Department of Defense

Assured Microelectronics Policy

Senate Report 113-85

JULY 2014

Office of the Under Secretary of Defense for
Acquisition, Technology, and Logistics

The estimated cost of this report for the Department of Defense is approximately $52,000 in Fiscal Year 2014.
This includes $47,000 in expenses and $4,340 in DoD Labor.
Cost estimate generated on July 7, 2014. Reference # 4-E848DBE

Department of Defense Assured Microelectronics Policy. Senate Report 113-85

Under Secretary of Defense for Acquisition, Technology, and Logistics
3020 Defense Pentagon
Washington, DC 20301-3020

Contents

Figures

Tables

This page intentionally blank.

1 Introduction

This Report on Assured Microelectronics Policy is in response to Senate Report 113-85, page 179, accompanying S. 1429, the Department of Defense Appropriations Bill, 2014, SAC-D, which states:

> *"Assured Microelectronics.—The Committee understands that the Department of Defense issued an instruction which mandates assurance measures for all information and weapons systems that are national security systems, mission assurance category one, or are otherwise critical military and intelligence systems. The Committee directs the Department to deliver a report within 180 days of the enactment of this act on the progress implementing this assured microelectronics policy."*

The policy referred to in the Senate Appropriations Committee (SAC) report is Department of Defense (DoD) Instruction (DoDI) 5200.44, "Protection of Mission-Critical Functions to Achieve Trusted Systems and Networks (TSN)," November 5, 2012. The Instruction provides a strategy for acquisition programs to integrate robust systems engineering, supply chain risk management (SCRM), security, counterintelligence (CI), intelligence, information assurance, software assurance, and hardware assurance (with an emphasis on microelectronics) for managing risks to system integrity and trust. The Instruction provides guidance for managing the risk that a foreign intelligence or other hostile elements could exploit supply chain vulnerabilities to sabotage or subvert mission-critical functions, system designs, or critical components (CC).

DoDI 5200.44 applies to national security systems as defined by section 3542 of title 44, U.S.C., Mission Assurance Category 1 systems, and to other DoD information systems determined by a DoD Component's acquisition executive or chief information officer to be critical to the direct fulfillment of a military or intelligence mission. The policy requires that these programs perform a criticality analysis to identify mission-critical functions and the supporting CC to determine the information and communications technology that must be assessed for security risks and protected. CC can be software, firmware, or hardware. Protection of CC can be addressed by SCRM, cybersecurity, and other security-related countermeasures. To help identify where hardware and software protection may be warranted, a threat assessment is performed as part of the analysis of security risks, which includes an all-source intelligence review by the Defense Intelligence Agency (DIA) of the supply chain for CC.

Comprehensive planning for, and implementation of, acquisition program protection and the technical discipline of system security engineering (SSE) are the keys to maintaining trust in systems and the microelectronics and other CC in them. The planning process must integrate all the protection measures that support assured CC development (hardware assurance, software assurance, SCRM, etc.). The goal of these protective measures is to reduce the risk to the mission by mitigating identified threats and vulnerabilities, such as malicious code insertions or

counterfeit parts or the loss of technical information. Risk to system trust is managed throughout the entire system life cycle beginning with design and before the acquisition or integration of CC into covered systems.

The DoD Chief Information Officer (CIO) and the Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)) have led the establishment of a network of knowledgeable TSN focal points at the DoD Components to foster systemic implementation of DoDI 5200.44. The TSN focal points are assisting the Office of the Secretary of Defense (OSD) with the refinement of TSN policy and guidance and with program engagement to support Program Protection Plan (PPP) development and implementation of TSN throughout the life cycle, including during Operations and Support. In addition, DoD CIO has created cybersecurity controls to implement key TSN responsibilities and published TSN implementation guidance (e.g., criticality analysis guidance and SCRM Key Practices) on the Risk Management Framework (RMF) Knowledge Service, in a dedicated section for TSN and SCRM content. As a result, senior program management and acquisition officials are gaining greater insight and becoming more involved in the protection of Critical Program Information (CPI) and mission-critical functions and components.

1.1 Background

In a policy memo published in October 2003, the Deputy Secretary of Defense called for a "Defense Trusted Integrated Circuit Strategy." The memo recognized the need for a defense industrial base that provides access to trusted suppliers of critical microcircuits used in sensitive defense weapons, intelligence, and communication systems. The strategy mandated the following:

- Identification of facilities that could qualify as "trusted sources" for application-specific integrated circuits (ASIC);
- Identification of the types of microcircuit products these facilities can produce;
- Near-term solutions for ensuring Department acquisition strategies maximize competitive opportunities while preserving domestic capability;
- Development of design and test procedures for assuring microcircuit integrity and for accessing the next generation of specialized defense applications; and
- Preservation of a healthy domestic commercial microcircuit industrial base.

In January 2004, in response to the Deputy Secretary's memo, the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) issued several policy memos that established interim guidance on trusted suppliers for ASICs. Through the policy memos and congressional funding, the USD(AT&L) initiated a pilot program with the National Security Agency (NSA) that led to the formation of the Trusted Access Program Office (TAPO) and a

contractual arrangement with the IBM Corporation for the manufacture of leading-edge microelectronic parts in a trusted environment. Over the next several years, the pilot expanded to include a security accreditation program through which the DoD Defense Microelectronics Activity (DMEA) evaluates and accredits suppliers for trusted microelectronic services, which encompass integrated circuit design, aggregation, brokerage, mask manufacturing, foundry, post processing, packaging/assembly, and test services.

USD(AT&L) and the Assistant Secretary of Defense for Networks and Information Integration/ DoD CIO introduced the TSN strategy in December 2009 in the "Report on Trusted Defense Systems in Response to National Defense Authorization Act," a report to Congress required by section 254 of Public Law 110-417, "Trusted Defense System," of the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009. The Trusted Defense System legislation required the Department to:

- Assess select acquisition programs to identify vulnerabilities in the supply chain of electronics and information processing systems that potentially compromise the trust in those systems.
- Assess methods for verifying the trust of semiconductors used in mission-critical components.
- Establish an integrated strategy for managing risk in the supply chain of electronics and information processing systems.
- Establish policies and actions for assuring trust in integrated circuits.

Since the introduction of DoDI 5200.44, the Department has made significant progress toward implementing its TSN strategy (Figure 1).

DoD Progress in Implementing the TSN Strategy

- *USD(AT&L) revised DoDI 5000.02 to reference DoDI 5200.44 and provide specific policy, e.g., the required use of software assurance and related tools, for acquisition programs regarding the implementation of TSN, to include CC and supply chain protection.*
- *In FY 2013, the first year after publication of the DoDI 5200.44, USD(AT&L) approved 18 PPPs.*
- *The DIA Threat Assessment Center (TAC) has conducted over 1,678 all source intelligence threat assessments to date.*
- *Currently, the DoD Trusted Supplier program has accredited 62 facilities to provide trusted services, of which 17 are foundries.*
- *The Trusted Access Program Office (TAPO) has renewed its multi-year contract to maintain DoD access to advanced, trusted microelectronics fabrication technology.*

Figure 1. DoD Progress in Implementing the TSN Strategy

As shown in Figure 2, DoDI 5200.44 is only one aspect of an integrated policy framework for program protection planning, which has undergone, and continues to undergo, significant revision to keep pace with rapidly evolving threats, technologies, best practices, and related policies and guidance.

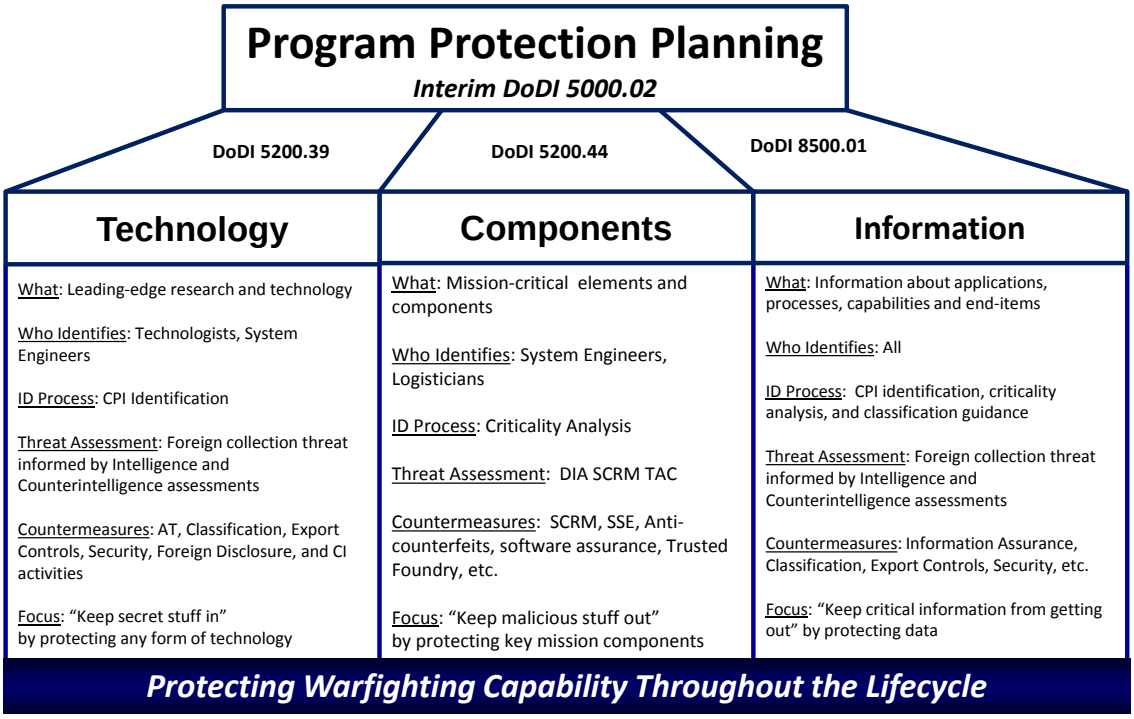

Figure 2. Program Protection Planning

In November 2013, the USD(AT&L) published an Interim DoDI 5000.02, "Operation of the Defense Acquisition System," to encourage greater efficiency and productivity in defense spending and the implementation of the Department's Better Buying Power initiatives. Included in the revised instruction is language linking the defense acquisition process and program protection planning with DoDI 5200.44; DoDI 5200.39, "Critical Program Information (CPI) Protection within the Department of Defense," Change 1, December 28, 2010; and DoDI 8500.01, "Cybersecurity," March 14, 2014.

DoDI 5200.39 requires the protection of CPI through the use of CI, intelligence, security, systems engineering, and other defensive countermeasures. To mitigate the exploitation of CPI, a risk management approach is used to select protection measures and to document them in a PPP. The instruction requires that programs refine their PPP at each milestone or as directed by the Milestone Decision Authority (MDA), and it also requires that programs protect CPI throughout the life cycle.

DoDI 8500.01 implements a multi-tiered risk management process for cybersecurity to protect U.S. and DoD interests aligned with policy previously established by the National Institute for Standards and Technology (NIST) and the Committee on National Security Systems. It also

requires that risks associated with vulnerabilities inherent in information technology (IT), global sourcing and distribution, and adversary threats to DoD use of cyberspace must be considered in DoD employment of capabilities and that cybersecurity risk management be implemented early in the acquisition of IT and in an integrated manner across the life cycle.

A companion instruction, DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology," March 12, 2014, establishes and requires the use of an integrated enterprise-wide decision structure for cybersecurity risk management, which informs acquisition processes for all DoD IT, including requirements development, procurement, and both developmental and operational test and evaluation. The interrelationship between these two instructions, along with DoDI 5000.02 and DoDI 5200.44, are explained further in USD(AT&L) Defense Acquisition Guidebook (DAG) Chapter 13, Program Protection.[1]

In addition, DoD participated with the General Services Administration (GSA), under the Executive Order (EO) 13636, Cybersecurity for Critical Infrastructure, February 12, 2013, to publish the report "Improving Cybersecurity and Resilience through Acquisition" in November 2013. The report extends DoD TSN/SCRM lessons learned to broader Federal Government acquisition and procurement through a risk-based approach. Tables 1 and 2 list the progression of DoD assured microelectronics policy and guidance.

Table 1. Progression of Major DoD Assured Microelectronics-Related Policy

Date	Policy	Title
10/10/2003	DepSecDef memorandum	Defense Trusted Integrated Circuit Strategy
1/27/2004	USD(AT&L) memorandum	Interim Guidance on Application Specific Integrated Circuits
1/27/2004	USD(AT&L) memorandum	Encouraging Industry Participation in the Trusted Foundry Program
1/27/2004	USD(AT&L) memorandum	Expansion of the Trusted Foundry Program
7/16/2008	DoDI 5200.39	Critical Program Information Protection Within the Department of Defense (Change 1 issued 12/28/2010)
2/19/2009	DepSecDef memorandum	Directive-Type Memorandum (DTM) 08-048 – Supply Chain Risk Management to Improve the Integrity of Components Used in DoD Systems (Reissued 3/25/2010 as DTM 09-016)
11/5/2012	DoDI 5200.44	Protection of Mission-Critical Functions to Achieve Trusted Systems and Networks (TSN)
2/12/2013	EO 13636	Improving Critical Infrastructure Cybersecurity
4/26/2013	DoDI 4140.67	Counterfeit Prevention Policy
11/26/2013	DoDI 5000.02	Operation of the Defense Acquisition System Interim
3/12/2014	DoDI 8510.01	Risk Management Framework (RMF) for DoD Information Technology
3/14/2014	DoDI 8500.01	Cybersecurity

[1] https://acc.dau.mil/docs/dag_pdf/dag_ch13.pdf

Table 2. Progression of Major DoD Assured Microelectronics-Related Guidance

Date	Type	Title
12/22/2009	USD(AT&L) and ASD(NII)/DoD CIO report	Report on Trusted Defense Systems in Response to National Defense Authorization Act, Section 254
7/2011	DASD(SE) document	Program Protection Plan (PPP) Outline and Guidance
5/13/2013	DASD(SE) document	"Program Protection." Chapter 13 in Defense Acquisition Guidebook
11/2013	GSA-DoD Report	Improving Cybersecurity and Resilience through Acquisition
1/2014	DASD(SE) document	Suggested Language to Incorporate System Security Engineering for Trusted Systems and Networks into Department of Defense Requests for Proposals
2/2014	DASD(SE) document	Program Protection Plan (PPP) Evaluation Criteria, Version 1.1

DASD(SE) and the DoD CIO continue to support extensive collaboration efforts with industry, the NIST, and other Government agencies. For example, they have teamed with the National Defense Industrial Association (NDIA) System Security Engineering Committee[2] and the International Council on Systems Engineering (INCOSE) Systems Security Engineering Working Group[3] to advance the SSE discipline. In addition, DASD(SE) and DoD CIO are supporting the development of the following NIST documents:

- NIST Special Publication (SP) 800-160, Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems.[4]
- NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations.[5]

All of the aforementioned policies and guidance, with complementary logistics management policies and technical specifications discussed in the following sections of this document, help to create a comprehensive and effective process for acquiring trusted microelectronics across the life cycle.

1.2 Report Organization

Section 2 of this report discusses the Department's approach to program protection planning. Section 3 discusses assessment of the threat. Section 4 discusses vulnerability assessment and countermeasures that the Department is using to manage supply chain risk. Section 5 discusses the approach for assuring microelectronics throughout the life cycle. Section 6 includes a summary of the Department's initiatives and status in this area.

[2] http://www.ndia.org/Divisions/Divisions/SystemsEngineering/Pages/default.aspx
[3] http://www.incose.org/practice/techactivities/wg/details.aspx?id=securitywg
[4] Out for public comment
[5] Second Draft out for public comment

2 Program Protection Planning

The Department requires acquisition programs to produce and maintain a robust PPP throughout the acquisition life cycle. This requirement strengthens and facilitates the programs' adherence to the TSN strategy. The PPP must identify CPI and mission-critical functions and components, associated threats and vulnerabilities, a plan for applying countermeasures to mitigate risk, a plan for exportability and potential foreign involvement, and an analysis of program protection costs and benefits. The PPP is used to manage risks to warfighting capability from foreign intelligence collection; from hardware, software, and cyber vulnerability or supply chain exploitation; and from battlefield loss throughout the system life cycle. The PPP is the primary means by which DoD is integrating assured microelectronics policy into program management, engineering, and the configuration, parts, and contract management disciplines.

The DASD(SE) "PPP Outline and Guidance," Version 1, July 2011, requires applicable systems as described in DoDI 5200.44 to employ cost-effective countermeasures to mitigate the risk of intentional compromise of microcircuits and other CC that would result in a Criticality Level I (total mission failure) or Level II (significant/unacceptable mission degradation) impact, as determined by the criticality analysis performed by the Program Management Office (PMO). The microcircuits and other CC that are the focus of this guidance perform mission-critical functions, such as those that process or control intelligence, cryptology, command and control, and classified information, as these functions are particularly desirable targets for anyone intent on undermining the integrity of a system.

The PPP process enables comprehensive and integrated life cycle planning and execution of acquisition program security activities. DASD(SE) leads the review process for PPPs that are submitted in support of each milestone decision review for Major Defense Acquisition Programs and Major Automated Information Systems when USD(AT&L) is the approval authority. Per Figure 3, in FY 2013, the first year after publication of the DoDI 5200.44, DASD(SE) supported the review and approval by USD(AT&L) of 18 PPPs.

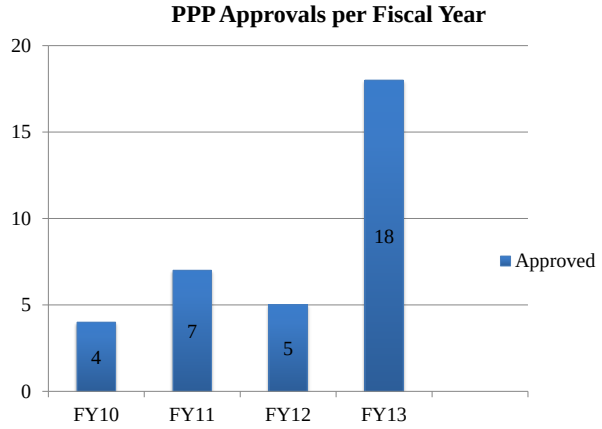

Figure 3. PPP Engagements by the Office of the Secretary of Defense

In addition, DASD(SE), along with the DoD CIO, has responded to numerous requests to provide training and insight into program protection planning and risk mitigation processes and practices. DASD(SE) publishes tutorial and other products that are available on the DASD(SE) website[6] to assist programs in the development of comprehensive program protection planning and its implementation.

DASD(SE) has also published "Program Protection Plan (PPP) Evaluation Criteria," Version 1.1, February 2014, which is used in conjunction with the DASD(SE), "Program Protection Plan (PPP) Outline and Guidance," Version 1, July 2011, to assist both the program protection planning and review processes. Similarly, designated DoD Component MDAs and their staffs review and approve PPPs under their cognizance.

In addition to PPP reviews, the Department reviews requests for proposal, as well as other program requirements and acquisition documentation, to ensure that program protection is adequately addressed by programs for which the USD(AT&L) is the MDA. DoD Components conduct similar reviews for the programs under their cognizance. DASD(SE) published "Suggested Language to Incorporate System Security Engineering for Trusted Systems and Networks into Department of Defense Requests for Proposals," January 2014, to support both requests for proposal development by the DoD Components as well as their review by DASD(SE).

3 Threat Assessment and Risk Management

To assist in identifying threats, DoDI 5200.44, Enclosure 2, paragraph 6 requires the DIA to produce intelligence and CI assessments of supplier threats to acquisition programs for critical weapons, information systems, and service capabilities. DIA has established a Threat Assessment Center (TAC) to conduct these all source threat assessments on behalf of covered programs.

The intent of the threat assessment is to protect mission-critical functions and CC, including critical microelectronics, by identifying and defending against the risk that an adversary may sabotage, maliciously introduce unwanted functions, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

The risk management process is an important part of the systems engineering process. It incorporates the threat assessment with supply chain vulnerability and weapon or information system criticality assessments. The criticality assessment includes the identification of microcircuits and other CC that warrant risk mitigation. The process assists in the selection of

[6] http://www.acq.osd.mil/se/initiatives/init_pp-sse.html

product and process countermeasures to reduce the risk of a successful exploitation of potential vulnerabilities. Risk management for a new system in acquisition starts in the Materiel Solution Analysis (MSA) phase of an acquisition program and is refined and updated at successive acquisition milestones and Systems Engineering Technical Reviews (SETR).

Supplier threat assessment requests are submitted by the DoD Component TSN focal points to the DIA TAC based on the PMO identification of CC through its criticality analysis of the planned system. An annotated work breakdown structure may be used to identify suppliers of CC to assist with the creation of DIA TAC requests. The PMO may start to submit the program's TAC Requests for Information (RFI) as soon as the system's mission-critical functions and the required supporting technologies are identified. Near the end of the MSA phase, as threat information becomes available for identified technologies and potential suppliers, the PMO can conduct its SCRM to assist in defining the lowest risk system architectures based on the identified design alternatives.

Early in the system life cycle, TAC RFIs may be more focused on suppliers in general technology areas than later in the acquisition life cycle when they should be submitted against suppliers of CC. For the policy and procedures regarding the request, receipt, and handling of DIA TAC RFIs and TAC reports, refer to DoDI O-5240.24, "Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)," June 8, 2011; Incorporating Change 1, October 15, 2013 (controlled document)).

4 Vulnerability Assessment and Countermeasures

The microcircuit supply chain and related hardware industries, such as for printed circuit boards and other CC that perform critical weapon and IT functions, are vulnerable to exploitation by adversaries. Of concern are supply chain attacks to the hardware, firmware, and/or software in a weapon or IT system that inserts malicious functionality or that degrades the performance or reliability of the system. Such attacks can occur during the design, fabrication, distribution, or integration of CC into a system. A sophisticated adversary has many potential ways to insert intentionally tainted microcircuits into a global commercial supply chain that is often outside the Department's control. The purpose of using a risk management approach is to focus limited PMO resources on addressing the most critical and vulnerable components and to decrease susceptibility to adversary attacks.

4.1 Product Inspection and Testing

Hardware assurance countermeasures for protecting individual microcircuits against counterfeiting, degraded reliability and malicious functionality insertion include product inspection and test and system-level environmental evaluations using the likely attack scenarios of substitution and exploitation. Software and firmware that are determined to be critical may

undergo static software analysis and other software assurance countermeasures to verify they are free of malicious functionality. Supply chain risk mitigation includes the use of industry-accepted configuration and parts management best practices, purchasing system and chain of custody controls, and the use of cleared facilities and personnel.

Vulnerability to exploitation and the appropriate selection of countermeasures depends on the type of microcircuits of concern, their criticality to mission success, and the ability of an adversary to target. Acquisition programs manage risk by identifying and employing the most cost-effective countermeasures available, recognizing that the complete elimination of counterfeits, malicious insertion, or intentionally degraded performance is rarely possible even in environments that require high-fidelity system assurance.

Technical performance specifications and standards are routinely used when commercially available microcircuits will not meet military performance and reliability requirements. For example, the DoD space and missile community frequently cites two performance specifications in their contracts, i.e., MIL-PRF-38535, "General Specification for Performance Specification Integrated Circuits (Microcircuits) Manufacturing," December 20, 2013, and MIL-PRF-38534J, "General Specification for Performance Specification Hybrid Microcircuits," April 13, 2014. These specifications establish general performance, quality, and reliability requirements. Both mandate the use of MIL-STD-883J, "Test Method Standard, Microcircuits," March 14, 2014. MIL-STD-883J establishes uniform methods, controls, and procedures for testing microelectronic devices, including basic environmental tests to determine resistance to deleterious effects of natural elements and conditions surrounding military and space operations; mechanical and electrical tests; workmanship and training procedures; and such other controls and constraints deemed necessary to ensure a uniform level of quality and reliability for demanding aerospace applications.

The simple adoption of these specifications is not likely to allow a program to detect or prevent the insertion of malicious vulnerabilities into microcircuits. Conventional methods, controls, and procedures for testing microcircuits can detect damage to markings, packaging, and crude attempts at counterfeiting, but they will not uncover intentional and surreptitiously implanted flaws internal to the device. The analysis of microcircuit designs, design tools and data, fabrication tooling, substrates, dies and die layers, and the electronic bit stream that devices produce when activated are time consuming and require advanced skills and equipment.

Some of the more advanced integrity analysis techniques are described in MIL-STD-1580B, "DoD Test Method Standard Destructive Physical Analysis for Electronic, Electromagnetic, and Electromechanical Parts," March 4, 2014. This document has been developed for use by the DoD and National Aeronautics and Space Administration aerospace communities. The techniques described in MIL-STD-1580B involve physical delayering, imaging, and electrical and thermal signal analysis.

Advanced integrity analysis is useful for detecting counterfeits, evaluating product quality, and identifying design software and fabrication nonconformance. Intended for use where high reliability in extreme environments is required, including space, launch vehicle, and nuclear weapons applications, these techniques are suitable for forensic analysis to determine the cause of a suspected defect, and, in their most advanced forms, are useful for detecting malicious functionality. Numerous organizations in the DoD Components use these techniques to promote hardware and software assurance on behalf of acquisition programs as system vulnerabilities and supply chain threats are identified. Projects, such as the Defense Advanced Research Projects Agency (DARPA) Integrity and Reliability of Integrated Circuits (IRIS) program and similar ongoing research efforts at NSA and DoD labs, including the Naval Surface Warfare Center (NSWC), Crane, Indiana, and the Air Force Research Laboratory, Wright Patterson Air Force Base, Dayton, Ohio, are helping to improve the DoD Components' methods for detecting counterfeits and malicious functions.

4.2 DMEA-Accredited Suppliers

A major emphasis area of the Department's assured microelectronics policy is the use of the Trusted Foundry and DMEA-accredited trusted suppliers to assure the trustworthiness of critical microcircuits used in covered systems when they are custom-designed, custom-manufactured, or tailored for a specific DoD military end use.

DMEA is the program manager for the DoD Trusted Supplier accreditation program. The program provides a cost-effective means to assure the integrity and confidentiality of integrated circuits during design and manufacturing while providing the U.S. Government with access to leading edge and legacy microelectronic technologies for both sensitive and non-sensitive applications. DMEA accredits suppliers in the areas of integrated circuit design, aggregation, brokerage, mask manufacturing, foundry, post processing, packaging/assembly, and test services. These services cover a broad range of technologies and are intended to support both new and legacy applications; both classified and unclassified. The DoD Trusted Supplier program provides guaranteed access to leading edge trusted microelectronics services for the typically low-volume needs of the Government. As of July 14, 2014, there were 62 facilities accredited to provide trusted services (Appendix A), of which 17 were foundries.

Companies self-fund the security infrastructure needed for DMEA trusted accreditation as well as the Cooperative Research and Development Agreements (CRADA) used to sponsor security clearances and apply customized security protocols. The companies fund the process for managing security personnel, data collection, and staffing of their trusted supplier program. CRADA enable DMEA to acquire intellectual property and production processes from suppliers. When a given product line ends, instead of buying a lifetime supply of parts, CRADA allows on-demand, post-production of a wide variety of parts and simplifies re-engineering of new parts when needed.

DMEA accreditation does not necessarily mean a supplier will automatically provide customers with trusted microelectronics services as a normal business practice. To assure a trusted process flow is used, acquisition programs are advised to specify a trusted flow in contract statements of work when purchasing ASICs that require trust from a DMEA-accredited supplier. Legacy programs that predate DoDI 5200.44 may already have incorporated ASICs into a system design from an unaccredited source. Remanufacturing an ASIC for a trusted flow may be cost and schedule prohibitive, especially if a lifetime supply has been purchased in advance. When trusted services for CC cannot be arranged, programs must select and implement alternative countermeasures for mitigating supply chain risk.

In addition to the accreditation process, DMEA and NSA co-fund the Trusted Foundry contracts that ensure developers of defense systems have access to leading-edge trusted microelectronics across a wide range of technologies and services. The TAPO facilitates and administers the current trusted foundry contracts and agreements with the IBM Corporation to produce advanced microelectronics parts in a trusted environment. Any Government-sponsored program can use the TAPO to access IBM's trusted foundry services. IBM foundry services include multiproject wafer runs, dedicated prototypes, and production in both high- and low-volume models.

4.3 Field-Programmable Gate Arrays

Custom-manufactured ASICs represent less than 2 percent of the microcircuits that the Department acquires. Although they are important to protect from malicious attack, they are not the only microelectronics at risk. Field-programmable gate arrays (FPGA), which are frequently used as a more affordable alternative to custom-manufactured ASICs, come with their own security risks. An FPGA may be designed and fabricated as a commercial-of-the-shelf (COTS) item. However, as it moves through the supply chain, it is typically installed onto a printed circuit board and firmware is added, making it effectively a customized logic-bearing ASIC. Per chapter 2, paragraph 2.2.2 of draft NIST SP 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations," "logic-bearing components are especially susceptible to malicious alteration throughout the program life cycle." For programmable logic devices, such as FPGAs that are CC, DASD(SE) is advising programs that their risk mitigation strategy should include the use of security-cleared personnel and facilities where printed circuit board population occurs and where FPGA programming and software assurance are performed.

In 2013, as part of DoD's actions to develop a FPGA risk mitigation strategy, the NSA and DMEA co-chaired a study of commercial FPGA design, fabrication, and test processes. The purpose of the study was to identify FPGA vulnerabilities, which are currently fabricated offshore, and to develop threat models and countermeasures. This year, NSA is chairing phase two of the FPGA process study, which is focused on FPGA software design tools, firmware and software programming risks, and an evaluation of possible system and component-level risk mitigations. The results of the completed study will be used to generate future FPGA security

guidance for the DoD, intelligence, and industry microelectronics communities. Near-term, the Department, with the support of the intelligence community, is working on FPGA implementation guidance for program managers. DMEA led a separate study to determine the feasibility of designing and manufacturing a family of Trusted FPGAs with all applicable design, manufacturing, and software countermeasures. This study was conducted with a major FPGA vendor and an on-shore foundry.

DARPA IRIS, in collaboration with NSWC Crane, NSA, industry, and other organizations, is initiating the development of low-cost, non-destructive methods for evaluating trust in legacy FPGAs, which is a significant concern as FPGAs are still used in DoD systems after they are discontinued and are no longer available from the original manufacturer.

4.4 Off-the-Shelf Components

In addition to custom-fabricated ASICs and FPGAs, another significant category of microcircuit is military-off-the-shelf (MOTS). These devices are designed for use in military applications where strenuous performance and environmental conditions exist, such as radiation hardening against nuclear attack or for space applications. For MOTS, the use of blind buys as a way of masking end use is of limited benefit as a risk mitigating countermeasure. Consequently, DASD(SE) is advising acquisition programs to limit MOTS sourcing and custody to Government-evaluated suppliers, such as DMEA-accredited trusted suppliers or Defense Logistics Agency (DLA) qualified manufacturers, testing suppliers, and distributors.

In addition to ASICs and MOTS microcircuits, DoDI 5200.44 requires acquisition programs to address the supply chain risk of COTS microcircuits and printed circuit boards once a DoD-military end use is apparent. The vast majority of COTS products cannot be obtained from a DMEA-accredited or DLA-qualified manufacturer or distributor. A less reliable, but viable countermeasure when practical is to restrict microcircuit and related hardware procurements to U.S. original component manufacturers (OCM), when possible, and authorized/franchised distributors who have a history of providing products that are designed, manufactured, and distributed in a controlled manner that promotes product integrity and protection from counterfeiting.

Regardless of the type of microcircuit acquired, the DoD SD-1, “Parts Management Guide,” December 2013, recommends that processes used to qualify parts, parts manufacturers, and parts distributors be documented following established quality assurance policies, procedures, and applicable standards. Parts should be qualified for the application in which they are used. The qualification of parts manufacturers and distributors includes an assessment of the manufacturer’s documented processes, e.g., its statistical process control data and its process controls on manufacturing, material, shipment, storage, notification concerning process changes, customer satisfaction, and quality measurement systems. Depending on contract requirements, associated special process controls, such as counterfeit control, may be assessed.

4.5 DoD and DLA Qualified Lists

The DoD Qualified Manufacturers List (QML) focuses on qualifying an envelope of materials and processes rather than individual product(s). That envelope is qualified by carefully selecting representative worst case test vehicles or representative samples from production that contain all potential combinations of materials and processes that may be subsequently used during production. As evidence that those processes and materials meet the established qualification requirements, the envelope of processes and materials shall be listed on a QML. A QML will normally be appropriate for items of supply that have very rapid technological advancement or a myriad of variations or custom designs that make individual product qualification impractical or excessively expensive. QML microcircuits are manufactured, assembled, and tested in accordance with MIL-PRF-38535 and MIL-PRF-38534.

The DoD Qualified Products List (QPL) focuses on qualifying individual products or families of products. As evidence that those product(s) meet the established qualification requirements, the product(s) shall be listed on a QPL. A QPL will normally be appropriate for items of supply that are stable and will be continually available for an extended period of time, thereby making it practicable to qualify individual product(s) without incurring prohibitive testing costs.

The DLA Qualified Suppliers List of Distributors (QSLD) is a listing of pre-qualified distributors for electronic components in Federal Supply Class (FSC) 5961 and 5962 that are purchased and managed by DLA. QSLD products are provided by suppliers and distributors that combine accepted commercial practices and quality assurance procedures that are consistent with industry and international quality standards. They may be tailored when necessary to product-unique requirements.

The DLA Qualified Testing Suppliers List (QTSL) is a list of suppliers with the processes and testing capability to substantiate the authenticity of items in FSCs 5961 and 5962 with no pedigree information. It is intended to mitigate the risk of counterfeit semiconductors and microcircuits with no pedigree or traceability information to an approved manufacturer. QTSL products are provided by suppliers that combine accepted counterfeit mitigation practices and quality assurance procedures that are consistent with industry and international quality standards. Suppliers in the program can be relied upon to supply these electronic components when there are no offerors with traceability to an approved manufacturer, i.e., when there are no offerors in compliance with the QSLD program.

The NSA trusted access contractual arrangement with IBM, the DMEA accreditation process, and the above DLA practices complement the implementation of DoDI 5200.44. They, along with other related processes, tools, and techniques, are helping to control quality, configuration, and security of software, firmware, hardware, and systems throughout the life cycle; detect, reduce the occurrence, and mitigate the consequences of products containing counterfeit components; and implement item-unique identification for traceability of CC.

4.6 Working with Industry

Ongoing Government and industry work to develop anti-counterfeit practices supports overall hardware and software assurance efforts, but the practices generally are not sophisticated enough to detect or mitigate malicious exploitation of CC. The savvy malicious actor designs the exploitation to look and perform exactly as intended until the time of their choosing. It is vital that the Department work closely with industry to develop the use of commercially acceptable SCRM practices that address both the risk of counterfeiting and malicious attacks.

The Department is receiving input from industry to help DoD identify specific supply chain vulnerabilities and develop risk mitigations. Organizations such as the Society of Automotive Engineers (SAE) and the NDIA have, for example, provided such input.

Industry standards groups, such as SAE, International Standards Organization (ISO), and the Open Group are advancing the use of quality assurance controls for detecting counterfeit and malicious functionality in microcircuits.

4.7 New Marking Technology

In 2014, in an effort to advance product marking technology, the DARPA initiated the Supply Chain Hardware Integrity for Electronics Defense (SHIELD) program. SHIELD is seeking innovations from industry to develop an extremely small (100 micron x 100 micron) and inexpensive component, or dielet, that authenticates the provenance of, and that can be integrated with, vendor products without impacting their functionality. New industry and Government standards for component authentication and SCRM will be established during the execution of the program. Technical areas to be developed include the following:

- New on-chip hardware-root-of trust secret key containers,
- Full onboard encryption engine,
- Passive intrusion sensors that detect potential compromises and tampering,
- ID chip self-destruct mechanisms to counter attempted reverse engineering,
- Wireless communication and power,
- New manufacturing process technologies to fabricate, personalize, and place these devices,
- Components that readily affix to today's electronic and other components and products,
- Integration and design of the small ID chips comprising these features, and
- Demonstration of the capability in an actual DoD acquisition program.

Other organizations across the Department, intelligence community and interagency are also doing significant science and technology work in microelectronic security and in new marking technologies that have potential to be leveraged in support of TSN.

5 Life Cycle Management

Contractor configuration and parts management are used to establish and control product attributes and the technical baseline at each milestone and SETR. These processes provide system security engineers with a way to instill security risk management considerations during CC selection, acquisition, system integration, and during operation and sustainment. They also facilitate the monitoring of the supply chain for possible product or source changes and to convey to the logistics and purchasing communities any special sourcing and handling considerations.

DAG 13, paragraph 13.4.5 on Trusted Microelectronics, has been rewritten to emphasize configuration management practices as an important mechanism by which microcircuit security can be addressed. DoDI 5200.44, paragraph 4.c., requires that programs "control the quality, configuration, and security of software, firmware, hardware, and systems throughout their life cycles, including components or subcomponents from secondary sources." Interim DoDI 5000.02, Enclosure 3, paragraph 8, says "the Program Manager will use a configuration management approach to establish and control product attributes and the technical baseline across the total system life cycle." MIL-HDBK-61A(SE), "Configuration Management Guidance," February 7, 2001, advises that "Designating Configuration Items increases their visibility and management control throughout the development and support phases." Taken together, these and other existing policies and guidance can be leveraged to maintain the security of CC across the life cycle.

With the understanding that 75 to 80 percent of program costs support the Operations and Support phase of a system life cycle, the USD(AT&L) and DoD CIO have initiated efforts to mitigate the passing of risk from the acquisition community to the sustainment community. Figure 4 depicts the life cycle approach and the sharing of risk between the two communities. The mitigation efforts include: a more disciplined approach in managing the PPP through the entire system life cycle; evaluating a more comprehensive and integrated approach in developing the PPP and the Life Cycle Sustainment Plan (LCSP); and reinforcing continuous feedback on program and supply chain risk assessments between the two communities.

Figure 4. Transition of Supply Chain Risk from Acquisition to Sustainment

DoDI 5200.44 requires the use of a risk-based approach to detect, reduce the likelihood, and mitigate the consequences of products containing counterfeit components or malicious functions. Similarly, DoDI 4140.67, Counterfeit Prevention Policy, mandates a risk-based approach to control critical material such as critical microcircuits or other CC. DoDI 4140.67, Enclosure 2, paragraph 3, links the DoDI 5200.44 and program protection planning with other relevant policies to develop risk-based procedures for identifying critical material and developing quality assurance policies for the management of CC.

6 Summary

DoD has made considerable progress in implementing its TSN strategy, to include its assured microelectronics strategy. With the publication of DoDI 5200.44, the Department has outlined an overarching strategy to integrate robust systems engineering, SCRM, security, CI, intelligence, cybersecurity, and software and hardware assurance, with an emphasis on hardware and software assurance for managing risks to system integrity and trust.

A key enabler of the TSN strategy for assured microelectronics and other CC is the Department-wide requirement for acquisition programs to have a PPP to identify and manage CPI and mission-critical functions and components. The planning process includes an assessment of threats and vulnerabilities and the selection of countermeasures to mitigate the identified risks to warfighting capability from foreign intelligence collection and from hardware, software, and cyber vulnerability or supply chain exploitation throughout the system life cycle. The PPP is also the principal mechanism by which DoD is integrating assured microelectronics policy into program management, engineering, configuration, parts, and contract management disciplines.

The Department's systems engineering activities have supported these initiatives by linking numerous policies and processes with DoDI 5200.44, to include the requirement for systems integrators and component suppliers to use established policies for configuration and parts management and acquisition to control product security attributes as part of the technical baseline across the life cycle. This approach provides program management with an integrated and disciplined way of coordinating supply chain risk considerations during microcircuit selection, acquisition, and sustainment. It also facilitates the monitoring of the supply chain for possible product or source changes and to convey special sourcing and handling instructions to the logistics and purchasing communities.

Another critical factor to the advancement of the state-of-practice and art of program protection planning and the related SSE disciplines has been the ongoing alignment of mutually supportive initiatives. These include the DMEA Trusted Foundry Program, the DARPA IRIS and SHIELD Program, the NSA and DMEA sponsored FPGA studies, and industry partnerships. OSD continues to lead the TSN focal points from the DoD Components in information sharing, lessons learned, and best practices. The DoD CIO is also continuing to expand the TSN/SCRM dialogue beyond the protection of acquisition programs, to include the acquisition and procurement of the hardware and software for DoD networks and overall operations and sustainment of TSN. In summary, there continues to be collaboration and momentum among the various DoD, intelligence community and interagency organizations, with input from industry, to enhance the implementation of DoDI 5200.44 and broader program protection planning and to integrate them with other relevant Government and industry program, acquisition, and logistics management policies and practices.

Appendix A: Suppliers Accredited by the Defense Microelectronics Activity

Supplier Name	Location
Abraxas Corporation	Herndon, VA
Advotech Company, Inc.	Tempe, AZ
Aeroflex Colorado Springs	Colorado Springs, CO
Aeroflex Plainview, Inc.	Plainview, NY
Arkham Technology, Ltd.	Irvine, CA
Atessa, Inc.	Pleasanton, CA
Atlantic Analytical Laboratory, LLC	Whitehouse, NJ
BAE Systems Electronic Systems	Manassas, VA
* BAE Systems Microwave Electronics Center Nashua	Nashua, NH
Boeing Company, Space and Intelligence	El Segundo, CA
Boeing Company, The	Seattle, WA
Criteria Labs, Inc.	Austin, TX
* Cypress Semiconductor Minnesota, Inc.	Bloomington, MN
* Defense Microelectronics Activity	McClellan, CA
DPA Components International	Simi Valley, CA
e2v aerospace and defense, inc. (formerly QP Semiconductor)	Milpitas, CA
General Dynamics AIS - Bloomington, MN	Bloomington, MN
General Dynamics AIS - Scottsdale, AZ	Scottsdale, AZ
Harris Corporation Government Communications Systems Division	Melbourne, FL
* Honeywell Aerospace Plymouth	Plymouth, MN
Honeywell Federal Manufacturing & Technologies, LLC/Kansas City Plant	Kansas City, MO
* HRL Laboratories, LLC	Malibu, CA
Hunter Technology Corporation	Santa Clara, CA
i3 Electronics, Inc.	Endicott, NY
* IBM Corporation Burlington	Essex Junction, VT
* IBM Corporation East Fishkill	Hopewell Junction, NY
Integra Technologies, LLC	Wichita, KS
Intrinsix Corp.	Marlborough, MA
Jazz Semiconductor	Newport Beach, CA
Johns Hopkins University, Applied Physics Laboratory	Laurel, MD
* M/A-COM Technology Solutions Inc.	Lowell, MA

Supplier Name	Location
MacAulay-Brown, Inc.	Roanoke, VA
Maxtek Components Corporation dba Tektronix Component Solutions	Beaverton, OR
MIT Lincoln Laboratory Microelectronics Laboratory	Lexington, MA
NATEL Engineering Company, Inc.	Chatsworth, CA
* Northrop Grumman Aerospace Systems	Redondo Beach, CA
* Northrop Grumman Electronic Systems	Linthicum, MD
NSA Microelectronics Solutions Group	Fort Meade, MD
* ON Semiconductor - Gresham	Gresham, OR
* ON Semiconductor - Pocatello	Pocatello, ID
Pantronix Corporation	Fremont, CA
Photronics Texas Allen, Inc.	Allen, TX
Raytheon Missile Systems	Tucson, AZ
* Raytheon RF Components	Andover, MA
Ridgetop Group, Inc.	Tucson, AZ
Rockwell Collins, Inc.	Cedar Rapids, IA
* Sandia National Laboratories Microsystems Science, Technology, & Components	Albuquerque, NM
* Silanna Semiconductor	Sydney Olympic Park, New South Wales, Australia
Silicon Turnkey Solutions, Inc.	Milpitas, CA
Smart System Technology & Commercialization Center	Canandaigua, NY
* SRI International	Princeton, NJ
SypherMedia International	Westminster, CA
Sypris Electronics	Tampa, FL
Tahoe RF Semiconductor, Inc.	Auburn, CA
Teledyne Microelectronic Technologies	Lewisburg, TN
Triad Semiconductor, Inc.	Winston Salem, NC
* TriQuint Semiconductor Texas	Richardson, TX
USC – ISI Arlington	Arlington, VA
USC - ISI Marina del Rey	Marina del Rey, CA
USC-ISI - MOSIS	Marina del Rey, CA
Vortex Aerospace Design & Labs, Inc.	Melbourne, FL
White Electronic Designs Corporation	Phoenix, AZ

*Accredited Foundry
Source: DMEA accredited suppliers, http://www.dmea.osd.mil/otherdocs/AccreditedSuppliers.pdf

Acronyms

ASIC	Application-Specific Integrated Circuit
BOM	Bill of Material
CC	Critical Component
CI	Counter Intelligence
CIO	Chief Information Officer
COTS	Commercial Off-the-Shelf
CPI	Critical Program Information
CRADA	Cooperative Research and Development Agreement
DAG	Defense Acquisition Guidebook
DARPA	Defense Advanced Research Projects Agency
DASD(SE)	Deputy Assistant Secretary of Defense for Systems Engineering
DEPSECDEF	Deputy Secretary of Defense
DIA	Defense Intelligence Agency
DLA	Defense Logistics Agency
DMEA	Defense Microelectronics Activity
DoD	Department of Defense
DoDI	Department of Defense Instruction
EMD	Engineering and Manufacturing Development
EO	Executive Order
ESA	Engineering Support Activity
FPGA	Field-Programmable Gate Array
GSA	General Services Administration
ID	Identification
INCOSE	International Council on Systems Engineering
IRIS	Integrity and Reliability of Integrated Circuits

ISO	International Standards Organization
IT	Information Technology
LCSP	Life Cycle Sustainment Plan
MDA	Milestone Decision Authority
MicroE	Microelectronics
MIL-HDBK	Military Handbook
MOTS	Military Off-the-Shelf
MSA	Materiel Solution Analysis
NDIA	National Defense Industrial Association
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSWC	Naval Surface Warfare Center
O&S	Operations and Support
OCM	Original Component Manufacturer
OSD	Office of the Secretary of Defense
PD	Production and Deployment
PMO	Program Management Office
PPP	Program Protection Plan
QML	Qualified Manufacturers List
QPL	Qualified Products List
QSLD	Qualified Suppliers List of Distributors
QTSL	Qualified Testing Suppliers List
RFI	Request for Information
RMF	Risk Management Framework
SAE	Society of Automotive Engineers
SAC	Senate Appropriations Committee

SCRM	Supply Chain Risk Management
SE	Systems Engineering
SETR	Systems Engineering Technical Review
SHIELD	Supply Chain Hardware Integrity for Electronics Defense
SP	Special Publication (NIST)
SSE	System Security Engineering
TAC	Threat Assessment Center
TAPO	Trusted Access Program Office
TMRR	Technology Maturation and Risk Reduction
TSN	Trusted Systems and Networks
U.S.C.	United States Code
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics

References

Department of Defense (DoD) SD-1, "Parts Management Guide." Defense Standardization Program Office, December 2013. http://www.landandmaritime.dla.mil/downloads/psmc/documents/SD19FINAL.pdf

Department of Defense Instruction (DoDI) 4140.1, "Supply Chain Materiel Management Policy," December 14, 2011. http://www.dtic.mil/whs/directives/corres/pdf/414001p.pdf

Department of Defense Instruction (DoDI) 4140.67, "Counterfeit Prevention Policy," April 26, 2013. http://www.dtic.mil/whs/directives/corres/pdf/414067p.pdf

Department of Defense Instruction (DoDI) 5000.02, "Operation of the Defense Acquisition System Interim," November 26, 2013. http://www.dtic.mil/whs/directives/corres/pdf/500002_interim.pdf,

Department of Defense Instruction (DoDI) 5200.39, "Critical Program Information (CPI) Protection within the Department of Defense, Change 1," December 28, 2010. http://www.dtic.mil/whs/directives/corres/pdf/520039p.pdf

Department of Defense Instruction (DoDI) 5200.44, "Protection of Mission-Critical Functions to Achieve Trusted Systems and Networks (TSN)," November 5, 2012. http://www.dtic.mil/whs/directives/corres/pdf/520044p.pdf

Department of Defense Instruction (DoDI) O-5240.24, "Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)," June 8, 2011; Incorporating Change 1, October 15, 2013 (controlled document)). http://www.dtic.mil/whs/directives/corres/pdf/O524024p_placeholder.pdf

Department of Defense Instruction (DoDI) 8500.01, "Cybersecurity," March 14, 2014. http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf

Department of Defense Instruction (DoDI) 8510.01, "Risk Management Framework (RMF) for DoD Information Technology," March 12, 2014. http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf

Department of Defense and General Services Administration, "Improving Cybersecurity and Resilience through Acquisition," November 2013. http://www.defense.gov/news/Improving-Cybersecurity-and-Resilience-Through-Acquisition.pdf

Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)). "Program Protection." Chapter 13 in Defense Acquisition Guidebook. Washington, D.C.: DASD(SE), May 15, 2013.
https://acc.dau.mil/docs/dag_pdf/dag_ch13.pdf

Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)). "Program Protection Plan (PPP) Evaluation Criteria," Version 1.1. Washington, D.C.: DASD(SE), February 2014.
http://www.acq.osd.mil/se/docs/PPP-Evaluation-Criteria.pdf

Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)). "Program Protection Plan (PPP) Outline and Guidance." Washington, D.C.: DASD(SE), July 2011.
http://www.acq.osd.mil/se/docs/PPP-Outline-and-Guidance-v1-July2011.pdf

Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)). "Suggested Language to Incorporate System Security Engineering for Trusted Systems and Networks into Department of Defense Requests for Proposals." Washington, D.C.: DASD(SE) , January 2014.
http://www.acq.osd.mil/se/docs/SSE-Language-for-TSN-in-DoD-RFPs.pdf

Deputy Secretary of Defense (DepSecDef) memorandum, "Defense Trusted Integrated Circuit Strategy," October 10, 2003.

Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, February 12, 2013.
http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

MIL-HDBK-61A(SE), "Configuration Management Guidance," February 7, 2001.
https://acc.dau.mil/adl/en-US/142238/file/27622/MIL-HDBK-61A(SE)%20Configuration%20Management%20Guidance.pdf

MIL-STD-1580B, "DoD Test Method Standard Destructive Physical Analysis for Electronic, Electromagnetic, and Electromechanical Parts w/Change 3," March 4, 2014.
http://www.landandmaritime.dla.mil/Downloads/MilSpec/Docs/MIL-STD-1580/std1580.pdf

MIL-STD-1916, "DoD Preferred Methods for Acceptance of Product," April 1, 1996.
http://www.everyspec.com/MIL-STD/MIL-STD-1800-1999/MIL_STD_1916_1002/

MIL-STD-883J, "DoD Test Method Standard Microcircuits w/Change 2," March 14, 2014.
http://www.landandmaritime.dla.mil/Downloads/MilSpec/Docs/MIL-STD-883/std883.pdf

MIL-PRF-38534J, “General Specification for Performance Specification Hybrid Microcircuits,” April 13, 2014. http://www.landandmaritime.dla.mil/Programs/MilSpec/ListDocs.aspx?BasicDoc=MIL-PRF-38534

MIL-PRF-38535, “General Specification for Performance Specification Integrated Circuits (Microcircuits) Manufacturing,” December 20, 2013. http://www.landandmaritime.dla.mil/Programs/MilSpec/ListDocs.aspx?BasicDoc=MIL-PRF-38535

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-160, “Systems Security Engineering,” May 2014. http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-161, “Supply Chain Risk Management Practices for Federal Information Systems and Organizations,” June 2013. http://csrc.nist.gov/publications/drafts/800-161/sp800_161_2nd_draft.pdf

Under Secretary of Defense, Acquisition, Technology and Logistics (USD(AT&L)) and Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (CIO), “Report on Trusted Defense Systems in Response to National Defense Authorization Act, Section 254,” December 22, 2009. http://www.acq.osd.mil/se/docs/TrustedSystems-Exec_Summ-wAddendum-wTitlePgNoteinPDF.pdf

This page intentionally blank.

Department of Defense Assured Microelectronics Policy. Senate Report 113-85

Under Secretary of Defense for Acquisition, Technology, and Logistics
3020 Defense Pentagon
Washington, DC 20301-3020