features that identify counterfeiting or alteration, and characterization of second-order effects for facile identification of genuine parts. Additionally, manufacturers will be encouraged to develop technical means of providing an immutable chain of evidence of the manufacturing process’s access and actions, which will promote easier validation and serve as a deterrent for malicious activity (see section 3.3.2.).

Compliance with ITAR can be accomplished by protecting the design intent and operability through obfuscation, state locking, and split fabrication mitigations, which would only deliver an unfinished design or part and categorize it as other under ITAR classification. This would allow the manufacture of DoD goods across a broader supplier base. As part of the strategy, DoD will work with the State Department to ensure these mitigations satisfy ITAR requirements for industrial partners in addition to exploring possible reforms in this area with the interagency.

**Strategic Radiation-Hardened ASICs**

Strategic RH ASIC microelectronics represent a category of components that have no commercial application, and are used exclusively for DoD or military applications (red path, sector 5). There are two categories of these components, RHBP and RHBD. RHBP may require unique DoD-unique fabrication sources, whereas RHBD may be manufactured by more commercial sources. Depending on the application and other factors, the design IP may need to remain confidential. It may be possible to protect confidentiality using mitigations; however, some critical functions may require using a trusted flow. There is also a lack of assured design libraries for implementing RHBD at multiple foundries; the T&AM program and MINSEC initiative will invest in these libraries and confidentiality protections to increase the supplier base of RH parts.

Continuing with the case of a strategic RH ASIC, it might be determined that RHBP is absolutely needed to attain the necessary properties, but it would require a special process to be developed and qualified. As there are no commercial needs for this process, the USG would have to work to build out the capability, either with a commercial partner or as a captive capability, and keep it available (build capacity on Figure 6).

### 3.2. Mitigations

DoD systems can have varying assurance needs depending on the results of the criticality, threat, weaknesses, and vulnerability analyses. The various solutions in this framework are grouped into multiple classes based on the protections provided and the expected level of interference into supplier best practices (see Figure 7). DoD will use a layered approach based on these protections for securing its microelectronics, which will include a combination of actions taken either by the commercial manufacturer or by DoD. These mitigations have the potential to
increase the supplier base by decreasing the risk of CPI compromise. Protection requirements will differ based on the type of component and application.

Figure 7 – Technology-Enabled Portfolio of Protections

Mitigations toward the left of Figure 7 are generally less disruptive to standard business practices and allow DoD access to more SOTA components. For example, DARPA is working to show that DoD security features can be incorporated into a leading commercial product line with minimal or zero impact to their manufacturing process. Conversely, protections that require greater levels of Government involvement in the ASIC life cycle tend to emphasize the use of limited, strategic foundry partnerships in order to protect critical IP. Other protections may allow for blended partnerships that involve both commercial and strategic foundry partners.

Mitigations could also be used to facilitate ITAR compliance and reforms that would further expand the assured supplier base; however, even if further ITAR reform around microelectronics is not achieved, this microelectronics strategy will develop and allow programs and the DIB to employ protections that aim to natively satisfy the ITAR requirements (see Section 5, Changes in Policy, for additional discussion).

3.2.1. Secure Design Ecosystem

The strategy will extend an existing secure design ecosystem to allow experts in Government, academia, and industry to collaboratively work on next generation microelectronics. Secure design ecosystems include secure cloud-based or centralized remote server-based design environments, advanced design tools, hardware and software assurance tools, assured IP repositories, supercomputer simulators, and persistent experts. Within the system, DoD and other USG communities will be able to deliver advancements (e.g., in RH, radio frequency, and optoelectronic components) for modernization and obsolescence replacement activities. Creating secure design ecosystems that provide access to multiple microelectronics foundries and agile-fabs while delivering the necessary security, supply chain awareness, and authorities will prevent critical IP and technology from leaving the U.S. via licit or illicit means without authority. DoD has achieved authority to operate to process classified data on such design environments. Commercial server and cloud-based secure design environments have been piloted by DoD and commercial industry with significant security, provenance, traceability, and access control features. Access at the design stage will also create a base for students and workers to have the
capacity to build critical technologies within the U.S. while allowing an awareness and more control of the provenance and release of data from the secure cloud systems.

3.2.2. Supply Chain Awareness

Threats to the supply chain may come in the form of counterfeit, adulterated, or otherwise compromised parts that degrade the performance of DoD systems and decrease confidence that the part will maintain functionality throughout its life cycle. Assured access to microelectronics for DoD will be addressed by first building a proactive general awareness of the entire global supply chain, including our allied and domestic supply chains, and a specific awareness of supply chain for critical DoD needs. Supply chain awareness can be achieved through purchase of commercial data and services, collection and analysis of open-source data, and inputs from the intelligence and DoD acquisition community. Analytic tools will be developed to track and target select intelligence and counterintelligence assets to cover critical microelectronics areas. Even when a purely commercial manufacturing path is chosen, appropriate supplier vetting of every supply chain element from all source intelligence will be incorporated into the decision process (e.g., SCRM). This intelligence can be used to inform relevant authorities (e.g., ITAR and CFIUS) and facilitate policymaking.

Because the U.S. regularly operates with coalitions of allies on the battlefield, it is necessary to ensure that their technological capabilities are compatible with and do not compromise the assurance of ours. In addition, understanding and collaborating with allied nations will strengthen the U.S.’s position against adversaries that would threaten the supply chain. Understanding the global supply chain and its overlap with DoD’s current and future needs will allow the DoD greater insight into determining the required assurance category of a critical component—including its critical manufacturing processes, equipment, and materials—and the concomitant protections. This strategy will address the difficulty and obstacles currently present in DoD’s acquisition policy that make it difficult to acquire this information.

3.2.3. Trusted Practices

For critical defense system components that cannot be protected through other mitigations or where the trusted flow is most efficacious, DoD will maintain existing procedures such as the Trusted Foundries and Trusted Suppliers that help maintain IP confidentiality and integrity protections and a healthy, trusted supplier base.

3.2.4. New Technologies for Provenance, Authenticity, and Assurance

The widespread availability of inexpensive sensor, network, and information processing technologies has led to a shift in the way in which we understand our world. These data can be
exploited to assure designs using immutable evidence obtained from commercial best practices. This method is most applicable where a high degree of sensor coverage exists in the activities related to the design and manufacturing of an article of interest, such as secure design environments and largely automated facilities.

Historically, people developed a mental world model through individual experience and their interactions with concrete artifacts in the real world. Verification of one’s mental world model was performed by interfacing with other trusted people to compare and align world views (see Figure 8). There has been a shift to a data view, where sensors capture great volumes of data about events, people, and items of interest, which are recorded and stored in a vast collection of databases that can be combined to create a comprehensive and verified cyber world model (CWM).

Figure 8 – Evolving World Models
Transitioning from human mental world models to cyber world models, which incorporated data from sensors and recording devices whose outputs are captured in hashed crypto records that establish provenance and traceability for microelectronic components. Access to the recorded world data provides knowledge about who has access to or made changes and yields a complete understanding of a part. Combined, the system will inform the decision making necessary to evaluate the assurance of a part regardless of its origin.

DoD is interested in leveraging the concept of CWMs in conjunction with an immutable record (e.g., keyless signature infrastructure [KSI] or block chain) to support supply chain assurance. For example, it is possible to draw from the data available from secure design environments and largely automated facilities to create a keychain of records associated with a unique part. The individual data records of the keychain can be tagged to specific locations, hashed, and linked using cryptographic and block chain concepts to form an immutable chain of crypto-provenance. This creates a deterrence to those who would try to interfere with the system, allows rapid identification of compromised parts, and facilitates V&V of the processes with minimal interference on the operation and staffing of the facility. In addition, in facilities that easily
implement access control, such methods can be applied to assure IP confidentiality in addition to integrity by limiting access to artifacts that are created during the design and manufacturing process to authorized users. These cryptographic CWM records should be applied to all stages of manufacturing, integration, operations, and maintenance to provide a complete provenance and tractability of the parts in our critical systems. The strategy drives towards a vision of Government-contractor engagement resulting a complete chain of records on an individual part basis, thus enhancing overall assurance and access to commercial COTS components.

3.2.5. Disaggregation

Disaggregation splits an IC into two or more pieces before manufacturing that are later combined to form a complete circuit. It can be used to conceal the function, separate critical from non-critical functions, create an ecosystem of reusable hardware components (e.g., DARPA CHIPS), provide for more efficient use of the supplier base, and deny the operability of an ASIC device component by manufacturing pieces separately. Some of the disaggregation mitigations protect critical IP, thwart understanding of the combined article, prevent malicious insertion, and complicate attempts to target DoD’s supply chain.

Functional disaggregation separates critical micro-electronics into functional, independently-manufactured component parts that may omit critical aspects of the IP intent or function and can allow parts to be manufactured in commercial foundries. These parts and IP can be integrated in a trusted facility to complete the IP intent and function. Disguising the true use of the final component would allow DoD to employ SOTA commercial suppliers by avoiding release of the IP intent or functionality. This approach would allow DoD to alter smaller portions of a part without redoing the entire design, thus lowering design costs, enabling more rapid security upgrades and facilitating shifts between vendors. DARPA and the T&AM program are funding efforts to develop these capabilities and evaluating the resulting assurance.

Fine disaggregation separates an ASIC at the electronic interconnect level so that untrusted circuit layers can be connected using a secure interconnect layer such that only when everything is integrated together is the true intent revealed; that is, final functionality is withheld from outside entities until the components are integrated. Example of fine disaggregation include a DARPA effort in 3D ICs.

The strategy will continue investments in the R&D and employment of both kinds of disaggregation to protect components manufactured at commercial facilities, while supporting the development of standardized IP blocks that allow more rapid and cost-effective design and insertion.
3.2.6. Obfuscation

Obfuscation is a design approach that makes an IC purposefully complicated to prevent an understanding and exploitation of its underlying function, aiding both design confidentiality and limiting the ability to attack or subvert the system. Techniques of obfuscation can vary from low-level, foundry-implemented techniques to high-level design choices implemented at the outset. For example, critical functions can be camouflaged within a group of logic gates that are un-related, frustrating a casual intruder trying to understand their true function. To thwart state-level actors, techniques like logic locking and state space obfuscation and other assurance techniques must be used to significantly increase effort necessary to unwind the obfuscation and the IP intent or functionality. In the commercial sector, vendors have leveraged reprogrammable memory and electronically activated fuses to delay imprinting sensitive functions on a device until after the device has been manufactured. The strategy will continue investments in the R&D and employment of obfuscation techniques to protect components manufactured at commercial facilities.

3.2.7. Marking for Provenance and Authenticity

Marking countermeasures allow the authentication of genuine devices and mitigate threats from fraudulent products, and can be applied to both COTS and ASICs. Once a manufactured device is personalized, tracking countermeasures such as low-cost electronic component markers can allow DoD to determine the device’s provenance or identify counterfeit components (e.g., through DARPA Supply Chain Hardware Integrity for Electronics Defense [SHIELD]). The strategy will continue investments in the R&D and employment of marking techniques to protect components manufactured at commercial facilities. These techniques of marking and authentication are a vital part of the integrated supply chain provenance and tractability efforts mentioned in section 3.2.4.

3.2.8. Verification and Validation

V&V countermeasures provide assurance that components function as specified, which protect against quality and reliability issues, malicious insertions, and fraudulent products. Utilizing these countermeasures can implement protections against threats during fabrication and assembly by detecting:

- intentional compromise of a microelectronics design or manufactured part;
- accidental compromise of a microelectronics design or manufactured part; and
- unreliable, unauthorized, or counterfeit products.

To develop confidence in a component post-fabrication, multiple verification methods may be employed, such as forensic delayering, imaging, x-ray, circuit emanation, and bit-stream.
verification to compare portions of a fabricated part to its intended design. Because these actions are costly, the strategy will prioritize the most critical analyses to build up a body of knowledge of widely used defense microelectronics. Vendor engagements will also be leveraged to improve DoD’s ability to capture relevant information and perform V&V techniques, such as quality reports, wafer acceptance reports, and extended reliability testing data, which would be captured as described in the New Provenance Technologies section. Funding for expanded testing and screening would also enable DoD to establish best practices for vetting the physical response of commercial products in military environments (e.g., radiation and extended temperature environments). Through the T&AM program, DoD is developing and advancing V&V capabilities through the JFAC and establishing interaction models for defense utilization. The effectiveness of these techniques will be assessed and strengthened through mathematical modeling of residual risk and red-teaming activities.

3.2.9. Full Board Replacement for Countering Obsolescence

Because DoD system life cycles may be significantly longer than those of the commercial components on which the systems rely, obsolescence can be a significant issue. When parts become obsolete, DoD increasingly relies on supply chain awareness and V&V to mitigate the risks posed by counterfeiting and cloning. Alternatively, it is possible to redesign entire boards or use FPGA emulation to run in the same weapon systems with improved assurance, access to replacements, and expanded future capabilities.
4. Availability: Increasing the Supplier Base

The availability of microelectronics technologies will continue to be a challenge for DoD. The strategy will include working to expand the supplier base to ensure parts remain available while simultaneously fostering a domestic ecosystem that meets assurance needs. DoD strategy will upgrade existing USG captive elements and engage with commercial entities and organizations with technologies of interest outside the DoD. DoD cannot accomplish everything on its own but will look to create innovative new partnerships in appropriate areas. To enhance certain capabilities, DoD will engage in public-private partnerships, which may advance hardware assurance practices while developing technology to increase competitiveness and national security. These partnerships can serve the specific and developing needs of DoD program offices while ensuring the financial viability of industry partners.

The MINSEC strategy proposes significant investment in new capability development facilitated by innovation hubs that foster public-private partnerships for design innovation. Innovators from Government and industry will access modular IP, secure design environment IP, EDA tools, V&V tools, experts within Government and industry, SOTA and SOTP assured access, prototyping, and packaging to deliver overmatch (10-1,000x) capabilities for national security and commercial competitive applications such as machine learning, robust communication and precision timing, data analytics, the internet of things, and autonomous vehicles, among others important to the nation’s and DoD’s national security and competitiveness.

4.1. Government-Owned SOTA Foundries

A seemingly straightforward conclusion to solving both an assurance and an access issue is to build a captive foundry or foundries that could satisfy all of the USG’s microelectronics needs. As stated earlier, a key tenant of the strategy is to minimize the reliance on fully captive capabilities. A number of factors and historical experiences by the USG in building and sustaining microelectronics foundries form the basis for this strategy tenant and must be taken into consideration for all captive foundry decisions. These include today’s cost to build and maintain a SOTA facility ($10-20 billion to build and $1 billion or more per year to operate and recapitalize), attaining the volumes required to sustain reasonable product yield, the profound technical expertise required, and continued modernization costs, including sustainment of the design and IP ecosystem necessary to deliver required microelectronics performance. There is only one pure-play merchant foundry company in the U.S. at the leading edge of CMOS technology and two vertically integrated device manufacturers that offer foundry access in some cases. Commercial foundries service a large user base to deliver very rapid designs at

---

4. Availability: Increasing the Supplier Base

competitive costs by allocating investments with EDA companies, developing and proving out
the IP across a large user base. The goal of DoD strategy is to maximize the ability to meet USG
microelectronics needs and address the modern threat. Beyond the small percentage of truly
captive parts, these needs would not be adequately met by a USG facility.

4.2. DoD-Led Solutions

While building a stand-alone captive foundry is not efficient, the strategy will explore the
possibility of appending a USG-centered fab line onto existing SOTA facilities for production of
specialty parts (e.g., SOTA radiation-hardened microelectronics). Enhancing Government SOTP
facilities to enable split-fabrication and advanced packaging could also allow the completion of
wafers from SOTA facilities in a secure facility when proper design and manufacturing technical
information is available. Similarly, agile-fabs could provide an affordable option to meet DoD’s
low-volume needs but do not yet have an installed base of suitable equipment. The strategy will
also involve enhancement of the capabilities of existing USG captive foundries. For those needs
that have no commercial supplier due to process or protection requirements, DMEA will
continue to serve as a foundry of last resort.

4.3. Upgrading Existing Infrastructure

While it is not practical for USG agencies to own and operate a fabrication facility producing
CMOS ICs at the leading edge, the DoD has at its disposal several domestic SOTP suppliers that
could be readily upgraded closer to SOTA to expand their useful lifespan with relatively low
cost. For example, Trusted Suppliers in Government and industry operating at 90 nm or above
could be fitted with more advanced equipment that would bring their capabilities to at least 65
nm and copper back-end of line processes to allow more advanced capabilities for full flow
production and also enable split manufacturing of near-SOTA devices in these facilities.
Partnerships with industry to develop tool and lithography capabilities that enable 45-28 nm
processing would further extend capabilities and efficacy of IP protections through split
manufacturing. Building capacity in design and manufacture of assured microelectronics parts
will not be sufficient to rebuild U.S. dominance without similar efforts to develop the workforce.
This will be encouraged through the innovation hubs described previously.

4.4. New Commercial Partnerships

While upgrading existing infrastructure is critical, this alone will not be able to meet all of
DoD’s future needs. The domestic base can be enhanced by other means, such as by forming
public-private partnerships throughout the design and manufacture of components.
4. Availability: Increasing the Supplier Base

4.4.1. Ecosystem for Innovation

DoD will explore the creation of an ecosystem for innovation with public-private partnerships that connects innovators and developers from across industry, academia, and Government to adopters and consumers to provide essential overmatch capabilities for DoD and the Nation in areas of strategic importance (see Figure 9). The ecosystems for innovation will focus on the ability to express the best ideas while practicing assurance in a largely domestic ecosystem and network of design, fabrication and evaluation hubs across the United States. Implementation would require whole-of-Government investment.

Figure 9 – The Ecosystem for Innovation

New capability development ecosystems will connect the innovators developers with the DoD and commercial adopters to deliver modernized systems with overmatch capabilities for military and consumer markets in the domestic ecosystem. Public-private partnerships across the nation that focus on critical applications and prototype demonstrations using a secure design ecosystems, assurance tools and best practices, and access to domestic foundries and packaging, will generate 10-1,000x capabilities demonstrations for autonomy, artificial intelligence, secure communications, etc. and provide a competitive advantage in the marketplace and the battlefield.

Significant barriers and costs exist to innovation in hardware microelectronics development in the areas of design and expertise, fabrication and packaging access, and funding to develop and demonstrate prototype capabilities. The current venture capital climate in industry favors the development of software startups over hardware due to the ability to fund 10-100 software startups for the cost of one hardware startup. Barriers and costs in the design phase include:
4. Availability: Increasing the Supplier Base

- Electronic Design Automation (EDA) tools that can cost as much as $1 million a seat for advanced node designs,
- 3rd party IP that can cost in the millions for processing, memory, and input/output (I/O) cores,
- need for significant emulation and simulation resources to validate and verify the designs before committing to productions,
- need for very specialized and highly skilled experts in architectures, design, simulation, validation, synthesis and layout.

Barriers to access to fabrication facilities and costs include:
- photo-masks that can cost as much as $2-5 million for advanced node designs,
- contracting and fabrication costs ($10 million for a 14nm CMOS foundry run) for low-volume fabrication at SOTA facilities that cater to high-volume customers,
- complex packaging, assembly, and test supply chain that can be difficult to navigate.

To reduce these barriers and promote the development of assured and secure capabilities, the innovators will have access to an ecosystem for innovation that includes:
- cloud-based secure design environments across multiple hubs throughout the U.S. where teams from Government, academia, and industry, through competitive selection, capture the best ideas to solve specific DoD-centric challenges; the secure design environment provides designers access to—
  - administrators, business managers, and architects to ensure integration and adoption;
  - experts from Government and industry in design, V&V, and end-use experience;
  - critical third-party IP libraries;
  - EDA tools, software and hardware assurance and validation tools, and access to powerful supercomputer simulation and emulation capabilities to test the new designs before committing to fabrication;
  - software assurance, test, V&V capabilities, and experts that are available to engage with designers;
- access to SOTA and SOTP domestic foundries and packaging facilities (Government and industry), as well as flexible mini-fabrication facilities throughout the domestic ecosystem that the strategy will invest in building;
- access to integration and demonstration facilities to evaluate and promote adoption and insertion of new capabilities for commercial and Government use, which will modernize DoD systems and deliver a 10-1,000x competitive advantage over COTS parts alone;
- disruptive R&D outputs from DARPA and other sources to deliver new design tools and architectures to the secure design environments, and new materials, processes, and devices to the domestic fabrication and packaging ecosystem; and
4. Availability: Increasing the Supplier Base

- funding from Government to seed and match industry and defense program funding that will enable the innovators and developers to use the resources in the ecosystem for innovation to deliver the capabilities, which can be enhanced by acquisition reform that can provide multiple options for programs and the DIB to perform in independent demonstration of new microelectronics capabilities every two years against the program baseline and realize a decreasing cost per function while leveraging industry (see section 5.1.).

The ecosystem may incorporate R&D innovations (including new architectures, materials, and tools) from DARPA as they are developed. R&D will also play a significant role enhancing the fabrication and packaging of the new designs through the development of new tools and devices. By fostering program participation at universities, industry research centers, and Government labs, more participants in the ecosystem would be able to contribute, test, and realize their new technology, while further expanding the assured IP library that sustains the environment. Thus, the newly generated IP may be captured within the secure design ecosystems promoted by the DoD and may be made available to other internal experts for validation and reuse.

The ecosystem may be funded through a mixture of targeted Government and industry investments. Targeted investments in commercial technology would influence the design process for military applications while requiring only a fraction of the cost required to develop the technology internally. For example, DARPA has leveraged 10 to 1 commercial investments by a major FPGA supplier as they develop their next generation FPGA SoCs to promote features and assurance for DoD applications. These partnerships would extend to the processes for creating new technology standards such that DoD needs can be embedded from the outset. The strategy will also explore engagements with venture capital to encourage hardware design startups, which will use non-dilutive investments that reduce the up-front costs while providing DoD with early access to new IP through the ecosystem for innovation.

The Department has been approached by multiple domestic fabless semiconductor companies that have expressed interest in forming and investing in partnerships with the DIB and Government to create and foster a domestic ecosystem for innovation.

4.4.2. Benefits of Public-Private Partnerships

The ecosystem for innovation and other development partnerships may provide DoD with early and continuing access to new technology. Early access to the designs would provide significant benefits toward increasing assurance by allowing the insertion of DoD-centric security features, the practice of assurance throughout the design process, and the ability to begin V&V activities before products are released.
4. Availability: Increasing the Supplier Base

Engagements with COTS suppliers through these co-development partnerships may significantly expand the number of assured parts for DoD use and give DoD programs access to merchant processes beyond those offered by the Trusted Foundry. Working with industry to develop protocols that provide assurance through the block chain concept and other mitigations described earlier would expand the number of potential SOTA suppliers. In addition, the procedures developed by the JFAC will reinforce the manufacturing mitigations used by partner commercial entities and facilitate V&V through standard features and open architectures.

Access to SOTA fabrication facilities would also expand to effects of R&D throughout the domestic ecosystem. Collaborative agreements would create more opportunities for innovators, startups, research institutions, and other low-volume customers to have access to fabs instead of having to ship their prototypes overseas. This would allow greater capture of IP within the U.S. and provide benefits for advanced manufacturing processes and the innovation hubs described in the R&D section.

Those that partner with DoD on assured microelectronics will have a market incentive to participate because they can market their products as offering a high level of security and assurance. Commercial partners would be able to apply those practices for applications outside of the defense industrial system for critical applications, which could have competitive advantages over foreign parts whose producers do not respect consumers’ safety or confidentiality as a matter of record. Strengthening a sustainable domestic industrial base around dual-use products would provide DoD with expanded manufacturing sources and multiple pipelines of assured microelectronics.
5. Changes in Policy

As required, DoD will issue a directive describing the roles and responsibilities for providing access to assured microelectronics supply chains for DoD systems. In addition, existing hardware assurance policy set forth in DoDI 5000.02, DoDI 5200.44, and related system security engineering guidance will be reassessed and modified as needed to align the goals of the microelectronics strategy, which includes ASICs, FPGAs, programmable logic devices, and other components, with other department program protection policy. For example, the Department needs to establish a definition of hardware assurance complementary to the definition of software assurance in DoDI 5200.44.

The strategy also takes action to strengthen and broaden the supplier base domestically and increases assured access to the global ecosystem. Additional resources and policy changes within DoD are necessary to achieve these goals. These new approaches will expand and guarantee the domestic supply base of microelectronics for defense needs, increase access to allied and cooperative foreign supply chains, and protect our critical defense and national security systems from manipulation and malicious tampering by adversarial actors. Robust R&D, intelligence, and counterintelligence efforts are necessary to guarantee continued access to the microelectronics DoD will need in the future. Changes to other DoD policies regarding acquisition and program funding that can support the strategy are detailed in the following section.

5.1. Acquisition

The strategy will include a review of defense system acquisition and sustainment policies and incentive structures to identify changes that lower barriers for the rapid and frequent insertion of new innovative technologies. Acquisition reform, mission assurance, system security engineering, and open architectures are critical to facilitate the adoption of advanced commercial and co-development technologies. To keep pace with technological change, advanced capability insertions by the system developer community, every two years may provide DoD weapon systems with the edge needed to maintain their military overmatch superiority. Regardless of whether a technology is adopted or not, to keep pace with commercial microelectronics industry levels of investment, 15 percent to 20 percent of the budget for a DoD program for the acquisition of microelectronics should be allotted to competitive new capability insertion and demonstration projects every 1-2 years and compared to the baseline program capabilities. Such a dedication of resources to continuous modernization can be additionally motivated by

29 NDAA 2017 § 231(d)
30 Software assurance (SwA) is defined therein as “The level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the life cycle.”
5. Changes in Policy

Incentivizing acquisition and sustainment professions and programs to include assurance and supply risk in their program metrics into their contracting and professional grading. If efforts to capture supply and assurance risks into block chain provenance keys that can be applied to parts, boards, assemblies, and full systems are successful, the risk carried by every fighter, radar, radio, and other critical warfighting asset could be readily observable and each professional and program could be rewarded for their ability to reduce this risk. The efforts to build public-private partnerships can also be aided by acquisition policies that create incentives for contractors to use secured and assured components from those lines, maintaining investments within the U.S. supply chain.

Upon realization of secure design environments to develop, prototype, and reuse IP, DoD will put in place policy requiring their use. For other DoD-centric applications, the strategy will also pilot open architecture approaches with the DIB. For example, if similar components are used across the Services, they could be consolidated into a single part that would benefit from higher production volumes and decreased V&V costs.

To promote assurance throughout the acquisition process, additional requirements for V&V on all microelectronics articles used by DoD will be implemented to support the intent of the NDAA for FY 2018 and the DoD digital engineering initiative. The Department will pursue acquisition practices that include design data as deliverables, such as EDA files and embedded firmware, which are critical to facilitate independent:

- verification of digital and functional operation;
- support of failure analysis and forensic investigations; and
- archival of design models for model based engineering and model based systems engineering approaches and processes.

This approach will allow the Department to shift from a build then test philosophy to a design, simulate, and test methodology, which will deliver faster, assured, and sustainable technology development and replacement. The JFAC laboratories will be resourced and made responsible for the acceptance, storage, processing and analysis of this critical data for DoD.

5.2. Authority Outside DoD

DoD does not have the ability or authority to effect whole-of-Government solutions for a national microelectronics strategy as fully outlined in the MINSEC strategy. For example, important components of a national strategy might be a suite of incentives, tax policies, regulation reforms, and financial instruments that encourage private investment in domestic microelectronics design and manufacturing. These incentives are largely outside the purview of DoD; therefore, the Department will coordinate and collaborate with other Government agencies.
and Congress to develop a mutually acceptable package of incentives that attract foreign and domestic investment in a domestic ecosystem.

Significant investment in the microelectronics ecosystem would send a clear signal that the U.S. is serious about microelectronics leadership and would create incentives for the domestic industry to co-invest and engage as partners. Therefore, the strategy will include a request for significant funding and authority to foster public-private partnerships that provide contractors with assured access to microelectronics, including the solving of security concerns associated with design, the addressing of specialty needs, and the driving of new and innovative chip designs for defense applications.

The commercial industrial base for microelectronics is global, and the R&D of circuit designs are routinely sent overseas for production at small scale. Conversely, export controls (e.g., ITAR) are often a barrier for prototyping or manufacturing DoD-centric components overseas and for accessing leading-edge commercial foundries in the U.S. This limits the ability of defense design houses to use the best technology for their missions. ITAR and other export restrictions on microelectronics could be reduced or broadly eliminated if countermeasures such as the use of encryption keys and split manufacturing methods were used to protect design IP (see section 3.2., Mitigations). Promising technical solutions under development may permit a technically competent adjudication and adoption of ITAR reforms that permit DoD to safely and fully utilize the commercial industrial base.

5.3. Program R&D Investment

To develop and transition the technologies that will underpin the critical defense applications of the future, a consistent source of financing is required. In addition to baseline program requirements and capabilities, the strategy will include seeking ways to enable DoD programs to invest 15-20 percent of their annual microelectronics budget for independent development and demonstration of new dual-use microelectronics-based capabilities.
6. Results of the Strategy

As a result of the proposed strategy, the U.S. and DoD will:

- maintain technological leadership now and into the future, secured in a domestic ecosystem;
- ensure access to all necessary semiconductor technologies—including design, fabrication, packaging, and testing—from a robust base of suppliers with appropriate supply chain risk management;
- provide DoD programs and the DIB with the microelectronics components best suited to the needs of critical systems with the confidence that those systems will perform as intended and free of vulnerabilities over their life cycle;
- provide multiple options for programs and the DIB to quickly upgrade microelectronic components and realize a decreasing cost per function;
- create a competitive industrial base of microelectronics suppliers that can rapidly adjust to the dynamics of the industry; and
- provide DoD’s captive microelectronics suppliers and dedicated facilities that can provide cost-effective upgrade capabilities and deliver more advanced technologies for the specialty areas they serve.
Appendix I – Full Text of NDAA 2017 § 231

SEC. 231. STRATEGY FOR ASSURED ACCESS TO TRUSTED MICROELECTRONICS.

(a) STRATEGY.—The Secretary of Defense shall develop a strategy to ensure that the Department of Defense has assured access to trusted microelectronics by not later than September 30, 2019.

(b) ELEMENTS.—The strategy under subsection (a) shall include the following:

1. Definitions of the various levels of trust required by classes of Department of Defense systems.
2. Means of classifying systems of the Department of Defense based on the level of trust such systems are required to maintain with respect to microelectronics.
3. Means by which trust in microelectronics can be assured.
4. Means to increase the supplier base for assured microelectronics to ensure multiple supply pathways.
5. An assessment of the microelectronics needs of the Department of Defense in future years, including the need for trusted, radiation-hardened microelectronics.
6. An assessment of the microelectronic needs of the Department of Defense that may not be fulfilled by entities outside the Department of Defense.
7. The resources required to assure access to trusted microelectronics, including infrastructure, workforce, and investments in science and technology.
8. A research and development strategy to ensure that the Department of Defense can, to the maximum extent practicable, use state of the art commercial microelectronics capabilities or their equivalent, while satisfying the needs for trust.
9. Recommendations for changes in authorities, regulations, and practices, including acquisition policies, financial management, public-private partnership policies, or in any other relevant areas, that would support the achievement of the goals of the strategy.

(c) SUBMISSION AND UPDATES.—

1. Not later than one year after the date of the enactment of this Act, the Secretary shall submit to the congressional defense committees the strategy developed under subsection (a). The strategy shall be submitted in unclassified form, but may include a classified annex.
2. Not later than two years after submitting the strategy under paragraph (1) and not less frequently than once every two years thereafter until September 30, 2024, the Secretary shall update the strategy as the Secretary considers appropriate to support Department of Defense missions.
(d) DIRECTIVE REQUIRED.—Not later than September 30, 2019, the Secretary of Defense shall issue a directive for the Department of Defense describing how Department of Defense entities may access assured and trusted microelectronics supply chains for Department of Defense systems.

(e) REPORT AND CERTIFICATION.—Not later than September 30, 2020, the Secretary of the Defense shall submit to the congressional defense committees—

(1) a report on—
   (A) the status of the implementation of the strategy developed under subsection (a);
   (B) the actions being taken to achieve full implementation of such strategy, and a timeline for such implementation; and
   (C) the status of the implementation of the directive required by subsection (d); and

(2) a certification of whether the Department of Defense has an assured means for accessing a sufficient supply of trusted microelectronics, as required by the strategy developed under subsection (a).

(f) DEFINITIONS.—In this section:

(1) The term “assured” refers, with respect to microelectronics, to the ability of the Department of Defense to guarantee availability of microelectronics parts at the necessary volumes and with the performance characteristics required to meet the needs of the Department of Defense.

(2) The terms “trust” and “trusted” refer, with respect to microelectronics, to the ability of the Department of Defense to have confidence that the microelectronics function as intended and are free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during its life cycle.
Appendix II – Lexicon

Definitions

Assurance: the ability of DoD to have confidence that the microelectronics function as intended and are free of exploitable vulnerabilities (replaces § 231(f)(2) definition of trust).

Availability and Access: the ability to obtain technologies and capabilities needed to meet mission objectives (replaces § 231(f)(1) definition of assured); terms are synonymous within the program protection plan framework.

Bitstream: the data file that describes the program state of a field-programmable gate array.

Cloning: the creation of an exact copy of a genuine part outside of the control of the authorized manufacturer, potentially enabled by IP theft or reverse engineering.31

Commercial-Off-the-Shelf: generally catalog items purchased from the merchant marketplace based on their performance, cost, and availability.

Confidentiality: the protection of IP, ranging from proprietary design information to the information that resides in hardware, through mitigations; analogous to the program protection term protect IP.

Counterfeiting: the misrepresentation of an unlawfully reproduced part as being authentic and unmodified,32 potentially by incorporating components of legitimate, discarded devices.

Criticality Levels: categories of mission impact that would occur if a component or system failed.

I. Total mission failure – would result in a complete compromise of mission capability.
II. Significant degradation – would result in an unacceptable compromise of mission capability.
III. Acceptable degradation – would result in partial compromise of mission capability.
IV. Negligible – would result in minimal compromise of mission capability.

Appendix II – Lexicon

*Design Alteration:* the modification of a product’s specifications, design documents, or physical design to create system weaknesses.  

*Hardware Assurance:* refers to the level of confidence that microelectronics (also known as microcircuits, semiconductors, and ICs, including its embedded software and/or IP) function as intended and are free of known vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system’s hardware and/or its embedded software and/or IP, throughout the life cycle.

*Hardware Theft:* the unauthorized removal of genuine electronic parts, potentially to facilitate IP theft or reverse engineering.

*Hardware Trojans:* the addition or bypassing of IC logic to enable malicious actions, such as disabling encryption or enabling an externally-triggered device failure.

*Integrity:* the state of being free from defects or unwanted features that jeopardize performance or reliability; analogous to the PPP term *function as intended.*

*IP Theft:* the unlawful acquisition of classified, trade secret, or proprietary information associated with microelectronics designs or hardware.

*Mitigation Levels:* the categories of mitigations that may be used to protect systems with different criticality.

  - Level 1 – mitigations that need to protect against state actors (may include classification).
  - Level 2 – mitigations that are tailored for specialty Government situation, which may be provided through the JFAC.
  - Level 3 – mitigations that can be rendered by a third-party service provider.
  - Level 4 – mitigations that serve as deterrents for low-level actors, which can be broadly applied by industry.

*Obsolescence,* the lack of availability of a particular component, potentially as a supplier ceases producing or supporting the component.

---

Appendix II – Lexicon

*Reverse Engineering:* actions taken to determine the underlying structure, function, and composition of a device for the purpose of replicating or defeating the device.\(^{37}\)

*Software Assurance:* the level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the life cycle.\(^{38}\)

*Supplier Loss:* the inaccessibility of a particular supplier, potentially due to the supplier’s closure or acquisition.

*Unauthorized Production:* the manufacture of microelectronic components by a legitimate supplier without DoD’s permission, which can threaten the loss of critical IP.

**Abbreviations and Acronyms**

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASIC</td>
<td>application-specific integrated circuit</td>
</tr>
<tr>
<td>BiCMOS</td>
<td>bipolar CMOS</td>
</tr>
<tr>
<td>CAPE</td>
<td>Cost Assessment and Program Evaluation</td>
</tr>
<tr>
<td>CF</td>
<td>critical functionality</td>
</tr>
<tr>
<td>CFIUS</td>
<td>Committee on Foreign Investment in the United States</td>
</tr>
<tr>
<td>CHIPS</td>
<td>Common Heterogeneous Integration and Intellectual Property Reuse Strategies</td>
</tr>
<tr>
<td>COTS</td>
<td>commercial off-the-shelf</td>
</tr>
<tr>
<td>CMOS</td>
<td>complementary metal-oxide semiconductor</td>
</tr>
<tr>
<td>CPI</td>
<td>critical program information</td>
</tr>
<tr>
<td>CRAFT</td>
<td>Circuits at Faster Timelines</td>
</tr>
<tr>
<td>CWM</td>
<td>cyber world model</td>
</tr>
<tr>
<td>DARPA</td>
<td>Defense Advanced Research Projects Agency</td>
</tr>
<tr>
<td>DHS</td>
<td>U.S. Department of Homeland Security</td>
</tr>
<tr>
<td>DIB</td>
<td>defense industrial base</td>
</tr>
<tr>
<td>DIUx</td>
<td>Defense Innovation Unit Experimental</td>
</tr>
<tr>
<td>DMEA</td>
<td>Defense Microelectronics Activity</td>
</tr>
<tr>
<td>DoD</td>
<td>Department of Defense</td>
</tr>
</tbody>
</table>


\(^{38}\) DoDI 5200.44
Appendix II – Lexicon

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoDI</td>
<td>Department of Defense Instruction</td>
</tr>
<tr>
<td>DSB</td>
<td>Defense Science Board</td>
</tr>
<tr>
<td>DSS</td>
<td>Defense Security Service</td>
</tr>
<tr>
<td>DTRA</td>
<td>Defense Threat Reduction Agency</td>
</tr>
<tr>
<td>EDA</td>
<td>electronic design automation</td>
</tr>
<tr>
<td>ERI</td>
<td>Electronics Research Initiative</td>
</tr>
<tr>
<td>FOCI</td>
<td>foreign ownership, control, or influence</td>
</tr>
<tr>
<td>FPGA</td>
<td>field-programmable gate array</td>
</tr>
<tr>
<td>FY</td>
<td>fiscal year</td>
</tr>
<tr>
<td>GAO</td>
<td>Government Accountability Office</td>
</tr>
<tr>
<td>GOTS</td>
<td>Government off-the-shelf</td>
</tr>
<tr>
<td>GPP</td>
<td>general purpose processors</td>
</tr>
<tr>
<td>HBM</td>
<td>high bandwidth memory</td>
</tr>
<tr>
<td>IARPA</td>
<td>Intelligence Advanced Research Projects Agency</td>
</tr>
<tr>
<td>IP</td>
<td>intellectual property</td>
</tr>
<tr>
<td>ITAR</td>
<td>International Traffic in Arms Regulations</td>
</tr>
<tr>
<td>JFAC</td>
<td>Joint Federated Assurance Centers</td>
</tr>
<tr>
<td>JUMP</td>
<td>Joint University Microelectronics Program</td>
</tr>
<tr>
<td>KSI</td>
<td>keyless signature infrastructure</td>
</tr>
<tr>
<td>LDMOS</td>
<td>laterally diffused metal oxide semiconductor</td>
</tr>
<tr>
<td>MINSEC</td>
<td>Microelectronics Innovation for National Security and Economic Competitiveness</td>
</tr>
<tr>
<td>NDAA</td>
<td>National Defense Authorization Act</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>nm</td>
<td>nanometer</td>
</tr>
<tr>
<td>ONR</td>
<td>Office of Naval Research</td>
</tr>
<tr>
<td>OSD</td>
<td>Office of the Secretary of Defense</td>
</tr>
<tr>
<td>PPP</td>
<td>program protection plan</td>
</tr>
</tbody>
</table>
### Appendix II – Lexicon

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>QML</td>
<td>Qualified Manufacturers List</td>
</tr>
<tr>
<td>R&amp;D</td>
<td>research and development</td>
</tr>
<tr>
<td>RH</td>
<td>radiation hardened</td>
</tr>
<tr>
<td>RHBD</td>
<td>radiation hardened by design</td>
</tr>
<tr>
<td>RHBP</td>
<td>radiation hardened by process</td>
</tr>
<tr>
<td>RMF</td>
<td>risk management framework</td>
</tr>
<tr>
<td>ROIC</td>
<td>read out integrated circuit</td>
</tr>
<tr>
<td>SCRM</td>
<td>supply chain risk management</td>
</tr>
<tr>
<td>SHIELD</td>
<td>Supply Chain Hardware Integrity for Electronics Defense</td>
</tr>
<tr>
<td>SoC</td>
<td>system on a chip</td>
</tr>
<tr>
<td>SOI</td>
<td>silicon on insulator</td>
</tr>
<tr>
<td>SOTA</td>
<td>state of the art</td>
</tr>
<tr>
<td>SOTP</td>
<td>state of the practice</td>
</tr>
<tr>
<td>T&amp;AM</td>
<td>Trusted and Assured Microelectronics</td>
</tr>
<tr>
<td>TSN</td>
<td>trusted systems and networks</td>
</tr>
<tr>
<td>U.S.</td>
<td>United States</td>
</tr>
<tr>
<td>USG</td>
<td>United States Government</td>
</tr>
<tr>
<td>V&amp;V</td>
<td>validation and verification</td>
</tr>
</tbody>
</table>
## Appendix III – Policy Reference Documents

<table>
<thead>
<tr>
<th>DoD Reference</th>
<th>Location</th>
<th>Areas Addressed</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoD Instruction 5000.02, Operation of the Defense Acquisition System, Enclosure 3, Systems Engineering, Paragraph 13, Program Protection</td>
<td><a href="http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002_dodi_2015.pdf?ver=2017-08-11-170656-430">http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002_dodi_2015.pdf?ver=2017-08-11-170656-430</a></td>
<td>Managing risks to DoD 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</td>
</tr>
<tr>
<td>DoD Instruction 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks</td>
<td><a href="http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520044p.pdf">http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520044p.pdf</a></td>
<td>Minimizing the risk that DoD’s warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system’s mission critical functions or critical components</td>
</tr>
<tr>
<td>DoD Instruction 8500.01, Cybersecurity</td>
<td><a href="http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf">http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf</a></td>
<td>Ensuring appropriate level of confidentiality, integrity, and availability of DoD information in electronic format</td>
</tr>
<tr>
<td>National Institute of Standards and Technology Special Publication 800-30, Guide for Conducting Risk Assessments.</td>
<td><a href="https://csrc.nist.gov/publications/detail/sp/800-30/archive/2002-07-01">https://csrc.nist.gov/publications/detail/sp/800-30/archive/2002-07-01</a></td>
<td>A five-level assessment scale to define levels of risk (not trust), ranging from very low to very high, of the system, subsystem, and component vulnerability.</td>
</tr>
<tr>
<td>DoD Reference</td>
<td>Location</td>
<td>Areas Addressed</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Defense Acquisition Guidebook, Chapter 9, Program Protection</td>
<td><a href="https://www.dau.mil/tools/dag/Pages/DAG-Page-Viewer.aspx?source=https://www.dau.mil/guidebooks/Shared%20Documents%20HTML/Chapter%209%20Program%20Protection.aspx">https://www.dau.mil/tools/dag/Pages/DAG-Page-Viewer.aspx?source=https://www.dau.mil/guidebooks/Shared%20Documents%20HTML/Chapter%209%20Program%20Protection.aspx</a></td>
<td>Processes, methodologies, and techniques to enable program offices to identify information, components, and technologies, as well as determine the most appropriate mix of measures to protect the information, components, and technologies from known security threats and attacks.</td>
</tr>
<tr>
<td>Defense Acquisition University Course ACQ160, Program Protection Planning and Awareness</td>
<td><a href="http://icatalog.dau.mil/mobile/CourseDetails.aspx?id=2082">http://icatalog.dau.mil/mobile/CourseDetails.aspx?id=2082</a></td>
<td>Principles and policies of system security engineering. Course provides training on threats, vulnerabilities, risks, cost-benefit risk trade-offs, and required mitigations for DoD systems. Also addresses supply chain management and the need for acquisition program protection documents such as the Program Protection Plan, Cybersecurity Strategy, and security plans.</td>
</tr>
<tr>
<td>NDAA § 231(b) Element</td>
<td>Report Section(s)</td>
<td></td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------</td>
<td></td>
</tr>
<tr>
<td>(1)</td>
<td>3.1.</td>
<td></td>
</tr>
<tr>
<td>(2)</td>
<td>3.1.</td>
<td></td>
</tr>
<tr>
<td>(3)</td>
<td>3.2.</td>
<td></td>
</tr>
<tr>
<td>(4)</td>
<td>4.2., 4.3., 4.4.</td>
<td></td>
</tr>
<tr>
<td>(5)</td>
<td>1.1., 1.2.,</td>
<td></td>
</tr>
<tr>
<td>(6)</td>
<td>1.2., 3.1.2, 4.1., 4.2.</td>
<td></td>
</tr>
<tr>
<td>(7)</td>
<td>2.3.</td>
<td></td>
</tr>
<tr>
<td>(8)</td>
<td>2.4.</td>
<td></td>
</tr>
<tr>
<td>(9)</td>
<td>5.(1-3).</td>
<td></td>
</tr>
</tbody>
</table>
Appendix V – MINSEC: DEPSECDEF Priorities and Problem Areas of Focus

The USG currently faces many challenges to obtaining access to assured microelectronics due to few domestic SOTA foundries and packaging, market domination by commercial forces, excessive cost to access foundries, and accelerated market growth in Asia. Development complexity, costs, and lack of expertise and security are stifling innovation in SoC ASIC hardware. Additionally, DoD influence is limited and national security needs are not being met. The table below outlines the Deputy Secretary of Defense (DEPSECDEF) priorities and how the DoD MINSEC initiative will help to achieve the desired outcomes.

<table>
<thead>
<tr>
<th>DEPSECDEF Priorities</th>
<th>DoD MINSEC Actions and Investments</th>
<th>Outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enhance Lethality</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Focus on modernization to sustain war fighting systems</td>
<td>- Provide Assured access to advanced microelectronics</td>
<td>- Strong domestic assured source for Gov. and private innovative</td>
</tr>
<tr>
<td>and capabilities</td>
<td>through SOTA, SOTP, and Government foundries &amp; packaging</td>
<td>microelectronics products</td>
</tr>
<tr>
<td>- Align DoD R&amp;D with commercial companies to rip-off and</td>
<td>- Provide Assured secure development community (intellectual</td>
<td>- Significantly reduced barriers to rapid capability development with</td>
</tr>
<tr>
<td>deploy innovation</td>
<td>property (IP), electronic data automation (EDA), experts,</td>
<td>assurance for Gov. and cooperative emerging industries</td>
</tr>
<tr>
<td></td>
<td>secure computing, Government IP) for innovation</td>
<td></td>
</tr>
<tr>
<td>- Leverage what industry does well, and use it as a base</td>
<td>- Support Innovative co-development including COTS of 10-1000x</td>
<td>- Highly productive designers develop complex systems with assurance, at</td>
</tr>
<tr>
<td>for modernization</td>
<td>capabilities for US Government (USG) and strategic growth</td>
<td>a rapid pace and low cost with immediate demonstrations to maintain</td>
</tr>
<tr>
<td></td>
<td>application areas</td>
<td>technological superiority</td>
</tr>
<tr>
<td>DEPSECDEF Priorities</td>
<td>DOD MINSEC Actions and Investments</td>
<td>Outcomes</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td><strong>Drive Reformation</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Listen to what industry says about process issues that are impediments to innovation</td>
<td>- Acquire global business intelligence, invest in Intel and Counterintelligence</td>
<td>- Access to assured SOTA COTS devices</td>
</tr>
<tr>
<td>- Stop doing things that impede Government and Industry from working together</td>
<td>- Collaborate to ensure commercial &amp; DoD needs are considered and develop tools and technologies that allow rapid redesign of complex systems</td>
<td>- Immediate performance improvement and close parity to SOTA microelectronics for USG purposes &amp; create manifold sources for SOTA in and SOTP foundries in the U.S.</td>
</tr>
<tr>
<td>- Need to operate/innovate quickly</td>
<td>- Acquisition reform and incentives to encourage technology capability insertions every 1-2 years in programs</td>
<td>- Rapid low-cost co-development development of 10-1000x performance capabilities in DoD systems and low-volume production to capture innovation and manufacturing throughout the U.S.</td>
</tr>
<tr>
<td><strong>Form Alliances</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Nurture and grow the industrial base to show investments in semiconductors are important to increasing national security</td>
<td>- Leverage industry collaboration to develop disruptive materials and electronics to lead next generation of technology globally</td>
<td>- Develop onshore manufacturing and design capacity to own the next generation of microelectronics technology so U.S. has access to best global technologies</td>
</tr>
<tr>
<td>- Invest in commercial industry rather than infrastructure</td>
<td>- Develop enabling manufacturing technologies for enhanced microelectronics manufacturing in U.S.</td>
<td>- Significant R&amp;D co-investment in domestic ecosystem maintain U.S. leadership in the semiconductor industry</td>
</tr>
<tr>
<td>- Expand networks to partner with allies</td>
<td>- Partnerships with Allies for access and cooperative development, FMS, security awareness</td>
<td>- U.S. has assured access to best global technologies and allies help create disruptive R&amp;D and fabrication tools to stay ahead of competitors</td>
</tr>
</tbody>
</table>
Appendix V – MINSEC: DEPSECDEF Priorities and Problem Areas of Focus

The MINSEC initiative will address six broad categories of areas of concern including: access, assurance, and demonstration; enhanced manufacturing; disruptive R&D; incentives and market growth; proactive security and awareness; and strategic alliances. The table below provides greater detail on the identified problems, actions and investments through the MINSEC initiative, and desired outcomes.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Actions and Investments</th>
<th>Outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access, Assurance, and Demonstration</td>
<td>- Few domestic SOTA foundries and packaging, dominated by commercial forces, $ to access, growth in Asia</td>
<td>- Provide Assured access to SOTA, SOTP, and Gov. foundries &amp; packaging</td>
</tr>
<tr>
<td></td>
<td>- Development complexity, costs, and lack of expertise and security are stifling innovation in SoC ASIC hardware</td>
<td>- Provide Assured development community (IP, EDA, experts, secure computing, Gov. IP) for innovation</td>
</tr>
<tr>
<td></td>
<td>- DoD influence is limited and national security needs not being met</td>
<td>- Support Innovative co-development of 10-1000x capabilities for USG and strategic growth application areas</td>
</tr>
<tr>
<td>Enhanced Manufacturing</td>
<td>- Many domestic SOTP foundries are at 200mm and &gt;65nm nodes and aren’t being updated</td>
<td>- Enhance SOTP foundries to 65nm and copper back end and E-Beam litho now and Co-develop advanced fabrication (5-65nm) tools for existing 200mm</td>
</tr>
<tr>
<td></td>
<td>- Advanced-node flexible, scalable manufacturing is not available in U.S.</td>
<td>- Develop mini-fab to transform and distribute SOTA disruptive technology development for high-mix low-volume</td>
</tr>
<tr>
<td></td>
<td>- Innovative R&amp;D going to foreign sources to scale and integrate new device and circuits architectures</td>
<td>- COTS Co-development (FPGA, ML)</td>
</tr>
<tr>
<td>Problem</td>
<td>Actions and Investments</td>
<td>Outcomes</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------</td>
<td>----------</td>
</tr>
<tr>
<td><strong>Disruptive R&amp;D</strong></td>
<td>- USG investment in disruptive R&amp;D for next-generation microelectronics has significantly diminished&lt;br&gt;- Research is stagnant when an inflection point in the electronics industry marked by changes in Moore’s Law is about to occur&lt;br&gt;- The country that exploits this inflection point will maintain or obtain economic and security superiority</td>
<td>- Leverage DARPA JUMP program and industry collaboration to develop disruptive materials and electronics&lt;br&gt;- Lead the development of new circuit architectures for next-generation computing and strategic applications&lt;br&gt;- Develop tools and technologies that allow rapid redesign of complex systems</td>
</tr>
<tr>
<td><strong>Incentives and Market Growth</strong></td>
<td>- DoD acquisition slow, $$$, and difficult to leverage commercial or frequently refresh technology&lt;br&gt;- Current tax policy, regulations, and incentives discourage domestic investment&lt;br&gt;- Tax policy and incentives discourages R&amp;D compared to non-nationals</td>
<td>- Acquisition reform and incentives to encourage technology capability insertions every 1-2 years&lt;br&gt;- Work with Commerce and State to reform tax policy and encourage investment in domestic production&lt;br&gt;- Enact pre- and post-tax reform for R&amp;D in microelectronics</td>
</tr>
<tr>
<td>Problem</td>
<td>Actions and Investments</td>
<td>Outcomes</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------</td>
<td>----------</td>
</tr>
<tr>
<td><strong>Proactive Awareness &amp; Security</strong>&lt;br&gt;- Complex international Microelectronics supply chain and lack of intelligence focus and resources&lt;br&gt;- Lack of ownership and responsibility in USG and Outdated Authorities to take action&lt;br&gt;- DoD influence is limited and national security needs not being met</td>
<td>- Acquired global business intelligence, invest in Intel and Counterintelligence&lt;br&gt;- Empower responsibility for Awareness and careful use of Authorities&lt;br&gt;- Collaborate with industry on international standards to ensure DoD needs are considered</td>
<td>- Awareness of Global, Allies, Domestic and DoD Supply Chain&lt;br&gt;- Critical IP and capabilities from R&amp;D and domestic production are protected and nurtured within U.S. and allied ecosystem&lt;br&gt;- Commercial standards include DoD interests when possible</td>
</tr>
<tr>
<td><strong>Strategic Alliances</strong>&lt;br&gt;- Ca not go it alone to create the best of every technology&lt;br&gt;- Europeans and Asian partners invest heavily and have good models for R&amp;D for microelectronics&lt;br&gt;- Foreign Military Sales supports defense ecosystem and depends on having the best technology</td>
<td>- Partnerships with Allies for access and cooperative development&lt;br&gt;- Partnerships with Americas, Asia, Europe allies on R&amp;D&lt;br&gt;- Strengthen FMS and investments in technology from Allies</td>
<td>- U.S. has access to best global technologies&lt;br&gt;- Others help U.S. create disruptive R&amp;D and fabrication tools&lt;br&gt;- Defense ecosystem in U.S. is strong and enhanced by partner needs</td>
</tr>
</tbody>
</table>
Appendix VI – DoD MINSEC Initiative Funding Plans

The President’s DoD investment strategy for MINSEC was developed by DASD(SE) at the request of OMB and the NSC sub Policy Coordinating Committee on Semiconductors. The following is a detailed funding plan within DoD for FY 2019-2023 activities that are included in the FY 2019 budget to serve the needs of DoD around microelectronics. These funds are designed to be part of a larger Whole-of-Government investment to solve the economic competitiveness issues for the nation around semiconductors.

A. Overview.

• U. S. leadership in, and access to assured advanced microelectronics is vital to the national security and economic competitiveness.
  
  o Advanced microelectronics technology is fundamental to DoD priorities, and essential for autonomous, AI, next generation precision navigation and timing systems, electronic warfare systems, and strategic weapons.
  
  o The future of commercial space, biomedical technology, financial and data analytics, autonomous systems, agile communications, and internet-of-things are all reliant upon microelectronics innovation.

• Means of producing advanced, assured microelectronics within the U.S. is fragile.
  
  o Other nations are investing billions of dollars as part of their national strategies to achieve dominance in all major areas of microelectronics.
  
  o The U.S. struggles to attract investment for leading edge fabrication and design innovation despite a supporting infrastructure of research, design, IP rights, and physical plants that make the U.S. a valuable resource for the semiconductor industry.

• The Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics initiated the T&AM program, established in the FY 2017 to ensure assured microelectronics are available to meet the DoD’s needs. This program provides protections to ensure military unique chips are protected from malicious exploit (loss of DoD IP), and from malicious tampering during design and manufacturing. It also mitigates DoD’s reliance on sole source foundries for SOTA microelectronics.

• In recognition of critical near-term needs, DoD received an additional $251 million in FY 2018 in support of MINSEC, a new DoD initiative, to address gaps in availability, access, and assurance. This funding was distributed amongst program elements (PEs) for FPGA assurance and secure design environments, for DARPA Electronics Resurgence Initiative (ERI), and DMEA critical IP procurement, and access to advanced foundry processes.
• Additional DoD MINSEC funding totaling $2.185 billion was approved during the FY 2019 PB process to provide a multi-level response to current known threats that begins to: secure U.S. national microelectronics interests, reverse the erosion of domestic innovation and supply, and establish a strong leadership foundation for the next-generation of microelectronics technology for DoD applications.

• The following DoD MINSEC technical focus areas will be initiated in FY 2019 and will continue across the Future Years Defense Program to:
  
  o Develop next-generation disruptive R&D microelectronics technologies
  o Capture and secure microelectronics R&D and production in the U.S. ecosystem
  o Develop, demonstrate, and insert new microelectronics capabilities
  o Co-develop COTS programmable ICs and IP
  o Replace obsolete microelectronics using SOTA designs
  o Provide RHBP and RHBD techniques and IP to ensure the continued availability of DoD strategic radiation-hardened microelectronics
  o Provide radio frequency and optoelectronic design techniques and IP.

Deputy Assistant Secretary of Defense
Systems Engineering
3030 Defense Pentagon
3C167
Washington, DC 20301-3030

E-mail: osd.atl.asd-re.se@mail.mil
Website: www.acq.osd.mil/se

DISTRIBUTION STATEMENT A: Approved for public release. Distribution is unlimited.
DOPSR Case #18-S-2455